3-12-2007

ID Theft: A computer forensics' investigation framework

Olga Angelopoulou
University of Glamorgan

DOI: 10.4225/75/57ad41987ff2b
5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2007.

ID Theft: A Computer Forensics' Investigation Framework

Olga Angelopoulou
University of Glamorgan
oangelop@glam.ac.uk

Abstract

The exposure of online identities grows rapidly nowadays and so does the threat of having even more impersonated identities. Internet users provide their private information on multiple web-based agents for a number of reasons, online shopping, memberships, social networking, and many others. However, the number of ID Theft victims grows as well, resulting to the growth of the number of incidents that require computer forensics investigation in order to resolve this type of crime. For this reason, it appears of value to provide a systematic approach for the computer forensics investigators aiming to resolve such type of computer based ID Theft incidents. The issues that demand individual examinations of this type of crime are discussed and the plan of an ID Theft computer forensics investigation framework is presented.

Keywords

ID theft, incident investigation, digital evidence, computer forensics, computer crime, computer forensic investigator

INTRODUCTION

According to the Credit Industry Fraud Avoidance System (CIFAS) (2007), the UK's Fraud Prevention Service, in 2006 alone 80000 cases of ID Theft were recorded, comparing to 9000 cases in 1999. It appears as the wide use and the anonymity occurring on the Internet has influenced a number of people proceeding to Internet related, non-legitimate actions.

This is a global problem. ID Theft is considered as a standalone crime since 1998 in the United States as defined in the Identity Theft and Assumption Deterrence Act (1998) and belongs to federal crimes, where the establishment of the Offence is made as follows:

> *"knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."*

In the H. R. 2622, Fair and Accurate Credit Transactions Act of 2003, the American Identity Theft legislation provides the state approach of combating ID Theft and protecting the consumers. Based on the U.S. Federal Trade Commission's (FTC) report for National and State Trends in Fraud and Identity Theft 2004, of the 635,173 complaints received, 246,570 were ID Theft reports. The most common form of reported ID Theft was Credit Card fraud, followed by phone or utilities fraud, bank and employment fraud. It is very important to note that only 30% of victims notified a police department. It can therefore be assumed that the majority of people are either not aware that they could have contacted law enforcement agencies or prefer not to make their ID theft incident known.

In plain words, the intention and plan of the person who decides to steal someone's identity, the ID Thief, is to collect the more personal details the possible for the person he's interested in, attempt to use this information for the largest personal gain of his and finally continue his life under someone else's name. It seems that the popular saying 'there is no perfect crime' is not taken seriously from some individuals. However, the world's history has proved that no matter the precautions and strategies followed to combat a crime regardless its nature, the fraudsters will discover a way to conduct it. Under no circumstances should people give up the effort of eliminating a type of crime, nevertheless there should be also invented radical and innovative ways of discovering and uncovering evidence of those already taken place.

Based on the above unfolds the rationale of this paper presenting a piece of under development work. The first aim is to provide some insight of the basic terms, ID Theft and Digital Evidence and their sequence in order to lead to the successful computer forensics investigation. The issues concerning the importance of such an individual approach of ID Theft incidents towards Computer Crime are discussed; the design of the proposed ID Theft Investigation Framework is presented and defended by an example.

ID THEFT AND THE DIGITAL EVIDENCE

The fraudulent use of another's personal details has become an increasingly significant concern. One out of ten people in Britain was a victim of online fraud during 2006 revealed a survey, corresponding to 3.5 million British internet users (unknown, 2007). Attacks on financial institutions have risen from 39% in 2003 to 83% for 2004 (McKenna, 2004).

The Home Office (2006) defines Identity Theft as:

> *"Criminals can find out your personal details and use them to open bank accounts and get credit cards, loans, state benefits and documents such as passports and driving licenses in your name."*

Identity theft (ID Theft) can be perpetrated in a number of ways. Discarded documents containing personal details can provide a rich source of personal information. Simple forms of deception can also be used to extract the information from the victim an example would be an attacker poses as a legitimate government official or business person collecting personal data door to door. Other methods include the so called 'brute force' techniques such as the stealing of wallets and purses containing identification and credit and bank cards or the removal of personal documents during a burglary. In particular stolen mail, where the perpetrator may have access to bank and credit card statements, pre-approved credit offers, checks and tax information, can be used to gather information for an ID Theft. This may be followed up by social engineering. The perpetrator contacts the person who has lost his card claiming that they found it, asks for personal details and then uses this information fraudulently (Dwan, 2004).

