Volume 3, Issue 12, December 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Digital Forensics: Emerging Trends and Analysis of Counter-Security Environment

Anamika Joshi, Dr. D. S. Bhilare
School Of Computer Science
Devi Ahilya University Indore, India

Abstract— Corporates and organizations across the globe are spending huge sums on information security as they are reporting an increase in security related incidents. The proliferation of cloud, social network and multiple mobile device usage is on one side represent an opportunity and benefits to the organisation and on other side have posed new challenges for those policing cybercrimes. Cybercriminals have devised more sophisticated and targeted methods/techniques to trap victim and breach security setups. The emergence of highly technical nature of digital crimes has created a new branch of science known as digital forensics. Digital Forensics is the field of forensics science that deals with digital crimes and crimes involving computers. This paper focuses on briefing of digital forensics, various phases of digital forensics, digital forensics tools and its comparisons, and emerging trends and issues in this fascinated area.

Keywords— Digital forensics, Digital evidence, Digital forensics tools, Network intrusion, Information security,

I. INTRODUCTION

The convergence of the technological advances and the pervasive use of computers and digital devices worldwide have brought about many advantages to mankind, but it also provides avenues for misuse and opportunities for committing crime and wilfully commit social harm. While information security risks have dramatically evolved, security strategies have not kept pace with today's determined adversaries. Consequently, sophisticated intruders can bypass security defences to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives [1, 2 and 3]. This year's survey shows that detected security incidents have increased, as has the cost of breaches. And hot-button technologies like cloud computing, mobility, and BYOD (bring your own device) are implemented before they are secured [3, 4 and 5]. According to The Global State of Information Security Survey 2014 released by PwC US in conjunction with *CIO* and *CSO* magazines [3], the number of security incidents detected in the past 12 months increased by 25 percent over last year; however, the number of respondents who do not know how many incidents occurred has doubled over the past two years. The overall statistics are illustrated in the following table.

Year	Average number of security incidents	Average information security budget of PwC sample	Financial losses of $100,000 or more
2012	2,989	$2.8 million	19%
2013	3,741	$4.3 million	24%

The emergence of highly technical nature of digital crimes has created a new branch of science known as Digital forensics. Digital forensics is a new field that deals with digital crimes and crimes involving computers. The widespread use of digital forensics has resulted from two factors: the ubiquitous computers that followed from the microcomputer revolution and the increasing number of computer crimes. This paper is organized as follows. Section 2 presents the overview of digital forensics and its phases. Section 3 describes digital forensics tools and its comparisons. Section 4 presents the emerging trends and issues in this fascinated area and concluded in section 5.

II. OVERVIEW OF DIGITAL FORENSICS

This section introduces the field of digital forensics and its core process.

A. Definition of Digital Forensics:

A frequently cited definition for Digital Forensic Science is that of the Digital Forensic Research Workshop (DFRWS) of 2001[6]: "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 facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations". The Kruse and Heiser define digital forensics as [7]: "Preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis".

However, many experts feel that a precise definition is not yet possible because digital evidence is recovered even from devices that are traditionally not considered to be computers. Some researchers prefer to expand the definition to include the collection and examination of all forms of digital data, including that found in cell phones, PDAs, iPods, and other electronic devices. Digital forensics is a largely practitioner-oriented field; because of less standardization, temporal diversity, never-ending upgrade cycle and high degree of uncertainty it is difficult to categorize and classify it. There are various overlapping branches, areas, and terms are generating day by day. Its various activities have been categorized in numerous ways as shown in figure 1. The most obvious subdivision may be according to their 'domain of evidence' [8, 9].

1. Computer Forensics : Examination of desktop and laptop computers, media storage and file system (hard drives, optical discs, and floppy disks);
2. Network Forensics : Examination of networks, routers, servers, tapes and computer memory;
3. Database Forensics : Examination of databases and their metadata and log files; and
4. Mobile device forensics: Examination of mobile, handheld and embedded systems.

Other classifications and specialities may be

1. based on analysis e.g. live (volatile data) and static(non-volatile data) [10,11];
2. based on response e.g. reactive and proactive[12,13,14];
3. based on specific services and applications e.g. cloud forensics, email forensics, multimedia forensics, web forensics etc. [15, 16].

