THE INFORMATION-SEEKING BEHAVIOR OF DIGITAL EVIDENCE EXAMINERS

Idris Yildirim, B.A., M.S.

Dissertation Prepared for the Degree of

DOCTOR OF PHILOSOPHY

UNIVERSITY OF NORTH TEXAS

May 2011

APPROVED:

Linda Schamber, Major Professor
Brian O'Connor, Committee Member
Guillermo Oyarce, Committee Member
Herman Totten, Dean of College of Information
James D. Meernik, Acting Dean of the Toulouse Graduate School

Yildirim, Idris. *The information-seeking behavior of digital evidence examiners*. Doctor of Philosophy (Information Science), May 2011, 172 pp., 20 tables, 2 figures, references, 94 titles.

The current research sought to gain in-depth insights into the information-seeking behavior of Turkish National Police digital evidence examiners (DEEs); to explore the information sources that DEEs use and the factors affecting their decisions about source selection. Factors that affect information source selection and use by DEEs are: accreditation, workload, type of information, time, cost, availability, reliability/scientific importance, up-to-date data, prior experience with the source, relevance, interactivity and importance. The Internet was the information source most commonly used by participants during the examination stage; other sources included forums, experts, colleagues, forensic tools/kits and books. During the analysis stage, the most frequently mentioned information source was the investigation file, containing information about the elements of the crime; other sources included: personal experience, experts, detectives, the Internet, clients, professional training, the prosecutor, evidence submission forms, in-lab manuals, forums and colleagues. During the report-writing stage, most DEEs used in-lab manuals and report templates as information sources, but previously written reports, editing software, and colleagues were also used to obtain information about the format, style and language of reports as legal documents.

ACKNOWLEDGEMENTS

I would like to thank my thesis committee for their commitment to work with me on such an important project. I am especially indebted to Dr. Linda Schamber, committee chair, who approached this project with an endless flow of energy which proved to be fruitful. Her suggestions and advice were invaluable. I am also truly grateful other committee members, Dr. Brian O'Connor and Dr. Guillermo Oyarce. Without their advice and guidance this project would have been virtually impossible. Thank you all.

My warmest thanks go to Sibel for being my wife, love, sweetheart, best friend, confidant, supporter, fellow, and in short, the meaning of my life.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ACRONYMS

ASCLD/LAB	Accreditation by American Society of Crime Laboratory Directors/Laboratory Accrediting Board
CART	Computer Analysis Response Team
CD	Compact disc
DEE	Digital evidence examiners
DVD	Digital versatile disc
GPS	Global positioning system
GSA	Global Mobile Suppliers Association
GSM	Global system for mobile communications
ICT	Information and communication technologies
INSU	Information needs, seeking, and use
IS	Information sciences
ISP	Information search process
LIS	Library and information science
PDA	Personal digital assistant
RCFL	Regional Computer Forensic Laboratories
USB	Universal serial bus

CHAPTER 1

INTRODUCTION

In the current, technologically advanced world, the events of people's lives are recorded by ubiquitous information and communication technologies (ICT). This happens in two ways. The people of this modern age often deliberately record their actions. For example, they capture important events with video cameras, save personal contacts' information in their computers, and keep a history of recently searched addresses in Global Positioning System (GPS) devices. Another type of recording continuously occurs without the explicit intention or permission of people. Most people are not aware that almost everything they do in their daily lives is recorded by the digital devices and systems they use.

Particularly, the ubiquitous ICT provide a multitude of information about where people have been, whom they talk to, what they buy, what they watch, what they read and what they write. In conventional criminal cases, all this information could only be obtained after an extensive investigation. However, in modern criminal investigations, a careful examination of one's smart cell phone is all that is necessary to provide this information. People having smart phones can now access the Internet, read newspapers, send emails, search for information, watch TV, buy things, talk to their friends and broadcast their geographical position information via Global System for Mobile communications (GSM).

Besides cell phones, people use a number of electronic devices which may also store personal information and documents. To illustrate, some of these are GPS devices, audio and video players and recorders, personal computers, answering machines, fax machines and printers, pagers, radios, routers and switches, external hard disks (Universal Serial Bus [USB]

memories), etc. Due to the architecture of electronic devices and systems, the data regarding the activities of users remain imbedded within them. The data imbedded in digital devices and systems are in several different formats, such as logs, audio, and video.

Data residing in ICT is especially valuable for the participants in the criminal justice system, including investigators, prosecutors, judges, victims, and suspects. Currently, in many criminal cases, a kind of electronic system or device is presented as digital evidence that provides evidentiary information. Digital evidence assists the judicial system in finding out the true facts of a case, and the importance of digital evidence has recently been recognized by the criminal justice system. For this reason, the demand for investigation of ICT has been increasing.

Due to the increasing use of ICT in society, the probability of using digital evidence in legal cases, in order to support appositions of the prosecutor and defendant, has dramatically increased. As a result of the increasing demand for digital evidence examination, the number of public and private digital evidence laboratories has also quickly increased.

The information sources used by DEEs to obtain job-related information, factors affecting their information practices and the obstacles they face while looking for information should be scientifically investigated. Studying these issues may assist DEEs to design better training programs, facilitate the efficient and effective use of available resources and increase job performance by assessing information needs. The researcher was unable to find any study focusing on information seeking behavior of digital evidence examiners (DEEs) from the literature of information science (IS), and, thus, this study aims to fill this gap.

Definitions

Defining concepts used in academic studies is not an easy job. Since scholars from different disciplines investigate a phenomenon from different perspectives, each discipline often utilizes a slightly or completely different definition for the same phenomenon. As a result, it is possible to have as many definitions for a concept as there are disciplines that study it. However, it is necessary for researchers to define concepts and terms to establish a common understanding between themselves and end users, although it is often very difficult and complex to do so (Case, 2007).

The researcher also found the development of definitions to be a complex procedure. To provide all the available definitions of terms and concepts used herein is far beyond the scope of this study. To do so would make this review unnecessarily long and confusing. Instead, an abbreviated glossary of the terms and concepts relevant to this study will be provided in the following section. And, when necessary, the researcher will discuss some of the terms and concepts in more depth.

- Information: Case (2007) cited several studies in which definitions of information were collected and grouped into broad categories. For example, Wersig and Neveling (1975) listed 17 distinctive definitions of information that they grouped into six broad clusters. Schement (1993) identified 22 definitions of information in print between 1968 and 1989. People usually use the term “information” without thinking about its definition; it seems that everybody agrees on its definition and knows what it is. However, when people are asked to define “information,” we must face the reality that “information” means different things to different people living or working in different contexts.

Unless otherwise specified, in this study, information refers to “any difference that makes a difference to (the?) human mind” (Bateson, 1972, p. 453). “In other words, information is whatever appears significant to a human being, whether originating from external environment or a (psychologically) internal world” (Case, 2007, p. 40). The engagement of the human mind is essential, as indicated, in the definition of information.

- Information behavior: Wilson (2000, p. 49) described information behavior as “the totality of the human behavior in relation to sources and channels of information, including both active and passive information seeking and information use.” Similarly, Bates (2002, 3) pointed out the active, passive, directed or undirected characteristics of information seeking by defining it as “all the information that comes to a human being during a lifetime, not just in those moments when a person actively seeks information.”

- Models: A “model” explains specific problems and processes. Models usually explain a phenomenon by using diagrams, because diagrams help us understand concepts, relationships and processes. Wilson (1999) said that models of information seeking may be described as frameworks to conceptualize a problem, and may evolve into a statement of the relationship among theoretical propositions.

- Tasks: Vakkari (2003) described a task as "a piece of activity to be done in order to achieve a goal." Byström (2007) defined a “task” as a:

> … purposeful set of linked concrete or cognitive activities performed by people (or machines); normally, it has a meaningful purpose as well as an identifiable beginning and end. This kind of task is viewed as a dynamic activity, rather than a stable description. Task seen from the latter point of view is a description of what is expected from a person (or a machine), such as "make a personnel allocation plan for the next four weeks". Task often includes some type of requirement (for instance, in respect to duration or quality of performance or other issues of concern), and it may be either set by the task performer himself or by others. Similarly, task may be initiated by the task

performers themselves or assigned by others as well as performed in solitude or as a team effort. Task takes place both within and outside work. Task may be authentic or simulated and performed in authentic or simulated contexts. To summarize, task are multidimensional activities.

- Forensic science: The term "forensic" is currently used to describe things related to the criminal justice system, particularly public debates in the courtroom. Forensic science refers to "the application of the techniques of science to legal matters, both criminal and civil" (Bell, 2008, s. 162). Forensic science is an umbrella concept; there are several professions performing forensic science and the field may be divided into ten sections (e.g., criminalistics, pathology/biology, questioned documents, toxicology, etc.)

- Criminalistics: The purpose of criminalistics is to identify, record, and interpret physical evidence collected from a crime scene (Osterburg & Ward, 2000). The following examinations are generally considered to fall under the umbrella of criminalistics (Eckert, 1997; Ramsland, 2001):

a. Firearms and tool marks

b. Latent prints (fingerprints, palm prints, footprints, etc.)

c. Questioned documents

d. Drugs and other physical materials (glass, plastic, etc)

e. Trace evidence (hair, fiber, shoe marks, etc.)

f. Video / audio and digital material

g. Blood patterns

h. Crime scene investigation / evidence collection

i. Photography (conventional and digital)

Although the tasks of professionals performing computer forensics seem to fall under the category of criminalistics, some scholars argue that computer forensics is a distinctive sub-discipline of forensic science (Hall & Davis, 2005). This study will particularly focus on the activities of digital evidence examiners who apply computer related sciences to the matters of the legal system, both public and civil.

- Computer: The definition of a computer is very complex indeed because the size and shape of computers have changed a lot. Most people visualize a display, key board and a mouse, or other input tools, connected to a metal case, when asked to describe a computer. However, today, smart phones can do everything that a conventional desktop computer can do and automobiles are equipped with highly developed systems that work like a computer.

The central feature of computers is that they are programmable. The term programmable and programming shouldn't be confused with automatable and automating. A microwave is an automated system. It has a timer and a mechanism that produces heat for a preset time. On the other hand, the term, programming, means to install multiple instructions into the processing unit in the device, so that it can interpret, manipulate and respond according to the needs of the system. What distinguishes a computer from automated systems is that it can receive multiple instructions and execute them according to the needs of the system, can serve multiple purposes, and is an electronic device. In this sense, we can easily exclude many devices, such as automobiles, dishwashers, microwaves and calculators from being considered as computers (Franklin, 2006).

In this study, the term computer refers to an electronic device that can perform the same tasks that any other personal computers can perform.

- Digital evidence: The Scientific Working Group on Digital Evidence and International Organization on Digital Evidence (SWGDE) & International Organization on Digital Evidence (IODE) (2000) defined digital evidence as the “information of probative value that is stored or transmitted in a digital form.” SWGDE and IODE (2000) defined the associated terms as follows:
    - Acquisition of digital evidence: Begins when information and/or physical items are collected or stored for examination purposes. The term "evidence" implies that the collector of evidence is recognized by the courts. The process of collecting is also assumed to be a legal process and appropriate for rules of evidence in that locality. A data object or physical item only becomes evidence when so deemed by a law enforcement official or designee.
    - Data objects: Objects or information of potential probative value that are associated with physical items. Data objects may occur in different formats without altering the original information.
    - Physical items: Items on which data objects or information may be stored and/or through which data objects are transferred.
    - Original digital evidence: Physical items and the data objects associated with such items at the time of acquisition or seizure.
    - Duplicate digital evidence: An accurate digital reproduction of all data objects contained on an original physical item.
    - Copy: An accurate reproduction of information contained on an original physical item, independent of the original physical item.

In this paper, these terms are used consistent with their aforementioned definitions.

Digital evidence is obtained not only from traditional personal computers but also from a number of electronic devices and other digital media. Digital evidence can be in several different formats, such as audio, video or logs of entries. Computers are instrumental in conducting several different types of crimes, from money laundering to homicide to forgery. Most of the physical items that could possibly contain digital evidence can usually be easily recognized at the crime scene. In some cases, special skills are required to recognize other

physical items, such as different types of toys hiding USB drivers inside, cell-phones embedded in wrist watches, and shoes carrying GPS devices inside.

A high level of technical skills and knowledge is required not only during evidence collection but also in the following stages of computer forensics: storing, transferring, extracting, and reporting of digital evidence. Computer evidence, as referred to in the title of this study, doesn't necessarily mean evidence obtained only from computers, but also that obtained from other digital devices. Digital evidence examiners investigate digital evidence collected from computers and also from other types of digital devices.

- Computer forensics: Derived from the Bell's (2009) definition of 'forensics", computer forensics in this study refers to the applications of the techniques of computer-related sciences, such as computer science, network engineering, software engineering, etc. to legal matters, both criminal and civil.

- Digital forensics: After reviewing several suggested definitions of "digital forensic science," the conclusive definition of this relatively new field of forensics was:

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (Digital Forensics Research Workshop, 2001).

- Profession: Leckie, Pettigrew, and Sylvain (1996, p.162) defined "profession" as "service-oriented occupations having a theoretical knowledge base requiring extensive formal postsecondary education, having a self-governing association, and adhering to internally developed codes of ethics or other statements of principle". To illustrate, they listed some professionals - according to their definitions - as doctors, teachers, lawyers, nurses, librarians,

engineers, and accountants. They emphasize the themes of theoretical framework, education, administration and subculture in the professional realm in their definition.

Statement of the Problem

Digital devices are widely used. The number of GSM technology users had grown to over 270 million by the end of 2008 in North America (Global Mobile Suppliers Association, 2009). According to the website of GSA, the number of GSM subscribers all over the globe has grown to 4 billion. According to a report of the Institution of Information Technologies and Communication of Turkey (2010), the number of GSM subscriber was 61.5 million by the end of May 2010. The report stated that GSM service providers initiated 3G services in July 2009, and in one year, the number of 3G users had expanded to 8.7 million.

The likelihood of the existence of digital evidence in legal cases is very high in the modern world. An analysis of data collected from annual reports of the Regional Computer Forensic Laboratories (RCFL) (2006, 2007, 2008) showed that the number of mobile digital devices, such as cell phones and flash drives, processed by RCFL has consistently increased. Another noteworthy point is that the numbers of new types of digital media/devices such as hard drives and digital versatile discs (DVDs) processed by RCFL is increasing, while the numbers of older types of digital media/devices, such as floppy discs, compact discs (CDs) and tapes, are decreasing.

Recently, digital devices have been designed as all-in-one/multitask devices. In the information age, a cell phone is not just a phone: It is also an audio/video/image recorder, GPS

locater, form of portable data storage, radio/TV, and, perhaps, most importantly an Internet explorer.

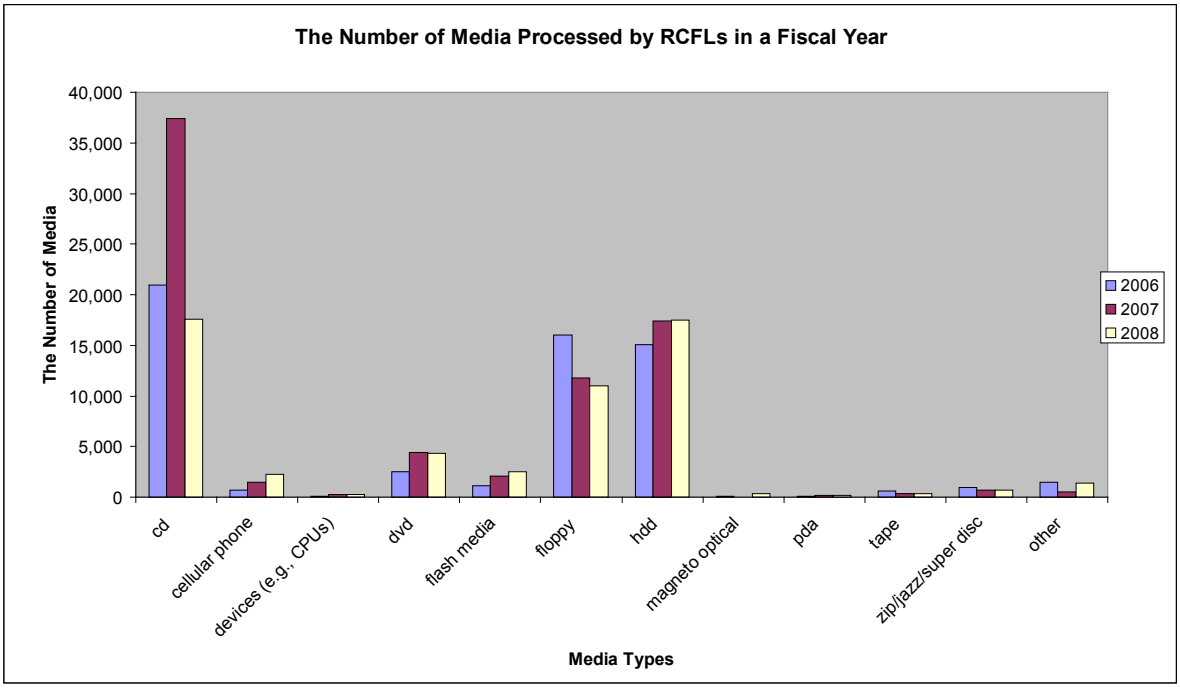

Figure 1. The number of digital media processed by RCFL in 2006, 2007 and 2008.

Phone records, emails, digital camera recordings, temporary Internet logs, transaction logs, digital financial data and digital office documents all are considered as possible digital evidence, especially in cases of fraud, identity theft, sexual harassment, and white-collar crimes.Cell phones and other digital devices provide valuable information in developing criminal investigations. Digital evidence examiners collect physical items from a crime scene, extract the raw data from physical items, analyze the extracted data and report their findings to their clients. The workload of digital forensic labs has been increasing over time as the awareness of digital evidence in the criminal justice system and the demand for digital investigation increase.

Data from annual reports of RCFL (2003, 2004, 2005, 2006, 2007, 2008) corroborate this trend (see Figure 2).

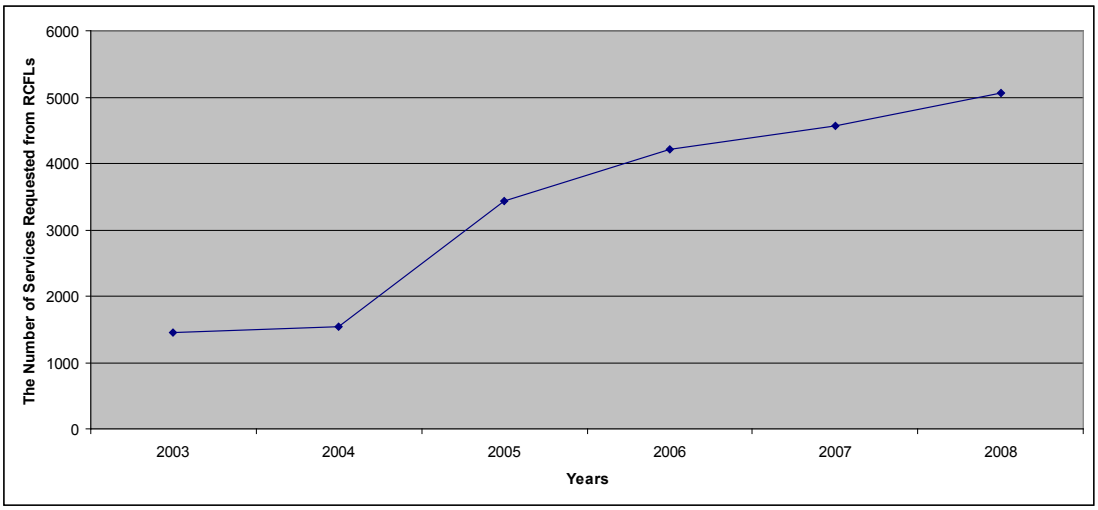

Figure 2. The number of service requests made to RCFL from 2003 to 2008.

Technology is changing rapidly. For this reason, it is obvious that computer and digital evidence examiners confront new challenges when they encounter newly produced digital devices. As can be seen in Figure 2, the number of newer media types, such as cell phones, DVDs and flash drives, processed by RCFL is increasing whereas the number of older types of media, such as floppy drives and CDs, is decreasing. It is necessary for DEEs to know new technologies not only superficially, but also in depth as well, so that they can extract and analyze the digital data embedded in these items. Therefore, DEEs must be able to adapt their knowledge and skills to new technologies. Most studies on DEEs have focused on modeling the digital forensic process and procedures of examining digital evidence.

The researcher believes that digital forensics should also be studied by applying the theoretical approaches of IS but was not able to find a study in the literature that investigated the information-seeking behavior of DEEs.

Purpose of the Study

Research focusing on the information-seeking behavior of professionals is necessary to answer the questions of why and how professionals look for and use information, why they prefer to use particular information sources rather than others, and what the problematic issues are in this process (Leckie et al., 1996). We can discover the information needs of employees at work, and provide them with the necessary support, according to the findings of the current study. In addition, this research may be helpful for administrators of DEEs to form suitable training programs.

The purpose of the current research was to gain in-depth insights into the information-seeking behavior of digital evidence examiners. This research aims to explore information sources that DEEs use; the factors affecting their decisions about source selection. As a result of this study, the researcher expects that this research will help administrators determine whether information resources are being adequately utilized, and what could be done to develop these resources.

Significance of the Study

The information seeking and using behaviors of people in an occupational setting have always attracted the interest of researchers in the field of Library and Information Science (LIS). Early studies have usually focused on the information-related habits of scientists and scholars. However, after the latter half of the 1970s, LIS researchers began paying attention to information behavior in the professional setting. One reason for studying information behavior

in professionals was to advance the theoretical analysis of information behavior (Leckie et al., 1996).

Amongst the literature of information behavior of professionals, one might conclude that the amount of research investigating the information behavior of professionals could be equal to the total number of professions (Leckie et al. 1996). However, although a number of studies have been conducted to examine the information behavior of professionals, the researcher was not able to find a study focusing on the information behavior of digital evidence examiners in the literature. That is why this study may be unique. This study is exploratory in nature, in that, for the first time, the digital forensic process is examined from an information science perspective.

Research Questions

The purpose of this study was to explore the information-seeking behavior of DEEs. Four research questions formulated for this study are:

1. What circumstances lead digital evidence examiners to seek information in their professional life?
2. What are the information sources used by digital evidence examiners in their work?
3. What characteristics influence information source selection and information use by digital evidence examiners.
4. What are the obstacles that digital evidence examiners face while seeking job-related information?

Summary

A relatively new category of professional, called the Digital Evidence Examiner, has emerged as ICT becomes widely used in society. As the number of digital devices that people use in their daily lives is continuously increasing and the awareness and knowledge about digital evidence increases among participants in the criminal justice system, DEEs are becoming more important. The criminal justice system has recently recognized the value of evidentiary information embedded in digital items. And although many studies have been conducted on DEEs, none of them has focused on their information-seeking behavior. The researcher, first, aimed to gain an insight into the information-seeking behavior of DEEs with this study. Then, the researcher planned to conduct a quantitative study, based on this study, in the near future. In addition, the researcher produced a survey tool that could be used in future studies

The following chapter reviews the literature of digital forensics and information-seeking models.

CHAPTER 2

LITERATURE REVIEW

In this section of the chapter, the history of digital forensics in the U.S. and Turkey will be briefly touched upon. Also, some of the digital forensic process models that will help us understand what DEEs do in their work is explained.

History of Digital Forensics

Computer forensic programs have been created to meet the demand from law enforcement agencies since the early 1980s. Law enforcement organizations initiated the first programs to analyze computers. In 1984, the FBI established the Computer Analysis Response Team (CART) in order to meet the growing needs of prosecutors and investigators in a more professional manner. Many other law enforcement organizations have duplicated CART's general organization and functions (Noblett, Pollitt, & Presley, 2000).

Law enforcement agencies have realized that the identification of all existing resources in the agency that could be used in computer forensic work is problematic, because those resources are usually dispersed throughout the agency. Nowadays, there is a trend for all digital evidence examinations to be conducted in a large laboratory environment serving a predetermined area which can cover a number of jurisdictions (Noblett et al., 2000).

Whitcomb (2002) addressed three important changes that occurred in the history of digital forensics:

- From computer forensics to digital forensics: From the early 1980s to the late 1990s, the term "computer forensics" only referred to the finding of latent evidence on a

computer. Later, the general term, digital evidence, was used in order to include digital data, audio, and video evidence collected not only from computers, but also from other types of digital devices (Whitcomb, 2002).

- From technical working groups (TWGs) to scientific working groups (SWGs): With the innovations of new technologies and common use of digital devices, the amount of digital evidence used in legal cases has increased. With the increasing demand for digital evidence examination, the number of digital forensic laboratories of different sizes has also increased. To bring standardized and scientific protocols and procedures to digital forensic services, groups of specialists were formed as technical working groups (TWGs) in the early 1990s. In 1999, the name or these groups was changed to scientific working groups (SWGs). SWGs consist of no more than 50 federal, state and local members, and are still active (Whitcomb, 2002).

- Accreditation by American Society of Crime Laboratory Directors/Laboratory Accrediting Board (ASCLD/LAB): After the formation of the SWGDE in 1999, they worked together with the American Society of Crime Laboratory Directors/Laboratory Accrediting Board (ASCLD/LAB) to establish a new accredited discipline, forensic science. Actually, ASCLD/LAB has accredited forensic laboratories that focus on different disciplines, such as crime scene, biology and latent prints, since 1982. In 2003, ASCLD/LAB officially recognized the digital evidence discipline as consisting of four sub-divisions: computer forensics, audio analysis, video analysis, and imaging analysis (Barbara, 2005).

Barbara (2005) pointed out an increasing demand in accreditation from ASCLD/LAB by other digital forensic laboratories:

> Currently, no one knows for sure just how many individual entities (laboratories) in the United States are currently performing forensic analysis in one or more of the sub-

> disciplines of Digital Evidence. One estimate indicates that there are probably 300 or more at the local, state and federal level, however, this number is probably underestimated. Also, the estimate does not include those in the corporate or business sector where there could be several hundred more entities performing this type of analysis. An interesting trend that may accelerate accreditation in the United States is the fact that several states have passed legislation requiring that any entity performing forensic analysis within the confines of that state must attain accreditation if the results of the examinations are to be used for prosecutorial purposes. The legislation is equally applicable to the governmental forensic crime laboratories and any corporate, business or private laboratories in those states that offer services in any of the ASCLD/LAB accredited disciplines. Thus, as the process continues to go forward, corporations and businesses will be expected to adhere to the same standards of practice as those followed in the governmental forensic crime laboratory community. One net result is that ASCLD/LAB may eventually have to consider the feasibility of establishing a separate infrastructure to inspect the large number of stand-alone laboratories that may seek accreditation in the Digital Evidence discipline. (p. 146)

Although there were several local digital forensic laboratories in existence, the FBI initiated a regional computer forensic laboratory (RCFL) program in 1999 to use resources and assets efficiently and to improve the quality of services provided by digital forensic labs. The cost of forensic hardware/software and associated expenses, such as furnishings, buildings, vehicles, and certified personnel salaries, is very expensive. Establishing a digital forensic laboratory costs at least $3 million and takes four to five years, from the first step of training personnel to getting accreditation from ASCLD/LAB. The first RCFL was opened in San Diego, in 1999, and the second one in Dallas, in 2000. The RCFLs were so successful that the number of RCFLs had grown to 14 in 2007. So far, 7 RCFLs have earned accreditation in digital and multimedia evidence from ASCLD/LAB (RCFL Annual Report Fiscal Year, 2003, 2008).

Besides regional laboratories, local laboratories still continue to examine digital evidence in local cases. However, as judges, prosecutors and lawyers become more familiar with the concept of digital evidence; they will demand accreditation for digital forensic laboratories to grant more scientific structure and believability to digital evidence. The FBI will

soon require that all digital evidence in federal cases be examined in digital forensic laboratories accredited by ASCLD/LAB. As a result, local law enforcement agencies which participate in federal cases will choose one of two options. The first option is to get their ASCLD/LAB accreditation; the second is to send their digital evidence to a RFCL which is accredited. The first option is very costly, and the second option will greatly increase the workload of RCFL. So, the number of accredited RCFL and other accredited private and local laboratories is expected to increase (Coopman, 2008).

The Digital Forensic Process

The purpose of this section is to provide insights into the nature of the work that DEEs perform in a digital evidence investigation process.

Hall and Davis (2005) stated that a new discipline emerged at the intersection of forensic sciences and ICT. There are a number of terms used to name this discipline, including digital forensics, network forensics, software forensics, computer forensics, etc. Scientific forensics and information technology intersect each other in two different ways. In one format, information technology is used as a tool to examine evidence obtained from a crime scene. In another format, information technology actually concerns a physical item that the evidence associated with; physical items that are collected from a crime scene.

The criminal also uses new innovations to commit crime. New technologies like computers, the Internet, wireless systems, and developments in digital media not only facilitate committing crimes but also create new types of crimes. To illustrate, computer crimes such as denial of service, identity theft and spreading computer viruses can be cited. Computers may

also be used as instruments in traditional crimes, such as fraud, terrorism and homicide. A significant example is that of a young woman who was murdered in the killer's house after she responded to a babysitting advertisement placed on craigslist.com by the killer (NY Daily News, 2009).

The first stage in the digital forensic process is evidence collection. Conventional evidence collected from a crime scene has a physical substance, form, and shape. In many cases, we can sense it; we can see, touch and smell it. For instance; a blood sample can be seen and touched, and a foot-print or tire-print can be seen as an impression on the ground. Some evidence has an odor that can be observed by an investigator at the crime scene, such as perfumes, alcohol and burned materials. However, this is not the case for digital evidence. Digital evidence is completely different; it cannot be touched, seen or smelled at the crime scene (Marcella & Menendez, 2008). And DEEs don't collect evidence from crime scenes in all cases; they may receive digital devices and media sent in by clients to their laboratory. Their clients may be individuals or institutions like police agencies.

Digital evidence originates on a physical item, but cannot be analyzed unless a digital evidence examiner extracts it. Even after extraction, digital data usually doesn't make sense, at first glance, to a person without proper training in digital forensics. For example, handwriting on a small piece of paper is traditional evidence that we can see and read at first glance, but a deleted text massage and a hidden document in a picture is digital evidence that people cannot see or make sense of without using the proper forensic tools and procedures.