However, personal identity is increasingly being stored and used in a range of digital forms. This can leave individuals exposed to possible threats as a result. Examples include; Phishing e-mails, web spoofing and numerous other techniques. This emerging and developing trend in crime can result in complex investigations that involve information technology, both as a medium for analysis and as evidence at the same time. Fraudsters are obtaining more sophisticated technological ways and manage to conceal their crimes.

The following table summarises all different methods by which ID Theft is performed, separated in offline and online:

Offline Techniques	Online Techniques
Stolen wallets or bags	Phishing
Stolen mail	Pharming
Deceased people	Web-Spoofing
Dumpster diving	Social Engineering
Burglars	Card Cloning
Shoulder surfing	Storage Devices and Media
Social Engineering	Biometrics
	Malicious Software
	Key-loggers
	CCTV Cameras
	Data Retrieval

Table 1: Summary of offline and online ID Theft Techniques

Digital evidence is any kind of digitally processed information that is stored in any sort of digital media. The data strengthens or neglects the assumption of an electronic crime in the terms of the investigation process. It can be therefore presented as supportive proof in a court of law. (Carrier B., 2006)

In the late 20th century Dr.Edmund Locard, director of Lyons Institute of Forensic Medicine, defined an important theorem for the foundation of the forensic science that is widely known as the *Locard Exchange Principle*:

> *"Any action of an* individual, *and obviously, the violent action constituting a crime, cannot occur without leaving a mark. What is admirable is the variety of these marks. Sometimes they will be prints, sometimes simple traces, and sometimes stains"* (Chisum W., J.,and Turvey B.E. (2006) from Locard, 1934).

The theorem has been transformed and misinterpreted during the years aiming to cover the science needs (Chisum, Tervey, 2006). The simplest form that can be found in literature is "*with contact between two items,*

there will be an exchange" (Thornton, 1997). Casey (2003) has noted that this fact holds true in the digital world as a digital exchange between two devices results in an exchange of information. For example a request to view a web page from a client may be logged on the server and the web page, if downloaded, may then reside temporarily on the client.

As stated from Marcella and Greenfield (2002), computer forensics demands accurate evidence and results of the investigation. For this reason, the use of state of the art equipment and methods should be used in order to reassure it. The world of Computer Forensics is dealing with a number of situations from industrial espionage to damage assessment and holds back to the beginning of the 1980s. Nevertheless, the last few years have made it widely known to the public and demand even more expertise. It is by nature a science that requires detail by all means and there is where the handling of the digital evidence should be based.

THE "SOLITARY" OF ID THEFT TOWARDS COMPUTER CRIME INCIDENTS

Initially, it is worth mentioning some issues concerning computer crime in general. Those types of crime where a computer or any other electronic device is involved in order to perform the crime or as the target of it are considered as computer crimes (Postnote Computer Crime, 2006). The criminals become more and more sophisticated nowadays and attempt to use technology by any means in order to avoid detection and perform the crime in greater detail and excess deception. A simple glance on news articles enhances the anxiety to information security people and the need to eliminate the problem. However, this could only happen on a virtual world as the use of computers and online transactions becomes only wider, giving the fraudsters' the chance to increase their ways of attacking systems.

Computer crime involves different types of offences as hacking, copyright, child pornography, fraud, viruses, and harassment. They can be categorised in different ways, according to the methods used in order to prevent them. Icove et al. (1995) in Computer Crime classify them with this approach, grouping them in:

- Physical security breaches
- Personnel security breaches
- Communications and data security breaches
- Operations security breaches

Each security breach involves several fraudster actions that lead to computer crime. Hence, computer crime as a general matter can be treated based on the facts and the incidents that surround it. This basically requires treating computer crimes independently, in order to achieve a more analytical and in depth examination of a case. The investigation process time will be accelerated as the investigator will be able to follow specific steps once the type of the crime is revealed and he will be able to track on a certain process.

Concerning the current research, the digital investigation of computer based ID Theft is a computer crime that requires the expertise of a computer forensic investigator in order to be resolved. The digital evidence that comes into sight after the analysis of a related to crime computer misuse is of critical value as it should be efficient to accuse someone with a crime or not. Therefore, the manipulation of the evidential data should be treated sensibly and with sensitivity.

As described in a number of existing published sources, ID Theft is besides considered as a major threat for individuals and corporations and consists of multiple types of crime. It involves multiple ways of achieving it, either by the aid of technology or not. This is the major difference from other types of computer crime and the way the digital evidence should be treated.