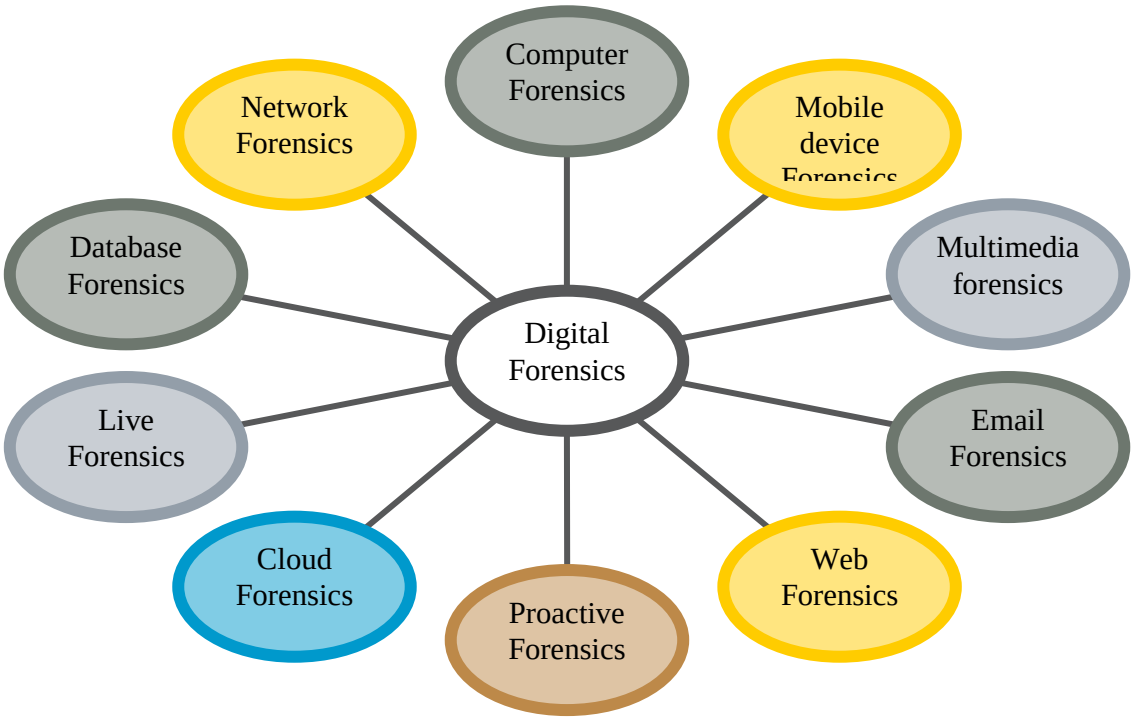

Figure 1 Classification of Digital Forensics

B. The Digital Forensics Process :

The most common goal of performing forensics analysis is to gain a better understanding of an event of interest by finding and analysing the facts and evidences related to that event. Digital forensics may be needed in many different situations, such as evidence collection for legal proceedings and internal disciplinary actions, and handling of malware incidents and unusual operational problems. Regardless of the need, forensics should be performed using the four-phase process shown in Figure 2[17]. The exact details of these steps may vary based on the specific need for forensics.

1) COLLECTION :

Identify, isolate, label, record, and collect the data and physical evidence related to the incident being investigated, while establishing and maintaining integrity of the evidence through chain-of-custody.

2) Examination :

Identify and extract the relevant information from the collected data, using appropriate forensic tools and

techniques, while continuing to maintain integrity of the evidence.

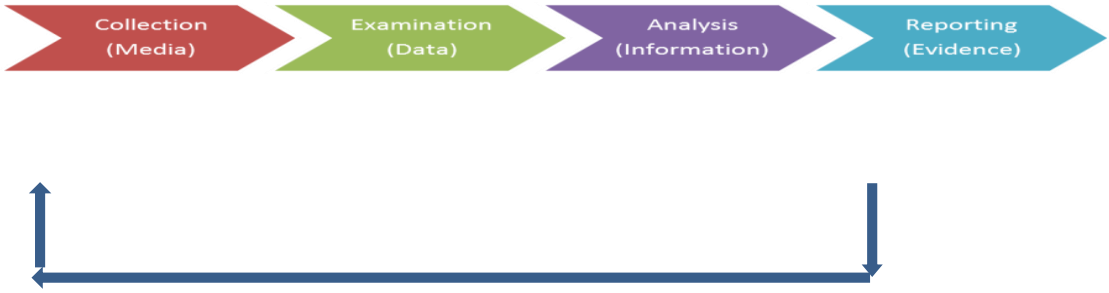

Figure 2 the Digital Forensics Process

3) Analysis:
Analyse the results of the examination to generate useful answers to the questions presented in the previous phases.

