Emerging trends and research in digital forensics

[a]**Anamika Joshi, [a]D.S. Bhilare**
[a]School of computer science Devi Ahilya University Indore, India

Abstract

Digital Forensics is the field of forensics science that deals with digital crimes and crimes involving computers. Digital forensics is used not only to investigate computerized crimes, such as network intrusion, fabrication and unauthorized access of data and illegitimate material distribution through digital services, but also to investigate crime where evidence is stored in any digital format on any digital device. Advancements in information technology such as cloud computing, social networking, personal devices such as smart phones; BlackBerrys, web 2.0 etc. is on one side represent an opportunity and benefits to the organisation and on other side have posed new challenges for those policing cybercrimes. This paper discusses the research category in digital forensics and identifies key research issues of each of the category.

KEYWORDS: Digital forensics, digital evidence, network intrusion, information security.

1. Introduction

Cyber-crimes or digital crimes have increased in frequencies, and their degrees of sophistication have also advanced. It poses major implications for national and economic security [1, 5]. Many industries and institutions, public-and private-sector organizations are at significant risk. This statement has been proved by the number of complaints received and processed by the Federal Bureau of Investigation (FBI) in collaboration with Internet Crime Complain Center (IC3) [2]. In 2012, the total complaints received are 289,874, in which the complaints reporting loss are 114,908. The overall statics are illustrated in the following table.

Overall Statistics	
Total complaints received	289,874
Complaints reporting loss	114,908
Total Loss	$ 525,441,110
Median dollar loss for those reporting a loss	$ 600
Average dollar loss overall	$ 1,813
Average dollar loss for those reporting a loss	$ 4,573

From the cyber-crime or complaints reported, it indicates that the number of crimes involving computers and internet have grown over the last decades and it needs some mechanism that can assist law enforcement to determine the Who, What, Where, When, and How for crimes. As a result, digital forensics (DF) has evolved to assure proper and sufficient presentation of digital crime evidentiary data into court and the role of digital forensic becomes important to get digital evidence.

Digital investigations are distinguished from other types of investigations in two very important ways. First, they may be remote crimes. That means that the attack was initiated at some indeterminate distance from the target. The attacker may have used any of a number of techniques to obfuscate his or her true location or/and can use anti-forensics methods that prevent forensic tools, investigations, and investigators from achieving their goals [3]. The crime scene, literally, could extend around the world from an organization. The second distinguishing factor is the amount of data available to analyse. In a serious digital incident there can be terabytes of data that may (or may not) contain even bytes of evidences [4].

The current trends and new technologies such as cloud computing, social media, personal devices such as smart phones; web 2.0 etc. represent an opportunity for IT to deliver significant benefits to the organisation. However, new technology also means new enhanced and diversified risk. The digital forensic also facing new challenges because of it and to meet this challenges there is a need to build/modify digital forensics tools and techniques and identify the new research and development requirements.

This paper is organized as follows. Section 2 presents the related work in DF community. Section 3 briefly categorized the research issues in digital forensic according to recent review and concluded in section 4.

2. Related work

Unlike many research areas, digital forensics is a largely practitioner-driven field. As a result, the majority of the tools and practices have been developed in response to a specific incident or class of incidents, rather than as the result of a research plan.

There have been several efforts to define and find research areas in Digital forensics. On August 2001 the first Digital Forensic Research Workshop [6] was held with the objectives to begin forming communities of interested individuals and to start a meaningful dialog for defining the field and identifying the difficult, high-priority challenges that lie ahead. The major goal was to establish a research community that would apply the scientific method in finding focused near-term solutions driven by practitioner requirements and addressing longer term needs, considering but not constrained by current paradigms. The research problems identified are Framework for Digital Forensic Science, the Trustworthiness of Digital Evidence, Detection and Recovery of Hidden Data, and Digital Forensic Science in Networked Environments (Network Forensics).This was first and important attempt which gives proper direction to the Digital Forensics.