In view of this influence, for the function of science, it could be considered that all technology aided evidential elements will be represented with the term 'online', whereas all non-technology aided will be called 'offline'. Consequently, the investigator has to take into consideration the volume of the offline sources that influence the outcome of the investigation, as a number of offline techniques could have been used to commit the crime. A characteristic example of this issue could be the offence of hacking. In such a case, the actual evidence will be hidden inside the suspect's computer, as the hacker's only weapon is that; and the assigned to the incident investigator will have to trace all evidential data from there. At the same time, in a computer-based ID Theft incident the investigator's findings depend on the fraudster's computer, in addition other sources, such as a card cloning machine and forged documents could enhance the evidence. However, this is not the purpose of the computer forensics investigator, but still differentiates this type of crime from any other computer related and raises the need of treating this type of computer crime in an individual manner.

Based on FTC's Identity Theft Data Clearinghouse (2007), ID Theft was established as the top complaint category in consumer fraud with 36 percent. Therefore, in order to support the need of treating a computer crime as an independent entity, an example of an ID Theft case for financial purposes can be considered, where the

investigator can first focus on credit history, transactions made on the victim's name, applications for bank accounts, loans and credit cards. This evidence trail is to be recovered in the form of data, logs etc. formats through various systems within one or even multiple financial organisations. As a result, the investigation is complicated and time-consuming. With identity-related ID Theft cases, the investigator will need to consider not only the financial evidence but the personal information gained, subsequent actions triggered by a hijacked identity etc.

The difficulty the investigators need to face when dealing with an ID Theft incident and what really makes this type of crime individually-treated is that they actually have to face two investigative categories; victim or perpetrator. This is where all starts, as the need to distinguish and separate the investigation process is going to differentiate such a detailed process from others. A victim's machine should provide such evidential data that will be able to prove the fraud against the computer user, while on the perpetrator's machine the evidential data should be treated in such a way that will reveal the deception's proof. One might argue that the existing computer forensic investigation frameworks can cover this argument. However, a generic guideline cannot reach to a far detailed phase of the investigative process as it aims to cover all different types of computer related crimes. In respect to the existing computer forensic frameworks and based on the substantial increment of ID Theft the need to aid the computer forensic investigation of this type of crime leads to the point that the investigation process needs to be focused on a different perspective each time as different sort of evidence is required.

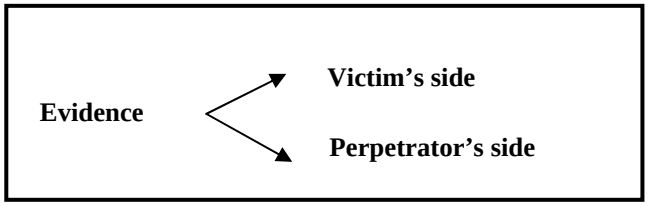


Figure 1: The different aspects of evidence concerning ID Theft incidents

People who work at this field need to be able to use constructive methods in order to facilitate their actual aim that is to provide evidential data after a computer forensic investigation. The threat of becoming an ID Theft victim becomes even greater day by day for everyone, especially those who use the Internet by any mean, make transactions, socialize, interact, anything that someone could take part on through it. Simply because the use of Internet and the public dependency will only grow, there should be invented and developed efficient ways that could cope with this *rapidly spreading threat*.

The following sections are going to support the above arguments on a practical approach, describing the theoretical procedure of designing and implementing such a computer forensics investigation framework.

DESIGN DESCRIPTION

There is the need at this stage to describe 'why' and 'how' the foundation of this work is set. For this reason, the following paragraphs are going to set the principles of this work.

The fact is that in order to accomplish a comprehensive and structured investigation about a computer forensic case, the steps followed should be of extreme diligence. The procedure that is followed should give an answer to the question of what information might be stolen and how this information could be stolen. The major aim is to collect the data that give evidence and can prove a possible attack. Only after a detailed and constructed approach the data analysis can return and verify the only premise that might appear in the beginning of the research; that the investigator has to deal with an ID Theft case.

Fundamentally, a framework is considered as **tool to aid in planning, monitoring and evaluation of research projects** (Carrier, 2006). The general investigation scientific method presented by Carrier and Spafford at the DFRWS 2006 though, structures a checklist of high-level phases on a theoretical foundation in order to propose and describe a procedure in a digital investigation research field. The phases have been applied on existing frameworks and demonstrate an accurate approach to the specific area of research. These include:

- Observation, where the researcher needs to observe the field in order to create a clear picture about the processes and the activities that take place on the investigation.
- Hypothesis Formulation, where the researcher focuses on the results of the observation phase and is able to categorise the techniques that will aid the analysis of the findings.

