ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering
Tome V (Year 2012). FASCICULE 2 [April–June]. ISSN 2067-3809

[1.] Petar ČISAR, [2.] Sanja Maravić ČISAR

GENERAL DIRECTIONS OF DEVELOPMENT IN DIGITAL FORENSICS

[1.] TELEKOM SRBIJA, SUBOTICA, SERBIA
[2.] SUBOTICA TECH-COLLEGE OF APPLIED SCIENCES, DEPARTMENT OF INFORMATICS, SUBOTICA, SERBIA

ABSTRACT: *Digital forensics is essential for the successful opposition of computer crime. It is associated with many challenges, including rapid changes in computer and digital devices, and more sophisticated attacks on computer systems and networks and the rapid increase in abuse of ICT systems. For a forensic investigation to be performed successfully there are a number of important steps that have to be considered and taken. Since digital forensics is a relatively new field compared to other forensic disciplines, there are ongoing efforts to develop examination standards and to provide structure to digital forensic examinations. This paper provides an overview of the expected global directions of development in digital forensic investigations, as well as the actual trends in this area.*
KEYWORDS: *digital forensics, forensic process, development, solutions*

INTRODUCTION

The digital age is characterized as the wide-ranging application of computer technology as a way that enhances former possibilities. The usage of computer systems as a tool in private, commercial, educational, governmental, and other facets of modern life has improved the productivity and efficiency of these entities. At the same time, the introduction of computers as a criminal tool has enhanced the criminals' ability to perform, hide, or otherwise aid unlawful or unethical activity. In particular, the mass use by the general population, coupled with apparent anonymity, seems to encourage computer crimes. These "cyber-crimes" are not necessarily new form of crimes, but rather classic crimes exploiting computer power and accessibility to information. They are a consequence of excessive availability and user proficiency of computer systems in malicious hands. In order to locate, catch and prosecute criminals involved in digital crime, investigators must implement consistent and precisely defined forensic procedures.

Over the past years, computer forensics has come to the foreground as an increasingly important method of identifying and prosecuting computer criminals. Prior to the development of sound computer forensics procedures and techniques, many cases of computer crime were left unsolved. There are many reasons why an investigation might not lead to a successful prosecution, but the predominant issue is one a lack of preparation: tools and skills required to successfully gather digital evidence.

Digital evidence or electronic evidence is any probative information stored or transmitted digitally and a party to a judicial dispute in court can use the same during the trial [3].

Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines etc. Individuals attempting to investigate suspicious activity may also lack the financial resources or tools to conduct such an investigation adequately and ensure that the evidence is indisputable in all circumstances. Moreover, there are instances when all of the above have been adequately put in place, but, due to a lack of training and correct procedure, the evidence collected can be disputed.

As a result, computer forensics seeks to introduce cohesion and consistency to the wide field of extracting and examining evidence obtained from a computer at a crime scene. It is particularly important that the extraction of evidence from a computer is performed in such a way that the original incriminating evidence is not compromised.

DIGITAL FORENSICS

Digital forensics is a relatively new science. Derived as a synonym for computer forensics, its definition has expanded to include the forensics of all digital technology. While computer forensics is defined as "the collection of techniques and tools used to find evidence in a computer" [1], digital forensics has been defined as "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" [2]. Some authors make a clear distinction between computer and digital forensics. Yet, for the purposes of this paper, no real distinction is made.

Digital forensics can be defined in other, more general ways. For instance: digital forensics is the application of computer investigation and analysis techniques in the interests of determining potential legal evidence

[4]. Or: extracting evidence from computers or other digital devices [5].

Digital forensics has become prevalent because law enforcement recognizes that modern day life includes a variety of digital devices that can be exploited for criminal activity, not just computer systems. While computer forensics tends to focus on specific methods for extracting evidence from a particular platform, digital forensics must be modeled in such a way that it can encompass all types of digital devices, including future digital technologies. Unfortunately, there is no standard or consistent digital forensic methodology, but rather a set of procedures and tools created based on the experiences of law enforcement, system administrators and hackers. This is problematic because evidence must be obtained using methods that are proven to reliably extract and analyze evidence without bias or modification.