The extracted raw data is analyzed by using sophisticated forensic tools. The goal of DEEs at this stage is to find answers to questions asked by the court or client. One of the

common methods used is keyword searching. Digital media submitted for examination usually contains such a large amount of data that manual analysis is impossible in many cases.

The last stage of the digital forensic process is to report the findings. DEEs in some cases testify in courts, and present their findings. In other cases, they may just write a report to their clients.

Although digital forensics has been studied for a relatively short period of time, the number of research studies in the literature is increasing and becoming more dynamic, as the concept of digital evidence is changing so quickly. Pollitt (2007) described the changes in the field as "a rapid metamorphosis: from skilled craftsmanship into a true forensic science." Most of the literature on digital forensics comprises proposed models of the digital forensic process and technical guides that mostly describe how to collect, examine, and analyze digital evidence.

A criminal investigation may be defined as a process consisting of several phases. Several models of forensic investigations have been proposed to guide investigators, and to build standards for digital forensics. As an active agent in the development of digital forensics, Pollitt (2007, p. 1) listed fifteen published papers in his review that he described as "papers which represent data points in the development of digital forensic models." He, in fact, reviewed major proposals of digital forensic models in the literature.

Models in the literature of LIS help us understand concepts, relationships and processes of information behavior. In the literature of digital forensics, models are proposed in order to:

- Improve the scientific structure of investigation
- Make it easier to understand and follow the stages of an investigation
- Provide frameworks for research

- Standardize the process of investigation

It is not possible to cover all the available models of digital forensics in this section. However, the basic model of digital forensic process of Kent, Chevalier, Grance and Dang (2006) is briefly explained because this model of the digital forensic process is used for general task categorization in the data collection stage of this study. Kent et al. (2006, p. 2) described the forensic process as:

> The process for performing digital forensics comprises the following basic phases:
>
> - **Collection:** identifying, labeling, recording, and acquiring data from the possible sources of relevant data, while following procedures that preserve the integrity of the data.
> - **Examination**: forensically processing collected data using a combination of automated and manual methods, and assessing and extracting data of particular interest, while preserving the integrity of the data.
> - **Analysis**: analyzing the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
> - **Reporting**: reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process.

The collection, examination, analysis, and reporting stages of digital evidence are used as the particular sub-task categories in this study.

Models of Information-Seeking Behavior

Wilson (2000) stated that “information behavior” is not a correct term for an academic field. Technically, in terms of grammar, some scholars said it is an incorrect term to use, because information doesn’t have a physical body that behaves. The verb “to behave” is

something people do. Instead of “information behavior,” the term “human information seeking and use” seems to be more understandable. However, despite all these arguments, “information behavior” is a term that is commonly used in the titles of articles of information science literature. Briefly, information behavior can be defined as the name of the field that studies how people need, seek, produce and use information in several different contexts, including their daily and work environments (Pettigrew, Fidel, & Bruce, 2001).

Nearly 10% of the research in library and information science (LIS) focuses on information needs, seeking, and use (INSU) (Julien & Duggan, 2000). The term “Information seeking” and “information behavior” is usually used as shorthand for activities related to INSU and those two terms are used interchangeably (Courtright, 2007). Wilson (2000, p. 49) described information behavior as “the totality of the human behavior in relation to sources and channels of information, including both active and passive information seeking and information use.” Similarly, Bates (2002, p. 3) pointed out the active, passive, directed or undirected characteristics of information seeking by stating that it is “all the information that comes to a human being during a lifetime, not just in those moments when a person actively seeks information.”

Wilson (1999) stated that models of information seeking may be described as a framework to conceptualize a problem, and may evolve into a statement of the relationship among theoretical propositions. Most models in the general field of information behavior attempt to describe an information-seeking activity, or the relationships among stages in information-seeking behavior.

Wilson (2000) used four terms to define human information behavior: information behavior, information-seeking behavior, information-searching behavior, and information-use behavior. Human behavior related to sources and channels of information is considered as information behavior; it includes both active and passive information seeking. The purposive seeking of information is the key element of information-seeking behavior. A need(s) triggers information-seeking behavior that satisfies users to some extent. Information-searching behavior includes interactions with all kinds of information systems, including both the human-computer interaction and the human intellectual interaction (in one's mind). A person will use the existing knowledge by acting both physically and mentally, and, therefore, information-use behavior covers both these activities.

Some of the most influential models and theories in the information-seeking literature are those of Wilson (1981, 1994, 1996, 1999), Dervin (1983, 1992, 1999, 2003), Ellis (1989), Ellis, Cox, and Hall (1993), Kuhlthau (1991) and Schamber 1991, 1994, 2000). In the following sections, the researcher reviews several widely used models.

Information-Seeking Models Proposed by Wilson

By creating and revising his models (1981, 1994, 1996, and 1999), Wilson has helped to explain information-seeking behavior and contributed to the literature of information science for almost three decades. In his first model, Wilson (1981) indicated that needs are the origin of information-seeking behavior. As a result of needs, the user demands both information systems and information sources, and, eventually, will either succeed or fail in finding and using information.

In his second model, Wilson explained information-seeking behavior in terms of an individual's environment; social role; physiology, affect, and cognitive needs. The work, socio-cultural, politico-economic and physical environments all affect user needs. In the course of responding to these needs, the user initiates information-seeking behavior. However, a person may encounter barriers at the personal, interpersonal and environmental levels during information-seeking behavior.

Wilson's 1996 model is a revision of his 1981 model; the 1996 model introduces some new components to the older model. Firstly, the barriers in the previous model are now described as intervening variables, which include psychological, demographic, role-related or interpersonal, environmental, and source characteristics. Information-seeking behavior is also sub-grouped into categories such as passive attention, passive, active, and ongoing search. In addition, two other concepts were defined. The first one, activating mechanisms, consists of a stress/coping theory that explains why information-seeking behavior does not emerge after certain needs arise, the risk/reward theory that explains why certain kinds of information are used more than others, and the social learning theory which indicates that a person can successfully adapt any behavior to acquire the desired information. The second concept concerns information processing and use.

Lastly, Wilson presented a problem-solving model of the information-seeking and searching processes in 1999. He stated that "information seeking and retrieval are occasioned by uncertainty" (p. 265). To solve a problem, a person engages in goal-seeking behavior. And through this problem-resolution process, the individual moves from uncertainty to certainty by following the defined stages of problem identification (what is my problem?), problem

definition (what kind of problem do I have?), problem resolution (how do I find the solution to my problem?), and solution statement (I found the answer or solution to my problem).

Sense-Making Model

The origin of the sense-making theory goes back to the 1970s (Dervin, 2003). It was first proposed in 1983 and is still in use today. It is widely used in different fields such as communication, cultural and postmodern studies, education, sociology, psychology, and philosophy. Sense-making consists of five components: time and space, context, gap, bridge, and outcome. As an individual begins his/her journey, called information-seeking behavior, the first step may be a new one or a repetition of past behavior. When an individual encounters a gap during the journey, it is not possible for a person to move forward until he/she adopts a new behavior (bridge). Some of the information gaps Dervin has identified are decision stops, barrier stops, spin-out stops, perceptual embeddedness, and situational embeddedness. Dervin constructed the sense-making triangle of elements known as situation-gap-help/use, with the experience of an individual playing an important role in continuing his/her journey. The important thing, at this point, is that the gap is seen differently by each observer, depending on the situation and the viewpoint of the observer in time-space.

Sense making can be defined as a process model, a theory and a methodology. Sense making is a process model because it describes how a person seeks information through time and space. The sense-making approach is a cognitive approach, in that it focuses on how individuals perceive gaps – which is similar to information needs as conceptualized in the information-seeking models of Wilson- and make sense of those gaps. The conclusion of the

process is the outcome which refers to the use of information to complete a task. The sense-making approach is used in many studies to explain information-seeking behavior in individuals. Sense making is also a theory because it consists of fundamental assumptions about the nature of human behavior. Sense making presents a theoretical approach that provides a framework for many research studies. Sense making resulted in a paradigm shift in information science by shifting the focus on information systems to users; it provided a methodology in which human perception is placed at the center.

Behavioral Model of Information-Seeking by Ellis

Ellis's (1989) model detailed several different types of activities adopted in information-seeking behavior: starting, chaining, browsing, differentiating, monitoring, extracting, verifying and ending.

- Starting: An individual may be familiar with a research area, or he/she may be inexperienced in the new topic. The primary starting point for a user to find information in a new area may be to seek out people who have experience in that area and ask them for key references and names of authors.

- Chaining (may occur in two ways): 1) Backward chaining: This is considered formal information seeking and includes following up with references, footnotes, and sources cited in the material – "identifying references from material" (Ellis 1989, p. 241). 2) Forward chaining: Involves initiating a new activity, it is less common in researchers' information-seeking activities and depends on the use of special bibliographic tools — "identifying references to material" (Ellis, 1989, p. 241).

- Browsing: The simple type of browsing involves looking thorough the pages of books, journals, or periodicals to assess their contents. Similar to abstracting, the purpose of browsing is not to search for any particular topic, but to check the work to see if it includes any material appropriate for the current research. Besides gaining familiarization with the resources, differentiation occurs as the individual distinguishes differences between the sources. Therefore, browsing and (abstracting or differentiating?) are related activities.
- Differentiating: This is an activity that observes the differences in sources according to their nature and quality. This step is the most common in the information-seeking pattern adopted by researchers.
- Monitoring: Continuously monitoring developments in the field of interest is an important feature of information-seeking behavior. The researcher monitors improvements in the field by using informal contacts, published materials, newspapers, and journals.
- Extracting: In this step, researchers work on particular sources to locate materials of interest. For this purpose, researchers may directly consult with the source, use collective catalogs, or adopt a combination of those two methods.
- Verifying and ending: These two characteristics of information-seeking behavior were added with the 1993 model. They are activities used to confirm the accuracy of information, and activities occurring at the end of researching the topic, such as preparing a paper for presentation or publication (Ellis, Cox, & Hall, 1993).

Information Search Process (ISP) Model of Kuhlthau

Kuhlthau's (1991) information search process (ISP) was based on the constructive

activity through which a user finds meaningful information to extend his/her knowledge of a particular type of research or of an interesting area. Kuhlthau identified her perspective as phenomenological rather than cognitive and distinguished several affective aspects of the process of information seeking. ISP consisted of three areas (feelings, thoughts, and actions), six stages (initiation, selection, exploration, formulation, collection, and presentation), and appropriate tasks.

- Initiation: This is the first stage of the information search process. The user seeks background information, and frequently the user may have feelings of uncertainty and vague thoughts. The task at this point is only to recognize the need for information.
- Selection: In the selection stage, the general topic for study or the approach to be followed is identified. The feeling of uncertainty turns to optimism after this stage, and the user is ready to begin searching. If the approach to be followed or selection fails to retrieve appropriate material, feelings of anxiety arise again until the problem is solved.
- Exploration: In this stage, the user investigates information about the generality of the selected topic and seeks relevant information. However, the user may not be certain about the exact information he/she needs, and, as a result, may feel confusion, frustration, and doubt.
- Formulation: This stage marks the point of the information search process at which the user resolves his/her uncertainty. As it becomes obvious to the user which information he/she needs, he/she can focus on that information, and, thus, the user's confidence increases.
- Collection: Interaction between the user and the information systems begins in this stage. The task of the user is to collect the relevant information identified in the previous step.

Since he/she now has a clear sense of direction, the user easily identifies the information to collect and his/her confidence continues to increase.

- Presentation: This is the last stage of ISP. After the search is complete, the next task is to prepare the outcome for presentation or however the individual chooses to use the information. If the presentation of the results is successful, the user feels relieved. On the other hand, if he/she fails, the user feels disappointed. The user's thoughts at this stage are focused on completion of the information search process.

Information Retrieval and Information Seeking

Wilson presented a nested model in 1999 to encompass several models and represent their relationships to each other. This model consists of series of nested fields. He stated:

> Information behavior may be defined as the more general field of investigation, with information-seeking behavior being seen as a sub-set of the field, particularly concerned with the variety of methods people employ to discover and gain access to information resources, and information-searching behavior being defined as a sub-set of information seeking, particularly concerned with the interactions between information user (with or without an intermediary) and computer-based information systems, of which information retrieval systems for textual data may be seen as one type. (Wilson, 1999, p. 263)

To Wilson (1999), information retrieval-searching is not a separate concept from information seeking behavior (ISB). Instead, it is subset of ISB. In Wilson's 1981 and 1996 models, the origin of information-seeking behavior is with the needs of the user. Similarly, Krikelas (1983) discussed need-creating events or environments as a key element that triggers information-seeking behavior. Ellis's (1989) information-seeking model and Kuhlthau's (1991) information search process (ISP) model both use the same first step (starting and initiation) and continue to the same last step (verifying and ending and presentation). In all models, the seeker

begins information-related activities as a result of a need/problem/gap and uses a source to retrieve needed information. In the end, the seeker feels satisfied when he/she finds the needed information, with satisfaction being related to finding relevant information.

At this point "information retrieval" (IR) and "relevance" arise as important concepts. Harter and Hert (1997, p.3) defined IR system as a "black box" that:

> Accepts input and produces output. IR is a practical act, conducted by a user for a reason –attempt to satisfy a human need by consulting an information store. By an IR system we mean a system that retrieves documents or references to documents, as opposed to data. An IR system is employed when there are so many items in the information store as to make unfeasible the approach of examining each item individually.

Like many other terms in information science, relevance also has several different definitions due to the countless contexts in which it is discussed, and the existence of several different approaches due to the interdisciplinary nature of information science. Relevance has been discussed from different perspectives since the 1950s. The most problematic side of relevance is the factors affecting relevance judgment (Schamber, 1994). Schamber, in her review, provided a well categorized list of eighty factors affecting relevance, provided by large scale research studies. This proves that "relevance" is a complex issue to study. Researchers focusing on the context of ISB study not only the human evaluation of outputs but also all ISB processes. Recently, IR researchers have also attempted to understand the process of ISB. As a result of paradigms throughout the field, IR and ISB have been studied in conjunction with the approaches of decision making, cognition, situation, and dynamics (Schamber, 1994).

Schamber (1994) reported that the literature of IR, specifically relevance, and the literature of ISB intersect as new paradigms occur in IS. Decision-making research related to relevance focuses on problems, tasks and goals of the users who assess the value of

information, and IR systems. Decision-making models help us to understand ISB as well as IR and relevance. Cognitive perspective was examined by many scholars in IR literature, and, as discussed earlier, from a cognitive perspective, the concept of relevance is present in all ISB models.

In ISB models, relevance is usually formulated as the perceptions of users about problems (situation/context) and tasks in which users need information to make decisions. A widely accepted feature of IB is its dynamic nature. Kuhlthau (1991, 1993) approached relevance as dynamic, constructive, personal, and affective phenomenon, since the perceptions of users change as they go through the different stages. Similarly, in Ellis's (1989) model, a flexible ISB model, the mental model of the seeker is dynamic. Their perception of relevance changes as they consider alternative outputs (Schamber, 1994).

Schamber (1994) listed the questions which have been asked in the literature of IR studies for fifty years, but not answered completely or adequately. Questions related to behavior include: "What factors contribute to human relevance judgment?" (p.34), and "What process does relevance assessment entail?" (p. 34). Relevance is a cognitive, dynamic and situational phenomenon, and relevance is an essential concept for the majority of IB. Schamber (1994) emphasized that searching behavior, dynamic interactions, retrieving behavior and feedback are rich areas to study. Besides, she pointed out that research aiming to develop a standard for the measurement of relevance judgment in different situations will be promising. Although traditional information science research has often dichotomized information retrieval research and information seeking research, retrieving and relevance should be studied together, in order to explain human IB.

Information Behavior of Engineers and Digital Evidence Examiners

The amount of research investigating the information behavior of professionals could be as extensive as the total number of professions and roles within each profession. However, a review of the literature indicated that DEEs have never been a focus group in information behavior research. One reason for this may be that it is a relatively new type of profession.

The work context for DEEs and engineers demonstrates similar characteristics. It is a consistent finding that most engineers work in private firms and that they produce knowledge or a kind of service. Similarly, most DEEs work in public or private laboratories that vary in size, and they usually produce a service for their clients. DEEs may also work as academics who contribute to the literature of digital forensics, and their work requires the ability to process a high level of technical information (Barbara, 2005).

DEEs work at the intersection of ICT and forensics, they basically work on digital devices and their education is usually in the computer-related sciences and engineering. In this study, due to the similar work characteristics of engineers and DEEs, it was proposed that the literature on the ISB of engineers would provide a framework to study the ISB of DEEs. Therefore, the literature on the ISB of engineers is reviewed here to construct a theoretical framework for this study.

Researchers in LIS have been extensively interested in the information behavior of engineers for the last forty years. Allen and Gerstberger (1967) investigated the criteria utilized by engineers in the choice of different technical information channels in problem-solving activities. They conducted their study in two divisions of a large electronic firm, and 19 out of 33 pre-selected engineers provided the data for the study over a period of 15 weeks. Allen and

Gerstberger collected the data by using specially designed questionnaires; they measured the frequency of information source use and determined which of four criteria (1: Accessibility, 2: Ease of Use, 3: Technical Quality, 4: Degree of Experience with Information Source) were used by engineers in the selection of particular information sources.

Allen and Gerstberger (1967) found a direct relationship between perceived accessibility of information channels and the frequency of use of that information source. They found no significant evidence that engineers predominantly use channels with the highest perceived technical quality. However, they found that both accessibility and perceived technical quality influenced the choice of their first source. They also found that prior experience influenced the perception of accessibility. That is, as the engineer's experience with a channel increased, the level of perceived accessibility of that source also increased.

The general model of information seeking of professionals was drawn by Leckie et al. in 1996. In their study, they mainly reviewed the research related to the information behavior of several groups of professionals; health care professionals, engineers, and lawyers. They profiled these professions based on their information behavior, and, then, they synthesized the characteristics of information behavior of selected professionals. Eventually, they proposed a general model that they asserted could be applied to any professional field. Their study, with limitations in mind, opened new doors to future research about the information seeking of professionals. They formulated a general model of information seeking of professionals with six major components: work roles, associated tasks, characteristics of information needs, and three factors affecting information seeking: (a) awareness, (b) sources, and (c) outcomes.

The basic assumption of the model is that work roles and associated roles/tasks are the trigger mechanism for information seeking of professionals. Nevertheless, information behavior is affected by some variables which can eventually influence the outcome. In this model, five roles in various different professions: service provider, administrator/manager, researcher, educator, and student are often mentioned. Specific tasks such as counseling, assessment, report writing and supervising, are addressed in the second layer of the model.

Variables influencing the information needs of professionals are individual demographics (age, specialization, profession, geographic location, career stage), context (information need in a specific situation), frequency (new or recurring information need), predictability (unexpected or predictable), importance (the level of urgency), and complexities (difficult or easily resolved). The researchers broadly characterized the sources of information by types of channel format, as formal or informal; internal or external; oral or written; and personal.

Leckie et al. (1996) noticed that although engineers work for common organizational entities, and engineers basically receive an extensive education at the bachelor level, the number of subspecialties in engineering is numerous. In addition, engineers work in institutions which vary in size and type, be they public or private.

According to the findings of Leckie et al. (1996), engineers individually worked in different areas, such as research, testing, design, construction and manufacturing, consulting, sales, and teaching. Engineers usually focused on problem solving, and the outcome of their work is usually a service, a process, or a product rather than knowledge. Leckie et al. (1996)

found that engineers produced far less information than they needed during the generation process.

Engineers usually need information to generate information encoded in material form. In general, libraries are not used by engineers. On the other hand, oral communication is overwhelmingly preferred in engineering. Leckie et al. estimated that engineers spent from 20% to 80% of their work hours in information seeking, although the information need of engineers varied according to their role in the work environment. The degree of confidentiality and secrecy in the work environment also affected the information seeking of engineers. In engineering, the originality as much as the accuracy, of information is important. An awareness of the available information sources may also have an impact on the outcome of their information-seeking behavior.

Leckie et al. (1996, p. 167) concluded that the information behavior of engineers is "the result of a complex interplay of variables, from job function, work environment, qualifications, discipline, and career stage to accessibility of information, its ease of use, and technical quality."

Factors Affecting Information-Seeking Behavior of Engineers

The factors affecting information source use by engineers have been listed and categorized in different ways in the literature. For instance, Anderson, Glassman, McAfee, & Pinelli (2001) categorized the factors affecting decisions of aerospace engineers and scientists with regard to use of information sources as: (a) task characteristics, (b) carrier characteristics

and (c) user characteristics. They described these three categories of characteristics as the major variables affecting information seeking of aerospace engineers.

Anderson et al. (2001) mainly addressed: (1) accessibility, (2) ease of use, (3) cost, (4) technical quality, (5) usefulness, (6) promptness or the time it takes to deliver the information and (7) importance as the characteristics of written information sources used by aerospace engineers. Anderson et al. (2001) listed perceived levels of task complexity and uncertainty as determinants related to task characteristics. Finally, they categorized relevance and prior use - familiarity - as the user characteristics influencing information source selection of aerospace engineers.

Kwasitsu (2003) listed several characteristics that influenced engineers' selection of information sources: accessibility, availability, technical quality, relevance, currency, reliability, ease of use, experience with source, cost of use, lingo/technical jargon, and personal mastery.

Characteristics of Information Sources

Not all characteristics of information sources were defined in the same way in information-seeking studies. Although some characteristics, such as financial cost and proximity of information sources, were usually defined in the same way, definitions and operationalization of characteristics such as accessibility, quality, relevance, ease of use and usefulness have been problematic.

"Accessibility" is an elastic term. Like many other characteristics of information sources, "accessibility" can be investigated by approaching it subjectively or objectively. It seems that an objective, universal definition of "accessibility" is impossible to find. Predetermined objective

definitions of accessibility usually did not include all possible dimensions of accessibility. For example, Gerstenfeld and Berger (1980) measured accessibility as the amount of time spent looking for information, regardless of the effort made by the seeker during that time. Pinelli, Bishop, Barclay, & Kennedy (1993) operationalized accessibility as the physical distance to the information source.

Anderson et al. (2001) studied the accessibility of information carriers from the perspective of the principle of least effort. They found out that engineers tend to minimize their efforts during the search for information needed in their work life. Anderson et al. (2001) operationalized the principle of least effort by determining one's preference for seeking information from:

- One's own store of information as opposed to seeking information from others
- Oral communication as opposed to written communication
- Communication with sources inside the organization as opposed to communication with sources outside the organization
- Direct communication with a source as opposed to through mediating carriers, such as those provided by library personnel, who are not authorities in the discipline under study (p. 133)

Fidel and Green (2004) represented several dimensions of accessibility. They emphasized that new innovations, like the Internet and mobile communications, have made researchers think about accessibility differently. For instance, physical distance is not an important variable for online sources. Information from a long distance away can be assessed by using a handheld mobile device. For online sources, accessibility of sources may be measured as the proximity of information technology or system used to reach online sources, regardless of the actual physical distance to the online source.

Fidel and Green (2004) listed factors affecting engineers' selection of information sources in two general categories; accessibility and quality. They detailed the factors mentioned by respondents during interviews as the following:

- Accessibility
  - sources I know
  - saves time
  - is physically close
  - has the right format
  - can give the right level of details
  - is accessible
  - is available
  - has a lot of different types of information in one place
  - sources with which I felt comfortable
  - can be searched with keywords or codes
  - is attractive
  - is not busy
- Quality
  - can give data that meets the needs of the project
  - is most likely to have the information needed
  - the information is not available elsewhere
  - can give the latest information
  - is reliable
  - gives definite answers
  - is accurate

Gerstberger and Allen (1968) studied participants' own perceptions of accessibility; they stated that engineers' perceptions of accessibility guided their information practices.

Quality of an information source was often mentioned by respondents as a factor affecting their selection of sources, in addition to accessibility of information sources (Allen, 1977; Anderson et al. 2001; Barry 1993, 1994; Gertsberger & Allen, 1968; Pinelli et al., 1993; O'Reilly, 1982; Schamber 1991a, b). One's perception of the quality of an information source is based on one's previous experience with the source and/or public reputation of the source. In their studies, Barry (1993, 1994) and Schamber (1991a, b) included the same elements in the

coding and definitions. In the first sub-category of source quality coding, respondents had an idea about the quality of the source based on their personal experience. That is, they observed the source, and had an idea about the extent to which the source met general standards. In the other sub-category, respondents actually predicted the quality of a source based on what the respondent heard or read about the source. Schamber included another element of quality in the coding of criterion categories; consistency. It was defined by Schamber as the extent to which the source delivered information of the same quality, or accuracy, over time. Among several characteristics, Anderson et al. hypothesized that accessibility and quality are two competing characteristics of written information sources.

Anderson et al. (2001) listed prior use and relevance under the category of user characteristics. They proposed that there is a greater probability that information seekers will obtain information from information sources recognizable to them rather than from new information sources. Fidel and Green (2004) found that successful prior use (sources I know) was the most common factor affecting the selection of information sources among engineers. This variable is also known as “familiarity” (Leckie et al., 1996).

In ISB studies, another factor mentioned by respondents is relevance. That is, the extent to which the information source is seen to be relevant to the respondent. Relevance has been discussed from different viewpoints since the 1950s. The most problematic side of relevance is the factors affecting relevance judgment (Schamber, 1994). It appears that the phrases “factors affecting professionals’ selection of information sources” and ‘relevance criterion” are used interchangeably. As seen in Table 1, criterion categories in IR research are similar to factors studied in ISB research.

Table 1

Comparison of Categories of Relevance Criteria from the Studies of Barry (1993, 1994) and Schamber (1991a, b)

Factors	**Definitions**	
Depth /Scope /Specificity	Barry	Depth/Scope
	Schamber	Specificity; Summary/Interpretation; Variety/Volume
	The extent to which information is in-depth or focused; is specific to the user's needs; has sufficient detail or depth; provides a summary, interpretation, or explanation; provides a sufficient variety or volume	
Accuracy / Validity	Barry:	Objective Accuracy/Validity
	Schamber:	Accuracy
	The extent to which information is accurate, correct or valid	
Clarity	Barry:	Clarity
	Schamber:	Clarity; Verbal Clarity; Visual Clarity
	The extent to which information is presented in a clear and well-organized manner	
Currency	Barry:	Recency
	Schamber:	Currency
	The extent to which information is current, recent, timely, up-to-date	
Tangibility	Barry	Tangibility
	Schamber:	Specificity
	The extent to which information relates to real, tangible issues; definite, proven information is provided; hard data or actual numbers are provided	
Quality of Sources	Barry	Source Quality; Source Reputation/Visibility Reliability; Expertise; Directly Observed; Source Confidence;
	Schamber	Consistency
	The extent to which general standards of quality or specific qualities can be assumed based on the source providing the information; source is reputable, trusted, and expert	
Accessibility	Barry	Obtainability; Cost
	Schamber	Accessibility; Availability; Usability; Affordability
	The extent to which some effort is required to obtain information; some cost is required to obtain information	
Availability of Information /Sources of Information	Barry	Availability within the Environment; Personal Availability
	Schamber:	Verifiability
	The extent to which information or sources of information are available	
Verification	Barry	External Verification; Subjective Accuracy/Validity
	Schamber	Source Agreement
	The extent to which information is consistent with or supported by other information within the field; the extent to which the user agrees with information presented or the information presented supports the user's point of view	
Affectiveness	Barry	Affectiveness
	Schamber:	Entertainment Value
	The extent to which the user exhibits an affective or emotional response to information or sources of information; information or sources of information provide the user with pleasure, enjoyment or entertainment.	

Characteristics of Task (Complexity and Uncertainty)

The concept of "task" has been persistently studied in the field of information science (Byström, 1996, 1999, 2002; Byström & Järvelin, 1995; Herzum & Pejtersen, 2000; Kuhlthau, 1993, Mick, Lindsey, & Callahan, 1980; Rasmussen, Pejtersen, & Goodstein, 1994). In many studies of task-based information behavior, task complexity has been conceptualized "in terms of perceived a priori determinability of information inputs, processing and outputs" (Byström, 2002, p. 582).

Byström (2002) theorized that the level of task performers' knowledge of the task procedure and requirements at the beginning of a task is negatively correlated with the level of perceived task complexity and positively correlated with the frequency of use of information sources. In other words, if a task performer has less knowledge about a task, he/she will see the task as being more complex, compared to others with more knowledge of the task procedure and requirements. Therefore, the task performer will use a greater number of information sources in order to learn how to accomplish the task at hand.

Similarly, as the level of uncertainty the task performer feels increases, the number of sources used to complete the task also increases (Kuhlthau, 1999; Pinelli et al., 1993). Roger (1983) described uncertainty as the level of predictability of different alternatives when faced with an incident. In this sense, uncertainty means a lack of predictability in the information and situation; when people feel uncertainty, they seek information to increase the level of predictability. That is, individuals typically want to have a better idea of what the outcome of an event will be and to make more accurate predictions, thus, individuals seek information. The higher the level of uncertainty, the greater the amount of information needed, and the higher

the number of sources used. This theory is supported by the studies of Brown and Utterback (1985), Anderson et al. (2001), and Pinelli et al. (1993).

Anderson et al. (2001) reported that researchers studied task characteristics as factors affecting information behavior from different aspects, such as task uncertainty and task complexity. After a discussion of several findings on task complexity, they concluded that "as task complexity increases (a) the use of internal channels decreases, and (b) the number of sources increases" (p. 134). Anderson et al. (2001) also confirmed that a positive relationship exists between the perceived level of uncertainty and the number of sources used in a task.

Demographics

Demographic characteristics of information seekers such as age, gender, experience, and education have been studied for a long time. Academics have often found a significant relationship between demographic characteristics and information-seeking choices, when they studied these factors independently from other variables. However, when these variables were studied in multivariate analysis, evidence showed that the relationship between demographic characteristics and information-seeking behavior was non-significant or had little impact (Anderson et al. 2001). In this study, the demographics of interviewees are provided to describe the sample.

CHAPTER 3

METHODOLOGY

Introduction

The goal of the current research was to examine the information-seeking behavior of DEEs in depth. This study employed a qualitative approach to research design by utilizing semi-structured intensive interviews. The interview instrument was designed by Wai-Yi (2002) on the basis sense-making time-line approach. A qualitative approach seemed to be more suitable to achieving the goal of this study.

In the following sections, research questions, characteristics of qualitative methods, the sampling technique and data collection instrument, and content analysis as a data analysis tool is discussed.

