IOSR Journal of Engineering
Mar. 2012, Vol. 2(3) pp: 392-398

Digital Forensic Tools

Vishal R. Ambhire[1], Dr. B.B. Meshram[2]
[1]*Computer Engineering Department, Veermata Jijabai Technological Institute, India*
[2]*Computer Engineering Department, Veermata Jijabai Technological Institute, India*

ABSTRACT

Digital Forensics has rapidly evolved over the last decade and continues to gain significance in both the law enforcement and the scientific community. The subject of digital forensics can be quite challenging. Digital forensics is in its infancy and teaching digital forensics includes the techniques as well as the tools that assist in the process. This paper provides an overview of Digital Forensics methodologies, modeling, analysis and applications.

Keywords: **Digital Forensics; cyber crime; analysis; evidence; Internet.**

I. INTRODUCTION

Digital forensics has been defined as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations.

Digital forensics techniques are used more in the case of criminal investigations. The investigations done may vary widely depending upon the evidence collected. Digital forensic examinations generally use computer-generated data as their source.

Digital forensic is used in the crime investigation for the national investigation organization like prosecution, police and the necessity of digital forensic technique is increasing even from civil field like general enterprise and banking company.

II. THE DIGITAL FORENSICS MODELS

These various models have assumed that the entire investigative process for computer forensics would be undertaken. This can be extremely time consuming given the volume of data to examine and in most cases it involves the transfer of the system(s) or a forensic copy(s) of the data located on the storage media to a lab environment for a thorough examination and analysis.

In order to meet the demand for timely information derived from digital sources a different process model is proposed that is based on forensically sound principles and at the same time is sensitive to time constraints (i.e., critical investigative information can be derived in a short timeframe).

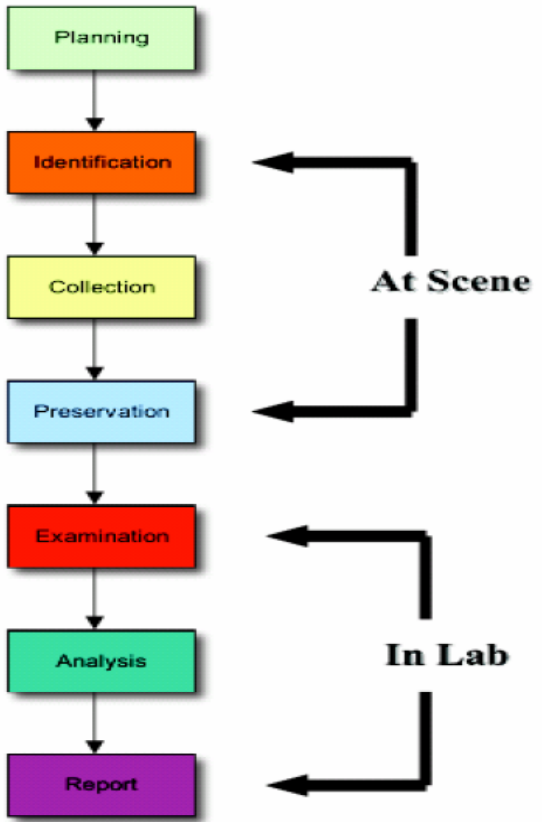

Fig. 1 Digital Forensic Models.

The foci of the model are to:

1) Find useable evidence immediately;
2) Identify victims at acute risk;
3) Guide the ongoing investigation;
4) Identify potential charges; and
5) Accurately assess the offender's danger to society.

While at the same time protecting the integrity of the evidence and/or potential evidence for further examination and analysis.

III. INVESTIGATION PREPARATION

Cyber crime investigators start cyber crime investigation, after the incident report received or detected related cyber crime. The goals of the investigation preparation are to ensure that the operations and infrastructure are able to fully support
an investigation.

The investigation preparation becomes important role of investigating systematically. The operations preparation provides training and equipment for the personal that will be involved with the incident and its investigation.