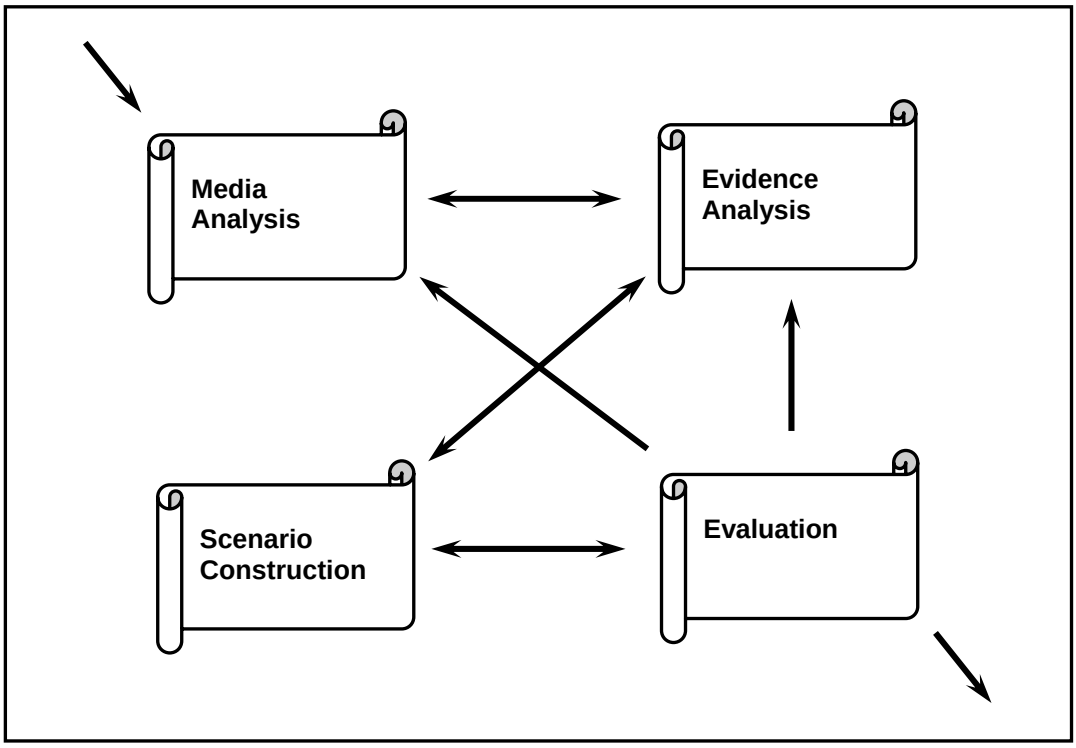
- Prediction, this phase will support the Hypothesis Formulation as the results of this part will prove whether or not the Hypothesis is formed on a constructed basis and will lead the researcher to the last phase.
- Testing and Searching, where the tests and experiments that take place on a generally approved manner will probably result to new predictions and evaluate the Hypothesis the researcher has set.

The procedure described should give answers to questions for the existence of an **x** file to a **y** event and should be responded accurately only after a successful analysis of the data. The investigator should be able to have access and examine each one of them, every file and any event that influences the file's behaviour.

ID THEFT INVESTIGATION FRAMEWORK DESIGN

For the ID Theft Investigation Framework the research of the existing literature has revealed that the most suitable approach would be first to identify and define the phases that will lead the researcher to the appropriate procedures, based on the model described above and consequently the implementation of a conceptual framework that will aid the forensic investigator. The idea is based on the concept of handing over the procedure on a fundamental basis. This way the process will correspond to any possible procedure during the investigation. The presented process is adjusted to the needs that an ID Theft incident investigation requires as it is going to be analysed on the following chapter. The phases at the first level of the process follow a generic pattern. However, in the advance of the process the model will reveal the second level phases that contain the processes of the framework and the third level phases, including the activities that tae place. Every Phase is influenced by the inputs and the outputs (I/Os) that resign it.

Therefore, the study should be distinguished in four phases, where every phase represents a major procedure throughout the ID Theft investigation lifecycle. The impact on every phase is featured from all influential actions taken place on each phase. This states the first level of the framework's formulation.



Graph 1: First Level Investigation Process Phases

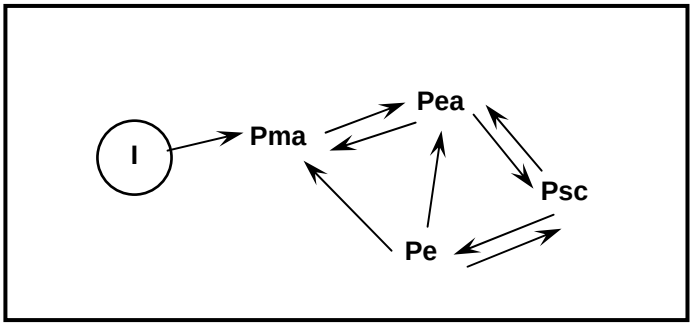
According to the procedure that is proposed to guide the researcher in order to formulate the investigation process, the above graph outlines the first level of it. There is always one start and one end point concerning the investigation. The forensic analyst needs to begin under a concrete method and finish so. Hence, the Media Analysis (Observation) is the phase that appears of extreme importance in order to provide the data that will prolong to the Evidence Analysis (Hypothesis Formulation). The findings of the disk analysis will move forwards to the analysis and the decision whether this evidence can stand as accurate to the Scenario Construction (Prediction), where it is going to validate or not the Evidence Analysis. However, the analyst should always be able to return from the Evidence Analysis to the Media Analysis for any further data that