Research Questions

In order to have an in-depth understanding of the information-seeking behavior digital evidence examiners, the researcher asked four general questions:

1. What circumstances lead digital evidence examiners to seek information in their professional life?

2. What are the information sources used by digital evidence examiners in their work?

3. What characteristics influence information source selection and information source use of digital evidence examiners.

4. What are the obstacles that digital evidence examiners face while seeking job-related information?

Qualitative Approach

King, Keohane, & Verba (1994) asserted that the only differences between qualitative and quantitative research are stylistic. They stated that while quantitative and qualitative research appears to be very different, the actual difference is in the styles and techniques used by researchers. The main difference is that quantitative research depends on a large quantity of numbers and statistical methods, while qualitative research is more about definitions, case studies, history, and similar data sources, but utilizes few numerical measurements.

Bryman (1984) provided more insights into the differences between qualitative and quantitative research. First, he argued that with respect to flexibility, qualitative research seems to be more flexible than quantitative data. The reason is that qualitative research focuses more on discovering original or unanticipated findings, and is open to an alteration of the research with unforeseen developments. On the contrary, the quantitative research design has more fixed sets of rules and methods for measuring hypotheses, and this prevents adjustment of the research design to accomodate unanticipated developments during the research (Bryman, 1984).

The quantitative method is usually employed to find out whether an assumption can be generalized. The qualitative method of research is applied to describe a specific phenomenon, or to come up with an explanation for the occurrence of a specific phenomenon (Gormon & Clayton, 2005). Since the aim of the current research is to gain an in-depth insight into the information-seeking behavior of digital evidence examiners, a qualitative method is more appropriate. A sense-making approach is considered a suitable approach in this study because it

not only provides a theoretical framework, but also provides a method to examine human information-seeking behavior.

IRB Approval

This study was reviewed and approved by the UNT Institutional Review Board on May 25, 2010. As a requirement of the IRB approval process, TNP was approved before starting the research. The letter of IRB approval and attached Consent Notice for Interviewees are presented in Appendix D.

Population and Sampling

The population of this study is all the examiners who hold some type of certification and have the authority to collect and examine digital evidence, and work in public and private laboratories which were established to provide digital forensic services in Turkey. The population in this study is known, in short, as Digital Evidence Examiners (DEEs). DEEs include all examiners who collect and examine digital evidence, not only from computers, but also from other physical digital items. While computer examiners specifically specialize on evidence collected from computers, in digital forensic laboratories, other digital devices, beside computers, such as GPS devices, flash memories, and cell-phones are examined.

To describe the population and their work environment, instead of using the terms “computer evidence,” “computer forensics” and “computer examiner,” the terms ”digital evidence,” “digital forensics” and “digital evidence examiner” are used. Digital forensics, digital

evidence, and digital evidence examiner are broader terms than computer forensics, computer evidence and computer examiners, respectively.

Sampling techniques were chosen according to the purpose of the study. Probability samples were not appropriate or even possible for all studies, because the researcher did not intend to generalize the relationships between dependent and independent variables beyond the sample to a larger population. Instead, the researcher intended to understand the information-seeking behavior of DEEs and build a foundation for further studies. This is why non-probability samples were appropriate in the current study (Sullivan, 2001).

Although non-probability samples are helpful in some research situations like the current one, an important limitation of non-probability samples is that researchers cannot assert that their results are representative of a certain proportion of the population. A second important limitation of non-probability sampling is that sampling errors cannot be known, because it is impossible to apply the techniques used to estimate sample size to non-probability sampling (Sullivan, 2001).

In this research, availability sampling which is a type of a non-probability sampling was used. Availability sampling refers to targeting the samples which are available to the researcher. This type of sampling is appropriate and widely used in research in which the researcher cannot develop a complete sampling frame. As mentioned above, it is not possible for the researcher to know how many digital examiners and digital forensics laboratories exist in Turkey, since there are many public and private laboratories. In addition, time and financial constraints make availability sampling suitable for this research (Sullivan, 2001).

Subjects were recruited from two different digital forensic laboratories that organizationally operate under the administration of the Turkish National Police, and permission was obtained from the Turkish National Police to conduct this study. An invitation email was sent to all digital evidence examiners working in those two laboratories, in which they were asked if they would like to participate in this study. The interview instrument and consent notice were sent to them as attachments to the invitation email. Examiners were asked to read the interview instrument and consent notice, and to respond by email, if they agreed to participate. Otherwise, they were not asked to take action. A total of 10 examiners responded to the email. The researcher interviewed the examiners who agreed to participate in the study over the telephone, and the associated expenses were paid by the researcher himself.

Data Collection

In this study, the interview technique was used to collect data. Interviewing is a commonly used method in qualitative research. An interview refers to oral communication that takes place between an interviewer and a respondent; the interviewer asks questions which are structured to some extent, and the respondent answers the questions or makes comments about the questions. The answers and comments of the respondent are recorded - usually audio taped - during the interview upon the approval of the respondent. If the respondent doesn't agree to be audio-taped, then the interviewer will use a note-taking technique (Sullivan, 2001).

Interviews provide several advantages. Interviewing gives the researcher the flexibility needed for an in-depth understanding of a phenomenon. In addition, in-depth interviews are

usually unstructured, meaning that questions are not constructed before the interview. The interview starts with a broad, open-ended question, and, then, as the conversation continues, the interviewer asks other open-ended questions based on answers he/she gets from the respondent (Sullivan, 2001). In this study, the researcher used a semi-structured time-line interview instrument.

Time-Line Interviews

In the current study, a specific type of interviewing was utilized. It is known as micro-moment time-line interviewing, which was developed by Dervin (1992, 1999). This interview method was used to investigate the micro-level information-seeking behavior of the respondent. In-depth open-ended questions were asked during the interview, and the interviewer could change the wording of a question or ask more detailed questions, according to the development of the conversation. In time-line interviews, the possible information sources used by the respondent were not mentioned initially by the interviewer. Instead, the respondent was free to mention and talk about any information source that he/she used. The aim of the interview was to understand the reasons for the respondent's behavior, as it related to information seeking and use (Barry & Schamber, 1998).

In the time-line interviewing technique, the interviewer asks the respondent to recall a critical, important or influential situation. Then, the interviewer asks the respondent to tell him/her what happened initially. The interviewer continues by asking about the next sequence of events. The interview ends after the interviewer asks the respondent about the situation, gaps, bridges and outcomes in each time-line incident (Dervin, 1983, 1992; Schamber, 2000). In

this study, the researcher began time-line interviews by asking about a particular situation, which was a digital evidence investigation. The interviewer (also the researcher) then asked questions about gaps (also called information need), bridges (one example could be an information source), and outcome (the success of the information-seeking efforts and the perceived satisfaction level with the information sources).

Interview Instrument

The interview instrument used in the current study was adapted from the study of Wai-Yi (2002) and is given in Appendix B. Wai-Yi used sense-making to examine information seeking and use in the workplace.

The adapted interview questionnaire is composed of two parts. The purpose of the first part of the interview questionnaire was to conduct time-line interviews and collect data about work roles, tasks, and information needs of digital evidence examiners. The second part aimed to obtain data about information sources used by digital evidence examiners.

In the time-line interviews, the steps of the digital forensic process were operationalized as: collection, examination, analysis, and reporting. The interviewer asked questions about the information behavior of participants in each step of the process. These steps were called time-line events. The purpose of the questions asked in the second part of the interview was to find out which information sources digital evidence examiners use, and what characteristics of information sources affect their source selection to achieve their task goals that they describe in the first part of the interview.

The adapted interview instrument used in this study is presented in Appendix A. A brief explanation of the interview instrument is provided as an introduction. The researcher, first, asked if the respondents had read the consent form. Then, the researcher began the interview, after the interviewee said that he had read the consent form. The researcher made certain necessary changes while adapting the actual interview instrument to the context of digital forensics. For example, the researcher replaced “an engineer (or an auditor or an architect)” with “a digital evidence examiner (or a computer examiner)” in the first question. In the second question, the word “job” was replaced with “task” and “in your workplace” was omitted. No changes were made to the third question. In the fourth question, again, the word “job” was replaced with the word “task” and the steps of the digital forensic process were listed according to the categorization of Kent et al. (2006)

In the questions regarding information needs, used sources and outcomes in each step, the present tense of the questions was replaced with past tense.

Administering Interviews

A Nokia 5800 model cell phone was used during the interviews, and the voice recording feature of the cell phone was very helpful. The researcher interviewed the 10 participants over the phone. In order to reduce expenses, the researcher called land lines when possible, by using a calling card that was not charged for calls to landlines in Turkey. The researcher recorded the interviews on the phone to prevent data loss. First, the participants were asked if they had read the consent notice, then a short explanation about the interview instrument was given before

starting the interviews. All participants agreed to be audio-recorded, and all interviews were audio-recorded.

The average length of an interview was 30 minutes. The first five interviews took approximately 45 minutes, while the other five interviews took about 25 minutes. It was really interesting that the first half of the interviewees appeared to be more comfortable than the second half. The first half did not hesitate much in talking about their jobs. However, the other half of the interviewees were not comfortable; the answers they gave were usually short. The researcher, then, tried to explain that there is no right or wrong answer about what sources they use, and that he was mostly focusing on their information needs.

Another thing that may have caused this situation is that the second half of the interviewees were not ranked as examiners. Nor were they in supervisory positions. Perhaps, they didn't feel secure enough to talk about the details of their tasks. Talking over the phone was a disadvantage for the researcher in this aspect. Examiner F didn't even want to answer the questions in the first part of the interview, and said that he could not give detailed information about the cases he processed. In fact, the interview instrument didn't ask for any detailed or identifying information about the specific cases that they remembered best. However, the perceptions of "detail" and "the secrecy of investigation in criminal cases" varies from one person to another, and the researcher didn't force any of the interviewees to give answers to the questions.

The researcher sometimes explained the questions by giving examples when needed. During some interviews, the researcher noticed that it was very difficult indeed to keep people focused on the question currently being asked. Interviewees sometimes answered other

questions before the researcher had even asked them. If a question had already been answered, then the researcher skipped the question.

The interviews were conducted in a natural manner. Since there is an eight hour time difference between the U.S. and Turkey, some interviews were made in the very early morning hours (e.g., 2a.m.). All respondents were cooperative for the most part and answered all questions, except for Examiner F. While interviewing Interviewee D, the line dropped three times because of low signal strength on the interviewee's phone, and the researcher reminded Interviewee D where the conversation had stopped each time the connection was reestablished. This is another disadvantage of telephone interviews.

Data Analysis Procedure: Qualitative Content Analysis

Researchers in the field of information and library science (ILS) have been using the method of content analysis as an analytical tool in many different research designs. Content analysis has been used both in quantitative and qualitative research. Content analysis has been defined as:

> A research technique for making replicative and valid inferences from data to their context (Krippendorff, 1980, p. 21).
>
> A research method that uses a set of procedures to make valid inferences from text (Weber, 1990).
>
> An approach of empirical, methodological controlled analysis of texts within their context of communication, following content analytic rules and step by step models, without rash quantification (Mayring, 2000, p. 2).
>
> Any qualitative data reduction and sense-making effort that takes a volume of qualitative material and attempts to identify core consistencies and meanings (Patton, 2002, p. 453).

> A research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns (Hsieh & Shannon, 2005, p. 1278).

These definitions show that content analysis is more than just counting words. Content analysis is also used to discover themes, ideas, meaning, and emotions in a specific text. The definitions address two important characteristics of content analysis as applied to qualitative research: (1) content analysis lets researchers understand a phenomenon subjectively and (2) the method of content analysis provides a scientific way to make subjective inferences.

Qualitative vs. Quantitative Content Analysis

Berg (2001) listed four ways that qualitative content analysis differs from quantitative content analysis.

- Research areas in which they are used: First, quantitative content analysis has been widely applied in mass communication. On the other hand, qualitative content analysis is especially useful in exploring the meanings within text, and is often applied in anthropology, qualitative sociology, and psychology.
- Inductive vs. deductive: Second, quantitative content analysis is mostly deductive in nature, whereas qualitative content analysis is mostly inductive. Deductive processes of analysis are theory driven. In quantitative content analysis, the goal of the researcher is to test hypotheses or expand on previous empirical research. In contrast, in qualitative content analysis, the researcher utilizes a ground theory approach to some extent. The core of qualitative content analysis involves the compression and reduction of raw data into themes and categories by utilizing valid interpretation and inferences. This is a form of inductive

reasoning by which themes and main categories arise from raw data. However, deductive reasoning has also been used in qualitative content analysis. Researchers may also use variables and concepts defined in previous research in their own qualitative analysis (Berg, 2001).

Hsieh and Shannon (2005) examined three different types of qualitative content analysis in terms of the involvement of deductive reasoning. In conventional qualitative content analysis, researchers use only inductive reasoning to ground theories. However, in directed content analysis, the researcher initially begins coding with a theory. Later on, the researcher adds new themes and concepts to existing ones as he/she makes valid inferences. In the third one, summative content analysis, words are initially counted, and then, latent meanings are included.

Based on these definitions, the current study can be considered as a directed content analysis. The researcher first used concepts developed by previous studies. The raw data was, first, coded based on the findings of previous empirical studies. The extent to which a researcher uses deductive reasoning depends on the scope of the research question. In the following section, in which the process of content analysis is discussed, the researcher addresses the theories and concepts utilized to perform coding. Whenever, the researcher and two other coders identified a new theme or concept, it was added to the existing coding scheme.

- Sampling techniques: Sampling techniques differ in quantitative and qualitative content analysis. Probabilistic sampling techniques should be used in quantitative content analysis to maintain the validity of statistical evaluations. Random sampling is mostly used in quantitative content analysis. On the other hand, non-probabilistic sampling techniques are

used in qualitative content analysis, and the sample size is usually small. Availability and snowball sampling techniques are mostly used in qualitative content analysis.

- Products of analyses: The main product of quantitative content analysis is the production of numbers. In qualitative content analysis, the researcher produces descriptions or categories. Weber (1990) criticized quantitative content analysis, noting that it does not address semantic and syntactical information within text. He emphasized that the best approach in content analysis is to combine quantitative and qualitative methods in one research design.

Reliability and Validity in Content Analysis

The purpose of the qualitative method is to understand phenomena occurring in specific situations. This is the reason for applying a naturalistic approach to qualitative research as opposed to the logical positive approach used in quantitative research. Observations and interviews are often used in the naturalistic - qualitative - research. On the other hand, surveys are more often utilized in logistic positive - quantitative - research. However, researchers must show that their testing methods and findings are accurate and credible. In the quantitative approach, the researcher must maintain reliability and validity.

Reliability refers to:

> The extent to which results are consistent over time and an accurate representation of the total population under study is referred to as reliability and if the results of a study can be reproduced under a similar methodology, then the research instrument is considered to be reliable. (Joppe, 2000, p. 1)

Validity refers to:

> Validity determines whether the research truly measures that which it was intended to

> measure or how truthful the research results are. In other words, does the research instrument allow you to hit "the bull's eye" of your research object? Researchers generally determine validity by asking a series of questions, and will often look for the answers in the research of others. (Joppe, 2000, p. 1)

Stenbacka (2001) stated that "the concept of reliability is even misleading in qualitative research. If a qualitative study is discussed with reliability as a criterion, the consequence is rather that the study is no good" (p. 552). Lincoln and Guba (1985, p. 290) asked the question, "How can an inquirer persuade his or her audiences that the research findings of an inquiry are worth paying attention to?" At this point, the quality of the study arises as an issue of concern for researchers. Eisner (1991) simply asserted that a good study helps people understand a confusing and complex issue. However, it is not easy to judge how good a study really is. The concepts of reliability and validity seem to be more complex to explain, demonstrate and test in a qualitative versus a quantitative paradigm. The reason is that the literature provides many different approaches to validity and reliability in a qualitative paradigm. To show that their study is reliable and valid, researchers utilizing a qualitative approach need to demonstrate that their studies meet certain criterion such as:

- Credibility, neutrality or confirmability, consistency or dependability, applicability or transferability, and inquiry audit (Lincoln & Guba, 1985).
- Quality, rigor and trustworthiness (Davies & Dodd, 2002; Golafshani, 2003; Lincoln & Guba, 1985; Seale, 1999)
- Generalizability (Patton, 2001)

It is obvious that there is no consensus about the concepts that could be substituted for reliability and validity in the qualitative paradigm. Golafshani (2003) emphasized that the abovementioned criterion should be redefined for the qualitative paradigm.

It is very difficult to formulate universal definitions and to make distinctions among the abovementioned criteria. It appears that the criteria are overlapping; that quality encompasses all the other criteria, and trustworthiness encompasses credibility and consistency. The reliability and validity of the study also impact the generalizability. For this reason, the researcher must, first, identify the procedures he followed to ensure reliability and validity in the current study. Then, he must indicate what criteria should be applied to the procedures he followed.

Pilot Study

As a pilot study, the researcher interviewed an examiner who is not one of the 10 respondents. The researcher investigated whether an interview instrument is useful, understandable and appropriate in this research context. In the pilot study, the researcher confirmed that examiners in Turkey also follow the four steps of the digital evidence examination process, as utilized in the interview instrument. The only difference was that examiners in Turkey usually don't collect evidence, such as digital devices and digital media, from crime scenes. They mostly work on digital devices and media previously collected from crime scenes and delivered to their laboratory by other units. The researcher benefited from the time-line interview technique in regard to this point; he didn't ask questions about the steps that respondents didn't participate in.

The researcher also discussed the interview questions with the interviewee in the pilot study. The pilot interviewee didn't make any recommendations, except for mentioning that they do not perform the evidence collection task. Therefore, the researcher did not make any changes to the interview instrument after the pilot study. The interview instrument was useful

and the structure of the interview was helpful in collecting and analyzing the data. The pilot study demonstrated that this study meets the criteria of confirmability and consistency.

Reliability of Recording, Transcribing and Translating Interviews

The researcher made audio recordings of telephone interviews and transcribed the interviews manually, by himself. After transcription, the researcher emailed the interview texts to the interviewees to get their confirmation of the content. None of the interviewees requested changes to the content of the interview texts. This indicates that the transcriptions of the interviews in Turkish were confirmed by the interviewees. The translation of the transcribed text was done by the researcher, and double checked, later on, by three other graduate students whose native language is Turkish.

The researcher was sufficiently skilled in translating the interviews from Turkish to English. He began learning English when he first started high school, and in his first year of Police College (which is actually a formal high school), he attended classes in English for one academic year. He received 28 hours of English instruction a week for one complete academic year and continued studying English during his higher-level education. The researcher graduated from the Intensive English Language Institute at the University of North Texas and earned his master's degree from the Criminal Justice Department at Eastern Kentucky University. In addition, upon completion of this study, he will have earned his doctoral degree in the U.S. However, in order to prevent data loss during the translation from Turkish to English, he enlisted three other graduate students to help him. These graduate students are also native speakers of Turkish. They are not only speakers of both Turkish and English, but are also

familiar with the literature of information science and criminal justice, which made their training easier. The three graduate students compared their translations before starting the independent coding process. Necessary corrections were made to the translations until all interpreters were unanimous in their agreement.

Audio recordings, transcribed interview texts, and translations were provided in digital format on a CD for audit purposes. The CD is protected by software against the making of illegal copies and will be kept in a secure box for three years. At the end of three years, the CD will be destroyed. The processes of recording, transcribing and translating met the criteria of confirmability, consistency, auditability, and trustworthiness.

Intercoder Reliability

Intercoder reliability refers to the extent to which coders are agreed upon variables and themes in raw data. Weber (1990) stated that "to make valid inferences from the text, it is important that the classification procedure be reliable in the sense of being consistent: Different people should code the same text in the same way" (p. 12). Weber further noted "reliability problems usually grow out of the ambiguity of word meanings, category definitions, or other coding rules" (p. 15). In this study, intercoder reliability was maintained by recruiting three more coders in addition to the researcher. This ensured that each interview text was coded by someone other than the researcher. The average agreement between coders was 90 percent. The coding process is described in the following section entitled, The Process of Qualitative Content Analysis. Having a 90 percent agreement between coders demonstrates that this study met the criteria of quality and dependability.

Generalizability

Generalizability is also known as external validity (Neuendorf, 2002); it refers to the extent to which the findings of the study are valid for the rest of the population. Generalizability is a common method used to test the validity of quantitative research. However, Patton (2002) noted that the use of generalizability as tool to test the validity of qualitative research depends on the case under study. In this study, the researcher did not intend to attain generalizability. Instead, the researcher intended to identify the variables that influence the information behavior of digital evidence examiners, so that those variables can be used in future quantitative studies using larger sample sizes. The researcher established the criteria of trustworthiness and reliability.

The Process of Qualitative Content Analysis

Step 1: Preparing the Data

The researcher collected data by applying an interview technique. The data were first completely transcribed, or transformed, into written text. Since the data were in Turkish, the researcher translated the Turkish text into English. Then, the translated text was examined by another person who was qualified in Turkish and English. Although content analysis of the text in Turkish would be easier for the researcher, the researcher conducted his analyses on the translated text in order to maintain trustworthiness, credibility, confirmability, auditability, and transferability.

Step 2: Defining the Unit of Analysis

Weber (1990) emphasized that defining the unit of analysis is the most important step in content analysis. In this study, the unit of analysis was the individual themes. An individual theme refers to the manifestation of an idea (Minichiello, Aroni, Timewell, & Alexander 1990). Identified themes were transformed into codes after categorizing the themes, and, later on, an acceptable agreement percentage between coders in further stages of content analysis was established. Since a theme refers to an idea, themes can be expressed at different levels. Sometimes, a theme may be identified by only one word, because that word indicates a characteristic. Sometimes, a paragraph or whole document is necessary to depict a single theme. For this reason, the researcher identified themes in single words as well as in multiple words in larger structures of text.

Step 3: Identifying Themes

The researcher realized that interview data is, in fact, very difficult to analyze because during interviews, people usually don't pay attention to the organization of ideas as they speak; there is a lot of free-flow conversation and replication of ideas. In addition, interviewees change the topic very quickly while talking; they start one sentence and then stop in the middle of it. Then, they start talking about another related subject. The researcher also noticed that professionals tend to speak about how they perform their duties, rather than talking about the information sources they use and their information needs.

The researcher started identifying themes by creating tables for each interview, as illustrated in Appendix E. These tables consist of two columns: the Turkish text of the interview

was placed in left column, while the English translation of the text was put in the right. In this way, coders were able to establish whether the English text provided the same meaning as the Turkish text. Then, the researcher used the feature of "add comment" of MSOffice Word to annotate the identified themes. After finishing the annotations, the researcher developed an initial coding scheme. Since the interview instrument was structured according to the research questions, identifying themes was relatively easy compared to the case of using an unstructured interview instrument.

Step 4: Developing Categories and a Coding Scheme

The researcher began creating categories for a coding scheme on the basis of previous studies, such as the general model of information seeking of professionals (Leckie et al., 1996) and the task-based information seeking model (Byström, & Järvelin, 1995).

A numbering system is then applied to the coding scheme, where numerical digits represent different levels of the themes. For example, the themes listed under 1.x. are related to research question one which addresses the circumstances leading digital evidence examiners to seek information. The digit that follows the first digit distinguishes themes under a general category (see Appendix C). Table 2 shows the general categories as adapted from previous models. The coding scheme and manual is provided, along with a unique numeric identifier and code assigned to each individual theme, in Appendix C.

Table 2

General Categories Derived from Previous Studies

Number	Research question	General Category	Definitions
1	RQ1:What circumstances lead DEEs to seek information in their professional lives?	Context	Any situation in which a digital evidence examiner feels the need for job-related information.
2	RQ2: What are the information sources used by DEEs in their work?	Sources	Any type of information source from which DEEs obtain job-related information
3	RQ3: What characteristics influence information source selection and information use by DEEs?	Factors	Any variable that seems to have an influence on the information source selection and use by the digital evidence examiner
4	RQ4: What are the obstacles DEEs face while seeking job-related information?	Obstacles	Any challenge or difficulty mentioned by the interviewee while searching for job-related information

Step 5: Coding Scheme Refinement

As mentioned above, the researcher applied directed qualitative content analysis in this study. The researcher developed this study using two previously developed models: The general model of information seeking of professionals (Leckie et al. in 1996) and the task-based information seeking model (Byström, & Järvelin, 1995). An initial list of categories was generated from these models. In fact, the research questions were also derived from these models, and the interview instrument was designed according to the research questions. The coding categories were modified when a new category emerged (Miles & Huberman, 1994).

Step 5: Assessing Coding Consistency

The researcher ensured the consistency of coding by developing a coding manual. In the

coding manual, the researcher listed category names and definitions or rules to assign codes (Weber, 1990). The researcher trained three other coders in regard to the scope of the study, the nature of content analysis, how to identify themes, how to create a coding scheme, and the variables presented in prior research. The researcher asked coders to code randomly assigned interview texts according to the coding scheme.

The researcher maintained intracoder reliability by examining the coding manual several times during the analysis. After the coding manual was completed by the researcher, other coders began coding the text independently. The intercoder reliability was ensured in this way. The percentage of agreement between coders was 90. The process of content analysis was completed manually in this study.

CHAPTER 4

FINDINGS AND DISCUSSION

Introduction

In the literature of information science, there are three major conceptual frameworks: cognitive, social and multifaceted (Pettigrew et al., 2001). In the cognitive approach, researchers focus on the individual's attributes. Studies of the cognitive approach examine how a person applies his/her own world view to the practices of information behavior. An important research question raised by this approach is: Why does a person think or behave in a certain way in seeking and using information? Context in the cognitive approach is just the setting in which the information behavior of an individual is studied (Pettigrew et al., 2001).

On the other hand, researchers applying the social approach study the information behavior that does not fit within cognitive frameworks. In the social approach, context is an important factor in shaping an individual's and organization's information behavior. Another approach is the multifaceted, which focuses on the interaction/multi-directional relationships among individual(s), context, and organizations. This approach states that due to the complexity of human behavior, the cognitive or social approach, alone, is not sufficient to explain human information behavior (Pettigrew et al., 2001). A society is the larger context in which people live. As big changes occur in this context, individuals and institutions adapt themselves accordingly. Since enormous changes have been occurring at the intersection of the online and offline worlds in society, it is obvious that "information behavior" should be studied from a multifaceted perspective.

Courtright (2007) provided very good illustrations of the contextual factors shaping

information practices. She presented the similarities in contextual factors in everyday-life and workplace settings and listed those factors as: rules and resources, culture, social networks, social norms, collaborative requirements in the workplace, task or problem situations, and the work domain versus human activity.

The researcher utilized a multifaceted approach in this study, by studying the interaction/multi-directional relationships among individual(s), context, and organization. After asking the first, second and fourth research questions, social aspects of the information behavior of DEEs were addressed by focusing on work life as a context. With the third research question, the cognitive approach was utilized by studying individual information practices and perceptions. However, it was very difficult to separate those dimensions from each other because their borders are blurred. In the following sections, the findings regarding the social and cognitive dimensions of information behavior of digital evidence examiners (DEEs) are discussed.

Interviewee Demographics

All participants were male. The participants worked in either of two different laboratories located in the capital city of Turkey. The ages of the interviewees varied from 30 to 40.

Digital Forensics in Turkey

In Turkey, public and private, and local and regional digital forensic laboratories of different sizes provide digital forensic services at different levels of professionalism. There are

three main public institutions that perform digital evidence examinations in Turkey: Criminal Police Laboratories, Gendarme Criminal Laboratories, and the Scientific and Technological Research Council of Turkey (TÜBİTAK).

In addition to the main regional criminal laboratory located in Ankara, the TNP oversees other digital forensic laboratories that specialize in digital evidence obtained during investigations of certain types of crimes, such as terrorism and organized crime. Those laboratories are mostly local.

The interviews and websites of laboratories show that digital forensic services in Turkey started in 2002. It is impossible for the researcher to know the number of examiners in Turkey, or particularly in TNP, because several departments have digital evidence laboratories of different sizes that process particular types of physical items or digital objects. The interview participants stated that digital forensic laboratories have the same quality as labs in the U.S. and Europe. They often mentioned that they stay up-to-date with new developments in the field and also stated that forensic kits and tools are updated and upgraded on a regular basis.

Research Question 1: Context and Information Needs

The first research question in this study is: What circumstances lead DEEs to seek information in their professional lives? The goal of this question is to gain an understanding of the relationships between the characteristics of work, roles, tasks and sub-tasks of the examination process and information needs of DEEs. It is a consistent finding that information needs trigger information seeking, and the characteristics of the information needs of

professionals depend on the characteristics of their work, roles, tasks, and sub-tasks (Byström, & Järvelin, 1995; Leckie et al., 1996).

The researcher asked the following questions to learn about the characteristics of DEE's work:

1. Please describe your work as a digital evidence examiner (or a computer examiner).
2. Please describe a case that you have completed and that was important or challenging for you.
3. What was the objective of achieving that task?
4. Please tell me which steps you needed to go through to complete that case.

Work as a General Context

The interviewees' answers to Question 1 are listed in Table 3. The interviewees' answers provided some noteworthy points. Interviewee A mentioned a specific authority, which was the Office of the Prosecutor sending the evidence. In the criminal justice system in Turkey, prosecutors supervise criminal investigations. In the absence of informing prosecutors or without getting their approval, the police take no action. One way of initiating a digital evidence examination is for the prosecutor responsible for the investigation of a criminal case to request an examination of digital media. Interviewee B pointed out that his laboratory mostly handles digital evidence collected in organized crime cases. Interviewee C touched upon a problematic side of digital evidence examination: offenders usually try to hide, delete or encrypt digital data that can be considered as evidence in the crime they are committing.

Interviewee D said that digital evidence examination starts after the crime is committed and the evidence collection stage is completed. He also mentioned that the field known as "computer crimes" in the U.S. is called "informatics crimes" in Turkey. He explained that there are different types of crimes under the heading of informatics crimes, and emphasized that what they do is not to directly prevent computer crimes. In fact, they examine digital evidence collected during the investigation of different types of computer crime cases, such as white-collar crimes and internet [cyber] crimes.

Interviewee E clearly pointed out the three stages of digital evidence examination: examination, analysis and reporting of findings. Interviewee F emphasized that DEEs follow certain procedures in digital evidence collection and examination. Interviewee G brought a different perspective to the responses by noting that DEEs conduct examinations on the basis of information they received about the case from the party submitting the evidence. That is to say, the more information they get about the case, the more successful they will be in their examinations. Interviewee I pointed out that they operate within the confines of the legal platform, noting that they determine whether the evidence is collected legally. There are certain procedures they have to follow in order to protect the integrity of the evidence during examination and analysis.