COMPUTER FORENSIC PROCESS

According to [6], computer and network forensics methodologies consist of three basic components:

- *Acquiring the evidence while ensuring that the integrity is preserved.*
- *Authenticating the validity of the extracted data, which involves making sure that it is as valid as the original.*
- *Analyzing the data while keeping its integrity.*

The U.S. Department of Justice published a process model that consists of four "traditional" phases [7]:

- *Collection (Acquisition) - involves the search, recognition, collection and documentation of the evidence.*
- *Examination - This phase is designed to facilitate the visibility of evidence, while explaining its origin and significance. It involves revealing hidden and obscured information, as well as the relevant documentation.*
- *Analysis - This looks at the product of the examination for its significance and probative value to the case.*
- *Reporting (Presentation) - This entails writing a report outlining the examination process and pertinent data recovered from the overall investigation.*

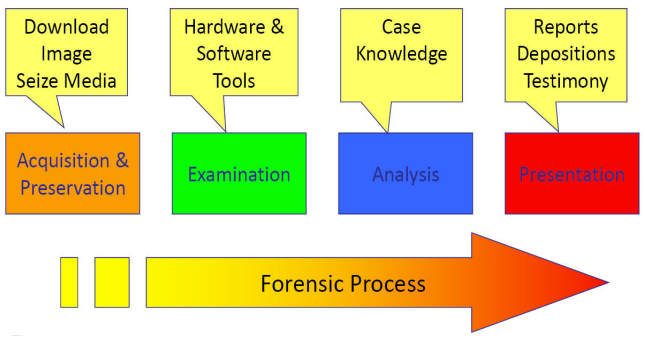

Figure 1. "Traditional" Digital Forensic Process

The Digital Forensics Research Workshop (DFRW) is another significant participant in developing the forensics process. The unique aspect of DFRW is that it is one of the first large-scale consortiums led by academia rather than law enforcement. This is an important distinction because it will help define and focus the direction of the scientific community towards the challenges of digital forensics. The DFRW has worked to develop a forensics framework that includes such steps as "identification, preservation, collection, examination, analysis, presentation, and decision" [2]. Based on this framework, the scientific community may further develop and refine this model.

A computer forensic framework can be defined as a structure to support a successful forensic investigation. This implies that the conclusion reached by one computer forensic expert should be the same as that of any other person who has conducted the same investigation [8].

Starting from the previous forensic protocols, there are common steps that can be abstractly defined to produce a model that is not dependent on a particular technology or electronic crime. The basis of this model is to determine the key aspects of the aforementioned protocols as well as ideas from traditional forensics. This proposed model can be thought of as an enhancement of the DFRW model since this is where it originates from. The abstract digital forensics model proposes a standardized digital forensics process that consists of the following components [9]:

- *Identification: which recognizes an incident from indicators and determines its type.*
- *Preparation: which entails the preparation of tools, techniques, search warrants, and monitoring authorizations and management support.*
- *Approach strategy: it develops a procedure to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim.*
- *Preservation: which involves the isolation, securing and preservation of the state of physical and digital evidence.*
- *Collection: that entails the recording of the physical scene and duplicate digital evidence using standardized and accepted procedures.*
- *Examination: which involves an in-depth systematic search of evidence relating to the suspected crime.*
- *Analysis: which involves determination of the significance, reconstructing fragments of data and drawing conclusions based on evidence found.*
- *Presentation: this involves the summary and explanation of conclusions.*
- *Returning evidence: this ensures physical and digital property is returned to the proper owner.*

In accordance with digital forensic analysis methodology [10], three processes are essential: preparation/extraction, identification and analysis.
For the realization of mentioned processes the following forensic techniques are used:

- *Post – mortem analysis: file system, registry, event logs, recovery of deleted files*
- *Live analysis: volatility – system date, time, running processes, network connections, users logged on, open files, full memory dump*
- *Network analysis: traffic analysis*
- *API analysis: API commands, data processed*
- *Forensic readiness*

DIRECTIONS OF DEVELOPMENT IN DIGITAL FORENSICS

Digital forensics has been forced to adapt to actual fields in digital crime. For instance:

- *Identity theft*
- *Internet fraud*
- *Financial crime*
- *Money laundering, gambling*
- *Hacking, network intrusion*
- *Theft of intellectual property and piracy*
- *Robbery*
- *Child pornography*
- *Homicide, harassment and stalking*
- *Terrorism*

In the past, when someone was suspected of a computer crime or act that was in conflict with corporate policy, the typical process would be to seize the hard disk after hours, take a bit stream image, analyze the disk and create a report ("traditional" forensics). This is becoming an increasingly difficult process. More and more companies now have a global presence with offices spread around the world. These distributed networks have numerous PCs attached to them.
Thus the new trend in digital forensics is to use the corporate network to immediately respond to incidents. It allows capturing and analyzing volatile data, including active network sessions and running processes. It even allows seeing what ports and IP addresses these processes are communicating with.
It is far better to see what is actually happening as opposed to trying to piece it together after the fact from fragments found across the drive. More and more sophisticated users hide their activities by using specific programs and then using cleansing software to erase any Internet history on the hard drive. Although the proxy server will still show network entries, it does not capture enough information to be useful. By using a product for "live" investigations one can track exactly what is being said and to whom.
This leads to the latest trend in digital forensics - online digital forensics over the network. From the moment when someone becomes suspected for irregularly using the computer resources, the control of proxy servers starts for network traffic. Once this traffic begins has to take a look at a specific machine in real time. In this way it is possible to dump and analyze the memory and find out a number of key information, such as the content of the e-mails, what is in the Internet cache files at the time and the IP addresses of other machines that may be in communication.
A positive fact is that all of this can be done even if the machine is located in another country. Other features include the ability to traverse the registry of the target machines in a live state. Files can also be acquired over the network.
The only downside is in case of running on a slow network, it can be difficult and time-consuming to acquire the entire drive. The theory is that it is possible to narrow the search considerably by doing an online analysis, and through this analysis to find out what exactly is looked for. Then the evidence related to the crime can be acquired.
Forensic investigations may also be realized in LAN and WAN resources in the enterprise. Whether responding to an urgent need for examination across a corporate WAN or functioning as a forensic service permanently attached to a corporate security equipment, investigation tools have been developed to address forensic-grade data harvesting and reporting in widely dispersed environments. Enterprise forensic tools often possess the capability to investigate live systems remotely and analyze volatile memory contents and network metrics as well as local machine activities in situ [11].
There are two market-leading products with two different implementation strategies: Encase Enterprise (by Guidance Software) and LiveWire (by WetStone Technologies). Both accomplish the same result in that they both have the ability to dump, search and analyze memory and the files on the remote computer (data acquisition, file recovery, indexing/search and file parsing), however LiveWire does it without the need for the program to be running on the machine being analyzed.
Features (EnCase) [12]:

- *Acquire data from disk or RAM, documents, images, e-mail, web mail, Internet artifacts, Web history and cache, HTML page reconstruction, chat sessions, compressed files, backup files, encrypted files, RAIDs, workstations, servers, and with Version 7: smart phones and tablets.*
- *EnCase produces an exact binary duplicate of the original drive or media, then verifies it by generating MD5 hash values for related image files and assigning CRC values to the data. These checks and balances reveal if and when evidence has been*

tampered with or altered, helping to keep all digital evidence forensically sound for use in court proceedings or internal investigations.

- Recover files and partitions, detect deleted files by parsing event logs, file signature analysis, and hash analysis, even within compounded files or unallocated disk space.