might appear of value during the examination of the media, as well as he should always be able to revisit the Evidence Analysis at any stage in the Scenario Construction for any information that could emerge and indicate further investigation. Then, the Scenario Construction will need to be evaluated in order to prove its validation that is going to direct to the end of the process. However, the Evaluation phase requires the possibility to recall any of the previous phases of the investigation process in order to prove the objectivity of the research outcome. The following table sets the Variable Names at this Phase of the process in order to be used during this level of the procedure.

First Level Investigation Process Variable Names	
Description	**Variable**
Incident Investigation	I
Media Analysis	Pma
Evidence Analysis	Pea
Scenario Construction	Psc
Evaluation	Pe

Table 2: First Level Investigation Process Variable Names

A graphical representation demonstrates the process that is proposed to be followed from the ID Theft Investigation Framework concerning an Incident.

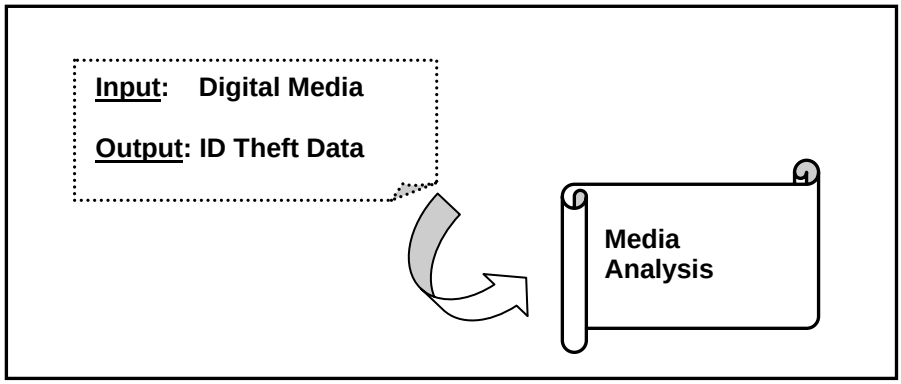


Graph 2: Incident Investigation Process Lifecycle

Every phase at this level of the investigation process needs to respond to an input and an output (I/O) practice. This provides the necessity of defining the processes and the activities that will be set for the further analysis of this research. The I/Os support the general process in the terms of continuity during the investigation's lifecycle. Below, there is a graphical representation of every phase in correspondence with the First Level I/Os that manipulate it. Every phase of the process requires as an input the output of the preceding phase for supporting the coherence of the research outcome.

Media Analysis

The Pma requires as an input any type of Digital storage Media that could give as an output possible ID Theft data in order for the further investigation to take place. At this point the term Digital Media is going to represent any type of computer storage device.



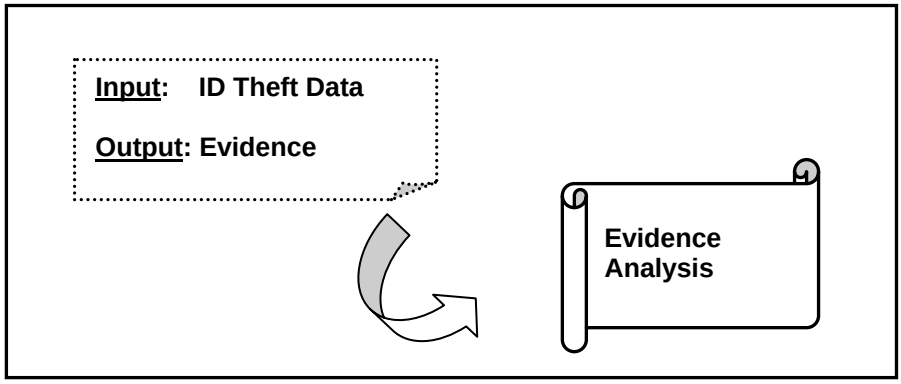
Graph 3: Phase 1 - Media Analysis I/Os

Possible Digital storage media	
Computer / Laptop / Server Hard Disk	PCMCIA cards
External Hard Disk	Memory Cards
Mobile Phone / SIM Card	USB Memory Stick
Raid Hard Disks	PDA
Tape Back-ups	Floppy Disk
CD / DVD	