Only Interviewee J noted that he collects digital evidence from a crime scene. He especially emphasized that digital evidence examination was conducted by applying appropriate techniques and using special tools and kits according to the circumstances of the investigation.

Table 3

Answers to Interview Question 1

ID	Comment
A	What we do in general is to determine if the digital materials we receive, such as CDs, DVDs, flash drives, cell phones and memory contain particular points asked by prosecutors, and to send our expertise report to the office requesting examination.
B	Our work is more pertinent to organized crimes. The function of our unit is to examine, analyze, and report digital evidence collected and delivered after conducted operations by narcotic, financial, informatics, and organized crime departments existing in Turkey. Eventually, we forward the case to the criminal justice system.
C	What I do as a professional investigating digital evidence is to discover the evidence relevant to the case in hand in the computers and other related parts such as hard drives, floppy discs, CDs, and DVDs collected from crime scenes. That evidence could be hidden, encrypted or purposely protected. Our goal is to reveal those and present them to the court.
D	There are a number investigation methods in this field called informatics crimes. One side of the phenomenon is Internet crimes; The other side of it is digital evidence examination. There are crimes committed real-time. There are financial crimes as another aspect. We search for digital evidence in digital materials collected after the crime was committed, and in other digital media allegedly containing information relevant to the crime.
E	We examine the materials collected from the crime scene. The materials which are capable of storing digital data could be potential evidence for the ongoing investigation. We try to get evidence from them [digital materials], and we report our findings about those [digital materials].
F	We primarily discover particular points related to the investigation on digital materials obtained by law enforcement agencies as a result of their operations. They obtain digital media by applying the appropriate procedure.
G	To examine and analyze digital materials according to the provided information about the case, and to report findings as written documents.
H	Our laboratory is a regional center serving other agencies located in surrounding cities. We conduct examinations on the digital evidence sent by associated departments according to their requests. We also conduct investigations in our city since we are already involved in local investigations.
I	As digital media examiners, we determine whether the digital media to be examined is obtained legally. We protect legally obtained digital media to prevent loss of data, and we copy an image of the drive. We always work on the image of the drive, not on the actual original drive.
J	Our job is to examine - according to attributes of the crime - any kind of digital media (hard drives, USB memories, CDs, DVDs, digital cameras, radio cassettes, memory cards) which were used in crime, or could be helpful to solve the case. If we find evidence which is not pertinent to the case but still has a value as an element of a crime, we, then, inform responsible parties of law enforcement departments. We can shortly describe our work as: to examine digital media and report our findings. According to the circumstances during the investigation, we can take images of drives at the crime scene by using appropriate techniques and tools, and, then, perform a detailed analysis in the laboratory.

In short, digital evidence examiners rarely collect digital evidence from crime scenes, but mostly examine and analyze digital media delivered to them, and report their findings

about the digital evidence in those digital media according to legal regulations, by applying certain techniques and using special hardware and software determined by the type of crime and digital media. As can be seen in their job description, the work environment of digital evidence examiners shapes their information behavior. Legal regulation and responsibilities, technical differences in the digital devices, and the variable nature of different types of crimes forces DEEs to act according to the context.

The examiners described their work in a similar way. The most common themes regarding their work, in the most general context, are as follows:

- They examine digital media submitted by other units investigating criminal cases.
- After that, they analyze the data extracted or retrieved during the examination stage.

Finally, they write a report presenting their findings. In the report, the examiners answer the questions asked by the evidence-submitting party.

Work Roles

Another part of the context shaping the information behavior of DEEs is their role, or job position, in their work life. Although the interviewees didn't directly provide their job positions, they provided enough data for the researcher to determine their classification. The first role they may play can be called an "Examiner." As seen in Table 3, all participants listed "examiner" as the main role they play. In one of the laboratories, the examiners were divided into two groups: experts and assistants. Assistants begin the examination after receiving basic mandatory training, and each assistant reports to an expert. The expert reviews his work and approves it. After working for a while and getting sufficient training and experience on the job,

assistants become eligible to take an exam to become an expert. In the other laboratory, there was no comparable formal classification. However, the examiners know who is more experienced, and the more experienced ones are considered as experts, informally, in the second lab.

The role an examiner plays in the work environment is one of the factors affecting what type of information that the examiner searches for in their work life. The examiners said that they look at technical magazines to follow newly developed hardware and software. All examiners play the role of marketing personnel to some extent; they participate in the process of buying new tools and upgrading or updating those tools, by indicating what they need or deciding what to buy. The data from the interviews revealed that all examiners search for information about new hardware and software in certain information sources, such as technical magazines and conferences. They want to buy the newest, most developed product on the market because their main motivation is to perform successful examinations, and they want to follow the trends of the market. Certain types of information sources provide certain types of information; for example, several participants said that they used the Internet and technical journals to follow new developments in technology and digital forensics. An important finding in the study by Leckie et al. (1996) was that the role professionals play in the work environment determines the type of information DEEs need. Eventually, that will affect the decisions of professionals with respect to the information source used to find necessary information. It seems that that is also the case for DEEs. As seen in Table 4, experts are expected to play certain roles, such as instructing other assistants, researching newly developed techniques, and addressing issues raised by assistants.

Table 4

Categories of Described Work Roles

Work role	Comment
Researcher, Expert,	A: It is important to ask an expert in regard to getting the information we seek. If he doesn't know the topic, he will say that he will search for information. In fact, searching, looking for the unknown in books, the Internet, forums, and conferences is considered his responsibility. The expert doesn't carry out a digital evidence examination. He doesn't handle a hard drive and take its image. He only answers assistants' questions. If there is something he doesn't know, he should educate himself.
Assistant	A: Working as an assistant, I first asked the expert I am responsible to (among us, jobs are usually done in a master-apprentice system).
Mentor (instructor)	A: We mostly educate ourselves by asking the expert. There is a master/apprentice system here between the expert and other assistants. However, the expert still has to educate himself because that is his main responsibility.
Marketing Personnel	B: We keep up with the software and hardware existing in the market. We buy up-to-date, commonly-used software. We use up-to-date software. The software we use in our laboratory is the same software used in the U.S. and Europe. D: with regard to digital evidence examination, the most important thing for us is the software and hardware we have. When we I say 'hardware', I refer to computers of which our technological capacity is very rich. The computers or other digital media sent to us to be examined are seized from people who intimately follow the technology. So, we always have to have hardware with high capacity and that is up-to-date. Beyond all this, new versions of software with regard to digital data investigation are frequently being produced in the market. New features are added into new versions that make it a more powerful tool.
Digital Evidence Examiner	See Table 1

Specific Tasks and Information Needs

Byström (2007) listed a number of contemporary information studies in which the concept of task provides a framework. Many widely known models explain information seeking and information retrieval on the basis of the concept of task. As discussed earlier in the literature review, the model of information behavior of professionals also theorizes the information behavior of professionals on the basis of work roles and tasks. In this section, tasks of DEEs and associated elements will be discussed in detail.

Table 5

List of Assigned General Tasks

ID	Type of crime	Type of evidence	Task	Comments
A	NA	Hard drive	To conduct the necessary examination within the scope of the case	The thing wanted from us was … there was only information about the type of the crime on the letter, and we were asked to conduct the necessary examination with regard to the type of crime. That was a challenging job because there was no specific information. At the beginning, we had no idea about what and where to look for it.
B	Organized crime, identity theft	Digital cameras, flash discs, computers, CDs, DVDs,	To examine password protected digital media and log registries on Internet servers	In that case, lots of digital media were delivered to our laboratory. There were different kinds of digital media. Digital cameras, hard drives, flash discs. Digital media belonging to nearly 50 people were delivered. When you consider all computers, digital devices, CDs, DVDs used by those people, you can imagine how difficult that job was.
C	Cybercrime	Hard drives	To investigate an unauthorized access to a commercial database	That was an online shopping website. There was an unauthorized access to the website. There was somebody who stole credit card information of costumers, and was planning to use that information to purchase things. Internet security personnel had noticed that person before committing the crime. However, since it was subject to a criminal trial, the case was sent to us by the court to find out how that person attacked the website and to discover digital evidence supporting the case, if there was any.
D	Homicide	Desktop computer	Investigation of desktop computer and MSN messenger records	About one or two years ago, in a northern province, a girl and her boyfriend lived along with her mother. They planned to kill her mother. When her mother screamed on the scene, neighbors call the police. The girl and her lover threw the computer through the window into the home garden and tried to escape, when they noticed that the police arrived. The police caught them. Police sent the computer to us to see if there were important evidence in on this computer. Although the computer was not damaged, we couldn't find anything significant pertinent to the crime in the hard drives until we properly analyzed the records of MSN conversations. It is actually easy to access and resolve those records if user recorded the conversations on the computer. If the person didn't record with his consent MSN conversations, they are are kept as encrypted in the computer. Microsoft itself sets it that way. So it was very difficult to access that information. That was our first case of that kind.

(table continues)

Table 5 *(continues).*

ID	Type of crime	Type of evidence	Task	Comments
E	Child Pornography	CD	Examination of CDs damaged by the suspect	In one case somebody accused of storing child pornography images on CD created deep crevices on the CD in order to prevent recovery of those images. In normal circumstances, such damaged CDs are not readable by PCs. We, however, could extract the content of the CD by using a device named as "…." which operates based on the grinding method.
F	NA	NA	NA	NA
G	Cybercrime-malware	Hard drive	To find out if the owner of the computer used the seized computer to commit crime	I cannot say that the case was too difficult for me. It was a time consuming a botnet and malware analysis job. Since there was an international dimension of crime, it was a very important case. We were asked to determine whether the computer was directly used to commit crime or it was botnet (slave) computer.
H	Terrorism	Hard drive	Examination of an encrypted hard drive	In a case, a lot of digital evidence were obtained at the end of operations against a terrorist organization which has been good at informatics and sent to our office to be examined.
I	NA	Hard drives and other digital medias		I do not remember a specific incident, but in general the cases we handle can be categorized as follows: • Examination of the physically damaged drives that were used by terrorist organization. • Extracting the contained images from digital devices like DVR's hard disk and the examination of those digital images in computer environments. • Examination of different databases created using encryption software installed on the operating system • Extracting the content of files and the disks encrypted by users applying different encryption algorithms • Other than Windows-based operating systems, examination of other operating systems. • Detection of steganografic files and extracting the content • Removing RAID structured servers separately to bring to our laboratory for examination.
J	Identity theft	Hard drive	Examination of a laptop	In 2007, in an eastern province, we were watching somebody who had a record of stealing other people's credit card information. We had already investigated him several times. That person was usually accessing the Internet via wireless connections in luxury cafes while eating lunch and drinking tea. Based on the information we had about him, we captured him, but there was no laptop in his backpack. Since we couldn't find the laptop, he was free was free to go Then, we closely observed him for 2-3 months. We noticed that he was ordering somethings by using someone else's credit card. We could get the information about the shipment. We got him at the moment the shipping company delivering the product to his address.

The analysis of the interview texts revealed that the most common task DEEs perform is processing digital evidence. However, assigned tasks differ among DEEs with respect to the type of crime investigation in which the evidence was collected, type of evidence, specific examination requests, and stage of the examination (sub-tasks). Table 5 shows a list of the specific tasks assigned to participants, and also shows other characteristics of the tasks, such as type of evidence and type of crime

The researcher found that the variables: type of crime, type of evidence, and sub-tasks of digital evidence examination affect information source selection of DEEs to some extent. DEEs are usually asked to determine if a digital media contains digital evidence related to an alleged crime. To answer this question, DEEs need to know what constitutes this type of crime, and what the elements of that crime are. Interviewee A didn't give information about the type of crime he worked on, but he says that:

> The office submitting the case should write what they expect us to do. For example, when submitting a case, one says that "please, do necessary examinations to determine whether such and such digital media belonging to such and such people contains such and such element of such and such crime." Each "such" takes its place in our list as a keyword. This is an example of an examination request we want to receive. We don't want the opposite. For example, one says "please, send your report after completing the necessary examination on the digital media regarding such and such crime." In a case like that, we only know the type of crime, nothing else. That is a tough situation.

Information about the type of crime is especially helpful in the analysis stage of evidence examination. In that stage, DEEs answer questions asked by the party submitting the evidence. Searching for keywords is one of the methods of analysis interviewees applied. Interviewee A said that he would have one keyword by knowing the type of crime. He, later on, could increase the number of keywords to five by collecting information about the case from different information sources. The Office of the Prosecutor and detectives that participated in

the investigation had the most detailed information about the case. So, DEEs usually used those information sources to construct a keyword list, if insufficient information was provided when the evidence was submitted.

Interviewee E described a case in which he was asked to determine whether the submitted CD contained images of child pornography. He said that it was his first digital evidence examination related to child pornography. In such a case, the first thing an examiner needs to know is, as an element of child pornography, what the criteria are to determine whether someone is a child or adult, just by looking at his/her image. Similarly, in the cases of other interviewees, examiners needed to know what constituted the crime they were working on. So, DEEs perceive that there are different information needs according to the different type of crimes for which they receive digital evidence.

Interviewee B recalled a case that he worked on in which a lot of evidence was collected in an organized crime investigation. The digital devices he received in that case included digital cameras, flash drives, computers, CDs, DVDs, encrypted hard drives, and log registries of Internet servers. These digital devices are very different from each other, and DEEs must use different methods to access and extract the contents of the digital media embedded in those devices. DEEs usually need technical information about the type of digital evidence; this is helpful for DEEs in the examination stage while extracting digital data, and in the reporting stage while justifying the methods they used in the examination and analysis stages. The sources used and factors affecting information source selection of DEEs will be discussed for each stage of digital evidence investigation in the following sections.

Table 6 shows the stages in which interviewed examiners participated during the cases they recalled best. Only Examiner J participated in all four stages of the digital evidence examination process. Examiner G reported that he just participated in the analysis and reporting stages because the digital data was already extracted, and the image of the hard drive was submitted for analysis. The other eight examiners reported that they participated in the last three stages: examination, analysis, and reporting. Although DEEs, mostly, did not participate in the first stage, they gave sufficient information about their information needs in regard to the evidence collection stage.

Table 6

Steps of the Digital Evidence Examination as Sub-Tasks

ID	Collection	Examination	Analyzing	Reporting
A		√	√	√
B		√	√	√
C		√	√	√
D		√	√	√
E		√	√	√
F		√	√	√
G			√	√
H		√	√	√
I		√	√	√
J	√	√	√	√

Evidence Collection as a Sub-Task and Information Needs

Interviewee B said that the legal system in Turkey doesn't allow him to be involved in evidence collection; evidence collection and examination must be conducted by different persons:

> B: There is an important point here. We don't directly take part in the collection of digital evidence. Operational branches collect digital evidence, and send them to our laboratory. We examine and analyze. Then, we send the report we prepared to the

> prosecutors and courts. This is simply the work we do. Digital evidence is gathered by criminal investigator units. The reason for this is the different treatment of the legal system in Turkey. The person collecting evidence at the crime scene, and the person who examines the evidence have to be different people. To ensure the impartiality of the investigation, this is an applied rule. An examiner cannot process digital media if he collects it on his own. Because of this practice, the crime scene investigator unit collects evidence and sends it to digital evidence examiners.
>
> C: Yes, we have participated in the examination, analysis and reporting stages, because we are running the laboratory. The computer had already been seized by the court order before we were involved. We do not participate in that stage. After seized computers are delivered to our laboratory, we enter the circuit of investigation. We complete the remaining other three stages after that.

DEEs need to have adequate information about the owner of the digital media, suspects, the nature of the crime, and the crime scene to conduct a successful examination. They rely on the other units for getting those types of information. They need information because they analyze digital data and make decisions based on that information. Interviewee B said that they get the party submitting the evidence to fill out a form that they have prepared to get the needed information regarding the evidence collection stage. DEEs try to meet their information needs related to the first stage with this form, but not everybody fills out that form completely.

> B: There is a form that we prepared. In the form, we ask for information about how the evidence was obtained, whom it belongs to, what kinds of crime examinations will be done, the keywords to be searched. We ask other investigators for this information while submitting evidence. Filling out this form completely, will decrease the number of questions in mind at the beginning of the examination or will help find answers to the questions in your mind immediately. The more information that is missing in this form, the more questions will arise. Think of a hard drive. There is so much data on a hard drive that we can imagine it like an ocean. In the cases that we have forms with missing information, we are facing a difficult process that it is like searching for a drop in the ocean.

DEEs usually did not experience problems in collecting evidence when necessary because every action they take has a legal basis. That is the reason they need to know the legal

regulations regarding evidence collection and examination. They have to be sure that the evidence was legally obtained.

> B: We had no problem obtaining those records. We requested the records by contacting the relevant department with a court order. Of course, the court must be complete and flawless. We had already known the Servers' IP. With a court order, we didn't have a problem during gathering these records. However, the analysis of the records took a long time. We received some international technical assistance in this long period.

DEEs are rarely involved in evidence collection. Interviewee J mentioned that he obtained a laptop as evidence from a suspect. Interviewee J works in a branch laboratory rather than the central laboratory. His laboratory is in a small city in which the relationships among units are less formal than in major cities. He explained how he was involved in the evidence collection stage:

> We were watching somebody who had a record of stealing other people's credit card information. We had already investigated him several times. That person was usually accessing the Internet via wireless connections in luxury cafes while eating lunch and drinking tea. Based on the information we have about him, we captured him, but there was no laptop in his backpack. Since we couldn't find the evidence, the laptop, he was free to go. Then, we closely observed him for 2-3 months. We noticed that he was ordering things by using someone else's credit card. We could get the information about the shipment. We got him at the moment the shipping company was delivering the product to his address …

Interviewee J said that there is certain information that must be obtained about evidence in the first stage, such as owner of the evidence and characteristics of the evidence.

> First, the seized materials as evidence are labeled at the scene. Before processing and collecting the digital materials, the certificate showing that the materials belong to the owner is signed by the owner. Evidence is numbered with unit numbers, and the number of the investigation in order to distinguish it later on. Following that, if an image is taken at the scene, HASH values of digital material is written on forms. Seized materials are carefully placed in evidence envelopes to avoid damage from external factors. Necessary information is written on the envelope.

It seems that DEEs sometimes had problems in getting adequate information in evidence collection. The units may not know the importance of the information that DEEs request about evidence and its owner. As Interviewee B mentioned above, the less information the units collecting the evidence provide, the more questions DEEs have in mind while following the stages of a digital evidence investigation. In such cases, DEEs call the units submitting the evidence back and try to obtain the information they need. They cannot always get extra information because the party submitting the evidence may not want to share information for several reasons. In some cases, the people involved in the crime may have a high position in society and the units submitting the evidence may not want the case publicized.

> Interviewee A: This is an example of an examination request we want to receive. We don't want the opposite. For example, one says "please, send your report after completing the necessary examination regarding such and such crime on the digital media." In a case like that, we only know the type of crime, nothing else. That is a tough situation. I don't know if it helps you but it is about politics.

Information Needs in the Examination Stage

In this section, the information needs of DEEs during the examination stage is discussed. The examination stage refers to "forensically processing collected data using a combination of automated and manual methods, and assessing and extracting data of particular interest, while preserving the integrity of the data" (Kent et al., 2006, p. ES2). Table 7 shows the information needs of respondents during the examination sub-task of a general digital evidence investigation task. To obtain data about information needs of DEEs, the researcher asked the question: Did you have any questions in mind? What were they? What information did you need in the examination stage? The participants freely talked about what they needed to know

in the examination stage. Their needs are listed in Table 7 in the form of questions that were constructed on the basis of respondents' answers.

Table 7

Information Needs in the Examination Stage

ID	Information needs	Examiner Comment
A	• What other accessories or parts are needed to make a proper investigation on a digital device/media according to the service request? • How can I avoid damaging the original drive? • Under what conditions, must a digital device/media be stored? • How do I have to package and ship a digital device/media? • Which tools do I need to take a laptop or desktop apart? • What procedures do I have to follow while working on a hard drive? • Do I have enough storage space and time to extract digital data?	Regarding hard drives; we prefer to receive them separate from the computer case due to easy storage and reduced cargo costs after the examination. Yet, sometimes we may need the computer case to identify the system date and time. However, in most cases, we only need the hard drive. If we receive the hard drive installed in the computer case, we unplug it. In some laptops it is hard to unplug the hard drive. After we unplug the drive, we take an image of the hard drive. We do this to avoid damaging the original hard drive. Image producing is a practice similar to taking a picture of the hard drive and it is different from copy and paste. In imaging, every bit is exactly saved. The problem in this process is the large capacity of hard drives. Sometimes we received a hard drive with a capacity of 1 / 1.5 terabyte. In such cases, availability of storage to save the image of such a large capacity and the length of the saving procedure are common problems.
B	• How can I disassemble digital devices in order to reach digital media in the device? • Where can I get information about aged, old-technology devices? • How can I extract data from an encrypted digital media? • What are the different ways of obtaining passwords of protected data?	In one of the cases, we had a very old MacBook in our hand. We could not disassemble and remove the hard drive. Even the Mac Service had difficulty doing it and it took them about 6-7 hours to do that. The hard drive had a capacity of 2Gb and was a very old one. This was one the hardest cases we have had …We follow up the emerging technology and keep state-of-the-art equipment. We usually did not have any problem producing images of the digital media and analyzing them. However, encrypted digital media is an exception. In a case of evidence examination of encrypted digital media, we retrieved the passwords through a separate investigation. We used the retrieved passwords to decrypt the hard drive and were able to access the content.
C	• Do I have enough resources to complete this examination? • Do I have adequate knowledge to complete this job? • Do I have enough time to increase my resources in terms of tools, kits and knowledge?	At this stage, as the case was about a website, we felt that we needed more training and information about the programming and design of the on-line shopping web sites and about the security features and mechanisms on such websites. Yet, we were thinking about refusing the case. Our main focus and experience was on hardware and networks. We did not have any experienced examiner on programming in our lab. However, we realized that we had time to search and train ourselves.

(table continues)

Table 7 *(continued)*.

ID	Information needs	Examiner Comment
D	• How do online messenger/chat programs work? • What techniques can I use to recover conversation records? • How do hackers hide traces of their criminal acts?	There were some incidents that were difficult for us. First, we faced major difficulties due to ever-changing technology, ever improving hardware and software, and maintaining ourselves up-to-date. Especially, crimes committed over MSN chats, e-mailed verbal assaults, and hackings (hackers know a great deal about computers and how to hide their traces) are problematic cases we face.
E	• What are the ways of extracting the content of a physically damaged CD? • How can I examine other types of physically damaged digital media?	Examining the content of CDs is normally an easy task. However, as the CD surface was intentionally damaged by making deep scratches we could not access the content.
G	• What is the capacity of the tool I use? • What are functions of hardware and software I use to examine digital media/device?	Of course, as we utilize Forensic Kits for IT inspection and analyses, we have to know those kits and their functions well.
H	• What encryption software is commonly used? • How can I determine which encryption program was used? • What are the tendencies in criminal groups about deciding which encryption to use? • Where can I get information about new types of encryption software?	We usually don't have any problems at the examination stage. We are very experienced about such issues. But, there are surely things we need more information about. We knew that TrueCrypt was the most common encryption software used by those terrorist groups. The software we were using at that time in examination was identifying folders encrypted with TrueCrypt, but not encrypted drives. We looked into every source including foreign information sources.
J	• What are the circumstances in the case? • How can I decide to take an image on the scene or in the lab?	It depends on the examination. Personally, if there is a computer or other material to be examined, I either go to the site myself, or bring it to the lab to save the image of the drive.

DEEs work in digital forensic laboratories. The examination stage starts with receiving the digital device or media. In the examination stage, the content of digital storage is extracted by using some manual or automated tools. In most cases, DEEs don't have any problems with that because they have very good, up-to-date hardware and software in their laboratory. As can be seen in Table 7, there are very different situations in the examination stage, such that DEEs need extra information about the evidence they work on. Examiner A said that he might need other accessories and parts of the digital device in order to perform the assigned task. He also

mentioned that the size of the hard drive might be problematic for them. He said that they sometimes experienced unusual things in very ordinary examinations. For example, in one case, they couldn't take the image of a hard drive on a workstation he always used, but they could on another workstation. Examiner A said that:

> A: Our working environment is a lab. Working conditions are ideal. We utilize professional equipment for imaging. We have a rather routine and automatic system for imaging. We do not need much expertise in imaging. We usually plug the drive in and the equipment automatically produces the image. Of course when we have a technical problem we need information to solve the problem.

Examiner B said that they need more information in the examination stage because they sometimes receive very old digital devices. In such cases, they cannot even physically take the device apart without damaging it. Examiner B said that the other situation in which they need information is while working on password protected files and digital device or media. Examiner H said that he also needed extra information about encryption software. Examiner C said that they may receive some cases in which they examine a type of digital device/media for the first time. He said that they first need to know if they have enough resources to complete the task. By resources, he was referring to experienced personnel, time and hardware/software. Examiner D and E also said that the tasks assigned to them were their first time examining such evidence. Examiner J said that his information needs depend on the situation.

As a result, in the examination stage, DEEs usually need more job-related information than usual, and therefore, spend a lot of time on information seeking in the following situations:

- When they encounter a technical problem with hardware or software they use or digital device/media

- When a type of digital device/media is submitted to their laboratory for investigation for the first time
- When the digital device/media subject to examination is too old
- When the digital device/media subject to examination is newly produced
- When the digital device/media is highly protected with strong passwords or encryption software
- When the owner of the digital device/media subject to investigation is very knowledgeable about computers and networks
- When the digital device/media doesn't have a standardized format

Information Needs in the Analysis Stage

In the analysis stage, DEEs "analyze the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination" (Kent et al., 2006, p. ES2). Table 8 shows the information needs of participants while analyzing examination results. Questions in the table are derived by the researcher according to the participants' answers to the question "Did you have any questions in mind? What were they? What information did you need in the analysis step?"

Interviewee A said that he needed to know how to use analysis tools, and he also emphasized that he needed to know what keywords to search for. Interviewee B pointed out that the information which is normally supposed to be collected in the collection stage is usually essential for a successful analysis.

Table 8

Information Needs of DEEs in the Analysis Stage

ID	Information need	Examiner Comment
A	Which forensic tools are available to make the analysis of large amounts of digital data easier? Do I know how to use those tools? What are the capabilities of those tools? How do I define keywords? What do I need to know to define keywords?	First of all, we need to know the devices and models in detail. We use an analysis program called "encase forensics" for hard disc investigations. We are supposed to know how to use the program very well. We need to know what questions to ask and in what way to ask. The logic of this program and the work of forensic kits are slightly different from traditional research methods. Bit by bit, it is searching for the topic you want. One of the most popular modules is "keyword search module". Therefore, keywords related to case are defined. If you have information about the case, we can define them ourselves on the basis of our experiences. But, sometimes we may receive some cases with only the subject of the crime written down. This case was like this, nothing included other than the name of the crime. No suspect's name, what was expected was not clearly written, almost no information about the case had been submitted, only the name of the crime had been written and, then, we are asked to investigate the hard disc. In such cases, we have extreme difficulties in identifying the keywords.
B	• Related to whom am I going to look for evidence? (?) • What other digital media is related to one suspect? • What type of crime is associated with the digital data subject to analysis? • What are the elements of the crime? • What do I need to look for in the digital media? • According to what criteria am I going to decide that the submitted digital media contains digital evidence constituting the alleged crime?	In this type of incident, firstly, in a clear and precise way, it is essential to find out who owns which evidence. Afterwards, the evidence belonging to one person should be put in one group, and investigated all together as one examination. For example, five types of digital evidence have been identified belonging to one suspect. The results of our examination of that evidence are being presented within the same report. Formerly, we decided the owner of evidence. Of course, the most important thing for digital evidence examiners is the summary of the investigation file prepared by detectives. We initially read the summary to see what the suspect did showing the commitment of the alleged crime. We aim to get information about the suspect by reading the summary. The suspect is a question mark by himself. Everyone has an area of expertise … Some are pretty good at fiscal crimes [they know the elements of the crime in detail]; some are very good in cyber crimes. Therefore, the one who is an expert in fiscal crime can be more successful in examining digital evidence obtained in a financial crime case. I think that computer forensics is a field that requires different specialization in its sub-fields.

(table continues)

Table 8 *(continued)*.

ID	Information need	Examiner Comment
C	• How can I validate whether my analysis gives reliable results?	But, we didn't have anything that could be a reference. We hadn't received any similar examination request like that until that time. Simply, everything can be changed so easily in the digital world. We thought that validation of all our works was needed. Also we asked ourselves what was the best way to examine, how else could we do that, how could we answer possible questions from the court. Obviously, we made cross checks. Sometimes, one of us behaved as the one critiquing our work. We defended our work against his claims to see if there was any missing point in our report. We generated a court atmosphere as it were.
D	• What technique should I use? • What type of files should I look at in order to find evidence related to this type of crime?	In general, during analysis, first, we make a plan according to the demand and the assignment we have received. We ask what to search and find what techniques can be used. In fact, it was just Internet records. That was a homicide case. We needed to shed light on the case. We were supposed to find what was on the computer related to the homicide. We looked for an e-mail or messenger conversation, or voice record. We searched for possible office documents showing plans of homicide. Therefore, in that case, we focused on office documents, Internet [messenger, chat] records, especially the deformed files and files in ZIP or RAR formats. We did a plan about what we ought to look for that will help investigators solve the case.
E	• What is the legal definition of child pornography? • Who is legally a child? • Who is legally an adult? • How can I decide if the images extracted from the CD belong to a child or an adult?	To identify whether the images retrieved from CDs are related to child pornography.
H	• Where can I get keywords to search for?	We asked for a detailed list of keywords from the unit conducting operations. We used this keyword list, and have successfully obtained the evidence.
J	• What type of information should I look for in digital data in identity theft cases? • How do criminals hide digital traces of their offenses? • What is the best technique to apply in analysis according to which type of crime?	In our examination, we found out that the laptop belongs to the suspect. We also detected credit card numbers and shipping addresses in many files with deleted extensions among system files. We found out that the suspect had deleted file extensions, and saved those files by giving extensions as if they were system files. Some files are given .bat extension. But, we have identified files and collected all the digital evidences when we searched for people's names who previously tracked … Evidence examination is conducted according to the type of investigation. We have a list of priority of methods for each case. For example, while keyword search, and script execution are initially done in credit card cases, in the case of fuel-smuggling or the financial crimes, analysis of office documents [Word, Excel, Power point, etc.] are done at first. During examinations, in order to keep the integrity of evidence, we work on images of digital media.