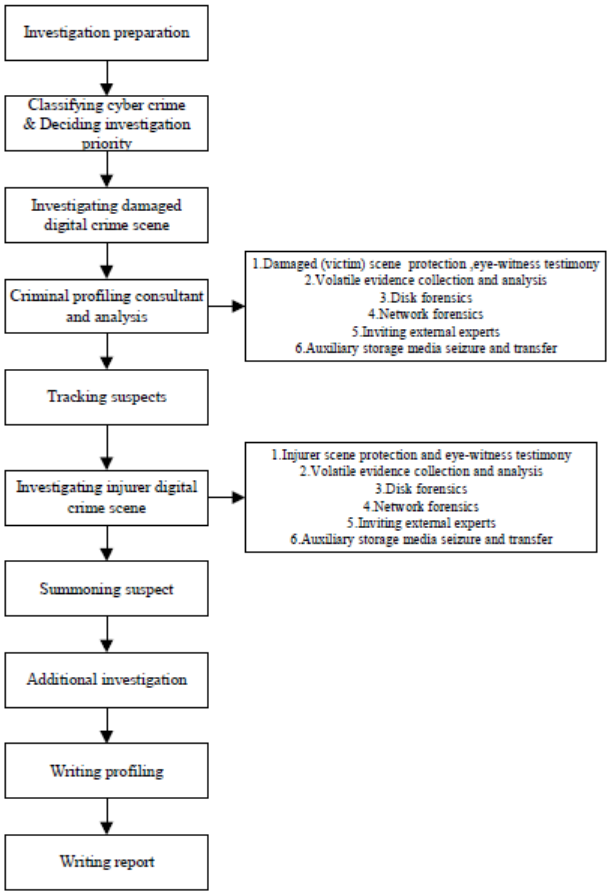

Fig. 2 Block diagram of the digital forensics investigation procedure model.

IV. METHODOLOGIES

The Educational Methodologies category includes research that needs to be conducted in order to effectively educate the many diverse populations that use, apply and evaluate digital forensics. The initial populations identified in figure 1 include Law Enforcement, the Legal Profession, Policy-makers, Corporations, Community, and Higher Education.

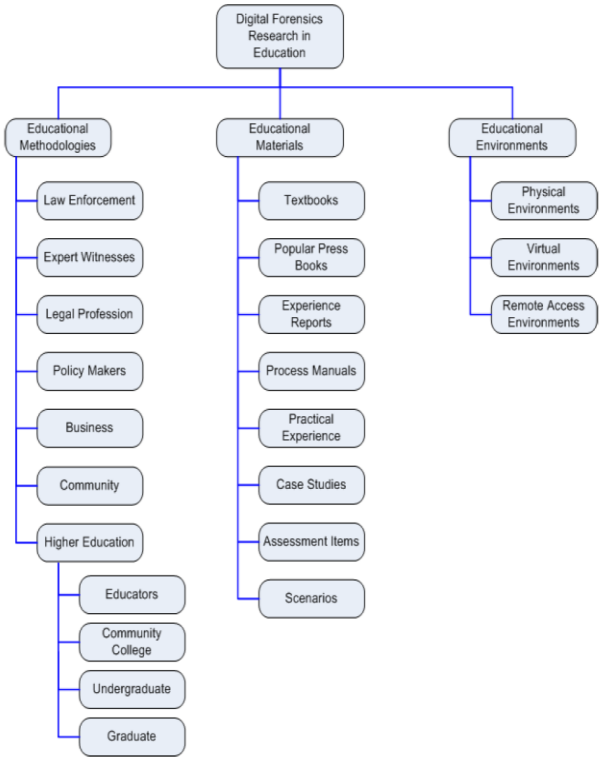

Fig. 3 Methodologies of Digital Forensic

A. Law Enforcement

One might consider the structure of law enforcement digital evidence practitioners as consisting of three levels; police first responders, digital forensic analysts, and federal agency officers.

At this lower level of law enforcement first responders the needs are very basic. The basic requirement for this group is to provide sufficient training and education so that they are can recognize
potential digital evidence, are not a danger to the digital evidence and that they do no harm to the investigation process.

The second level of responder tends to be a law enforcement officer facing a different set of challenges. At higher levels of the practitioner's hierarchical structure there is more support and resources available to practitioners. At the federal level practitioners are able to work in teams with better resourced laboratories.

B. Expert Witnesses

Expert witnesses are predominantly digital orensics practitioners and law enforcement, involved in the tasks of data conveyance. Their main role is to take collected digital evidence that has been analyzed
and processed and form expert opinions about the results obtained. The expert witness uses specialized software as a tool to make judgments regarding the evidence content and it is important that their opinion

be bent neither toward the prosecution nor the defense, but an unbiased statement of fact.