4) Report :
Reporting the results of the analysis, including:

- Findings relevant to the case
- Actions that were performed
- Actions left to be performed
- Recommended improvements to procedures and tools

III. DIGITAL FORENSICS TOOLS AND THEIR COMPARISONS

A wide variety of digital forensics tools, both commercial and open source, are currently available to digital forensics investigators. These tools, to varying degrees, provide levels of abstraction that allow investigators to safely make copies of digital evidence and perform routine investigations, without becoming overwhelmed by low level details, such as physical disk organization or the specific structure of complicated file types, like the Windows / OS registry. Many existing tools provide an intuitive user interface that turns an investigation into something resembling a structured process, rather than an arcane craft. The main objective of digital forensics tools is to extract digital evidence which can be admissible in court of law. Various digital forensics tools and their description are provided in [18, 19].Comparisons of some commercial and open source forensic tools is given in table 1.

Table 1: comparisons of digital forensics tools

Product	Supplier	UNIX / Linux	Windows	Remote Capture	GUI	Pre-forensic Audit
Coroner's Toolkit	Open Source	Y	N	N	N	N
Sleuth Kit / Autopsy Browser	Open Source	Y	N	N	Y	N
Encase Forensic	Guidance Software	N	Y	N	Y	Y
Forensic Toolkit	Access Data	N	Y	N	Y	Y
i2Analyst's Notebook	i2 Inc.	N	Y	-	Y	N
LogLogic LX2000	LogLogic	Y	N	Y	Y	N
Mandiant First Response	Mandiant	N	Y	Y	Y	Y
ProDiscover Incident Response	Technology Partners	N	Y	Y	Y	Y
Netwitness	Man Tech Intl.	Y	N	-	N	N

IV. EMERGING TRENDS AND ISSUES

The fusion of cloud computing, mobility, personal devices, and social media is representing an opportunity for IT to deliver significant benefits to the organization. However, new technology also means new enhanced and diversified risk. The digital forensic also facing a crisis as the result of advances and fundamental changes in the computer industry [20, 21]:

- Use of the "**cloud**" for remote processing and storage present new challenges because network data is often difficult to locate, thus acquisition might be challenging or even impossible.
- **Social networking** sites such as Google+, Facebook, Twitter, and YouTube have expanded rapidly in recent years, so there is a need for network forensic tools that address such an important area of usage.
- The digital forensics investigations were previously limited to the analysis of Single systems with single small capacity disks, now increasingly investigations require analysis of Multiple Systems with multiple large capacity disks, network storage, and encrypted volumes. **The growing size of storage** devices means that there is frequently insufficient time to create a forensic image of a subject device, or to process all of the data once it is found.
- **Mobile and embedded devices :**
  - The mobile phones are the most diverse , as they tend to have no standard interface, either at the hardware or software levels, essentially making the analysis process unique to each device model.
  - The short product cycles from the manufacturers to provide new mobile devices and their respective operating systems are making it difficult for law enforcement agencies to remain current with new technologies.
- **Encryption**: With Yahoo promising "encryption everywhere," Google moving to 2,048-bit certificates by year's end, HTTP 2.0 to be automatically encrypted, and a renewed interested in secure email, we've entered a new phase: the era of encryption by default over the network. One side it will enhance the security but on the other side it will be difficult to collect information for law enforcement agencies.
- **Solid State Drives (SSD)**: The traditional magnetic drives are being replaces with SSD. Solid state drives initiate the garbage collection routine automatically it leads problem from perspective of forensics analyst. First, verifying the integrity and admissibility of the evidence. Second, there is the automated destruction of potentially relevant data on the drive. If the garbage collection routine run during or after data acquisition, validation becomes exponentially difficult because the hash value won't match.
- The non-traditional networking devices are increasingly appearing in network. Examples of non-traditional network devices are office infrastructure (e.g. printers, copiers, scanners, fax machines), media players, game consoles, phones, smart TVs, routers and security cameras and even cars and home appliances. With millions of devices now connecting to the Internet and in many cases, running embedded operating systems like Android, these devices are becoming a magnet for cyber criminals to hack into. While these newer devices may not hold information themselves, they are often a gateway to access the network and access enterprise data. There is a need to develop methods to determine how these devices interacted with the network during a time period of interest.
- Malware that is not written to persistent storage necessitates the need for expensive RAM forensics.
- **Anti- Forensics**: Anti-Forensics is an attempt to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct. There is a need to develop or modify forensic tools to detect and control the availability of anti-forensics.