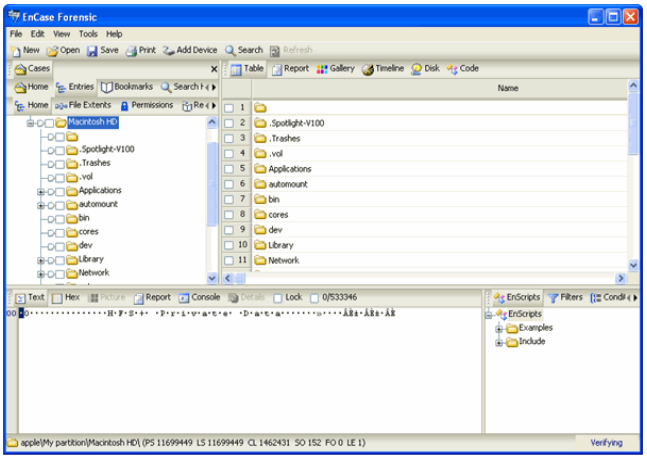

Figure 2. EnCase Screenshots

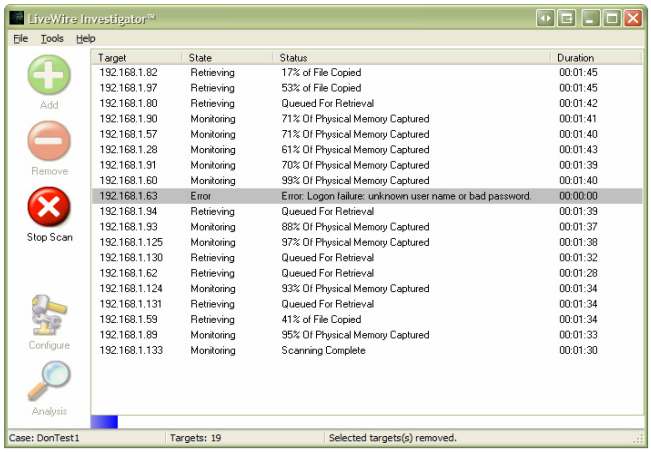

Figure 3. LiveWire Screenshots

With Encase Enterprise a service must previously be installed and running on the machine in order to allow for the machine to be accessed. This makes the deployment in the corporation not only complex, since any service must co-exist with other services; it also makes it very costly.

With LiveWire no such service needs to be running, making it extremely useful for a forensic consultant to go on site, bring their laptop with them, attach to the network and forensically acquire both the memory and the hard drive information of any computer on the network, including servers. All that is required is an administrator user ID and password of the machine being targeted. This makes LiveWire extremely useful, easier and far more cost effective.

Features (LiveWire) [13]:

- Live network investigation
- Live forensic discovery and triage of simultaneous target systems
- Acquire system information
- Physical memory imaging
- Remote screen shot
- Active port mapping
- Windows service discovery
- File system blueprinting
- Installed software cataloging
- Network state and open connections
- Intelligent file acquisition and safeguarding
- Dynamic indexing and analysis
- Dissection of recent user activities (web, messaging, applications)
- Automatic collection of most relevant and timely file system, registry and network connectivity actions
- Structured reporting capabilities to increase investigator productivity
- Automated time stamped audit trail

There is also a growing trend to encrypt the data stored on hard drives, particularly portable computers like laptops and notebooks. Although forensic examiners have some tools to get past these encryption schemes, they are not always successful. A live investigation allows using calls to the operating system of the target machine to extract and decipher the data.

With increasingly complex network infrastructures geographically dispersed across the globe, "live" investigations are the trend we are heading towards.

NETWORK AND HARDWARE CHALLENGES

Intensive technological development of ICT has led to the formation of various network and hardware challenges in the context of digital forensics. Some of them are:

- Network
  - Gigabit networks provide similar (if not faster) access speeds than local hard drive.
  - Centralized storage presents an acquisition challenge since often items of interest will not be stored on the target computer.
  - Storage of several gigabytes becomes cheaper.
- Hard Drive
  - Hard drive sizes continue to grow, but I/O access speeds are not keeping up. As a result acquisition and data processing continues to be more and more time consuming.