In June 2008 a group of digital forensics researchers, educators and practitioners met at CISSE 2008with the goal of collecting ideas for research categories, topics and problems in digital forensics. The result of this was an article by Nance, Hay and Bishop that attempted to define a Digital Forensics Research Agenda [7]. The authors identified six categories for digital forensics research: Evidence Modelling, Network Forensics, Data Volume, Live Acquisition, Media Types, and Control Systems.

Digital forensics has evolved significantly over period of time and was no longer a niche discipline. It is now considered a mainstream knowledge by professionals and industry alike, thus establishing the commercial and theoretical as well as legal point of view that the digital footprints that remain after interactions with computers and networks are significant and probative.

Digital forensics was once a niche science that was leveraged primarily in support of criminal investigations, and digital forensic services were utilized only during the late stages of investigations after much of the digital evidence was already spoiled. Now digital forensic services are sought right at the beginning of all types of investigations. Even popular crime shows and novels regularly incorporate digital evidence in their story lines, which give DF a popular cult like standing in general public's mind.

Beebe, in 2009[8] admitted as an area of future growth and improvement that digital forensics largely lacks standardization and processes, and what little widespread knowledge that we have is "heavily biased towards Windows platform, and to a lesser extent, standard Linux distributions."

Beebe elaborated the unaddressed issues of digital forensics, highlighting that the problem of scalability, lack of intelligent analytics beyond full-text search that could link up multi part scenarios, non-standard computing devices especially small and hand held devices, ease-of-use, and a laundry list of unmet technical challenges are the work that needs to be addressed in future with new technologies and research.

In 2010 Garfinkle argued in his paper entitled "Digital forensics research: The next 10 years" [4] that we have been in a "Golden Age of Digital Forensics," and that the Golden Age is quickly coming to an end. Increasingly organizations encounter data that cannot be analysed with today's tools because of format incompatibilities, encryption, or simply a lack of training. He believes that Digital Forensics is facing a crisis as the result of advances and fundamental changes in the computer industry like the growing size of storage devices, the increasing prevalence of embedded flash storage, the proliferation of operating systems and file formats, pervasive encryption, use of the cloud for remote processing and storage and digital forensic analysis shifted from single device to multiple devices. At the end this article summarizes current forensic research directions and argues that to move forward the community needs to adopt standardized, modular approaches for data representation and forensic processing.

The development of digital forensics tools is strongly driven by practitioners who can readily adapt cutting-edge research, while a variety of systematic barriers challenge these practitioners as per Walls [9] who develops digital forensic tools for use by law enforcement organizations in United States. In 2012 Garfinkle shares his 14 years' experience in developing DF tools in a paper entitled "Lessons learned writing digital forensics tools and managing a 30TB digital evidence corpus"[10].In this he explains that writing digital forensics tools is difficult than other kinds of software because of the diversity of data types that needs to be processed, the need for high performance, the skill set of most users, and the requirement that the software run without crashing.

3. Research Category in Digital Forensics

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 predict how the field of digital forensics will evolve. Based on various papers and Digital Forensics Research Workshop technical reports that we have reviewed, it seems that research in digital forensics can be categorized into six categories as shown in **Fig1**.

3.1 Framework:

Generally accepted digital forensics process framework is actively needed by digital forensics researchers, practitioners, and customers. A framework will provide a common starting point from which researchers and practitioners can identifies the research, new theories and development requirements [6].

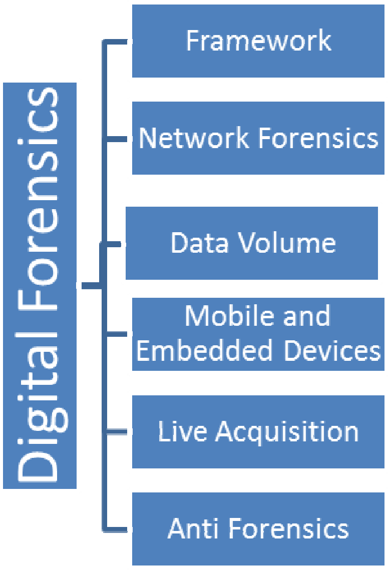

Figure 1: The six categories of Digital Forensics

In many digital crimes, the procedures used before 2001to accomplish digital investigation were neither consistent nor standardized. They were written with a focus on the details of the technology and without consideration for a generalized process [11]. In 2001, The Digital Forensics Research Working Group [6] defined a generic investigation process that can be applied to the majority of investigations involving digital systems and networks. This framework was an important foundation for future work.