Interviewee B touched upon an interesting point: that DEEs need to know the nature of a crime in order to perform a better analysis. He said that evidence collected in a white-collar crime investigation should be forensically examined and analyzed by an examiner who has knowledge about white-collar crimes. He noted that DEEs should also be categorized on the basis of their knowledge and expertise on a particular type of crime.

Interviewee C said that they had found a way to test if they made the correct decision in their analysis. Interviewee D made an analysis related to a homicide case; he was asked to determine if the computer contained any digital evidence of a homicide plan. Interviewee E needed to know how to determine if someone is a child just by looking at images on a CD. Again, Interviewee J needed to decide which method to use in his analysis.

In the analysis stage, questions asked by clients requesting a digital forensic investigation are answered, and the relationships between elements of the crime are discovered. Therefore, DEEs need detailed information about the elements of a crime: offender(s), crime weapon/tool, the crime scene, target of the crime, and timeline of events in order to perform a successful analysis. The information about the elements of a crime is supposed to be collected before the digital device/media is submitted to the lab. DEEs conduct analyses on the basis of available information about the elements of a crime. DEEs also need to know what the features of available tools are in order to make a better analysis. As can be seen in Table 11, DEEs are expected to make decisions like whether a relationship exists or if a digital media contains illegal documents.

In short, DEEs need information to help them make better analyses and decisions. They usually apply standardized routine methods and techniques in digital forensic investigations.

However, they may spend extra time in looking for information to meet their information needs in the analysis stage, when the following situations occur:

- When information about the elements of a crime is not provided or not sufficient.
- When the amount of data subject to analysis is extremely large.
- When a digital media/device is obtained in complex crimes such as organized crimes and cybercrime.

Information Needs in the Reporting Stage

In the reporting stage, DEEs write a report as an outcome of their digital forensic investigation. In the report, they describe which method they applied, which tools they used, what procedures they followed and list what they found out. They also may make recommendations to serve better. Table 9 shows information needs of participant while writing reports. The questions addressing their needs are listed as questions by the researcher on the basis of respondents' answers that were included in the table.

Table 9

Information Needs in the Reporting Stage

ID	Information need	Examiner Comment
A	• Which information about the case must be included in the report? • What skills should I improve to write better reports?	Writing a report requires specific procedures to follow up. In some laboratories there are special experts responsible for report writing. The one who examines the evidence and who writes the report could be different experts. After the examination, the analysis expert introduces findings, and the reporting expert writes the statement. This is because writing the report requires different skills other than research; the researcher could have poor writing skills, or he/she might have difficulties putting all findings into the writing in a proper way. This may result in a poorly written report, which has several disadvantages. In our laboratory the expert who makes the examination is responsible for writing the report. This results in a certain level of ability in both technical issues and written expression after a definite period of assistantship in our laboratory.

(table continues)

Table 9 *(continued)*.

ID	Information need	Examiner Comment
B	• How can I truly reflect the forensic process I followed in my report?	The final report usually has a nearly standard structure. However, a well-prepared report requires true reflections of examination and analysis stages, because a report, in fact, is the document based on the findings of examination and analysis stages. Therefore, I need to know every aspect of the case I am working on in these very early stages. If I manage to get sufficient information about the case in the examination and analysis stages, that is very good, otherwise my report may not be able to achieve its expected goals.
C	• What is the level of technical knowledge of the person/department requesting the report? • How can I simplify complex technical issues in my report?	The biggest problem we face in this situation is to be able to write a simple report for judicial authorities who are not IT experts. It resembles the doctor-patient relationship in which the doctor gives a medical terminology report to his patient who is not familiar with it. So, reports must include both technical issues and must be explicit at the same time. At this point we have difficulties in choosing and deciding the most appropriate language to avoid misunderstandings. Because we presented our report to a judicial authority - the people specialized in law terms rather than information technology terms - so, we certainly did not prefer having reactions like 'What do you mean by firewall, router, modem or webpage … etc?' Nevertheless, we thought the report would lack in prerequisites of a good report without technical terms. We worked hard to make the report explicit enough with IT terms to be comprehended well.
D	• How can I write a solid report?	The analysis part is the phase where examination ends and elements constituting the crime are discovered, or not discovered. After finding the evidence, your previous experience, knowledge, and logic are involved in the work to construct a better, significant and solid report. We do not have difficulties in the analysis stage in this sense.
E	• What information sources can I use to learn how to write forensic reports?	When I first started examining digital evidence, there were things I didn't know about how to write report. However, over time, I gained experience. At first, I looked at previously written reports.
H	• How simple should a report be?	In the report writing phase, usually international standards are used. On the other hand, we prefer a simplistic language in our reports to help judges, and public prosecutors understand them easily. We never had any problems, or did not receive any negative feedback in this sense.
J	• What information must a forensic report contain?	Our reports consists of three parts; introduction, evaluation, and conclusion. **a)** Introduction; In the introduction, type of the event, its inspection number, name of the related court, decision date and number, name of the file holder, and technical specifications are written **b)** Evaluation; In the evaluation part, explanations and specifications of the material which is subject to inspection are written such as its condition, operating system, size, partitions, specifications of files inside, information on general content, characteristics of crime related elements. **c)** Conclusion; In the final part, an expert opinion is introduced. (i.e. "No crime element found upon examination of the disc" or "… files are considered as the evidence for the crime that is under investigation"

Overall, the participants said that they usually need information about the language, style and format of forensic reports in the stage of reporting, since what DEEs do is very complex. They know that the people to whom they are sending reports are not as knowledgeable as them about the technical aspects of the case. Therefore, they need to explain how they processed the digital evidence in terms that are simple enough to understand but detailed enough to avoid critiques about the reliability of the forensic examination. The important point is that they need to estimate the level of technical knowledge of the person/department requesting the report and to write reports accordingly.

Research Question 2: Information Source Use

In this section, the results of the analysis of data about information source use of DEEs, in general, are presented. The qualitative data is analyzed in two different contextual frameworks. In the first part of the interviews, interviewees were asked about their information source selection and use in a specific context such as in a sub-task of a digital evidence examination. The interviewee provided information about their information use when they perceived an information need. In the second part of the interviews, participants were asked if they use a certain type of information source while performing their professional tasks, in general. In the second part, the researcher didn't describe a situation in which the interviewee would use a type of information. In order to make the questions in the second part less contradictory, the researchers asked about the role of an information source in an interviewees' work.

In the following sections, first, findings related to information source selection and use

by the interviewees in specific tasks is presented and discussed. Then, findings related to use of information sources, such as books, journals, forensic kits and software, conferences, library and information center, and online sources (Internet, social networks, databases) are presented and discussed. The use of the Internet, social networks and databases is discussed under one category, online information sources, because the participant didn't have a clear distinctive definition for each source. It is actually very complex to differentiate online sources from each other. For example, imagine that an examiner in a foreign country posts an explanation to a technical problem regarding the examination of a cell phone on a forum page of a forensic website. He shares this information because he thinks that somebody may encounter the same problem. With the sharing of experiences and solutions, a database of forensic knowledge is constructed over time. Then, another examiner searches for information about the problem on Google and reaches the forum page via Google. Now, how are we going to categorize the information source that the information-seeking examiner used? Should we say the examiner found the information by using colleagues outside his lab, the Internet, social networks, a website or a database? Therefore, the researcher will discuss his findings under the heading of online information sources, if the information was obtained via an online system, regardless of who provided the information and the structure of the virtual environment where the information is located.

Information Source Use in Specific Tasks

It seems that the characteristics of specific tasks are important factors influencing information behavior of DEEs.

Table 10

Sources Used by DEEs in the Examination Stage

ID	Sources used	Comments
A	• Expert in the laboratory • Books • Technical manuals • Forums • Colleagues outside the laboratory	In this case, we asked an expert in the lab. We tried to get the image in his computer. So, we succeeded. This experiment proved that we could get an image by trying different computers. Of course, we checked several forums on the net prior to implementing this. We used the books to find out what the problem was and why we were not able to get the image. Some of these sources recommended we try at different work stations in order to get results. If I summarize the process, firstly, I would apply an expert opinion. If I am not satisfied, I would search the books and technical manuals. The Web would be my last option. I would check forums and submit my questions on this platform to other colleagues. At the end, I could obtain the answers that I requested.
B	• Books • In-service training • Colleagues and experts outside lab • Internet • Software • Hardware • Suspect(s) • Acquaintances of suspect(s) • Technical services • Manufacturer	The sources that we utilize may be varied depending on the case type. For instance, if it is a new subject for us, we go to the books first. However, there is something else … In-service forensic trainings are extremely important. There are at least 4 or 5 in-service trainings in different forensic areas every year in Turkey. Some of the courses are not only held at the national level but also at the international level. In these gatherings, forensic experts share their experiences and influence each other in positive ways. We can be aware of new developments and ask questions for solutions to other people who have previously experienced the problem. Of course, published sources are important for us. If we are not able to find a satisfactory solution, we do a broad Internet search. Especially in public sharing web sites such as YouTube, we can find valuable documents even though they are not directly related to forensic sciences … There is some software to help crack passwords. We could crack passwords by using this software. Of course, we had the required training from the company, which is providing the software … It is because of technical incompetence sometimes. It is not possible to be perfect in all areas. There may be some problematic cases in which you feel yourself inadequate. You can find such examples everywhere in the world, also in Turkey. You may not access the hard drive that is protected with extremely complicated programs. We have experienced such kinds of cases, indeed. After interrogations we learned that the password was known by a friend of the hard drive's owner. So we retrieved information from a human source, a friend of the suspect, not from a technical document in this specific case. Our information sources are not limited to published documents, technical manuals, software, or web-related methods but includ suspects and those interacting with suspects … We could not disassemble and remove the hard drive. Even the Mac Service had difficulty doing it and it took them about 6-7 hours to do that.
C	• Forums (other experts in foreign countries) • Forensic websites-Internet • Detectives • More experienced experts	We interact with experts from various countries through the Internet forums very often. We get help from some websites providing a room for discussions of forensic problems, so we can ask questions. On the other hand, we kept in contact with the detectives. Other than that, we skimmed Internet sources to find out how these attacks were committed. We combined all findings and started the examination…. We assumed that some other experts might have tried to solve this type of case before us since the Internet reaches everywhere. We decided to ask those with prior experience. We wanted to learn, at least, what steps they followed during the process. To use the experienced people was our first choice. Secondly, we believed the only solution was the information. We thought about the location of information sources. This would be other experts in the field or we had to invent the wheel again. Therefore, we used the Internet sources for additional information.
D	• Internet	One of the important sources of information for us is the Internet. I got to obtain up-to-date information on technology-related issues. The Internet is an environment where you can access information easier and quicker. You can find what you're looking for, just about everything. In that case, we especially worked on how we should collect information about MSN messenger and chat programs, which methods we needed to use, which procedures we needed to follow because this was the first case of its kind, an examination of chat records. We hadn't received such a case before that. So the Internet and other sources we used were important information sources for us.

(table continues)

Table 10 *(continued)*.

ID	Sources used	Comments
E	• The expert in the lab • Internet • Forums • Books • Journal articles	Working as an assistant, I first asked the expert I am responsible to (among us, jobs are usually done in a master-apprentice system). That is the way an assistant educates himself; by learning from the expert. If the expert knows the topic, the assistant gets the information from the expert. If the expert doesn't know the topic, in that case, the expert's research kicks in. The expert, in such cases, browses the Internet, and reads forums. After getting a general knowledge on the topic from those sources, he looks up reference books and articles … The expert told me to grind the CD up to ten times. I did as he instructed. However, I was unable to access the content of the CD. Since grinding the CD more than a certain number of times would harm the CD, my expert searched for this issue on forums and we leant that we can actually grind a CD up to 18 times. He supported his finding with a scientific article. At that time, we could reveal the content of the CD.
F	• Hardware • Software	We use standard hardware and software in the examination stage.
G	• Books • Technical manuals • Websites • Forums	When I need such information, I use any source (book, manual, etc.) accompanying those kits. If no document were given with those kits, then, I use websites and other forums providing information on this field. This completely depends on the circumstances and available sources.
H	• Multiple sources	We looked into every source including foreign information sources.
I	• Previous training • Personal experience • Engineers in related fields • Technical services • Manufacturing companies	We remove and install hard drives of computers based on special training we received and our experience. With regard to catching up with new developments in technology, we increased our knowledge and experience with the help of instructors teaching in the engineering department of universities. Sometimes we got help from technical services of manufacturing companies. We can easily take images of hard drives by using licensed hardware and software.
J	• Personal notes • Internet • Colleagues working in the field	In some cases of examination, we absolutely experience such situations in which we receive some digital evidence we are not used to working with. A new device, a new application, a different type of file such as the Linux computer operating system, notebooks with unusual types of hard drives, files which are not recognized by Windows. When we experience such a situation, we firstly look for a solution in our personal notes. Besides, we frequently use the Internet as an information source. If the Internet doesn't offer a solution, then we contact our friends, and get help from them by sharing information.

Sources Used by DEEs in the Examination Stage

In this section, results of the analysis of qualitative data with respect to the information sources used by the participants in the examination stage are discussed. To obtain data about information sources, the researched asked the question "How did you find the answer to these questions? Did you get any help?" The answers are listed in Table 10. Some participants talked about information sources they used in a specific examination. Some preferred to talk about information sources in general. The researcher categorized information sources used by each examiner in the examination stage.

Since DEEs, mostly, need technical information in the examination stage, they usually use information sources that can provide technical information about: 1) the digital device/media they are working on, 2) forensic tools they are using or 3) the appropriate methods and procedures to be applied during an examination. Table 11 shows the total number of times an information source was mentioned by the participants.

As Table 11 shows, the Internet is the most common information source the participants mentioned for the examination stage. The other information sources frequently used by examiners in the examination stage were: forums, experts, colleagues, forensic tools/kits and books. It seems that DEEs use online information sources such as the Internet, forensic websites and forums to obtain general information about issues that are new to them. After doing their initial search on the web, they use additional information sources such as experts, colleagues and books that provide more specific and reliable information. Other sources the participant used are technical manuals, technical services, and companies producing forensic tools and kits. An interesting finding is that DEEs obtain technical information from suspects

and acquaintances of suspect(s) in some cases. It is an obvious fact that the selection of information sources depends on the situation.

Table 11

Frequency of Information Sources Mentioned by Participants for the Examination Stage

	A	B	C	D	E	F	G	H	I	J	Score
Books	•	•			•		•				4
Journal Articles					•						1
Personal Experience									•		1
Personal Knowledge									•		1
Personal Notes										•	1
Technical Manuals	•						•				2
Experts	•	•	•		•						4
Colleagues	•	•								•	3
Engineers in Related Fields									•		1
Forums	•		•		•		•				4
Internet		•	•	•	•		•			•	6
In-service Training		•									1
Forensic Tools & Kits		•				•			•		3
Suspects		•									1
Detectives			•								1
Acquaintances of Suspect(s)		•									1
Technical Services		•							•		2
Manufacturer		•							•		2
									Total		39

Interviewee B said that they sometimes couldn't technically hack passwords; however, they could obtain the password for the protected drives from an acquaintance of the suspect by interrogating him. This example shows that they used different techniques to get the information they needed. In addition, they sometimes used policing techniques such as interrogation and surveillance. Another interesting finding is that, as an interviewee mentioned, DEEs sometimes contact scholars teaching in engineering departments of universities. The

participant also mentioned that they use their personal knowledge and experience they have gained over time from basic training and from previous examinations they performed.

Information Sources Used in the Analysis Stage

The analysis of data with respect to the information sources used in this stage showed that DEEs mostly rely on other people who were involved in the case before them while analyzing digital data. These people include those who investigated the crime, interrogated suspects, prepared investigation files, collected evidence from the scene, and submitted the evidence for examination. In order to answer the questions that initiated the collection and examination, DEEs need to obtain detailed information about the elements of the crime. After having sufficient information about the elements of the crime, DEEs need to decide which method of analysis to use. DEEs meet their information needs by using their personal experience, previous professional training, reading investigation files, and contacting detectives, prosecutors, clients, and other experts (see Table 12).

Table 13 shows how often an information source was mentioned by the participants during interviews with respect to stage of analysis. It is clear that the most frequently mentioned information source is the investigation file (case file) that contains information about the elements of the crime. This finding supports the model of information behavior of professionals (citation) that tasks are the context in which information needs of professionals arise, the nature of tasks is a factor shaping information source selection of professionals. The information sources used by DEEs in the stage of analysis are: personal experience, experts,

detectives, the Internet, clients, professional training, the prosecutor, evidence submission forms, in-lab manuals, forums and colleagues, respectively.

Table 12

Information Sources Used in the Analysis Stage

ID	Sources used	Comments
A	• Personal experience • The expert • Internet • Detectives initially working on the case • Clients who submit the evidence • Case file • Prosecutor	First of all, there are keywords that the assistant composes by himself. Then, he asks the expert. The expert adds up the things he knows. The expert searches the Internet when needed. If the expert agrees, we contact the units participating in the investigation. We call the department or branch handling the case, ask them which keywords to look for. The expert may do his own research on the Internet. Eventually, you construct a list of keywords with the help of the expert. You look for the keywords in the images of hard drives. ... There are things we are supposed to do, we can search and find it. On the other hand, there are things that the office submitting the evidence is supposed to do. That was such a case. Since the office submitting the case has information about the case, it was a case that they would much rather answer the questions in our mind. We tried our best although we were unable to see the content of the case file. By using the information sources I mentioned I could increase the number of keywords from one to five. But, we didn't have a chance to see how good we did on this case by searching only five keywords, because as I said we didn't know what was in the case file in detail. The ideal is that the office submitting the case to us - in this case it was the office of prosecutor - mentions the name of the suspects, what they specifically want, what type of file they want us to look at. If they had done this in that case, we would have constructed a better list of keywords. As I said, other information sources are also helpful for us.
B	• Case files • Standard submission form	We first of all read all the files written by detectives working on the case. There is a form prepared by us called criminal informatics personnel. In the form of digital evidence submission, we ask for information about how evidence was obtained, whom it belongs to, what kinds of crimes investigations will be done, the keywords to be searched. We ask for this information from other investigators submitting evidences. Filling out this form completely, will decrease the number of questions in mind at the beginning of the examination or will help find answers to the questions in your mind immediately. The more information that is missing in this form, the more questions will arise. Think of a hard drive. There is so much data on a hard drive that we can imagine it like an ocean. In the cases where we have forms with missing information; we are following a difficult process that it is like searching for a drop in the ocean.
C	• Experts	We assumed that some other experts might have tried to solve this type of case before us since the Internet reaches everywhere. We decided to ask those with prior experience. We wanted to learn, at least, what steps they followed during the process. To use the experienced people was our first choice. Secondly, we believed the only solution was in the information. We thought about the location of information sources. This would be the other experts in the field or we would have to invent the wheel again.

(table continues)

Table 12 *(continued).*

ID	Sources used	Comments
D	• Personal experience • Personal knowledge • Training	The important thing in that case was to extract the data. After that, all we need to do is to read the data. We found records of conversations lasting months. We had to review all those data. If I recall correctly I read the texts for three days. I don't recall when the crime was committed, but I think it was in April. The records of conversations between the girl and her boyfriend went back to the last month of the previous year. So, we had to review all texts of conversations. After we read for a while, we began searching for certain words in the texts. For example, "killing", "homicide." We continued reading the text by searching for keywords…. It was a homicide case, so we used possible keywords such as "knife," "gun," "bump off" and other keywords used in slang references to killing and gun. We determined what keywords to use based on our experience and prior training.
E	• Expert	I worked with an expert to determine whether the seized CD contained child pornography or not. In that case, the expert explained the criteria to determine whether people in videos are children.
F	• Case file • Statements of suspects and plaintiff	In the stage of analysis, we identify important points by reviewing statements of suspects and plaintiffs
G	• Personal experience • Internet • Forums • Colleagues	Since the image of a drive had been submitted to us, I started analyzing the image based on my personal experience by skipping the first stage of the digital evidence examination. It is always possible to face a unique case when handling malware and botnet cases. I happened to me, too. In that case, it was the first time for me. To solve the problems I had, and to be successful, I used the Internet which is a big source of information and forums. In addition, I asked for help from my friends working in the field of digital evidence examination.
H	• Detectives	We wanted a detailed list of keywords from the detectives who handled the case and conducted operations. We used those lists, and we were successful in getting the evidence.
I	• Detectives	We usually organize a workshop with the detectives investigating the crime. In this way, we get the information we need to analyze the digital data.
J	• In-lab manuals • Case files	But, we have identified files and collected all the digital evidences when we searched for people's names who previously tracked … Evidence examination is conducted according to the type of investigation. We have a priority list of methods for each case. For example, while keyword search, and script execution are initially done in credit card cases, in the case of fuel-smuggling or financial crimes, analysis of office documents [Word, Excel, Power point, etc.] are done at first. During examinations, in order to keep the integrity of evidence, we work on images of digital media.

Table 13

Frequency of Information Sources Mentioned by Participants for the Analysis Stage

	A	B	C	D	E	F	G	H	I	J	Score
Personal experience	•			•			•				3
Personal knowledge				•							1
In-service training				•							1
Experts	•		•		•						3
Internet	•						•				2
Detectives	•							•	•		3
Clients	•										1
Investigation file (case file, Statements of suspects and plaintiff)	•	•				•				•	4
Prosecutor	•										1
Standardized submission form		•									1
In-lab manuals										•	1
Forums							•				1
Colleagues							•				1
					Total						23

Information Sources Used In the Reporting Stage

Consistent with the findings regarding information use in other stages, the participant said that DEEs use information sources in the reporting stage according to their information needs in that stage. The researcher found that DEEs usually need information about format, style and language of reports.

Interviewee A said that he shows his reports to the expert he is responsible to. He believed that the experience and professional knowledge of the expert was much greater than his own, and he made the necessary changes to his report according to the feedback he gets from the expert. He also mentioned that he asks his friends to check his reports, and said that they use a checklist to verify they have included all the essential information in the report. The checklist was constructed over time. Similarly, Interviewees D, E, G and I also said that they used a template prepared by the lab. From other information sources, DEEs obtain information

about the format, style and language of reports; these include legal documents, previously written reports, editing software, and colleagues.

Table 14

Information Sources Used in the Reporting Stage

ID	Sources used	Examiner Comment
A	• Expert • Colleagues inside the field • In-lab manuals and templates	We show each report we write to the expert. He had examined more digital evidence and written more reports than anybody else in the laboratory. The expert is more experienced than us. He may make corrections on the report. He can give feedback about how understandable the report is. He first checks the elements that have to be in a report. Are all materials listed in the report? Are questions answered adequately? Are all the information that must be in a report such as time, place, place and other information written on the report? Those are the things the assistant must write down, and that the expert should check. If we have questions that the experts cannot answer, then we ask our friends working in this field. The information about how to write such reports doesn't exist on the Internet. This is usually a unique situation. We have a checklist of what must be included in a report, but there sometimes is a really unique situation. We created that checklist by using our experience, prior training, and results of our research on the field. In an expertise exam, our reports are evaluated to make sure that we put everything on the checklist in our reports. In that case, we were writing the report to people without a high level of technical knowledge. For that reason, we endeavored to write the report sufficiently simple for them. We rarely receive feedback like "we didn't understand this part, do you mean that?" In that case, we received no feedback. From that, we anticipated that the report worked for them.
C	• Colleagues outside digital forensics	I don't how much the court understood our report. To prevent misunderstanding, and to help service requesting parties understand our reports completely we get somebody working in a normal laboratory [e.g. biology, ballistics] to read the report. We want to see if somebody out of digital forensic field understands the report. We submit our report after they confirm that the report is easy to understand.
D	• In-lab manuals and templates	Reporting is one of the easiest of the four phases. Examination and analyzing is done, now. We find a number of things that can be accepted as evidence. The remaining thing is to explain where we found the evidence, how we discovered the findings, what software and equipment we used, to other parties waiting for our reports without using too much technical jargon. We need to use fewer technical phrases in our reports because we usually submit our reports to prosecutors and judges who are usually poor with technical terms. We have to give them clear information. We in fact have a template of a report. In that template, there are spaces to fill in the necessary information about the case. An examiner starting this job may not know how to put words together. But, after doing this work at least two to three years, the examiner learns the literature of the writing report. After a certain time, the words come by themselves, spontaneously.

(table continues)

Table 14 *(continued)*.

ID	Sources used	Examiner Comment
E	• Previously written reports • In-lab manuals and templates • Experts	When I first started examining digital evidence, there were things I didn't know about how to write a report. However, over time, I gained experience. At first, I looked at previously written reports. Our laboratory already has a certain format. We write accordingly. In this case, I remember that I asked the expert once about how to express the results of our analysis, how it can be more understandable, if I gave a full response to all points. He provided information that helped me. We did not get any negative feedback from the office we sent the report to.
F	• Editing software	Using the necessary software, I report the evidence I found as a result of my analysis and the data that may be important for the parties requesting the examination
G	• In-lab manuals and templates	I had no problems in the reporting stage. I explained my findings using the current reporting format, with clear and simple language in the report and its appendixes.
I	• In-lab manuals and templates • Legal documents	"Reporting" is the most important stage of digital evidence investigation. You may be good at examination of digital evidence. But, when you're not writing a good report, evidence you put in the investigation file loses its power. From this perspective, we see the reporting as the most important part. In the report template, the authority claiming the examination, court orders and warrants, content of the crime, suspects' identity, the identity of experts must be included. Studying relevant laws and legal grounds, we have created our own report template. We write our reports according to this template.

As can be seen from Table 15, DEEs mostly use in-lab manuals and previously prepared report templates as information sources.

Table 15

Frequency of Information Sources Mentioned by Participants for the Reporting Stage

	A	B	C	D	E	F	G	H	I	J	Score
Colleagues inside the field	•										1
Experts	•				•						2
In-lab manuals and templates	•			•	•		•		•		5
Colleagues outside digital forensics			•								1
Previously written reports					•						1
Editing software						•					1
Legal documents									•		1
									Total		12

Outcomes of Information Seeking for DEEs

All interviewees said that they could, finally, find the information they were looking for, and successfully complete their assigned tasks. As some examiners mentioned, some tasks took

a long time to accomplish due to the large amount of collected evidence or the complexity of the case. The participants gave answers similar to Interviewee C about the outcomes of their information seeking:

> C: We accessed the information we needed after our research. We benefited from the comments of experts. We could answer all questions asked by the court submitting the case.

The participants, in general, indicated that they normally don't have many problems in performing their professional duties. The personal knowledge gained in professional training, and personal experience gained by processing several cases is usually sufficient to meet their information needs in many cases. However, technology is changing so quickly and the types of crimes in which digital devices are used are so numerous that DEEs are assigned to handle some cases, in which they have no prior experience or specific knowledge related to those cases. The first thing they do in such a situation is to make an assessment of whether the available resources are sufficient to process the case or if he/she can obtain sufficient resources within the timeline. The reason that all participants were successful in getting the needed information may be their accurate assessments of available resources.

Interviewee C provided data supporting this point:

> We first wanted to check whether we could get the information we needed to solve that case. I asked myself whether I have somebody around who knows the topic. Is it better for us to deny the case in advance? Then, we knew that we had time to do research on the topic and get technical information. We took our time. We got the information and expertise in this topic.

Over time, DEEs gain experience about what information they can obtain by using which information sources. This is called "awareness of information sources" (citation Ellis). After making the assessment that they have enough sources to get the information they will need,

they began working on the case. Otherwise they refused the case, saying that the resources of their laboratory are not sufficient to process the case. Interviewee D's statement was also another example of how much attention they paid to the awareness of information sources:

> In that case, we especially worked on how we should collect information about MSN messenger and chat programs, which methods we need to use, which procedures we need to follow because this was the first case of its kind, an examination of chat records. We hadn't received such a case before that.

DEEs produce a report at the end of the digital forensic process: this is the outcome of their work. The participants were confident in answering that they could get the information they needed to accomplish the investigation. However, they were not always sure whether the report they submitted was successful, from the perspective of clients and the service requesting party. They had an idea when the party receiving the report gave them feedback. Most DEEs think that reports are successful unless they receive negative feedback. Interviewee A said that he relied on the information provided by the party requesting the report. In his case, the information provided by the client was not sufficient. He explained that this was a weak point in the case, in his report, and encouraged the client to give feedback about the report:

> A: Yes, I could find answers to the question in mind. However, I don't know if the things we found, and submitted, were exactly what they wanted, if it could have been better. We don't know that, because it was not possible to access the content of the investigation file. In that case, we didn't receive feedback after we submitted our report. However, we emphasized in our report that we would be more productive if they give us more specific information about what they expect from the examination. So far: no feedback. Therefore, we thought the report was ok for them.

Information Source Use in General Context

Books

Table 16 shows whether the participants used books in their work, what type of books

they used and to what purpose they used books.

Table 16

Comments of Participants on the Use of Books

ID	Type of book & purpose	Comment
A	• Workbooks of forensic tools and kits • Technical books • Books on computer crimes and investigation	We use basic books related to computer crimes and their investigations and including technical subjects. We use manuals. Of course, we use an Encase workbook. We use other books that have been written on Encase.
B	• Books on file systems • Digital forensic books • Course books	Not many books on this subject are in Turkey. Most of our books are in foreign languages. And, those books belong to different branches of computer forensics. For example, we have books explaining file systems. We have forensic books on Windows. There are documents obtained from the course, course documents. They constitute a majority of library books.
C	• Electronic books • Booklets • Skimming over	In the classical sense, do not actually use books anymore. Rather we are using electronic books. Even more than booklets, articles, smaller in length. Not like reading the book from beginning to the end, we usually intend to get specific information from the book we already read in the past. So, we are usually looking at certain pages of a book, not all the book.
D	• Reference books in digital forensics • Theory of digital forensics • Books on cybercrime • Digital forensics books in English	Until about four to five years ago, books had been a particularly important source of information for us. After 2002, digital data examination was initiated in the laboratories of our organization. When we first started to work, the important thing was to learn the basics. Namely, how the work was supposed to be done, how the work is done around the world. Therefore, we particularly used books explaining theoretical aspects of this job, books telling the experience of experts who has worked especially in the U.S. for many years and other books written about cybercrimes. But, especially after 2006, 2007, to access those books is more expensive, more difficult compared to the Internet, and it is hard to find in Turkey, we rarely use books. We can obtain foreign books by paying extra money to international shipping companies and customs. It is a long procedure. Therefore, the Internet is the most common information source we are currently using. We hardly use books.
E	• Technical books • Problem solving	Yes, we are using books. We are using the books, especially about technical issues. Particular books explaining the problems we encounter in our examinations have been very helpful for us.
F	• Books of forensic tools and kits	We use books. Books, particularly written on kit and software we use have been very helpful to us
G	• Course books	I use the books, given in training courses that I attended, from time to time
H	• Technical books • Books of forensic tools and kits	Yes, we are using books. We are using the books, especially about technical issues. Books, particularly written on kit and software we use, have been very helpful to us.
I	• Books of forensic tools and kits	Yes, I am using books in my work. I use books written about forensics, software, databases, and hardware.
J	• Technical books • Problem solving • Books on operating systems	I am using books about software and technological issues. I mostly use instructive books. I use books of particular authors written on Linux, Mac.