C. Legal Profession

Educating the legal fraternity is a priority due to long-held views within the profession. Members of the legal profession have adopted different attitudes to digital forensic evidence in accord with their particular judicial perspective. There are three distinct perspectives that may be adopted by legal professionals; prosecution argues for the accused's guilt, defense argues their innocence, and the finder of fact being either the judge or the jury is expected to be neutral until persuaded by legal argument. Prosecution lawyers tend to become involved in legal
issues early in the investigation case and develop legal argument to support prosecution as cases progress. Defense lawyers tend to become involved with cases only after prosecution lawyers determine that a prosecution is likely to be successful. As such defense lawyers do not necessarily have the depth of case data exposure that is available to their fellow counsel.

D. Policy-makers and Legislators

This group includes legislators (e.g., Senators and Congressmen at various levels of government in the United States), their staff members, and staff members in a wide variety of agencies that have some level of responsibility for an area of government (e.g., the U.S. Federal Communications Commission). This group is responsible for producing the legal and regulatory framework in which a given society operates.

E. Corporations

Populations included here are corporate security officers, ethical hackers, system analysts, etc. with a focus on education rather than training. There can be some considerable time between the occurrence of an
incident and the recognition that an incident has occurred. It is during the period of time between the recognition of an incident and when it has been determined that law enforcement must become involved that the corporate warrior can define the success of an investigation.

F. Higher Education

There are many levels of higher education that need to be considered in order to identify appropriate content and educational methods for digital forensics
topics that work well for the various higher education
markets including community colleges, undergra- duate programs, graduate programs, and educators.

V. OPEN SOURCE

Generically, "open" means just that: the source code is open and available for review. Open source is considered as a piece of software which is freely available and redistributable, which provide access to the source code, which allow the end user to modify the source code at will, and which must not restrict the end use of the software.

VI. FORENSIC SOFTWARE TOOLS

A. EnCase

Since its founding in 1997, Guidance Software has grown to be a leading providing of computer forensic software and services with over 20,000 worldwide clients and 285 employees. Guidance Software states that their suite of EnCase® solutions enables corporations, government and law enforcement agencies to conduct effective digital investigations, respond promptly to eDiscovery requests and other large-scale data collection needs, and take decisive action in response to external attacks.

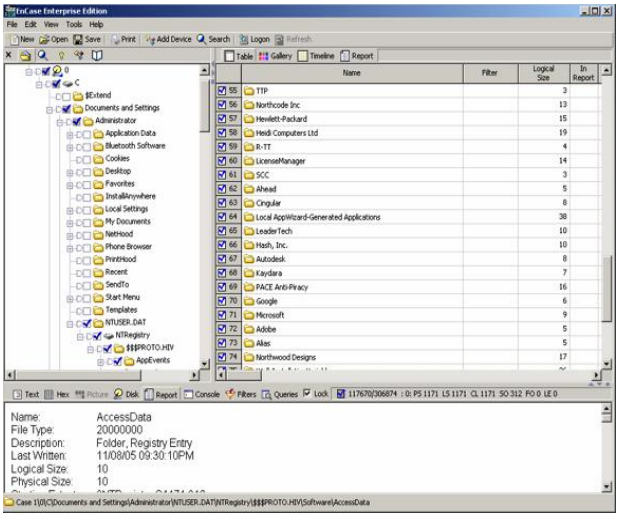

Fig. 4 Encase Screenshot.

An Initial Project Scope Analysis of EnCase included the following product features:

- Can read multiple file system formats such as FAT, NTFS, ext2, ext3, ReiserFS, UFS, and JFS.
- Can read multiple disk image formats such as Raw (dd), VMware, EnCase (.E01), and Safeback.
- Can remotely acquire disk images from networked computers running an EnCase acquisition agent.
- Data collection from a running and turned off computer utilizing EnCase Portable.
- Integrated keyword searching
- EnScript programming language automates almost any functionality with complete control over the details
- Disk browsing, searching, and EnScript are primary ways to view evidence
- Integrated viewer allows viewing of many popular file formats, such as image files

- Indexes zip files for analysis of compressed files/folders
- Can create hash values for any file in the ase
- Integrated registry viewer.