Table 3: Possible Digital storage Media

Evidence Analysis

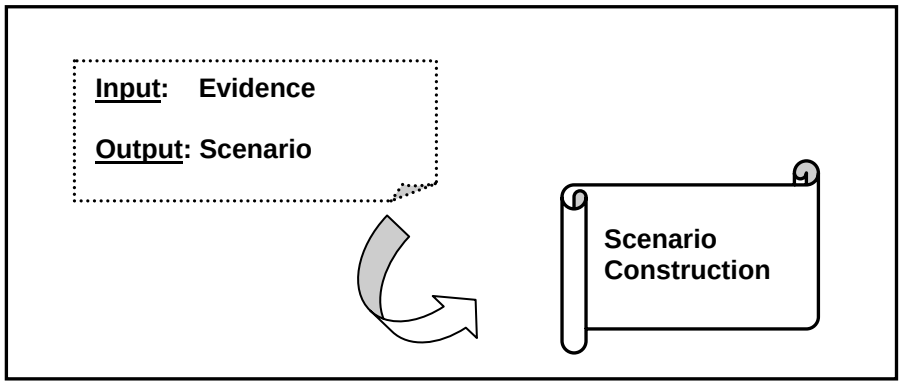
The Pea takes as input the possible ID Theft data provided by the Pma and will try to convert it to Evidence. At any time during an investigation further data may significantly come into view and the analyst will return to the previous phase for the analysis of the Digital Media.



Graph 4: Phase 2 - Evidence Analysis I/Os

Scenario Construction

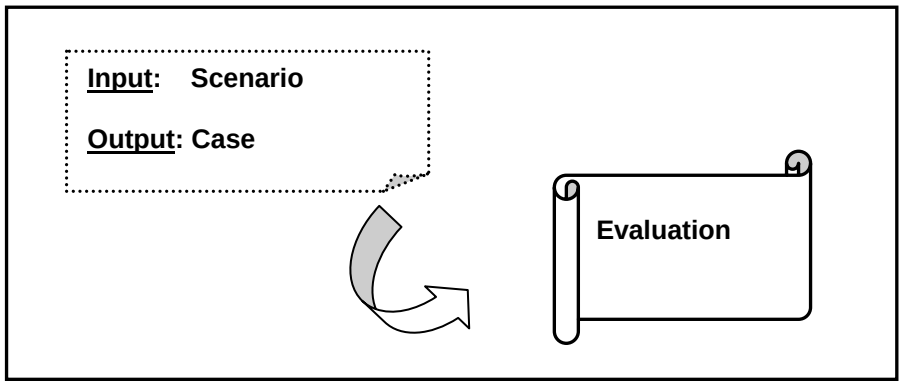
The input of the Psc should be anything else but the Evidence from the Pea aiming to produce a Scenario as an output. The scenario is the 'story' that is created by the investigator based on the findings of the media examination. Only when the required information is gathered, the analyst is able to present a coherent and efficient chronicle of the evidence. The reconstructed story of what has taken place to the original media. At this Phase it may be required for the analyst to search for further details on the two previous phases.



Graph 5: Phase 3 - Scenario Construction I/O

Evaluation

The Pe uses the Scenario from the Psc as an input in order to present the Case that is also the required output of the whole investigation. At this stage the Media Analysis will be either proved or disproved. However, the analyst needs to be able to revisit all previous Phases for the validation of the research outcome.



Graph 6: Phase 4 - Evaluation I/O

On a theoretical basis the Investigation Process obtains the following instruction format that is going to be analysed in detail on the analysis chapter. Each phase, the processes (I/Os) and the activities of the first level of the investigation framework are list numbered is order to create a logical continuation. By progressing the activities at this level of the procedure appear, where the separation of the framework in two parts comes into sight, the victim's and the perpetrator's that are going to lead to the second level of the Investigation Process.

First Level Investigative Process

Phase 1. Media Analysis
- Process 1.1. Digital Media
  - Activity 1.1.1. Source Identification
  - Activity 1.1.2. Digital Media collection
  - Activity 1.1.3. Copy/ image the source
- Process 1.2. ID Theft Data
  - Activity 1.2.1. Evidential data identification
    a. Victim
    b. Fraudster
  - Activity 1.2.2. Target identification
  - Activity 1.2.3. Threat agent identification / intention

Phase 2. Evidence Analysis
- Process 2.1. ID Theft Data
  - Activity 2.1.1. Data Analysis
  - Activity 2.1.2. Target Analysis
    a. Victim
    b. Fraudster
  - Activity 2.1.3. Threat Agent Analysis
- Process 2.2. Evidence
  - Activity 2.2.1. Evidence Collection
  - Activity 2.2.2. Evidence Classification