V. CONCLUSIONS

The threat of cybercrime is increasingly apparent to individuals and organizations across the globe. From phishing to hacking, scamming to grooming, and botnets to cyber-terrorism, the variety and ingenuity of exploits appear to expand constantly. Besides the advancement in the digital forensic investigation tools, the methodologies or techniques developed to obtain the information also become more advanced. One of the key factors of the situation is contributed by the way computing technology evolves. The rapid development of computing devices requires new methods or tools to be used by the digital forensic investigators to obtain the evidences as a legally acquired evidence to be presented in the court. As the computing technology evolves the way computer user use or transfer the data in their environment also different from traditional computing system. As an initial step to reduce the privacy issue, it is crucial to combat the problems at the root level. The root level solution is in our mind. Educating the human mind to become an ethical person in their work is one of the key factors that we think will help to reduce the issues in privacy. The method to educate people on privacy need to be effective enough, as we are human tends to explore something new to us. So, regardless how powerful the tools of digital forensics might evolve, for the unethical mind, the privacy of related parties can be compromised and we have to successfully create a structure of a secured network computing that can guarantee the privacy we want in future. This paper briefly describes this fascinated area digital forensics, various phases and its process. It also discusses various digital forensics commercial and open sources tools for forensics investigation and its comparisons. And at the end this paper predicts and gives the current trends of crisis in digital forensic that have been identified by many observers.

REFERENCES

[1] Anna Burgard and Christopher Schlembach , "Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet ", International Journal of Cyber Criminology, vol 7 (2): 112–124, July – December 2013.

[2] Deloitte," Cyber Crime: A Clear and Present Danger; Combating the Fastest Growing Cyber Security Threat", Center for Security & Privacy Solutions. p. 1-16, 2010.

[3] The Global State of Information Security Survey 2014 released by PwC US in conjunction with *CIO* and *CSO* magazines, Available at: www.pwc.com/gsiss2014.
[4] Information Security Breaches Survey 2013, technical report conducted by PwC in association with infosecurity, Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200455/bis-13-p184-2013-information-security-breaches-survey-technical-report.pdf.
[5] Information security predictions for 2014 from Symantec, Available at: http://www.symantec.com/connect/blogs/2014-predictions-symantec-0.
[6] Palmer, G." A Road Map for Digital Forensic Research". DFRWS Technical Report 2001.
[7] Kruse W. G. & Heiser J. G. Computer Forensics. Incident Response Essentials. Addison-Wesley 2001.
[8] John Sammons, The basics of Digital Forensics, Elsevier 2012.
[9] Digital forensics - Wikipedia, the free encyclopedia. Available at: en.wikipedia.org/wiki/Digital_forensics.
[10] Brian Hay, Matt Bishop, and Kara Nance. "Live Analysis: Progress and Challenges," IEEE Computing in Science and Engineering Volume 7 Issue 2, March 2009 Pages 30-37.
[11] Sasa Medevac, Alvin Huseinovic and Ernedin Zajko. "Combining static and live digital forensics analysis in virtual environment". IEEE XXII International Symposium on Information, Communication and Automation Technologies, 2009. ICAT 2009. Pages 1 -6.
[12] C. P. Grobler, C. P. Louwrens, and S. H. von Solms, "A Multi-component View of Digital Forensics". International conference on Availability, Reliability, and Security 2010, pp. 647-652, IEEE.
[13] Soltan Alharbi, Jens Weber-Jahnke, and Issa Traore." The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review", International Journal of Security and Its Applications Vol. 5 No. 4 2011.
[14] A. Orebaugh. "Proactive forensics," Journal of Digital Forensic Practice, vol. 1, p. 37, 2006.
[15] K. Ruan. "Cloud Forensics: An Overview," Proc. 7th IFIP Conf. Cloud Computing, Centre for Cybercrime Investigation, Univ. College Dublin, 2012.
[16] H.V. Zhao. "Behavior Modeling and Forensics for Multimedia Social Networks: A Case Study in Multimedia Fingerprinting", IEEE Signal Processing Magazine, Jan. 2009, pp. 118-139.
[17] Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang; Guide to Integrating Forensic Techniques into Incident Response , Recommendations of the National Institute of Standards and Technology 2006.
[18] List of digital forensics tools - Wikipedia, the free encyclopedia. Available at: http://en.wikipedia.org/wiki/List_of_digital_forensics_tools
[19] Andrew Zammit Tabona," Top 20 Free Digital Forensic Investigation Tools for SysAdmins", 2013. available at : http://www.gfi.com/blog/top-20-free-digital-forensic-investigation-tools-for-sysadmins/
[20] S. L. Garfinkel, "Digital forensics research: The next 10 years," Digital Investigation, vol. 7, pp. S64-S73, 2010.
[21] Farhood Norouzizadeh Dezfoli, Ali Dehghantanha, Ramlan Mahmoud, Nor Fazlida Binti Mohd Sani and Farid Daryabar, "Digital Forensic Trends and Future", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 48-76 2013.