Characteristics

EnCase is identified with certain characteristics:

- Requires a greater amount of time in training before a user can be effective in analysis
- Searching can be confusing
- No log file is available to investigators of their actions performed in a session
- Extensive search customization afforded through string conditions, EnScript language commands, GREP, and filters.
- Convenient analysis afforded by importing the image and hashing files in the background after importing .

B. FTK Imager

FTK Imager is an extremely valuable tool to any responder or analyst, allowing them to not only acquire images from systems (via the appropriate write-blockers or from live systems) but also to verify file s ystems of acquired images, be they raw/dd or "expert witness" (perhaps more popularly known as "EnCase") format, VMWare vmdk file format, etc. FTK Imager recognizes a number of file system formats, including not just FAT and NTFS, but ext2, ext3, and others, as well.

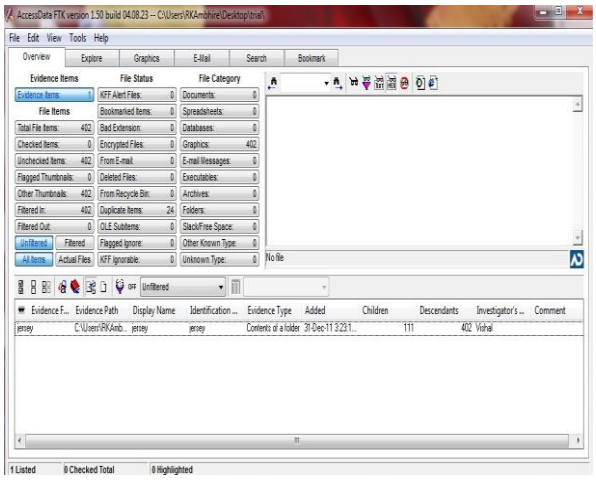

Fig. 5 FTK Imager Screenshot.

An Initial Project Scope Analysis of FTK included the following product features:

- Can read multiple file system formats such as FAT, ext2, ext3, and NTFS
- Can read multiple disk image formats such as Raw (dd), SMART, EnCase (.E01), Snapback, and Safe back
- Supports most modern email clients for email analysis
- Indexes zip files for analysis of compressed files/folders
- Known File Filter (KFF) feature aids the investigator in focusing on items of interest
- Interface is filter-based, with multiple different pre-programmed filters for evidence viewing
- Internal viewer allows investigator to view Word, PowerPoint, and Excel documents, and various image files
- Internal email viewer allows investigator to navigate email from various email store formats without having the email client used to generate the store
- Search feature using keywords
- Expanded functionality, such as registry viewing and password recovery, comes in the form of program integration with other company products
- Creates hash values for any file

Characteristics

- Requires substantially less time commitment to training to use the program
- Intuitive GUI design for speedy analysis
- Lengthy importing process restricts time for analysis of contents of the image
- Least customizable of all three software choices

C. ProDiscover Free

ProDiscover is a powerful computer security tool that enables computer professionals to find all the data on a computer disk while protecting evidence and creating evidentiary quality reports for use in legal proceedings.

ProDiscover lets you search through the entire disk for keywords and phrases with full Boolean search capability to find the data you want. You can use the hash comparison capability to find known illegal files or to weed out known good files such as standard operating system files by utilizing the included data from National Drug Intelligence Center in their Hashkeeper database. ProDiscover powerful search capability is fast and flexible, allowing you to search for words or phrases anywhere on the disk, including the slack space. The extensive on-line help capability and easy to use GUI interface allow you to quickly start using ProDiscover.

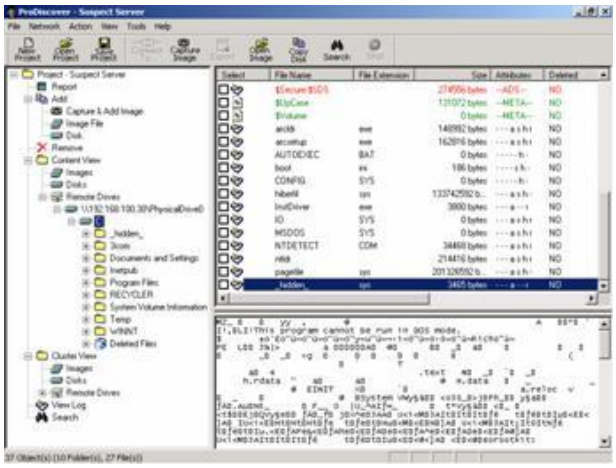

Fig. 6 GUI of ProDiscover.