Phase 3. Scenario Construction
- Process 3.1. Evidence
  - Activity 3.1.1. Structure of evidential data
  - Activity 3.1.2. Structure threat agent's profile
    a. Victim
    b. Fraudster
  - Activity 3.1.3. Structure analysed digital evidence
- Process 3.2. Scenario
  - Activity 3.2.1. Scenario Outline
  - Activity 3.2.2. Scenario Preparation Documentation

Phase 4. Evaluation

Process 4.1. Scenario
- Activity 4.1.1. Scenario Testing / Evaluation
- Activity 4.1.2. Scenario Clarification

Process 4.2. Case
- Activity 4.2.1. Case Construction
- Activity 4.2.2. Case Clarification
- Activity 4.2.3. Case Evaluation
- Activity 4.2.4. Evidential Case Representation

EXAMPLE FICTIONAL SCENARIO

Assuming there is a computer hard disk delivered to a computer forensics lab from a major company suspecting an employee for computer misuse, but without any further details. Consequently, this is going to be the first attempt to apply the above described first level framework, in an incident that the analyst is not provided with any further information.

In such a case, and for Phase 1 of the investigation process, the investigator receives the input of the Process 1.1 that needs to collect (Activity 1.1.1), identify (Activity 1.1.2) and image (Activity 1.1.3) the hard disk. The output process of this Phase is the 1.2, where for the needs of this example is ID Theft Data or even data that could stand as ID Theft evidence and this is what the investigator is challenged to discover. The Activity 1.2.1 reveals the first element, whether the evidence belongs to a victim or a fraudster. From this point the investigation process on a lower level framework should progress under a bipolar perspective according to the data provided from 1.2.1. However, for this example it can easily give the first glance charging the employee as a fraudster committing ID Theft from his work computer, including every instance of it, inside the company or towards outside targets. His machine could also state him as a victim of ID Theft, meaning that the company has probably got information leak to the outside. There is when Activity 1.2.2 identifies the target, that could be a vulnerable system, or information published on the public domain, as well as the Activity 1.2.3 where the threat agent and his intentions can be identified.

Phase 2, aims to analyse the evidence from the original media on Process 2.1, the investigator analyses the ID Theft data under three Activities 2.1.1, 2.1.2 and 2.1.3, data, target and threat agent accordingly. The target analysis activity is divided to victim and fraudster, as the inputs for each category are different and guide the investigation towards different perspective. In case the employee has been a victim, the investigator will be able to analyse the target from this side, if the employee was the fraudster perhaps the investigator will be able to collect more details about the target. Therefore, the Process 2.2 provides the evidence with the Activities 2.2.1 that collects the evidence and 2.2.2, where the evidence is classified.

Phase 3 constructs the scenario of the incident. At this point, Process 3.1 is the evidence extracted from the investigation, where Activity 3.1.1 structures the evidential data, while 3.1.2 structure the threat agent's profile that is divided to the victim's and the fraudster's side, as there is going to be different sort of data gathered to give the investigator the information required to construct the attacker's profile. Activity 3.1.3 structures the analysed digital evidence that refers to the incident as a whole. In such a manner, on Process 3.2 the activities that follow are 3.2.1, the scenario outline and 3.2.2, the documentation preparation. At this point the investigator has a clear aspect about his suspect. He could tell with structured evidence whether the suspected employee has committed ID Theft or has only been another victim.

However, he owes to continue with Phase 4, the evaluation of the scenario. So, on Process 4.1 that is the scenario, Activity 4.1.1 is followed, evaluates or not the scenario assumption and 4.2.2 clarifies the scenario. Process 4.2 leaves the investigator with a case where he needs to construct it (Activity 4.2.1), clarify it (Activity 4.2.2) and evaluate it (Activity 4.2.3). The last Activity 4.2.4 for the investigator is the evidential case representation, the computer forensic report, where all evidence will be described and could also stand in a court of law, charging the fraudster of the case that could be either the victim or not.

CONCLUSION:

When someone who can describe his relation with computers and the Internet as professional or even as advanced user, reaches to the point that feels insecure and suspicious with the interaction with them, then it obviously appears that the situation requires some attention. The statistics prove that the ID Theft is a type of old fashioned crime that transformed into a Cybercrime because of the intense 'investment' of online sources. There may be more 'bad' people in the world than good ones and the spur of committing the perfect crime that will never be revealed still runs in some people's minds.