Only one examiner (Interviewee C) said that they don't use printed books. He said that they mostly use small-size books explaining a specific topic; that is why he used the term "booklet" instead of "book." He also said that he only searches for specific information by skimming a book, and that he doesn't read the book from the beginning to the end. Interviewee D said that they used books to learn theoretical aspects and basics of digital forensics, when they first began working on digital evidence. It seems that DEEs usually use technical books, given to them in technical courses, to solve the problems they have during the digital forensic process. One purpose of using books is to obtain information about digital tools and kits. Some of the topics of books they used include cybercrime, operating systems, Encase software, file systems, computer crimes, and the investigation of computer crimes. Interviewee B said that important books related to digital forensics are usually in English and that those books are kept in the library, and examiners who know English benefit from them.

Journals

Table 17 shows whether the participants used journals in their work, what type of journals they used and to what purpose they used journals. One examiner said that he cannot follow journals, and four of them said that they rarely use journals. Five examiners said that they use journals. It seems that DEEs use two types of journals; one type of journal may be called "academic journals of digital forensics" which are directly related to the digital forensic process. Articles in these types of scholarly journals explain new examination methods and techniques. DEEs use those digital forensic journals to increase their professional knowledge and to find solutions to problems.

Table 17

Comments of Participants on the Use of Journals

ID	Usage	Type of book & purpose	Comment
A	Rarely	• New methods and techniques	We look online or in printed magazines occasionally. This is among an expert's tasks. Newly developed examination methods and techniques usually are presented in journals.
B	Yes	• Technical issues • New products • New developments in digital forensics	We have subscribed to eight monthly journals. These journals only contain detailed technical information. Also, some of them introduce new products on the market, there are some journals particularly on forensics, presenting new developments. Every month, we add them to our library. We also benefit substantially from these journals and magazines.
C	Rarely	• New products • Online journals on digital forensics	If you are referring to computer hardware magazines by saying technical journals, I don't use them much. I use them when doing research about a new product in the market or buying supporting hardware. Those magazines are designed for general users. We prefer journals directly related to digital evidence examination. I use online journals pertinent to my field of work. Apart from that, I would rather follow forums. Forums are more actively used.
D	Yes	• New developments in technology • New trends in digital forensics • Capacity of tools	I'm using technical journals only to keep track of the latest developments in technology. However, our aim is to obtain information about how better to examine digital evidence, what are the recent trends in evidence examination, what are the recent advances in hardware and software, which way the current trend is going, if the capacity of technological tools we are using will be sufficient in the near future. We benefit from technical journals on these subjects.
E	Rarely	• Problem solving • New methods of investigation • In English	Technical journals, I don't follow very well. I'll look at journals if there is an issue I get stuck on, and experts do not know about it. We follow technical journals very well; especially on new methods of investigation. These journals are usually in foreign languages. I know English.
F	Yes	• New technologies and equipment	I follow the technical journals. I have experienced that technical journals are useful especially on emerging technologies and equipment.
G	Yes	• New software and equipment	Especially, to track new products, to have an idea about equipment and software and also to read the written results of analysis.
H	No		I cannot follow technical journals very well.
I	Rarely		I rarely use technical journals.
J	Yes	• New information technology	I follow technical journals such as PCNet, CHIP because these magazines publish up-to-date news about newly developed technology and information technologies.

The disadvantage of those journals is that they are in English, and only examiners who know English can benefit from the journals. The second type of journal may be called "marketing journals" that introduce newly developed hardware or software that is directly or indirectly related to digital forensics. DEEs use those journals to find about new products and new trends in technology, and they benefit from these journals in keeping their tools and kits up-to-date, increasing their capacity. They also get information about new commonly-used information technologies because they will receive those new products as evidence in the near future; for example, iPhones. They need to keep up with the new technological developments in society so that they can plan their training and education in the laboratory accordingly. I conclude that DEEs use journals to obtain up-to-date information about new developments, specifically in digital forensics and, in general, in IT.

Conferences

Only 5 examiners said that they attend conferences without mentioning some kind of limitation. Four examiners said that they attend conferences under certain conditions. The participants, in fact, said that they rarely attend conferences for several reasons. Interviewee C said that he can attend conferences when he has the time and if the laboratory has enough funds; he said that although the institution supports examiners in attending conferences, he can't attend most of them due to the aforementioned constraints. Similarly, Interviewees D and I also mentioned financial and time constraints. In addition, Interviewee D complained about the lack of conferences directly related to digital forensics inside the country; he said that domestic conferences mostly focus on legal aspects of digital forensics, and that he still

attended those conferences to educate lawyers about the technical aspects of digital forensics. Interviewee E pointed out that obtaining the approval of the Head of the Laboratory is another constraint. Interviewee H openly admitted that he doesn't have time to attend conferences.

Table 18

Comments of Participants on Use of Conferences as Information Sources

ID	Usage	Type & Purpose	Comment
A	Yes	• Most current and detailed information • International	I attend conferences. Conferences provide the most current and detailed information. We can witness forensic practices at the conference which is not possible in journals. This way is much more helpful. We are participating in international conferences.
B	Yes	• Both national and international • New developments and practices • Making new contacts	A number of serious conferences and workshops are organized in this field either inside or outside Turkey. They provide information about new developments and practices. They are certainly very helpful. Especially, with regard to information sharing. More importantly, we can contact people working in this field and communicate with them later on.
C	Rarely		We attend conferences in the boundaries of our resources.(?) It is difficult to say that we attend most of them. We have a workload and our budget is limited. But, we try our best to attend conferences and our institution supports us.
D	Yes, but…	• Not to many conferences • Focus on legal aspects • Not directly related to digital forensics	The number of computer users in Turkey is less than in the U.S. and Europe. In addition, this field is relatively new. Most people in the judicial system are not knowledgeable enough about digital evidence examination. The number of conferences and seminars doesn't exceed two or three, and they mostly focus on legal aspects. As practitioners we usually get what we need. But, we still attend those conferences to contribute to the literature and to enlighten law-oriented people. We present issues about our field and answer their questions. Other than that, conferences - directly related to our field - that are important for us are held in the U.S. You know, geographically there is a long distance between the two countries. We also have some financial constraints. Therefore, it is very difficult for us to attend those conferences. On the other hand, domestic conferences don't meet our expectations. It is unfortunate not to participate in international conferences due to the financial constraints.
E	Rarely	• Making new contacts • Observing new practices in live presentations.	I attend conferences as the head of our department as long as I am allowed. It is useful to contact with other colleagues, and to observe new practices and applications. New developments are readily presented in those occasions.
F	Yes	• Mostly workshops	I make an effort to attend conferences. I mostly attend workshops.

(table continues)

Table 18 *(continued)*.

ID	Usage	Type & Purpose	Comment
G	Yes	• Seminars, fairs related technical issues	Yes, I attend conferences, seminars, fairs, such activities in which issues about data recovery, data analysis, and encryption are discussed.
H	No		I usually don't have the opportunity to attend conferences.
I	Rarely		It depends on the situation. If I don't have a workload and an awaiting investigation, I can attend.
J	Yes	• Seminars, conferences about digital forensics. • Self-improvement	I attended conferences, seminars and training focusing on informatics as much as I could. Information sharing or validating my knowledge on digital evidence examination helps me improve myself.

Like the use of other information sources related to digital forensics, language is a barrier to attending conferences, since only examiners who can speak English can attend conferences outside Turkey. The important thing is that those conferences related much more directly to their profession compared to domestically held conferences.

It seems that DEEs attend conferences to observe newly developed techniques and methods in-person, to make new professional contacts, so that they can discuss alternative solutions to problems they may have later on, and to educate other people about their job. DEEs also attend workshops and seminars in which specific technical problems and digital forensic practices are discussed.

Forensic Kits and Software

All interviewees said that forensic kits and software are very important in their work. Interviewee A said that they frequently update and upgrade the kits and software, and he believes that his success at work is directly related to the extent to which the forensic kits are up-to-date. Interviewee B said that they use forensic kits that are commonly used by DEEs around the world.

Table 19

Comments of Participants on Forensic Kits and Software

ID	Comments
A	Forensic kits and software are very important. We renew them every year. They are the basic tools we use. The accuracy of our work is directly related to keeping them up to date.
B	The kits and software we use are the ones commonly used all over the world. We have no software or device which is not used in the international arena. In order to maintain the integrity of evidence and to examine digital evidence accurately, we need this software and kits. We constantly update and upgrade the kits and software we use, we have to. In computer analysis, those kits and software are important sources of information for us.
C	There is no perfect software. Likewise, no hardware is perfect. Planning to examine all computer evidence with a single type of software, or hardware will result in a big disappointment. ... software and hardware available in this field have their own advantages and disadvantages, depending on the situation. Obviously, it is best to use the appropriate one according to the current situation at hand and specific business requirements.
D	Regarding the examination of digital data, the most important thing for us is the software and hardware. When I talk about hardware, I refer to computers with very high technological capacity. Digital devices and media submitted to us for examination could be obtained from people following technology very closely … So, we always need high capacity and new equipment. In addition to this, updated versions of software is constantly being produced. Software used in digital evidence examination becomes more powerful by having new features which don't exist in the previous versions. Hardware and software, we can say, is our most important source of information. Then, the Internet follows next.
E	Their manual and help menu provides many benefits to our profession. We use more information resources about how to use these kits and software. These are our course notes, books, and the Internet.
F	We use more information resources about how to use these kits and software. For example, our course notes, the Internet.
I	I get information about the forensic kits and software I am using from the help menu of the software, websites, open sources, forums dedicated to discussion of those software programs, and from qualified personnel of forensic tool manufacturers.
J	Forensic kits and software actually make our job much easier. They provide a lot of information that facilitates our work. My personal opinion is that the Digital Evidence Examiner does the job, not the forensic software. They are just tools. The examiner should be able to do an examination easily with personal knowledge and experience; even when there is no software to use.

In digital forensics the forensic kits are important information sources. However, Interviewee C pointed out that not all kits and software are perfect or can be used in every examination situation; he noted that they provide advantages and disadvantages depending on the situation. Interviewee (give letter) also emphasized the importance of forensic kits and software. Interviewees E, F and I said that they actually need more information about using those kits and software. In such cases, they said they look at the manual and help menus, course notes, books and the Internet. Interviewee J said that forensic kits and software are just tools that make their job easier; he thinks that the examiner is more important than the tool because the examiner tells the tool what to do.

It seems that forensic tools are very important for examiners in terms of providing work-related information. A noteworthy point is that forensic tools and software trigger the information needs of DEEs, since they are very complicated and powerful tools. The manufacturers frequently add new features following new developments in technology and newly produced digital devices. Therefore, DEEs constantly need to get information about new features and new forensic tools.

Online Sources

The researcher found out that participants use online sources excessively. Interviewee A said that they use internal online systems to track every procedure performed on the evidence. It was interesting that Interviewees A, B, D, E, F, G, I and J said that they use the Internet. Other online information sources DEEs use are forums, online journals, social networks, search engines, commercial websites and online databases.

Table 20

Use of Online Sources by DEEs

	Type	Purpose	Comment
A	• intranet • Internet • Online Journals	• To track work flow • to get up-to-date information • problem solving	We are using a system called "work-flow system" in our laboratories. We are using this system in an active way. Each stage of the work we do on the evidence is recorded and can be reviewed by this system from the entrance to end of examination. Any action and operation done on the evidence is recorded automatically on the system … We use the Internet to get up-to-date information, up-to-date online journals, to find a solution to a problem we encounter. However, the Internet is beneficial to some extent.
B	• Internet • Search engines • Forums • Social networks • Intranet • Database	• To share work related information • To solve problems	But, the real source of information for us is often the Internet. ... the largest of electronic networks, of course, is the Internet ... either search engines or communication resources of the Internet such as emailing; posting in forum pages actually creates a quite serious information flow… the first things done is actually an Internet search … I've done this so far. I try to do a good research on the Internet. Google, from my perspective, is an important source of information … We have approximately 100 personnel working under our department in different cities. Our friends have created their private forum page among themselves to share information. When something new comes out, when somebody learns something new, and it is immediately uploaded to this forum page. In this way, we have created a very large online digital database by sharing information.
C	• Online journals • Forums • Email	• To solve problems	If you are a professional in this field, then you absolutely must review certain journals, forum pages, and discussion sites. We overall have an experience on this topic. From time to time, we enter questions into search engines, and learn how to do things.
D	• Internet • Forums	• To learn about forensic practices • To solve problems	Therefore, the Internet is the most common information source we are currently using. We hardly use books …. There are some very useful forum pages in the Internet pertinent to digital evidence examination. In those pages, people post their problems and discuss different alternatives or solutions. We usually get answers in 30 minutes after we post the questions.
E	• Forums • Internet • Forums • Email	• To get initial information about a new case/topic • To follow new developments • To solve problems • To get initial information	We especially use the forums. Technology is changing very quickly. When faced with a new topic, one of the first things we do is to ask in the forum. What we do next is to find scientific articles and to do experiments to see if we have the correct solution … I use the Internet to follow developments in the field of digital forensics, to discuss the problems in forums with my friends or to post my questions via email. We also use it for experiments. We investigate websites which are subject to court trial.

(table continues)

Table 20 *(continued)*.

	Type	Purpose	Comment
F	• Internet • Forums	• To follow new developments • To solve problems • To get job related information	I use the Internet to follow new developments in the field of digital forensics, and to do research in order to find solutions to my problems…. We search forum pages frequently. Looking for related information in forums is usually the first thing I do.
G	• Commercial websites • Internet	• To get information about forensic kits and software • To get general information • To communicate	From time to time, I benefit from websites and forum pages of companies producing forensic kits and software. I usually find answers to my questions … I usually use the Internet to get general information about the issues related to my job. I am usually successful. Other than that, I use the Internet for communication purposes.
H	• Forums	• To solve problems	I use forums a lot; especially, to look for solutions to problems I encounter.
I	• Forums • Internet	• To solve problems	I meet my information needs by submitting questions to forums … I use the Internet to find solutions to the problems in the field of digital evidence examination.
J	• Internet	• To get general information about a new topic • To get information about computer technology	The electronic network is one of the most extensive resources we get information from. We can immediately access any information we are searching for. When first confronted with a new topic, we can immediately get preliminary information by using the Internet … I use the Internet to collect information and do research about computer technologies and digital evidence examination. Besides, I surf the Internet to keep a track of new issues … I use the Internet instead of the library and information pool.

Depending on the situation, DEEs use these online information sources mainly for six purposes (as indicated in Table 20):

- To learn about new developments in the technology
- To follow new developments in digital forensics
- To get general information about a new topic/case/problem
- To find solutions to job-related problems
- To share forensic experience and knowledge
- To track work flow

Library or Information Center

Interviewees A and B indicated that both laboratories have libraries. In both cases the libraries are not in the laboratories, but very close; the libraries are in the same building. Interviewees (A and B?) said that examiners use the books in the library rather than keeping a personal collection.

> Interviewee A: Yes, our section has a library. The library is not just for our laboratory but for all departments. We keep technical books we need in that library. We would rather use that library. We don't have personal collections. The library already contains all the required books. The library is always accessible and very close to our laboratory, in the same building
>
> Interviewee B: Our laboratories are separate from the personnel offices. We built a library in one of those offices. We have such books [technical] in that library.

Interviewee E said that they have an online "pool of information" and they often use it. He said that they use books to verify what they have just learned. Interviewee F supported what Interviewee E said, that he finds the online information pool more helpful than the library in terms of finding solutions quickly. On the contrary, Interviewee I said that he rarely uses the information pool. The researcher didn't have a clear idea about how often DEEs use libraries in their work life, but it seems that DEEs use online sources more often when looking for a solution to a problem.

Personal Contacts

DEEs satisfy a large portion of their information needs by using their personal contacts inside or outside their laboratory. The finding related to the use of conferences as information sources supports this assumption. As shown in Table 18, making professional contacts was one

of the main purposes of attending conferences for DEEs. Interviewee A indicated that personal contacts are used for professional purposes:

> I sometimes directly write to the experts I get acquainted with at conferences. I can directly ask them questions. Although, I have my personal contacts, I use them for institutional purposes.

The use of personal contacts to get job-related information is common among DEEs not only at the national level but also at the international level. Interviewee B explained the reason as follows:

> There is a high level of information sharing especially in computer forensics. This information sharing is not only among domestic institutions. All over the world, especially in Europe, police organizations significantly share information about computer forensics because agencies operating in the field of computer forensics need each other. The actual location of the owner of an IP could be in any country in the world. Somebody in Turkey can commit a crime in the U.S. The offender can tamper with any identifying data like IP. The forum pages dedicated to police organizations or websites of computer forensic companies are very informative for us. We benefit from those websites and forums.

Comparison of Information Sources

The participants had different perceptions of the importance of information sources. Interviewee A said that the most important information source for him is the basic technical courses in which DEEs learn to use forensic kits and software, and to apply certain techniques according to the type of digital evidence. He, however, said that basic training is not enough by itself; experience is also needed in the digital forensic process. To him, experience is gained through working on digital evidence and learning from experts in the lab, and he said that there is master and apprentice relationship between the experts and other examiners:

> A: Well, First, the courses are very important. Courses are the basis of our professional knowledge. For example, when we started using Encase, experts from the company came to our laboratory and taught relevant courses. Everything starts with those basic

courses. Being the foundation of our work, one of the most important sources is technical courses. Then, you add up new information from books, and the Internet. I think the most important of these is the basic courses. After the basic courses, the work will give one experience over time. A newcomer takes technical courses, but doesn't yet have experience. He needs to work for a while. The information of an examiner who has spent significant time in this field is priceless. We can say that a large portion of our knowledge is created via a master and apprentice relationship in the laboratory. I get a basic education, but I can get the information I need much faster from ones who have experienced worked on them for a time. I can obtain information instantly by directly asking an expert. On the other hand, it takes sometimes two days for me to search for that information in books. Thus, it is more accurate, more satisfying, and I can get a faster response. As an assistant, the most important source of information, for me, is the expert. I'm learning a lot from him. Courses are important. It's important to share information with others

In contrast, Interviewee E believed experts to be the most important information source because he believed that experts are the most accurate information source. He emphasized that the information obtained from the Internet should be tested by the laboratory:

E: it is important for me to find information quickly. The accuracy of information is important, too. It must be accepted and internalized by the laboratory. In this respect, more experienced friends (experts) I work with are the most important information sources. I can rank other sources from the most important to the least important as course notes, forums, books, and search engines, respectively.

From a different perspective, Interviewee F believed the Internet to be the most important information source:

F: Currently, the most important source of information is the Internet. In addition, my friends working in this field are also beneficial in terms of exchanging ideas.

Interviewee J also agreed with Interviewee F:

J: Recently, the Internet has become a very important source. The reason is that I can find information about almost anything without mediators.

Interviewee G brought a completely different approach to the subject. To him, there is not a single most important information source, he said it depends on the situation. The information source an examiner uses to get the information is the most important one:

> G: I cannot say that an information source is the most important and others are less important. It depends on the situation. Therefore, all sources I have mentioned are important. Knowledge is power. The more information sources I use, the more efficiently I use those sources, and the more I am successful.

With respect to using internal information sources as opposed to external information sources, the researcher concluded that DEEs mostly prefer to use internal sources, especially experts in the laboratory. Issues in digital forensics are very complex and there may be several things causing a problem. To get the information the examiner needs, the examiner has to first give detailed information about the problem or the need. DEEs perceive that explaining a problem face to face is much easier. This also indicates that DEEs prefer oral communication as opposed to written communication while searching for solutions to technical problems. Interviewee C explained this point by giving an example:

> C: We actually prefer oral communication because there is a complex case in your hands. I need to provide the big picture of the case from beginning to end, when I ask help from somebody. When you ask directly without providing proper information, it is not likely you will get a relevant answer. You may sound funny. It is difficult to answer without seeing the whole picture. That is somewhat similar to the doctor patient relationship. There may be a number of answers to the question of ”What causes arm pain?” on the other hand, if you give enough information to the doctor about the age, gender, and previous health problems of the patient, then you can get more relevant information. So, I prefer to explain the problem orally. That way, it is easier to explain. There is also a language barrier. To write the problem in detail is much more difficult.

In fact, the term “internal” is kind of blurry in the current technologically advanced world. Internal not only means “inside,” but it also refers to “near.” However, IT brings information sources from outside the laboratory inside. In other words, IT changes the external into the internal, where distances actually do not matter. Interviewee B said that they can use external sources as if they are internal sources.

B: Of course, at the moment of urgency, the most important thing we do is to use the phone. We use video IP phones among our units using video phones; we can solve problems by talking face to face, and by sharing information quickly and effectively.

Interviewee C pointed out another disadvantage of written communication:

C: E-mailing is not a quick way to obtain information. Once you submit your question, then, you wait for the person to see your message or to be available to reply. They also have a workload. It takes time to get a response.

It seems that DEEs use written communication when the information source is in a foreign country. Of course, information sources outside the country can only be used by DEEs who know the language of that information source.

D: I surely prefer oral communication with my more experienced colleagues in my laboratory when I need to discuss a technical issue, or if the person who can help me is in Turkey, then I call and ask questions over the phone. If I cannot get answers to my questions from my colleagues around me and in Turkey, finally, I write messages to my contacts via the Internet.

Research Question 3: Factors Affecting Information Source Selection

In this section, finding factors that affect information source selection and use by DEEs are presented. After collecting qualitative data, the researcher realized that it is very difficult to categorize factors such as situational factors, information source factors, task factors and cognitive factors. There is also no consensus on the definitions of these factors. Therefore, dependent and independent variables are used interchangeably. Because the relationships between variables are not clear, the researcher only listed identified factors without categorizing them. The factors affecting information source selection and use by DEEs can be listed as follows:

- Accreditation

- Workload
- Type of information
- Time line
- Cost
- Availability
- Reliability/scientific
- Up to date
- Easy to communicate
- Prior experience with the source
- Relevance
- Practicality /applicability
- Importance

Accreditation

Interviewee C said that accreditation of the laboratory forced them to use certain information sources. Accreditation ensures a certain level of quality in selecting information sources. Interviewee C said that he first determines that the information source carries certain qualifications. Then, he uses his own knowledge and experience to accomplish the task.

> C: You should have standardized practice procedures. The laboratory I am working in is an accredited one. The stages evidence will go through and the software and kits that will be used in examinations have been written down. It is impossible to examine evidence apart from those standards. Due to the quality requirements, we first search those sources. Secondly, I, of course, apply my own knowledge. Training I received and the experience I gained in evidence examination from the first day forward taught me which source to use in what situation.

Workload

The second factor is workload. Workload is not measured in this study; only the perceived workload of participants is reported. However, workload can be measured objectively if quantitative data is obtained. First, the digital evidence is categorized. Then, the average number of processed devices, in each category, is determined for the previous months. Finally, the numbers are compared with the number of digital devices still waiting for digital forensic processing. In this study, the level of workload was not measured this way; the researcher relied on the perceptions of respondents. It seems that when examiners work in a laboratory with a high workload, they tend to use information sources that they perceive as being fast to access. For example, Interviewee A said that "due to the workload, I don't have much time to search for information in books."

Type of Information

As explained in previous sections, the information needs of DEEs vary according to the specific tasks and sub-tasks they perform. The researcher found out that the type of information DEEs search for also varies according to their information needs. DEEs usually need technical information in examination sub-tasks, whereas they usually need information about the elements of a crime in analysis sub-tasks. Interviewee A said that DEEs search for information on the basis of forensic techniques they use to examine or analyze digital evidence. He gave examples explaining this factor:

> A: it is easy to teach technical issues to investigators, but it may take a long time to teach investigation to technical people. Once laboratories hired only technical personnel, but then, they noticed that merely technical knowledge is not sufficient. Investigative skills are also needed. I don't know if I could answer your question

> completely. Experience is crucial in some cases. You cannot find that anywhere else. Perhaps, some people may share their experience over the Internet. The Internet may be a good source of information. We mostly benefit from the experiences of experts, detectives investigating the crime and our own …
>
> We don't want them to identify the keyword to be searched. But, the more detailed information about elements of a crime they provide for us, the more successful we will be. To identify keywords is absolutely my responsibility. We can increase the number of keywords if we know more about the case. Sometimes, we merely guess what we are supposed to look for. We need to know what they expect from us. Books don't directly tell you which keyword you should look for. Each case has its unique dimensions. Offenders, location, the way it is committed, crime weapons are different in different cases. You cannot find that kind of information on the Internet. Digital evidence examination has two faces; technical and policing.

It appears that the type of information an examiner is looking for has no negative or positive affect on the frequency of use of an information source. In fact, the information type influences the decision of the examiner about using that source.

Time

It seems that time is an important factor influencing information-seeking practices of DEEs. The respondents addressed two different items related to the time factor. The first one is the time it takes to retrieve the information from a source. The second one is the length of time available to search a topic. These two concepts can be defined as "available time to access an information source," and after accessing a source "available time to retrieve information from a source" Regarding the first one, it seems that DEEs search for the information they need from as many different information sources as they have time for. Especially, when DEEs receive digital evidence that they didn't process at an earlier time, DEEs initially make an assessment about whether they have enough time to get the information they need to accomplish the task. The data indicate that there is positive relationship between the amount of time available and

the number of information sources used in a digital forensic case. That is, the more time examiners have to search for information, the more information sources they use. If they believe that they don't have enough time, then they simply refuse the case.

Regarding the second type of time factor, the participants indicated that they use certain information sources because they get the information faster from that source. It seems that the speed of retrieving information from a source has a positive effect on the frequency of use of that information source. That is, the faster the examiner can retrieve information from an information source, the more frequently he/she tends to use that information source. The statement of Interviewee D about the speed of information retrieval from a source is a good example of the first kind of time factor:

> The Internet is the biggest information source for us. Why? Because it is easy to access, it is fast, and at the same time it is up-to-date.

Cost

The factor of cost was especially mentioned by the participants while talking about attending conferences in order to obtain job-related information. According to the statements of participants, it appears that there is a negative relationship between the cost of an information source and the use of that source. In other words, as the cost of an information source increases, the frequency of use of that information source decreases. Statements of Interviewees C and D support this finding:

> C: We attend conferences in the boundaries of our resources(?). It is difficult to say that we attend most of them. We have a workload and our budget is limited. But, we try our best to attend conferences and our institution supports us.

D: Especially after 2006, 2007, since it is more expensive and more difficult to access those books compared to the Internet, and it is hard to find them in Turkey, we rarely use books. We can obtain foreign books by paying extra money to international shipping companies and customs. It is a long procedure. Therefore, the Internet is the most common information source we are currently using. We hardly use books.

D: Other than that, conferences - directly related to our field - that are important for us are held in the U.S. You know, geographically there is a large distance between the two countries. We also have some financial constraints. Therefore, it is very difficult for us to attend those conferences. On the other hand, domestic conferences don't meet our expectations. It is unfortunate not to be able to participate in those international conferences due to financial constraints.

Availability

The factors of availability and accessibility have been discussed over time. They have been redefined according to the changing concept of the distance between the seeker and the source in an information society. Earlier, only physical distance was used to determine whether a source was available or not. Today, this criterion seems to be useless because IT shortens, or even eliminates, distances. As discussed above, Interviewee C said that:

C: If you are working in a big institution, then there are a lot of people doing the same work. You can definitely communicate more easily with others on the other end of the phone.

Today, an information source is as far away as the system you use to access that source. In this sense, information sources that were previously defined as unavailable can be now be considered as available when you use ICT. It can be concluded from the answers of respondents that DEEs use the information sources available to them more frequently than other sources that are not available. However, this doesn't necessarily mean that there is a cause and effect relationship between availability and information source usage.

Scientific

Another factor mentioned by Interviewee E is that DEEs prefer to use more reliable and scientific information sources. Forensics is considered to be a science, and the methods and techniques applied in digital forensics have to be scientifically tested. It appears that scientifically-tested information sources are used more frequently compared with other sources:

> E: It is important to have scientific sources. When acquiring new information [practice], it must be supported with references and be tested first to be sure. The expert organizes a briefing meeting with other employees in the laboratory to share new information that he believes is accurate. In that meeting, information about the topic, new experiences and test results are presented. In the end, a decision about it is made. When other employees agree with the expert, this information is added to the information pool of our laboratory.

Up to Date

To what extent an information source is up-to-date is another factor mentioned by the interviewees. As Interviewee A said, DEEs use certain types of information sources because those sources provide up-to-date information.

> A: There are journals we subscribed to. We look at them from time to time because books may not be up-to-date … The most updated and detailed information is given in conferences.

Prior Experience with the Source

It appears that DEEs become familiar with information sources as they use them. Their prior experience with the information source influences their use of that source in the future. Successful prior use has a positive effect, whereas unsuccessful use has a negative effect on the

frequency of use of an information source. Interviewee D stated that he perceives forum pages as useful, and he can even give an average time to get a response to a posted question.

> D: There are some very useful forum pages on the Internet, pertinent to digital evidence examination. In those pages, people post their problems and discuss different alternatives or solutions. We usually get answers within 30 minutes after we post the questions.

Relevance

Interviewee B mentioned that the extent to which an information source is relevant to the question in mind is a factor affecting the decision of examiners about selecting that source. The participants didn't clearly identify their relevance criteria. Interviewee B said that he tries to obtain information from a source that he believes is relevant to his job. He explains how much effort he went to, to get some books, since he perceived them as relevant to his job:

> B: I try to get the information source we need regardless of its location in the world. The most important criterion for me when I decide to use an information source is whether that source satisfies me or not. If that gives the answers I need, I immediately buy it. For example, I have bought many books from EBay. I sometimes get books shipped from England, China, and the U.S. The location of the source is not important. If the answers we need are in it, we get it. I sometimes spend a lot of effort to find, and get a book. To find some printed sources is really difficult.