Features and Benefits:

- Create Bit-Stream copy of disk to be analyzed, including hidden HPA section (patent pending), to keep original evidence safe.
- Search files or entire disk including slack space, HPA section, and Windows NT/2000/XP Alternate Data Streams for complete disk forensic analysis.
- Preview all files, even if hidden or deleted, without altering data on disk, including file Metadata.
- Maintain multi-tool compatibility by reading and writing images in the pervasive UNIX® dd format and reading images in E01 format.
- Support for VMware to run a captured image.
- Examine and cross reference data at the file or cluster level to insure nothing is hidden, even in slack space.
- Automatically generate and record MD5, SHA1 or SHA256 hashes to prove data integrity.
- Utilize user provided or National Drug Intelligence Center Hashkeeper database information to positively identify files.
- Examine FAT12, FAT16, FAT 32 and all NTFS file systems including Dynamic Disk and Software RAID for maximum flexibility.
- Examine Sun Solaris UFS file system and Linux ext2 / ext3 file systems.
- Integrated thumbnail graphics, internet history, event log file, and registry viewers to facilitate investigation process.
- Integrated viewer to examine .pst /.ost and .dbx e-mail files.
- Utilize Perl scripts to automate investigation tasks.
- Extracts EXIF information from JPEG files to identify file creators.
- Automated report generation in XML format saves time, improves accuracy and compatibility.
- GUI interface and integrated help function assure quick start and ease of use.
- Designed to NIST Disk Imaging Tool Specification 3.1.6 to insure high quality.

D. Internet

Almost every case will require an examination of artifacts associated with Internet activity, such as instant messaging (IM), e-mail and web browsing. The value, time cost, and time criticality will vary widely, depending on circumstances including the specific applications involved, type of activity being examined, and whether the PC being examined belongs to a suspect or a victim (e.g., in a missing persons case). An effective practice is for the computer forensic examiner to evaluate what type of Internet activities they believe the suspect (or victim) was involved in, and to evaluate if and how each of those activities relates to the case. Types of activities may include web browsing, e-mail, instant messaging, reading or posting to USENET newsgroups, trading files.

1) Browser Artifacts

While the specifics vary, most web browsing applications store some method for storing “cookies”, either as a file or as separate files, some means of storing temporary Internet files, and some means of storing user information and preferences, such as typed Uniform Resource Locator (URLs) and “favorites”. The specific content of individual cookies is determined by each individual website and is rarely of evidentiary value. In most cases, the evidentiary value of a cookie is limited to its name.

Typically, the name of a cookie will match the URL of the site that deposited the cookie, indicating that the PC had visited that site at some point in the past. This does not go to show intent as the cookie will be created whether the browser was redirected from another site, or intentionally pointed to the site with a typed URL. Dates and times associated with cookies may help to determine when a site was visited and can be useful in creating investigative timelines.

Temporary Internet files are essentially cached copies of web page components (often graphics) stored on the local PC. The investigative value is that these files are stored locally without the intent or intervention of the user, and that some files, for example contraband images, are of evidentiary value in and of themselves. An investigator must keep in mind that these files are easily cleared out by most browsing applications, or with third party tools. Most importantly, investigators must weigh the potential value against the time it will take to search through even a moderately populated cache. Examiners should expect a search of temporary Internet files to take hours or days.

In many cases, that requires more time than the examiner has. A web browser’s storage of user information and preferences can be a quick source of useful

information. In cases where "Internet Explorer" is the browser, the index.dat file can contain a running record of sites visited, including access to web based e-mail (but not e-mail content), and even local files. The examples below (some information has been redacted) all represent data pulled from an index.dat file in less than five minutes, using a free third-party tool (see Figure 3). The "User Name" in each case, indicates the name of the windows account that "owned" the index.dat file in question.