FUTURE DIGITAL FORENSICS SOLUTIONS

In the field of digital forensics, over many years of practical experience, the following development trends (expectations) of adequate solutions were identified:

- In the field
  - Better tools with triage capability for the first responders.
  - Windows Explorer based tools will continue to be used in the field.

- Identify encryption before pulling the plug.
- Plug and play bootable USB devices
- Identify data stored remotely.

□ Imaging technology
- Data stored in a hybrid of logical and physical formats
- The file item becomes the atomic unit rather than the drive.
- Data reduction techniques to reduce the size of the image.
- Selective logical imaging of user data.

□ In the laboratory
- Forensics data mining tools are front ends for large SQL database.
- Distributed grid data processing architecture
- Data mining searches performed via index engines.
- Multi-user model - Investigators, examiners, paralegals, work in the data at the same time sharing files, notes, bookmarks, etc.
- Heavy emphasis on e-mail and Internet artifacts
- Emphasis on timelines
- Emphasis on data visualization

CONCLUSIONS

Each year, there is a constant increase in the number of digital crimes worldwide. As technology evolves, software improves, and computer users become more qualified, the crimes they commit are becoming more sophisticated. Law enforcement is in a perpetual struggle with these criminals to limit their opportunities. Part of this intention includes developing tools that have the ability to systematically search digital devices for pertinent evidence. As more and more devices become digitalized, tool development should also progress to include these, as well. In parallel with technological development, it is necessary to ensure the development of adequate forensic methodology which must be applicable to all current digital crimes, as well as any unrealized crimes of the future. This paper aimed to identify some of the most important directions of development trends and forensic solutions. Also, through two popular market products, the overview of actual forensic trends is presented. It may be noted that live analysis in real-time prevailed over traditional post-mortem analysis, and that network environment investigation became increasingly dominant condition for forensic software.

REFERENCES

[1.] Caloyannides, M.A.: Computer Forensics and Privacy, Artech House, Inc. (2001)

[2.] Digital Forensics Research Workshop, "A Road Map for Digital Forensics Research", 2001., Available: www.dfrws.org (current October 2011)

[3.] USLegal - Definitions, Available: http://definitions.uslegal.com/d/digital-evidence (current October 2011)

[4.] Pfeilsticker, M., Starnes, R.: Digital Forensics, Exodus Communications, Available: http://www.guug.de/veranstaltungen/ffg2002/papers/ffg2002-pfeilsticker.pdf (current October 2011)

[5.] Harrison, W.: Developing an Undergraduate Course in Digital Forensics, PSU Center for Information Assurance, Portland State University, Available: http://www.ccsc.org/northwest/2006/ppt/forensicstutorialHARRISON.pdf (current June 2011)

[6.] Kruse, W., Heiser, J.G.: Computer Forensics: Incident Response Essentials, Addison-Wesley, (2002)

[7.] National Institute of Justice: Electronic Crime Scene Investigation. A Guide for First Responders, 2001, Available: http://www.ncjrs.org/pdffiles1/nij/187736.pdf (current June 2011)

[8.] Van Solms, S.H., Lourens, C.P.: A Control Framework for Digital Forensics, IFIP 11.9, (2006)

[9.] Reith, M., Carr, C., Gunsch, G.: An Examination of Digital Forensic Models, International Journal of Digital Evidence, Volume 1, Issue 3, (2002)

[10.] Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Cybercrime Lab, http://www.cybercrime.gov (current June 2011)

[11.] Kleiman, D.: The Official CHFI Exam 312-49: For Computer Hacking Forensics Investigators, Available: www.syngress.com (current October 2011)

[12.] EnCase Forensic, www.guidancesoftware.com (current September 2011)

[13.] WetStone Technologies, www.wetstonetech.com (current September 2011)

ACTA TECHNICA CORVINIENSIS – BULLETIN of ENGINEERING

ISSN: 2067-3809 [CD-Rom, online]