Interactivity

As indicated by Interviewee A, DEEs attend conferences to observe and learn how forensic methods and techniques are applied. During conferences, forensic kits and software are demonstrated; DEEs perceived that human information sources demonstrate forensic practices interactively. Conferences are the perfect environments for the seeker and the

information source to interact. Other types of information sources in which DEEs interact strongly with human information sources are workshops and technical courses.

A: it is helpful to see things in practice during conferences.

Importance

The participants mentioned the level of perceived importance of a source as an indicator of how frequently they use that source. The analysis of interview transcripts indicated that there is a positive relationship between the level of perceived importance of a source and the frequency of use of that source. The statements of Interviewees A, C and D support this assumption:

> A: As an assistant, the most important source of information, for me, is the expert. I'm learning a lot from him.
>
> C: Actually, this may not be an exact list showing the importance level of each source. The rank of the information in that list depends on which source is more beneficial for you. The source in the first place [the most important] in one case can drop back to third place in another case. However, if I make a list in general other experts are the best information source, second is the Internet, third is experts working informatics security. Then follow, printed sources such as books and journals.
>
> D: With respect to our job, forums on the Internet are the most important source.

Research Question 4: Obstacles to Information Seeking

In this section findings related to the obstacles DEEs face while seeking job-related information are presented. The researcher categorized the obstacles as follows:

- Separation of digital evidence collection from other stages
- Unwillingness to share information due to bureaucratic or political concerns
- Lack of technical knowledge/education in other areas of criminal justice

- Rapid change in technology
- The nature of computer crimes
- Lack of reference books in Turkish

Separation of Digital Evidence Collection from Other Stages (Lack of Background Information about the Case)

As mentioned in the earlier pages of this chapter, DEEs don't participate in the evidence collection stage. Interviewee B pointed out that the legal system, in fact, doesn't allow them to collect evidence:

> B: Digital evidence is gathered by criminal investigator units. The reason for this is the different treatment of the legal system in Turkey. The person collecting evidence at the crime scene, and the person who examines the evidence have to be different people. To ensure the impartiality of the investigation, this is an applied rule. An examiner cannot process a digital media if he collects it on his own. Because of this practice, the crime scene investigator unit is collects the evidence, and sends it to digital evidence examiners.

This regulation, however, creates problems. In some cases, officers collecting the evidence don't follow the rules of evidence collection. There are certain procedures that the person collecting the evidence has to follow. An important part of evidence collection is to record the information about the user or owner of a digital device/media. The person collecting and submitting evidence may not know the technical aspects of digital evidence collection and the information needs of DEEs. Therefore, that person might not provide sufficient information for DEEs to be used in the following stages of the digital forensic process. If DEEs collected evidence from the crime scene, they would pay special attention to gathering the information they would need in the following stages. Interviewee A addressed this problem:

A: But, sometimes we received cases where only the subject of the crime is written down. This case was like that, nothing was included other than the type of crime. No suspect's name, what was expected was not clearly written down, and almost no information about the case has been submitted, only the name of the crime has been written and, then, we are asked to investigate the hard disc. In such cases, we have extreme difficulties in identifying the keywords.

Unwillingness to Share Information Due to Bureaucratic or Political Concerns

The second identified obstacle that DEEs face in digital forensics is that the other parties involved in the investigation of the crime, to which the evidence relates, don't want to share information due to bureaucratic or political concerns. Some cases are very sensitive, especially when politics and bureaucrats are involved in the case. As happened in the case Interviewee A described, the party submitting the evidence may not be cooperative:

A: The office submitting the case should write what they expect us to do. For example, when submitting a case, one that says "please, do necessary examinations to determine whether such and such digital media belonging to such and such people contains such and such element of such and such crime." Each "such" takes its place in our keyword list. This is an example of an examination request we want to receive. The other is the one we don't want. For example, one says "please, send your report after completing necessary examination on the digital media regarding such and such crime." In a case like that, we only know the type of crime, nothing else. That is a tough situation. I don't know if it helps you but it is about politics.

Interviewee B said that he noticed a problem when he first began working in the lab; the examiners were not sharing information. He said that there was lack of communication, and that he was able to solve the problem by providing alternative ways of communication and encouraging information sharing.

B: The first thing I noticed when I stated this job was the lack of information sharing, absence of information sharing. I saw that the communication among employees was missing. People were keeping information to themselves. There may be a number of reasons for that. I don't why it was like that. After, 2005-2006, we established a large communication infrastructure via emailing and forums. Now, we share new information

> we learn, and every new experience we get via forums. It is very important to share newly obtained information. And, we do so. We organize seminars and in-service training, lasting one week, once every three months in order to update our knowledge. I believe that such occasions are very important with respect to digital evidence examination. We collect our knowledge in two different databases: a web-based one, and in the internal network. Everybody has membership in those databases. We can access our database wherever we are, regardless of our location, via Internet. That is very helpful for us.

Lack of Technical Knowledge/Education in Other Areas of Criminal Justice

The third obstacle is that clients requesting a digital evidence examination don't have as much technical knowledge as DEEs. That is why DEEs are required to use a different, simpler language in their reports. Most DEEs don't feel comfortable using such language; they feel that they cannot completely justify the complex methods and techniques they use during the digital evidence process. DEEs have to maintain a balance between being understandable and being scientific. Interviewee B pointed out this problem and mentioned a factor causing this problem. The problem was that there was no technical education in the judicial system.

> B: our reports are technical reports although the contents of them usually solve criminal cases. Our reports give detailed information about who created a file in the system, when it was created, when it was modified, when it was deleted. The people we are submitting our report to don't have training in technical issues. That is why authorities in the criminal justice system sometimes don't understand the technical jargon we use. This is a fact. The police have such an institution of expertise but the judicial system doesn't have prosecutors or judges who especially focus on technical cases. This is actually a problem all around the world. We heard similar complaints and discussions at the conferences and seminars we attended. Considering this, we recently simplified our reports; we have been writing them more clearly and understandably.

Rapid Change in Technology

Another challenging fact in digital forensics is the rapid change in technology. It seems

that DEEs are having difficulty in obtaining information about forensic investigations of new products, since it takes some time to design, produce, test and approve forensic kits and software. Therefore, during the interim, DEEs cannot find reliable information.

DEEs are also having difficulty in finding information in the opposite situation, in which a "very old" digital devices is submitted for examination. The technology is changing so fast, and the number of digital devices so large that, in some cases, even disassembling a previously-produced digital device presents a big challenge.

> B: In one of the cases, we had a very old MacBook in our hand. We could not disassemble and remove the hard drive. Even the Mac Service had difficulty doing it and it took them about 6-7 hours to do that. The hard drive's capacity was 2Gb and was a very old one.
>
> C: Absolutely, we receive some challenging cases from time to time. The technology is changing so fast. It is very likely for us to encounter new things.
>
> D: There are many different types of software. People in this field use different types of software. So, we sometimes cannot find the exact answer relevant to the case in our hands. We are looking for information about a certain operating system but, instead, it explains how to solve the problem on another operating system. There are even many differences between different versions of the same operating system. For example, Windows adds lots of new things with a new version. It is not always possible for us to find out which instructions to give the computer, to search under which directory. Although, the Internet is the largest, the most up-to-date, and the fastest source of information, we still have difficulty in getting particular information.

The Nature of Crime, Especially Computer Crime

Another obstacle mentioned by the participants is the nature of crime. The offender tries to erase any evidence that incriminates him/her. Especially, in computer crimes, offenders are very knowledgeable about technical issues. They know how to delete, cover, or hide any digital traces of their actions. In addition, just as there is a market for producing forensic tools

to recover and to analyze digital data, there is also a big market for producing tools and software that focus on deleting data, or the security of digital data. These tools are so powerful that digital data deleted with certain tools cannot be recovered. Digital data encrypted with powerful software cannot be reviewed or, alternatively, it will take a long time to do so.

> B: As a challenge, we only had difficulty in hacking passwords. Dealing with passwords and encrypted digital media is problematic for all examiners in the world.

Lack of Reference Books in Turkish

The last obstacle the interviewees pointed out is the lack of reference books in Turkish. Materials for the science of digital forensics, including forensic kits and software, are produced in foreign countries. Therefore, all the important reference books are, mostly, in English. Even the examiners who know English complained about this issue. The problems DEEs face are very complex, and when they need information regarding a technical problem, it is still difficult to find the information even if the examiner knows English. Some problems can be solved only by contacting experts outside Turkey. In such cases, explaining the problem is also a difficult job, since the problem should be described in detail.

> B: most books relevant to our work are in a foreign language. To have books in a second language is a bit problematic for us. Mostly, my friends who know the second language use those books

> C: while searching for information, the biggest problem is to reach the correct person. There are a great number of issues in digital evidence examinations. You cannot always find people who specialize on the topics you want to ask about. Therefore, you ask the same thing of several experts, and get the relevant information. Those experts are not always near you. E-mailing is not a quick way to find information. Once you submit your question, then, you wait for the person to see your message or to be available to reply.

CHAPTER 5

CONCLUSION

Introduction

People are surrounded by information and communication technologies; personal digital devices, which are usually multi-task all-in-one devices, are ubiquitous. For instance, a smart cell-phone is a personal computer, a GPS locator, a multimedia device and also a digital storage media, and the number of these types of digital devices is increasing dramatically. In addition, security cameras are everywhere. A huge amount of information about the people using or associated with these technologies is saved inside digital devices automatically, as a requirement of the architecture of digital devices.

The information in physical digital items has a legally latent value, and law enforcement agencies have begun to recognize the value of the latent information in personal and public digital devices. Therefore, they will collect digital evidence, in addition to traditional physical evidence, to strengthen the case they are investigating.

Digital evidence examining has emerged as a new profession from the interaction of engineering sciences, such as computer, software and network engineering, and forensic sciences, especially digital forensics. Although there are numerous studies on the digital evidence examination process, it has never been studied from an information science perspective.

This study aimed to gain in-depth insights into the information-seeking behavior of digital evidence examiners (DEEs). The researcher specifically focused on their information needs, the information sources that digital evidence examiners use, the factors affecting their

decisions regarding source selection, and the obstacles DEEs encounter during the search for job-related information. The findings of this study assisted the researcher in making some theoretically helpful recommendations for administrators.

Research Question 1: Context and Information Needs

The researcher found that digital evidence examiners rarely collect digital evidence from crime scenes. They, mostly, examine and analyze digital media delivered to them, and report their findings about the digital evidence retrieved from those digital media according to legal regulations, by applying certain techniques and using special hardware and software determined by the type of crime and digital media. As can be seen in their job descriptions, the work environment of digital evidence examiners shapes their information behavior. Legal regulation and responsibilities, technical differences in the digital devices, and variability in the nature of different crimes all influence DEEs behavior; they act according to the context of the situation.

The role an examiner plays in the work environment is one of the factors directly influencing information needs of DEEs and indirectly influencing information source usage by DEEs. The roles that DEEs play include: Researcher, Expert, Assistant Mentor (instructor) and Marketing Employee. Experts are expected to play certain roles, like instructing other assistants, doing research on newly-developed techniques, and addressing other issues as requested by assistants. All examiners play the role of marketing personnel to some extent. They participate in the process of buying new tools, upgrade or update those tools by describing their needs or they make the decision about what to buy.

The data from the interviews revealed that all examiners search for information about new hardware and software in certain information sources such as the Internet, conferences and technical journals. They want to buy the newest, most developed product on the market, because their main motivation is to perform successful examinations; they want to follow the trends of the market. Certain types of information sources provide certain types of information. To illustrate, DEEs use technical magazines, which are not scholarly in nature, to obtain general information about newly-developed digital devices. In contrast, DEEs prefer to use scholarly journals to obtain specific information about newly developed forensic procedures and software.

The research revealed that the type of crime, type of evidence, and sub-tasks of the digital evidence examination shape the information needs of DEEs. That is, the type of crime, type of evidence, and sub-tasks have an influence on the decision of DEEs regarding information source selection and use, through shaping the information needs of DEEs. DEEs are usually asked to determine if a digital media contains digital evidence related to an alleged crime. To answer this question, DEEs need to know what constitutes a given type of crime, and what the elements of that crime are. Information about the type of crime is especially helpful in the analysis stage of evidence examination. Technical information about digital evidence is helpful for DEEs in the examination stage, while they are extracting digital data, and in the reporting stage, for justifying the methods they used in the examination and analysis stages.

DEEs need to obtain adequate information about the owner of the digital media, suspects, the nature of the crime, and the crime scene to conduct a successful examination.

They rely on the other police units in getting these types of information. They need this information because they analyze digital data and make decisions based on that information.

It seems that DEEs sometimes have problems in getting adequate information from evidence collection units. The units may not understand the importance of the information that DEEs request about the evidence and its owner. In such cases, DEEs call the units submitting the evidence on the phone and try to obtain the information they need. They may not always be able to get the desired information, because the party submitting the evidence may not want to share information for several reasons.

In most cases, DEEs did not have this problem because they have very good, up-to-date and powerful hardware and software in their laboratory. in the examination stage, DEEs usually need more job-related information than usual, and, therefore, spend a lot of time on information seeking in the following situations:

- When they encounter a technical problem with the hardware or software that they use or with a digital device/media
- When a new type of digital device/media is submitted to their laboratory to be examined for the first time
- When the digital device/media subject to examination is too old
- When the digital device/media subject to examination is newly produced
- When the digital device/media is highly protected with strong passwords or encryption software
- When the owner of the digital device/media subject to investigation is very knowledgeable about computers and networks

- When the digital device/media doesn't have a standardized format

Since DEEs need technical information the most in the examination stage, they usually use information sources that can provide technical information about: 1) the digital device/media they are working on, 2) the forensic tools they are using or 3) appropriate methods and procedures applied during the examination. The Internet was the information source most commonly used by participants during the examination stage. The other information sources that were often used by examiners in the examination stage are: forums, experts, colleagues, forensic tools/kits and books.

In the analysis stage, questions asked by the clients requesting digital forensic investigations are answered. Since the relationships between elements of the crime are discovered during this stage, DEEs need detailed information about the following elements of crime: offender(s), crime weapon/tool, the crime scene, the victim of the crime, and the timeline of events, in order to perform a successful analysis. The information about the elements of the crime is supposed to be collected before the digital device/media is submitted to the lab.

However, DEEs must spend extra time in searching for information in order to satisfy their information needs in the analysis stage, when the following situations occur:

- When information about the elements of a crime is not provided or insufficient
- When the amount of data subject to analysis is extremely large
- When a digital media/device is obtained in complex crimes such as organized crimes and cybercrime

For the stage of analysis, the most frequently mentioned information source was the investigation file (case file) that contains information about the elements of the crime. The following information sources used by DEEs in the analysis stage are: personal experience, experts, detectives, the Internet, clients, professional training, the prosecutor, evidence submission forms, in-lab manuals, forums and colleagues, respectively.

DEEs usually need information about the language, style and format of forensic reports in the stage of reporting. They know that the people they are sending reports to are not as knowledgeable as they are about technical issues. Therefore, they must explain how they processed the digital evidence in terms that are simple enough to understand but detailed enough to avoid critiques about the reliability of the forensic examination. DEEs mostly use in-lab manuals and report templates as information sources in this stage. Other information sources DEEs use to obtain information about the format, style and language of reports are legal documents, previously-written reports, editing software, and colleagues.

All interviewees said that they finally found the information they were looking for, and successfully completed their assigned tasks. DEEs produce a report at the end of the digital forensic process; the report consists of the outcome of their work. While the participants were confident that they could get the information they needed to accomplish the investigation, they were not always certain whether the report they submitted was considered as successful from the perspectives of clients and the service requesting party. They were more certain when the party receiving the report gave them feedback. DEEs perceived that the reports were successful unless they received negative feedback.

Research Question 2: Information Sources

It seems that DEEs usually use technical books, given to them in technical courses, to solve the problems they have during the digital forensic process. DEEs use journals to find out about new products and new trends in technology; they benefit from these journals in keeping their tools and kits up-to-date and increasing their abilities. It appears that DEEs attend conferences to observe newly developed techniques and methods in-person, to make new professional contacts, so that they can discuss alternative solutions to problems they may have later on, and to educate other people about their job. Forensic tools were very important for examiners in terms of providing work-related information. A noteworthy point is that forensic tools and software trigger the information needs of DEEs, since they are very complicated and powerful tools. The manufacturers frequently add new features according to new developments in technology and newly produced digital devices.

The researcher discovered that participants use online sources very frequently. The most commonly used online information source is the Internet. DEEs use online information sources for six main purposes:

- To learn about new developments in technology
- To follow new developments in digital forensics
- To get general information about a new topic/case/problem
- To find solutions to job-related problems
- To share forensic experience and knowledge
- To track work flow

DEEs satisfy a significant portion of their information needs by using their personal contacts inside or outside their laboratory. The use of personal contacts to get job-related information is common among DEEs, not only at the national level but also at the international level.

The participants had different perceptions of the importance of information sources. Experts, professional training, and the Internet were given as the most important information sources. With respect to using internal information sources as opposed to external information sources, the researcher concluded that DEEs mostly prefer to use internal sources, especially the experts in their laboratory. To get the information the examiner needs, the examiner has to, first, give a detailed description of the problem or the need for information, and DEEs perceived that explaining the problem face to face was much easier. This also indicates that DEEs prefer oral, as opposed to written, communication while searching for solutions to technical problems.

Research Question 3: Factors

The factors, identified from the data, that affect information source selection and use by DEEs can be listed as follows: accreditation, workload, type of information, time, cost, availability, reliability/scientific, up-to-date, prior experience with the source, relevance, interactivity and importance.

Obstacles

The obstacles DEEs face while seeking job-related information can be listed as follows:

- Separation of digital evidence collection from other stages
- Unwillingness to share information due to bureaucratic or political concerns
- Lack of technical knowledge/education in other areas of criminal justice
- Rapid change in technology
- The nature of computer crimes
- Lack of reference books in Turkish

Implications

Theoretical Implications

This study has some theoretical implications. The findings of the current study are theoretically consistent with the findings of previous studies targeting the information-seeking behavior of professionals. To illustrate, the participants indicated that their information needs are shaped according to the characteristics of the tasks they perform.

This study theoretically contributed to the literature of information science by exploring specific characteristics of the tasks DEEs perform. Although the findings of this study are not statistically significant in any way, the assumptions generated by the researcher about the information behavior of DEEs, on the basis of the collected data, will open new doors for scholars. Testing those assumptions, by conducting quantitative studies that use larger samples, will generate more reliable and valid findings.

This study also made a contribution to the literature of the information-seeking behavior of professionals by introducing a new concept named as “perceived interactiveness of the information source used” as a factor affecting decision making process of DEEs about

selecting job related information sources. Investigating digital evidence is a complex job. The collected data shows that DEEs usually prefers to use information sources which they perceive as more interactive.

Methodological Implications

The researcher applied a directed approach in this study; that is, he designed his study on the basis of previous studies. Then, he reported emerging concepts that were not discussed in prior research. This method is helpful if the researcher is conducting research under time constraints. However, applying a ground theory would be more productive, in terms of defining the weakness of prior research studies. In addition, the application of qualitative content analysis would have been more productive in the context of this research.

Implications for Criminal Justice

The researcher identified the relationships between the information needs of DEEs and information source selection and use by DEEs. The researcher also discovered several factors influencing the information behavior of DEEs; he also identified several obstacles DEEs may encounter while they are seeking job-related information. Based on the findings of this study, the researcher made some recommendations for administrators of digital forensic laboratories in Turkey.

- The examiner should be educated about the availability of information sources
- Newly arising information needs of DEEs should be discussed in routine employee meetings

- A separate research and development unit of DEEs should be created, in order to follow new developments in technology and digital forensics. This unit would also be responsible for testing new digital kits and software.
- This R&D unit should also cooperate with engineering departments of leading universities in Turkey, in order to initiate programs to produce domestic tools and software.
- When hiring DEEs, one of the qualifications of the applicant should be proficiency in English
- The budget allocated for DEEs to attend international conferences should be increased
- Police officers should be educated about the procedures of evidence collection

Future Research

As a product of this study, the researcher developed a survey tool for future studies. The researcher adapted the survey instrument created by Pinelli et al. (1993) to the context of digital forensics according to the findings of this study. The variables used in the survey instrument were derived from this study. The adapted survey instrument is presented in Appendix F.

Limitations of the Study

Major limitations of this study resulted from the nature of the research method used in the study. The researcher used a qualitative approach because it fit the purpose of the study; however, qualitative studies have some limitations by default. For example, the sample size is

small in many qualitative studies; therefore, probability samples were not appropriate, or even possible, for the current study. The researcher did not intend to generalize the relationships between the dependent and independent variables from the sample to a larger population. Instead, the researcher intended to understand the information-seeking behavior of DEEs.

Although non-probability samples are helpful in some research situations, like the current one, another important limitation of non-probability sampling is that sampling errors cannot be known. It is impossible to apply the techniques used to estimate sample size to non-probability sampling (Sullivan, 2001).

APPENDIX A

THE INFORMATION SEEKING BEHAVIOR OF DIGITAL EVIDENCE EXAMINERS

Explanation: During this interview, an information source refers to any information source that could assist a digital evidence examiner to achieve the goals of tasks in hand. This information source could be any type of information source such as things, people, internet, written documents, and audio/visual materials.

1. Please describe your work as a digital evidence examiner (or a computer examiner)?
2. Please describe a case that you have completed?
3. What was the objective of achieving that task?
4. Please tell me which steps you needed to go through to complete that case?
    - **Step 1. Collection:** identifying, labeling, recording, and acquiring data from the possible sources of relevant data, while following procedures that preserve the integrity of the data.
    - **Step 2. Examination**: forensically processing collected data using a combination of automated and manual methods, and assessing and extracting data of particular interest, while preserving the integrity of the data.
    - **Step 3. Analysis**: analyzing the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
    - **Step 4. Reporting**: reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process.
5. In Step …
    - Did you have any questions in mind? What were they? What information did you need in step …?
    - What did you try to find out?
    - How did you find the answer to these questions? Did you get any help?
    - Why did you choose to use this way to get the answer?
    - Did you have any difficulties to get the answer? What were they?
    - Did you finally get an answer to your questions? Did it help? How?
    - If you finally could not get an answer to your question? Why it was not helpful?

The above questions are repeated for each of the steps the respondents mentioned.

Questions related to information sources

1. Do you use books? What kind of books do you use?
2. Do you use technical journals? If so, for what purpose do you use them?
3. What is the role of forensic kits and software in providing the information you need?
4. What is role of electronic networks in providing information you need?
5. For what purposes do you use internet?
6. Do you use online databases to obtain information you need?
7. Do you attend conferences?

8. Do you use library or information center in your organization?
9. Do you use your personal contacts and social networks to get the information you need?
10. Compared to each other, which information sources we talked about earlier are more important than others? Why do feel that way?

APPENDIX B

INTERVIEW INSTRUMENT

Cheuk Wai-Yi, Bonnie (2002)

1. Obtain an overview of the respondents' tasks at work

Please describe to me your work as an engineer (or an auditor or an architect)?
Please describe a job that you have completed in your workplace?
What is the objective of achieving that task?

2. Tell me the steps that you need to go through to complete this job?

Task begin -> Step 1 -> 2 -> 3 -> 4 -> 5 -> 6 -> 7 -> … -> End task

3. In [Step 1], …

Do you have any questions in mind? What are they? [gaps: information need]
What do you try to find out?
What situation do you think you are in? [situation]
What do you feel? [affective]
How do you find the answer to these questions? Any help? [bridging the gap]
Why do you choose to use this way to get the answer?
Do you have any difficulties to get the answer? What are they?
Are there ways that you can get the answer, but you chose not to use them?
Did you finally get an answer to your questions? Does it help? How? [help]
How do you handle/deal with these useful answers?
If you finally cannot get an answer to your question? What can't it help?

4. The above questions are repeated for each of the step (i.e. from [step 1] to [End Task]) that the respondents have shared.

APPENDIX C

CODING SCHEME

Numeric Code	Category Level 1 (X._._._)	Category Level 2 (_.X._._)	Category Level 3 (_._.X._)	Category Level 4 (_._._X)
1.	Context			
1.1.		Work		
1.1.1.			Work Characteristics	
1.1.1.1.				Specialization on particular type of crime
1.1.1.2.				Operations on the basis of law and regulations
1.1.1.3.				Challenging due to the hidden, deleted or encrypted data
1.1.1.4.				Requires technical, investigative or linguistic skills
1.1.1.5.				Digital evidence submitted by other units
1.1.1.6.				Requires following certain procedures
1.1.1.7.				Serves in specified jurisdiction
1.1.1.8.				Requires sharing Information
1.1.1.9.				Requires following new innovations
1.2.		Role		
1.2.1.			Role Type	
1.2.1.1				Examiner
1.2.1.2				Expert
1.2.1.3				Researcher
1.2.1.4				Assistant
1.2.1.5				Mentor
1.2.1.6				Marketing Personal
1.3.		Task		
1.3.1.			The scope of task	
1.3.1.1.				To conduct necessary examination
1.3.1.2.				To examine password protected digital media and logs of internet access
1.3.1.3.				To investigate an unauthorized access to a commercial database
1.3.1.4.				To examine computer
1.3.1.5.				To analyze MSN messenger records
1.3.1.6.				To investigate a damaged CD
1.3.1.7.				To determine if the owner of the computer committed the crime
1.3.1.8.				To examine an encrypted hard drive
1.3.2			Type of Crime	
1.3.2.1				Organized Crime
1.3.2.2				Identity Theft
1.3.2.3				Cybercrime
1.3.2.4				Homicide
1.3.2.5				Child Pornography
1.3.2.6				Terrorism
1.3.3.			Type of Evidence	
1.3.3.1.				Hard Drive
1.3.3.2.				Digital Camera
1.3.3.3.				Flash Drive
1.3.3.4.				Computer
1.3.3.5.				CD
1.3.3.6.				DVD
1.3.3.7.				Other digital media
1.4.		Sub-Task1 Collection		
1.4.1.			Participation	
1.4.1.1				Yes
1.4.1.2				No
1.4.2.1.			Information need	
1.4.2.2.				How to fill evidence submission form
1.4.2.3.				Need to legal procedures regarding evidence collection
1.4.2.4.				Need to know how to document evidence collection
1.4.2.5.				Need to know technical protocols & procedures to follow
1.4.3..			Outcome	
1.4.3.1.				Success
1.4.3.2.				Fail
1.4.3.3.				No feedback from client
1.5.		Sub-Task 2 Examination		
1.5.1.			Participation	
1.5.1.1.				Yes
1.5. 1.2				No
1.5. 2.			Information need	

1.5. 2.1.			How to avoid damaging original data
1.5. 2.2.			How to store digital device/media
1.5. 2.3.			How to ship digital device/media
1.5. 2.4.			What procedure to follow during examination
1.5. 2.5.			How to take the device apart
1.5. 2.6.			If there is enough resources: time, storage, human, knowledge, tools kits
1.5. 2.7.			What other accessories or parts are needed to make a proper investigation
1.5. 2.8.			Where to find information about very old and new device
1.5. 2.9.			Where to find information about hacker and their practices
1.5. 2.10.			Where to find information about encryption software
1.5. 2.11.			How particular software works
1.5. 2.12.			The capacity of equipment
1.5. 2.13.			How to operate forensic tools and kits
1.5. 2.14.			How to evaluate situation
1.5.3.		Outcome	
1.5. 3.1.			Success
1.5. 3.2.			Fail
1.5. 3.3.			No feedback
1.6.	Sub-Task 3 Analysis		
1.6.1.		Participation	
1.6. 1.1.			Yes
1.6. 1.2.			No
1.6. 2.		Information need	
1.6. 2.1.			The forensic tools to use in analysis
1.6. 2.2.			How to use analysis tools and software
1.6. 2.3.			The features of analysis tools
1.6. 2.4.			How to define keywords
1.6. 2.5.			Elements of crime: suspect, victim, crime weapon, time and location, type of crime
1.6. 2.6.			Legal definitions of crime
1.6. 2.7.			How to validate the results of analysis
1.6. 2.8.			The procedures to follow according to characteristics of task
1.6. 2.9.			How to determine the digital device contains evidence
1.6. 2.10.			The type of information to look for
1.6. 2.11.			The techniques criminals use to cover their trace
1.6.3.		Outcome	
1.6. 3.1.			Success
1.6. 3.2.			Fail
1.6. 3.3.			No feedback
1.7.	Sub-Task 4 Reporting		
1.7.1.		Participation	
1.7. 1.1.			Yes
1.7. 1.2.			No
1.7.2.		Information need	
1.7. 2.1.			
1.7. 2.2.			The information that must be included in the report
1.7. 2.3.			Skills necessary to write a good report
1.7. 2.4.			How to represent findings in the report
1.7. 2.5.			The technical knowledge of the client
1.7. 2.6.			How to simplify complex procedures of examination
1.7. 2.7.			The sources providing information about writing report
2.8	Source		
2.1	Sub-Task 1 Collection		
2.2.	Sub-Task 2 Examination		
2.2.1.		Books	
2.2.2.		Journal Articles	
2.2.3.		Personal Experience	
2.2.4		Personal knowledge	
2.2.5		Personal notes	
2.26.		Technical Manuals	
2.2.7.		Experts	
2.2.8.		Colleagues	
2.2.9.		Engineers in related fields	
2.2.10.		Forums	

2.2.11.			Internet
2.2.12.			In-service Trainings
2.2.13.			Forensic tools & kits
2.2.14.			Suspects
2.2.15.			Detectives
2.2.16.			Acquaintances of suspect(s)
2.2.17.			Technical services
2.2.18.			Manufacturer
2.3.		Sub-Task 3 Analysis	
2.3.1.			Personal Experience
2.3.2.			Personal knowledge
2.3.3.			In-service trainings
2.3.4.			Experts
2.3.5.			Internet
2.3.6.			Detectives
2.3.7.			Clients
2.3.8.			Investigation file (case file, Statements of suspects and plaintiff)
2.3.9.			Prosecutor
2.3.10.			Standardized submission form
2.3.11.			In-lab manuals
2.3.12.			Forums
2.3.13.			Colleagues
2.4.		Sub-Task 4 Reporting	
2.4.1.			Colleagues inside the field
2.4.2.			Experts
2.4.3.			In-lab manuals and templates
2.4.4.			Colleagues outside the digital forensics
2.4.5.			Previously written report
2.4.6.			Editing software
2.4.7.			Legal documents
2.5.		Source In General	
2.5.1.			Books
2.5.2.			Journals
2.5.3.			Conference
2.5.4.			Forensic Kits And Software
2.5.5.			Online Sources
2.5.6.			Library or Information Center
2.5.7.			Personal contacts
3.	Factor		
3.1.		Situational	
3.1.1.			Availability
3.1.2.			Workload
3.1.3.			Time
3.2.		Perceived	
3.2.1.			Importance
3.2.2.			Relevance
3.2.3.			Availability
3.2.4.			Prior experience with the source
3.2.5.			Easy to communicate
3.2.			Accessibility
3.3.		Organizational	
3.3.1.			Accreditation
3.3.2.			Budget
3.3.			
3.4.		Source Characteristics	
3.4.1.			Type of information
3.4.2.			Practicality /applicability
3.4.3.			Cost
3.4.4.			Availability

3.4.5.			Reliability/scientific	
3.4.6.			Interactive	
3.5.		Task Characteristics		
3.5.1.			Up to date	
3.6.	Barrier			
3.0.0.1.				Separation of digital evidence collection from other stages
3.0.0.2.				Unwillingness to share information due to the bureaucratic or political concerns
3.0.0.3.				Lack of technical knowledge/education in other apparatus of criminal justice
3.0.0.4.				Rapid change in technology
3.0.0.5.				The nature of computer crimes
3.0.0.6.				Lack of reference books in Turkish

APPENDIX D

LETTER OF IRB APPROVAL

UNT
UNIVERSITY OF
NORTH TEXAS
Discover the power of ideas.