==========
URL : http://www.XXXXXX.com
Title : New Page 1
Hits : 17
Modified Date : 10/4/2005 9:05:35 PM
Expiration Date : 10/30/2005 9:05:36 PM
User Name : xxxxxx
==========
This example shows a user visiting a site 17 times, most recently on 10/4/2005
==========
URL : http://images.google.com/images?q=kitties&hl=en
Title : kitties - Google Image Search
Hits : 7
Modified Date : 10/4/2005 9:09:46 PM
Expiration Date : 10/30/2005 9:02:38 PM
User Name : xxxxxx
==========This example shows that a user performed a google image search on the term "kitties" 7 times, most recently on 10/4/2005
==========
URL : http://us.f307.mail.yahoo.com/ym/ShowFolder?rb=Inbox&reset=1&YY=85059
Title : Yahoo! Mail - xxxxxxxx@yahoo.com
Hits : 21
Modified Date : 10/4/2005 9:06:37 PM
Expiration Date : 10/30/2005 9:06:38 PM
User Name : xxxxxx
==========
This example shows a user accessing their yahoo account for the 21st time on 10/4/2005.
==========
URL : file:///D:/Program%20Files/mIRC/logs/%23Beginner.EFnet.log
Title :
Hits : 1
Modified Date : 10/4/2005 9:44:39 PM
Expiration Date : 10/30/2005 9:37:32 PM
User Name :xxxxxx
==========
This example shows the user accessing a file (in this case, an IRC chat log, but could be any type file) on the local drive for the first time on 10/4/2005.

2) E-mail Artifacts

E-mail artifacts may be of enormous evidentiary value, but can require a very expensive investment in time. Procedures for examining e-mail and extracting useful data are usually specific to the particular e-mail client, and can be time consuming to implement. If extraction of e-mail is successful, even a cursory screening of all the e-mail in a suspect's mailbox could take many hours. If web-based e-mail
is used, there is often no local storage of e-mail artifacts.

3) Instant Messeaging Artifacts

Most instant messaging clients maintain some type of contact information, and have the capability to record and store logs of the conversations that take place between the user and his or her online contacts. In most cases, this logging capability is off by default but can, and often is, turned on by the user. Contact information for most IM applications is maintained at the server, and may not be found on the local PC. Chat logs can contain a wealth of data, including the conversation itself, as well as the screen names of other parties. A single chat log may contain hours of conversation.

A thorough examination of multiple logs may bear a prohibitive cost in time. If it is necessary to examine chat logs, it is important for the examiner to have a clear idea of what he or she is looking for. String search tools should be implemented as much as possible. A "traditional" examination would likely involve a thorough examination of all of these, and many other artifacts.

VII. CONCLUSION

Some investigations are extremely time sensitive; hours can literally mean the difference between life and death for a victim or the escape of the suspect. Most law enforcement cases today involve digital evidence of some kind. The purpose of this theoretical framework is to provide management with a holistic view of what to consider when preparing the organization for forensic investigations, provide proof of compliance, and ensure evidence availability. Each tool has its strengths and weaknesses that require consideration when deciding when implementing them in an
academic environment.

Development in this field will continue to reach further avenues of lack, towards an optimum model for forensics, and common technical and legal standards across the globe.

ACKNOWLEDGMENT

I would like to thank all those people whose support and cooperation has been an invaluable asset during the course of this Seminar. I would also like to thank my Guide Dr. B.B.Meshram for guiding us throughout this Seminar and giving it the present shape. It would have been impossible to complete the seminar without their support, valuable suggestions, criticism, encouragement and guidance.

I am grateful for all other teaching and non-teaching staff members of the Computer Technology for directly or indirectly helping us for the completion of this seminar and the resources provided.

REFERENCES

[1] Carrier, Brian, Open Source Digital Forensic Tools: The Legal Argument, @stake Research Report, October 2002.
[2] Welcome to Access Data! Available at http://www.accessdata.com/.
[3] SourceForge.net: regviewer. Available at http://sourceforge.net/projects/regviewer/.
[4] libpff. http://sourceforge.net/projects/libpff/.
Casey, E. (2004). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. San Diego: Academic Press.
[5] Marcus K. Rogers and Kate Seigfried, The future of computer forensics, Computer and Security, 2004.
[6] "*Computer Forensics, IEEE Security and Privacy",* July/August 2005, James A. Whittaker & Michael Howard.
[7] *"Towards Models for Forensic Analysis"*, IEEE proceedings of the 2nd International Workshop (SADFE'07), Sean Peisert, Matt Bishop, Sidney Karin.
[8] "*Modeling the Network Forensics Behaviors"*, INSPEC'05, Sep 2005, Wei Ren & Hai Jin.