This situation leads to the improvement of tools and popularity of studying and research in computer forensics the last few years. It is the type of science that corresponds to the needs of digital investigations. Therefore for the conditions where ID Theft is combined with computer usage, computer forensics is the type of science that will be requested to provide the evidence. In such a perspective, there should be an effort to provide the computer forensic analysts with more detailed and concrete procedures that will help them accomplish their target.

For this reason, with respect and based on the computer forensics frameworks aiming to aid digital investigations, there is an approach of investigating ID Theft incidents with an independent investigation methodology. The ID Theft investigation framework distinguishes the examination in the victim's and the fraudster's side and the first level of this investigation process analysis was hence presented. This type of investigation method aims to provide results on a more focused basis regarding an ID Theft incident. Future work includes a more detailed approach to the findings of the investigation process based on the evidence left behind on a fraudster's digital storage media and the victim's accordingly. An experimental assessment on fictional cases by analysing reliable, residual data from hard disk drives will validate the research; and that will be accomplished in two parts, where the researcher behaves as the perpetrator in a closed network attack in the laboratory, and where the researcher uses the evidence that is left behind (from the first experiment) and acts as a forensic examiner, analysing the hypothetical victims' hard disk drives.

REFERENCES:

Beebe N.L., Clark J. G, 2005, A hierarchical, objectives-based framework for the digital investigations process, Digital Investigation, Volume 2, Issue 2, June 2005, Pages 147-167

Carrier B.D., Spafford E.H., 2006, Categories of digital investigation analysis techniques based on the computer history model, Digital Investigation
Volume 3, Supplement 1, September 2006, Pages 121-130
The Proceedings of the 6th Annual Digital Forensic Research Workshop (DFRWS '06)

Carrier B., 2006, Basic Digital Forensic Investigation Concepts, Internet, Available from: http://www.digital-evidence.org/di_basics.html, [Last Accessed: 12/03/2007]

Casey, E., April 2003, Determining Intent — Opportunistic vs Targeted Attacks, Computer Fraud & Security, Volume 2003, Issue 4, pp. 8-11

Chisum W.J., Turvey B., 2006, Crime Reconstruction, Academic Press Inc.,U.S., ISBN-10: 0123693756, Chapter 1: A History of Crime Reconstruction, p.23

CIFAS, 2007, Is Identity Theft Serious?, Internet, Available from: http://www.cifas.org.uk/default.asp?edit_id=556-56, [Last Accessed: 14/09/2007]

Dwan B., 2004, Identity Theft, Computer Fraud and Security, Volume 2004, Issue 4, Page 14-17

Federal Trade Commission, February 2005, National and State Trends in Fraud & Identity Theft, January – December 2004., pdf, downloaded from: http://www.ftc.gov/opa/2005/02/top102005.htm [Last Accessed: 11/09/2007]

Federal Trade Commission, February 2007, Consumer Fraud and Identity Theft Complaint Data, January – December 2006, .pdf, downloaded from: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf [Last Accessed: 14/09/2007]

Home Office Identity Fraud Steering Committee,2006, http://www.identity-theft.org.uk, [Last Accessed: 02/04/2007]

H. R. 2622, Fair and Accurate Credit Transactions Act of 2003, H. R. 2622, Fair and Accurate Credit Transactions Act of 2003, 2003, Internet, Available from: http://financialservices.house.gov/media/pdf/108hr2622ai.pdf [Last Accessed: 11/09/2007]

Icove D. et al., 1995, Computer Crime, A Crimefighter's Handbook, O'Reilly, ISBN: 1-56592-086-4

ID Theft and Assumption Deterrence Act, 1998, available from: http://www.ftc.gov/os/statutes/itada/itadact.htm, United States Code, **§ 003 (7),** 30/10/1998 [Last Accessed: 11/09/2007]

Marcella A. J., Greenfield R., 2002, Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes, CRC Press LLC, ISBN: 0-8493-0955-7

McKenna B., 2004, Cyber attacks on banks double from 2003, Computer Fraud and Security, Volume 2004, Issue 6, Page 3

Postnote Computer Crime, October 2006, Parliamentary Office of Science and Technology, Number 271, Available from: http://www.parliament.uk/documents/upload/postpn271.pdf [Last Accessed: 25/04/2007]

Thornton, J.I., 1997, "The General Assumptions And Rationale Of Forensic Identification", in David L. Faigman, David H. Kaye, Michael J. Saks, & Joseph Sanders, Modern Scientific Evidence: The Law And Science Of Expert Testimony, vol. 2, St. Paul: West Publishing Co.

unknown, 26/03/2007, One in ten Britons victim to online fraud, Available from: http://www.inthenews.co.uk/news/news/finance/one-in-ten-britons-victim-online-fraud-$1071167.htm [Last Accessed: 03/09/2007]

COPYRIGHT