OFFICE OF THE VICE PRESIDENT FOR RESEARCH AND ECONOMIC DEVELOPMENT
Research Services

May 25, 2010

Linda Schamber
College of Information
University of North Texas

Re: Human Subjects Application No. 10248

Dear Dr. Schamber:

As permitted by federal law and regulations governing the use of human subjects in research projects (45 CFR 46), the UNT Institutional Review Board has reviewed your proposed project titled "The Information-seeking Behavior of Digital Evidence Examiners." The risks inherent in this research are minimal, and the potential benefits to the subject outweigh those risks. The submitted protocol is hereby approved for the use of human subjects in this study. **Federal Policy 45 CFR 46.109(e) stipulates that IRB approval is for one year only, May 25, 2010 to May 24, 2011.**

Enclosed is the consent document with stamped IRB approval. Please copy and **use this form only** for your study subjects.

It is your responsibility according to U.S. Department of Health and Human Services regulations to submit annual and terminal progress reports to the IRB for this project. The IRB must also review this project prior to any modifications.

Please contact Shelia Bourns, Research Compliance Administrator, or Boyd Herndon, Director of Research Compliance, at extension 3940, if you wish to make changes or need additional information.

Sincerely,

P Kaminski, PhD

Patricia L. Kaminski, Ph.D.
Associate Professor
Chair, Institutional Review Board

PK:sb

1155 Union Circle #305250 | Denton, Texas 76203-5017 | TEL 940.565.3940 | FAX 940.565.4277
TTY 940.369.8652 | research.unt.edu

University of North Texas Institutional Review Board

Consent Notice for Interviewees

Before agreeing to participate in this research study, it is important that you read and understand the following explanation of the purpose, benefits and risks of the study and how it will be conducted.

Title of Study: The Information-Seeking Behavior of Digital Evidence Examiners.

Principal Investigator: Dr. Linda Schamber, University of North Texas (UNT) faculty from Department of Library and Information Sciences.

Purpose of the Study: The purpose of this study is to gain a deep insight into information seeking behavior of digital evidence examiners (DEE). This study looks for answers to the following questions:

1. What circumstances lead DEEs to seek information in their professional life?
2. What are the information sources used by DEEs in their work?
3. What characteristics/factors influence information source selection and information use of DEE?
4. What are the obstacles DEE face while seeking job-related information?

Study Procedures: Participation in this research study is voluntary. Your decision to participate or to withdraw brings no penalty or loss of rights or benefits. Open ended question will be asked during this interview. You may avoid answering any of the questions. The interview questionnaire is composed of two parts and expected to take 45 minutes in total. There are no correct or wrong answers to interview questions. The purpose of the first part of the interview questionnaire is to make time-line interviews and collect data about your work roles, tasks, information needs, and information related barriers between you and the information you needed. Second part aims to obtain data about information sources you use during performing your professional duties. The interview will be audio-taped upon your approval in order to prevent data loose. Then, the interview will be transcribed. A copy of interview transcript will be emailed to you to review. Final interview transcripts approved by you will be used in the data analysis stage.

Foreseeable Risks: No foreseeable risks are involved in this study

Benefits to the Subjects or Others: This study is not expected to be of any direct benefit to you. However, it is expected that studying digital evidence examiners information seeking behavior may be helpful for administrators to utilize information resources efficiently, and better allocation of digital evidence examiners to appropriate tasks.

Procedures for Maintaining Confidentiality of Research Records: No personal identifiable information will be collected and the confidentiality of your individual information (if any) will be maintained in any publications or presentations regarding this study. In the transcripts of the interviews, your name will be coded such as Interviewee A or Interviewee 1. The recorded voice files and the interview transcripts will be maintained separate from each other in safe boxes for the following 3 years. At the end of the three year period, they will be destroyed. You may have a copy of this page for your records.

Questions about the Study: If you have any questions about the study, you may contact Dr. Schamber via email schamber@unt.edu or to Idris Yildirim- idinusa@yahoo.com at telephone number: 001-940-312-8929.

Review for the Protection of Participants: This research study has been reviewed and approved by the UNT Institutional Review Board (IRB). The UNT IRB can be contacted at (940) 565-3940 with any questions regarding the rights of research subjects.

APPROVED BY THE UNT IRB
FROM 5/25/10 TO 5/24/11
KB

1 of 1

APPENDIX E

IDENTIFYING THEMES

J: Bu incelemeciye gore değişir, kişisel olarak benim görev yaptığım birimde soruşturma dosyası ile ilgili delil olarak el konulacak bir bilgisayar veya başkaca metaryal var ise bizzat gider ya olay yerinde imajını alırım yada el koyar iş yerinde getirip imajını alırım, Delil olarak el konulan malzemeler ilk once olay yerinde etiketlenir, olay yerinde el koyma işlemi yapmadan once malzemenin el konulduğu kişinin malzeme üzerine kendisine ait olduğunu belgeleyen imzası alınır, HDD'ye Numara verilir, bu numaralama soruşturma numarası ile birim numarası gibi daha sonradan ayırt etme özelliği olan numaralardır, bunun akabinde, olay yerinde IMAGE alınmış ise HASH değerleri tutanağı yazılır, Malzemeye el konulmuş ise dış etkenlerden hasar görmemesi için delil zarflarına özenle konur delil zarflarının üzeri yazılır Delil incelemesi soruşturmanın türüne gore öncelik sırası gözetilerek yapılır, Misal Kredi Kartı soruşturmasında Keyword, Script çalıştırılması öncelik alırken, bir akaryakıt kaçakçılığı veya Mali Türden yolsuzluk, ihale gibi soruşturma olduğunda kullanılan programlar, oluşturulan office dosyaları ağırlık ve öncelik kazanmaktadır. İncelemeler sırasında delil bütünlüğünün bozulmaması için elde edilen veriler, dosyalar, bulundukları ortamlardan yani IMAGE içerisinde bulundukları durumlarına gore raporlanırlar, dosya bulunduğu ortamdan bir başka ortama kopyalandığında özelliklerindeki değişiklikler dikkate alınarak buna gore hareket edilir. Ülkemizde yasalarda datanın standard incelenmesi ile resmi bir prosedür yok ama suç unsuru olarak tespit edilen bir dosyanın delil olarak değerlendirilmesi için gereken ek bilgiler ve dosya ile ilgili ne,neden, nerede, nasıl, gibi sorulara cevap olacak ek bilgiler mutlaka yazılır.	J: It depends on the examination. Personally, if there is a computer or other material to be examined, I either go to the site myself, or bring it to the lab to save the image of the drive. First, the seized materials as evidence are labeled at the scene. Before making process in collecting of the digital materials, the certificate showing that the materials belong to the owner is signed by the owner. Evidences are numbered with unit numbers, and the number of investigations in other to distinguish later on. Following that, if the image is taken at the scene, HASH values of digital material is written on forms. Seized materials are carefully placed in the evidence envelopes to avoid damage from the external factors. Necessary information is written on the envelope. Evidence examination is conducted according to the type of investigation. We have a list of priority of methods for each case. For example, while keyword search, and script execution are initially done in credit card cases, in the case of fuel-smuggling or the financial crimes, analysis of office documents [word, excel, power point etc.] are done at first. During examinations, in order to keep the integrity of evidence, we work on images digital media. The law doesn't bring a standard about investigation of digital evidence however, some information regarding who, where, what, how is always written in order to legitimate the evidence.	**Comment [W241]:** Context/sub-task/collection/information need: DEE need to know certain procedures that applied in evidence collection **Comment [W242R1]:** Context/sub-task/collection/information need: Documentation: DEE need to know how to document evidence **Comment [W243]:** Contexts/task/task characteristics/type of crime: DEE apply different evidence investigation methods in different type of crime, so they need different technical information. For example: keyword searching, analysis of office documents **Comment [W244]:** Context/work/work characteristics/information need/legal information: DEE need to know the law as they operate in criminal justice system.

APPENDIX F

SURVEY INSTRUMENT FOR FUTURE STUDIES

Section 1: Questions Related to Information Sources

Approximately how often do you use the following **Information Sources** as part of your professional duties?

	Never	**Rarely**	**Sometimes**	**Often**	**Always**
Journal Articles	1	2	3	4	5
Conference Papers	1	2	3	4	5
Audio/Visual Materials	1	2	3	4	5
Technical presentations	1	2	3	4	5
Your Memory	1	2	3	4	5
Technical Manuals (e.g. documents about how to use EnCase)	1	2	3	4	5
Forensic Guides	1	2	3	4	5
Social networks (e.g. online discussion forums, and email groups)	1	2	3	4	5
Supervisors	1	2	3	4	5
Colleagues	1	2	3	4	5
Clients					
Other (please specify) _____	1	2	3	4	5

In terms of performing your present professional duties, **how important** is each of the following **information sources**? (Please rate by choosing an appropriate number from 1=Not at all Important to 5=Very important)

	Not at all Important				Very important
Journal Articles	1	2	3	4	5
Conference Papers	1	2	3	4	5
Audio/Visual Materials	1	2	3	4	5
Technical presentations	1	2	3	4	5
Your Memory	1	2	3	4	5
Technical Manuals (e.g. documents about how to use EnCase)	1	2	3	4	5
Forensic Guides	1	2	3	4	5
Social networks (e.g. online discussion forums, and email groups)	1	2	3	4	5
Supervisors	1	2	3	4	5
Colleagues	1	2	3	4	5
Clients					
Other (please specify)	1	2	3	4	5

Section 2: Questions Related to Written Sources

In this section, we want you to rate **how important a characteristic of a specific written source** is, if you were deciding whether or not to use it in your work.

If you were deciding whether or not to use ***Journal Articles*** in your work, how important would the following factors be? (Please rate by choosing an appropriate number from 1=Not at all Important to 5=Very important)

	Not at all Important				Very Important
Are easy to physically obtain	1	2	3	4	5
Are easy to use or read	1	2	3	4	5
Are inexpensive	1	2	3	4	5
Have good technical quality	1	2	3	4	5
Have comprehensive data and information	1	2	3	4	5
Are relevant to my work	1	2	3	4	5
Can be obtained at a nearby location or source	1	2	3	4	5
Had good prior experience using them	1	2	3	4	5

If you were deciding whether or not to use ***Conference/Meeting Papers*** in your work, how important would the following factors be? (Please rate by choosing an appropriate number from 1=Not at all Important to 5=Very important)

	Not at all Important				Very Important
Are easy to physically obtain	1	2	3	4	5
Are easy to use or read	1	2	3	4	5
Are inexpensive	1	2	3	4	5
Have good technical quality	1	2	3	4	5
Have comprehensive data and information	1	2	3	4	5
Are relevant to my work	1	2	3	4	5
Can be obtained at a nearby location or source	1	2	3	4	5
Had good prior experience using them	1	2	3	4	5

If you were deciding whether or not to use ***Forensic Guides*** (please specify the name of a guide if possible e.g. SWGDE Documents) _____ in your work, how important would the following factors be? (Please rate by choosing an appropriate number from 1=Not at all Important to 5=Very important)

	Not at all Important				Very Important
Are easy to physically obtain	1	2	3	4	5
Are easy to use or read	1	2	3	4	5
Are inexpensive	1	2	3	4	5
Have good technical quality	1	2	3	4	5
Have comprehensive data and information	1	2	3	4	5
Are relevant to my work	1	2	3	4	5
Can be obtained at a nearby location or source	1	2	3	4	5
Had good prior experience using them	1	2	3	4	5

If you were deciding whether or not to use ***Technical Manuals (e.g. documents about how to use EnCase)*** in your work, how important would the following factors be? (Please rate by choosing an appropriate number from 1=Not at all Important to 5=Very important)

	Not at all Important				Very Important
Are easy to physically obtain	1	2	3	4	5
Are easy to use or read	1	2	3	4	5
Are inexpensive	1	2	3	4	5
Have good technical quality	1	2	3	4	5
Have comprehensive data and information	1	2	3	4	5
Are relevant to my work	1	2	3	4	5
Can be obtained at a nearby location or source	1	2	3	4	5
Had good prior experience using them	1	2	3	4	5

Section 3: Questions Related to Job-Related Tasks

In this section, we would like understand **how task characteristics** affect your **use of information sources**.

Think about the most important job-related project, task or problem you have completed during the past 6 months. Which category best describes this work? (Check **ONLY ONE** box)

Educational (For example, professional development or preparation of a lecture)

Collection (That is, identifying, labeling, recording, and acquiring digital evidence)

Examination (That is, forensically processing collected digital evidence using a combination of automated and manual methods)

Analysis (That is, analyzing the results of the examination, using legally justifiable methods and techniques)

Reporting (That is, reporting the results of the analysis, describing the actions taken, explaining how tools and procedures were selected)

Management (For example, planning, budgeting, and managing the digital evidence examination process

Other (Please Specify)_____

How would you describe the overall complexity of the project, task or problem you categorized in Question 8? (Please circle a number).

Very Simple 1 2 3 4 5 Very Complex

How would you rate the amount of uncertainty that you felt when you started the project, task or problem you categorized in Question 8? (Please circle a number).

Little Uncertainty 1 2 3 4 5 Great Uncertainty

What steps did you follow to get the information you needed for this project, task or problem? [Please rank these items (e.g. #1, #2, #3 and so forth) and put an X beside the steps you didn't use.]

____ Used my personal store of information, including sources I keep in my office, or I carry with me.
____ Spoke with coworkers or people inside my organization
____ Spoke with colleagues or people outside my organization
____ Spoke with a librarian or information specialist
____ Searched (or had someone search for me) an electronic (bibliographic) database in the library
____ Used literature resources (e.g., manuals for digital evidence processes) found in my organization's/laboratory's library

If you used none of the above steps, please check: _____

Which one of the following best describes the kind of duties you performed while working on the project, task or problem you categorized in Question 8?

Digital/Computer Evidence Examining
Science
Management
Other (Please specify)_____

Section 4: Demographics

What is your gender?

1 Male 2 Female

What is your age? _____

What is the highest level of education you completed, and your major? (Check one number)

No College degree
Bachelor's in _____
Master's in _____
Doctoral in _____
Other (please specify) _____in _____

How many years of experience do you have in digital forensic services?

Number of years: _____

REFERENCES

Allen, T. J. (1977). *Managing the flow of technology transfer and the dissemination of technological information within the organization*. Cambridge, MA: MIT Press,.

Allen, T. J. & Gerstberger, P. T. (1967). *Criteria for selection of an information source*. Cambridge, Massachusetts: M T.

Anderson, C. J., Glassman, M., McAfee R. B., & Pinelli, T. (2001). An investigation of factors affecting how engineers and scientists seek information. *Journal of Engineering and Technology Management*, *18*, 131-155.

Barbara, J. J. (2005). Digital evidence accreditation in the corporate and business environment. *Digital Investigation, 2*(2), 137-146.

Barry, C. L. (1993). *The identification of user relevance criteria and document characteristics: Beyond the topical approach to information retrieval* (Unpublished doctoral dissertation). Syracuse University, Syracuse, NY.

Barry, C. L. (1994). User-defined relevance criteria: an exploratory study. *Journal of the American Society for Information Science*, *45*(3), 149-159.

Barry, C., & Schamber, L. (1998). Users' criteria for relevance evaluation: A cross-situational comparison. *Information Processing and Management, 34*(2/3), 219-236.

Bates, M. J. (2002). Towards an integrated model of information seeking and searching. *New Review of Information Behavior Research*, *3*, 1-15.

Bateson, G. (1972). Steps to an ecology of mind. New York: Ballantine.

Bell, S. (2008). *Encyclopedia of forensic science*. New York, NY: Facts On File.

Berg, B. L. (2001). *Qualitative research methods for the social sciences.* Boston: Allynand Bacon.

Brown, J. W., & Utterback, J. M. (1985). Uncertainty and technical communication patterns. *Management Science, 31*, 301–311.

Bryman, A. (1984). The debate about quantitative and qualitative research: A question of method or epistemology? *The British Journal of Sociology*, *35*(1), 75-92.

Byström, K. (1996). The use of external and internal information sources in relation to task complexity in a journalistic setting. In Ingwersen, P. & Pors, N.O. (Eds.), *Information science: integration in perspective* (pp. 325-341). Copenhagen: The Royal School of Librarianship.

Byström, K. (1999). *Task complexity, information types and information sources: examination of relationships*. (Doctoral dissertation). Acta Universitasis Tamperensis ser. A Vol. 688. Tampere, Finland: University of Tampere. Electronic version available at http://www.hb.se/bhs/personal/katriina/kbm.htm

Byström, K. (2002). Information and information sources in tasks of varying complexity. *Journal of the American Society for Information Science and Technology, 53*(7), 581-591.

Byström, K. (2007). Approaches to "task" in contemporary information studies. *Information Research, 12*(4) paper colis26. Retrieved from http://InformationR.net/ir/12-1/colis/colis26.html]

Byström, K., & Järvelin, K. (1995). Task complexity affects information seeking and use. *Information Processing & Management, 31*(2), 191-213.

Case, D. (2007). *Looking for information: A survey of research on information seeking, needs, and behavior*. Second edition. New York: Academic Press/Elsevier Science.

Coopman, R. (2008) Local law enforcement and its digital forensics future. Retrieved from http://libcat.post.ca.gov/dbtw-wpd/documents/cc/42-Coopman.pdf

Courtright, C. (2007). Context in information behavior research. *Annual Review of Information Science and Technology, 41*, 273-306.

Davies, D., & Dodd, J. (2002). Qualitative research and the question of rigor. *Qualitative Health Research, 12*(2), 279-289.

Dervin, B. (1983). An overview of sense-making research: Concepts, methods and results. Paper presented at the annual meeting of the International Communication Association. Dallas, TX.

Dervin, B. (1992). From the mind's eye of the user: The Sense-Making qualitative-quantitative methodology. In J. D. Glazier & R. R. Powell (Eds.), *Qualitative research in information management* (pp. 61-84). Englewood, CO: Libraries Unlimited.

Dervin, B. (1999). On studying information seeking methodologically: The implications of connecting meta-theory to method. *Information Processing and Management, 35*, 727-750.

Dervin, B. (2003). From the mind's eye of the user: The sense-making qualitative-quantitative methodology. In B. Dervin & L. Foreman-Wernet (Eds.), *Sense-Making Methodology Reader* (pp. 269-292). Cresskill, NJ: Hampton Press Inc.

Digital Forensics Research Workshop (2001). A road map for digital forensics. Retrieved August 2, 2008, from *Research,* http://www.dfrws.org/2001/dfrws-rm-final.pdf.

Eckert, W. G. (1997). Historical development of forensic sciences. In W. G. Eckert (Ed.) *Introduction to forensic sciences*, 2nd Edition. CRC Press: New York.

Ellis, D. (1989). A behavioral model for information retrieval system design. *Journal of Information Science, 15*, 237-247.

Ellis, D., Cox, D., & Hall, K. (1993). A comparison of the information seeking patterns of researchers in the physical and social sciences. *Journal of Documentation, 49*(4), 356-369.

Fidel, R., & Green, M. (2004). The many faces of accessibility: engineers' perception of information sources. *Information Processing & Management, 40*, 563-581.

Forensic (2010). In Merriam-Webster online dictionary. Retrieved April 15, 2010, from http://www.merriam-webster.com/dictionary/forensic

Franklin, C. J. (2006). *The investigator's guide to computer crime*. Location?: Charles C Thomas Publisher, Limited.

Gerstberger, P. G., & Allen, T. J. (1968). Criteria used by research and development engineers in the selection of an information source. *Journal of Applied Psychology, 52*(4), 272-279.

Gerstenfeld, A., & Berger, P. (1980). An analysis of utilization differences for scientific and technical information. *Management Science, 26*(2), 165-179.

Global Mobile Suppliers Association (2009). GSM/3G Stats. Retrieved August 19, 2009, from http://www.gsacom.com/news/statistics.php4

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, 8 (4), December 2003, 597-607. Retrieved from http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf

Gorman, G. E., & Clayton, P. (2005) *Qualitative research for the information professional*. 2nd ed. London: Facet.

Hall, G. A., & Davis, W. P. (2005). Toward defining the intersection of forensics and information technology. *International Journal of Digital Evidence, 4*(1). Retrieved August 10, 2009, from http://www.utica.edu/academic/institutes/ecii/publications/articles/B49F0174-F1FB-FE05-EBBB4A8C87785039.pdf

Harter. S. P., & Hert, C. A. (1997). Evaluation of information retrieval systems, *Annual Review of Science and Technology, 32*, 3-94.

Hertzum, M., & Pejtersen, A. M. (2000). The information-seeking practices of engineers: Searching for documents as well as for people. *Information Processing & Management, 36*, 761–778.

Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277-1288.

Institution of Information Technologies and Communication of Turkey, (2010). Üç Aylık Pazar Verileri Raporu. Retrieved from http://www.btk.gov.tr/Yayin/pv/ucaylik10_1.pdf

Joppe, M. (2000). *The research process.* Retrieved February 25, 1998, from http://www.ryerson.ca/~mjoppe/rp.htm

Julien, H., & Duggan L. J. (2000). A longitudinal analysis of the information needs and uses literature. *Library & Information Science Research, 22*(3), 291-309.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006), Guide to integrating forensics techniques into incident response, *National Institute of Standards and Technology (NIST)* Special Publication (SP) 800-86, NIST, Computer Security Division, Information Technology Laboratory, Gaithersburg, MD. http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

King, G., Keohane, R. O., and Verba, S. (1994). *Designing social inquiry*. Princeton: Princeton University Press.

Krikelas, J. (1983). Information seeking behavior: Patterns and concepts. *Drexel Library Quarterly, 19*, 5-20.

Krippendorf, K. 1980. *Content analysis: An introduction to its methodology*. Beverly Hills, CA: Sage.

Kuhlthau, C. C. (1991). Inside the search process: Information seeking from the user's perspective. *Journal of the American Society for Information Science, 42*(5), 361-371.

Kuhlthau, C. C. (1993). *Seeking meaning: A process approach to library and information services.* Norwood, NJ: Ablex.

Kwasitsu, L. (2003). Information-seeking behavior of design, process, and manufacturing engineers. *Library & Information Science Research. 25*, 459-476.

Leckie, G. J., Pettigrew, K. E., & Sylvain, C. (1996). Modeling the information-seeking of professionals: A general model derived from research on engineers, health care professionals, and lawyers. *Library Quarterly, 66*(2): 161-193.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry*. Beverly Hills, CA: Sage Publications.

Marcella, A. Jr., & Menendez, D. (2008). Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes, 2nd Ed. Boca Raton, FL: Auerbach Publications.

Mayring, P. (2000). Qualitative content analysis. *Forum: Qualitative Social Research, 1*(2). Retrieved July 28, 2008, from http://217.160.35.246/fqs-texte/2-00/2-00mayring-e.pdf.

Mick, C. K., Lindsey, G. N., & Callahan, D. (1980). Toward usable user studies. *Journal of the American Society for Information Science, 31*(5), 347-365.

Miles, M., & Huberman, A. M. (1994). *Qualitative data analysis*. Thousand Oaks, CA: Sage Publications.

Minichiello, V., Aroni, R., Timewell, E., & Alexander, L. (1990). *In-depth interviewing:Researching people*. Hong Kong: Longman Cheshire.

Neuendorf, K. A. (2002). *The content analysis guidebook*. Thousand Oaks, CA: Sage Publications.

Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and examining computer forensic evidence [on-line]. *Forensic Science Communications, 2*(4). Retrieved from http://www.fbi.gov.hq/lab/fsc/backissu/oct2000/computer.htm.

NY Daily News (2009). 'Craigslist killer' Michael John Anderson gets life in murder of Katherine Olson. Retrieved August 1, 2009, from http://www.nydailynews.com/news/national/2009/04/02/2009-0402_craigslist_killer_michael_john_anderson_.html#ixzz0dTDMq06j

O'Reilly, C. A. (1982). Variations in decision makers' use of information sources: the impact of quality and accessibility of information. *Academy of Management Journal 25*, 756–771.

Osterburg, J., & Ward, R. (2000). *Criminal investigation*. Cincinnati, OH: Anderson.

Patton, M. Q. (2002). *Qualitative research and evaluation methods.* Thousand Oaks, CA: Sage.

Pettigrew, K. E., Fidel, R., & Bruce, H. (2001). Conceptual frameworks in information behavior. *Annual Review of Information Science and Technology*, *35*, 43-78.

Pinelli, T. E., Bishop, A. P., Barclay, R. O., & Kennedy, J. M. (1993). The information-seeking behavior of engineers. In A. Kent, & C. M. Hall, *Encyclopedia of library and information science*, *52* 167-201. New York: Marcel Dekker.

Pollitt, M. M. (2007) *An ad hoc review of digital forensic models*. Second International Workshop on Systematic Approaches to Digital Forensic Engineering. 43-54.

Rasmussen, J., Pejtersen, A. M., & Goodstein, L. P. (1994). *Cognitive systems engineering*. New York: Wiley.

RCFL Annual Report Fiscal Year 2003. (2003). Retrieved August 1, 2010, from http://www.rcfl.gov/downloads/documents/RCFL_Nat_Annual.pdf

RCFL Annual Report Fiscal Year 2004. (2004). Retrieved August 1, 2010, from http://www.rcfl.gov/downloads/documents/RCFL_Nat_Annual04.pdf

RCFL Annual Report Fiscal Year 2005. (2005). Retrieved August 1, 2010, from http://www.rcfl.gov/downloads/documents/RCFL_Nat_Annual05.pdf

RCFL Annual Report Fiscal Year 2006. (2006). Retrieved August 1, 2010, from http://www.rcfl.gov/downloads/documents/RCFL_Nat_Annual06.pdf

RCFL Annual Report Fiscal Year 2007. (2007). Retrieved August 1, 2010, from http://www.rcfl.gov/downloads/documents/RCFL_Nat_Annual07.pdf

RCFL Annual Report Fiscal Year 2008. (2008). Retrieved August 1, 2010, from http://www.rcfl.gov/downloads/documents/RCFL_Nat_Annual08.pdf

Ramsland, K. (2001). *The forensic science of C.S.I*. NY: Berkeley,CA: Boulevard Books.

Schamber, L. (1991). *Users' criteria for evaluation in a multimedia environment*. In J.-M. Griffitbs (Ed.) Proceedings of the 54th Annual Meeting of the American Society for Information Science, 28, 126-133. Medford, N J: Learned Information.

Schamber, L. (1994). Relevance and information behavior. In M. E. Williams (Ed.) *Annual Review of Information Science and Technology, 29,* 33-48. Medford, N J: Learned Information.

Schamber L. (2000). Time-line interviews and inductive content analysis: Their effectiveness for exploring cognitive behaviors. *Journal of American Society for Information Science, 51*(8), 734–44.

Schement, J. R. (1993). Communication and information. In J. R. Schement & B. Ruben (Eds.), *Information behavior*. (Vol. 4, pp. 3-33). New Brunswick, NJ: Transaction Publishers.

Scientific Working Group on Digital Evidence and International Organization on Digital Evidence & International Organization on Digital Evidence. (2000). Digital evidence: Standards and principles forensic science communications (2)(2), Retrieved from http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

Seale, C. (1999). Quality in qualitative research. *Qualitative Inquiry, 5*(4), 465-478.

Stenbacka, C. (2001). Qualitative research requires quality concepts of its own. *Management Decision, 39*(7), 551-555.

Sullivan, T. J. (2001). *Methods of social research*. Orlando,FL.: Publisher.

Vakkari, P. (2003). Task-based information searching. *Annual Review of Information Science and Technology (ARIST), 37*, 413–466.

Wai-Yi, B. C. (2002). *Using Sense-making to study information seeking and use in the workplace*. Retrieved from http://communication.sbs.ohio-state.edu/sense-making/inst/instcheuk02workplace.html.

Weber, R. P. (1990). *Basic content analysis*. Newbury Park, CA: Sage Publications.

Wersig, G., & Neveling, U. (1975). The phenomena of interest of information science. *Information Scientist, 9*, 127-140.

Whitcomb, C. M. (2002) An historical perspective of digital evidence:A forensic scientist's view. *International Journal of Digital Evidence, 1*(1), pp.

Wilson, T. D. (1981). On user studies and information needs. *Journal of Documentation*, 37(1), 3-15.

Wilson, T. D. (1994). Information needs and uses: Fifty years of progress? In B. Vickery (Ed.), *Fifty years of information progress: A journal of documentation review*. (pp. 15-51). London: Aslib.

Wilson, T. D. (1996). Information behavior: An interdisciplinary perspective. *Information Processing and Management, 33*(4), 551-572.

Wilson, T.D. (1999). Models in information behavior research. *Journal of Documentation, 55*(3), 249-270.

Wilson, T. D. (2000). Human information behavior. *Informing Science, 3*(2), 49-55.