A number of models and methodologies have been developed in the digital forensics field. The common elements shared by these models are identification, collection, preservation, analysis, and presentation. Some of them added addition detailed steps into the element to make the step more clear and precise.

Most of the models [6,11,12,22,13,14,15,17,19,20,24, and 28]are reactive in nature as the investigation is performed after the incident is reported. Only some of these models have explicitly mentioned the proactive process which gather and preserve digital evidence before and at the time of an incident occurs [26 and 27], some of the models such as [16, 18, 21, 23, and 25] also implicitly includes proactive process.

However, the nature of incidents and attacks has changed .As future work many papers [3,4,29,30] suggested that in order to address anti-forensics, to determine the root-cause of an incident and to successfully prosecute the perpetrator, the investigator needs relevant, admissible live digital evidences (for example volatile evidence, swap files, network processes etc.) which is possible by proactive forensics investigation.

The current investigation is very complex and time consuming as the single system with single small capacity disks are replaced by multiple systems with multiple large capacity disks and network storage. So in response to changing contexts there is a need a framework which can meet current challenges.

3.2 Network Forensics:

Network forensics is a branch of digital forensics that focuses on the monitoring and analysis of network traffic. It deals with volatile and dynamic data. It generally has two uses. The first, relating to security, involves detecting anomalous traffic and identifying intrusions. The second use, relating to law enforcement, involves capturing and analysing network traffic and can include tasks such as reassembling transferred files, searching for keywords, and parsing human communication such as emails or chat sessions and linking it to the ‘time frame’. The possible emerging network challenges and areas are [7, 48, 49, and 50]:

- 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 processing of network forensic data in real time could involve many different protocols and the amount of data could potentially be very large. 10-Gbps traffic flow with a two-hour sliding window requires 10 Tbytes of storage.
- While workstation and server network forensics are somewhat well understood, but it is less clear how network data from non-end-points, such as switches and routers could be collected, analysed and presented as evidence.
- 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, and even cars and home appliances. There is a need to develop methods to determine how these devices interacted with the network during a time period of interest.

A number of researchers have worked on this area such as collect information from computer networks to support forensics investigation. But there is a need to create and improve networking tools and processes to handle above mentioned new challenges.

3.3 Data Volume

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. Today a 2TB hard drive can be purchased for $120 but takes more than 7 h to image; systems and individuals of interest can easily have more storage than the police crime lab responsible for performing the analysis.

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. To handle this problem many research works has been done on this direction firstly selected evidence acquisition like Kenneally and Brown [33] has suggested The Risk Sensitive Evidence Collection (RSEC) Methodology. RSEC is on-scene Pre-searching and subsequent identification of evidence/artifacts and selective artifact/evidence extraction from live or dead systems. Instead of imaging whole disk and filtered out data during the analysis of a collected image, its shift filtering from analysis to collection to reduce the overall time needed in collection and analysis, and it's also reduce the storage requirement.

Brian Jones, Syd Pleno, and Michael Wilkinson [34] also suggest the use of random sampling in investigations and they discuss how the New South Wales Police Force, State Electronic Evidence Branch (SEEB) has implemented a “Discovery Process”. Using random sampling of files and applying statistical estimation to the results, the branch has been able to reduce backlogs from three months to 24 hours.

Secondly, applying data mining research to digital forensics [35] to gain some or all of the following benefits: (i) reduced system and human processing time associated with data analysis; (ii) improved information quality associated with data analysis; and (iii) reduced monetary costs associated with digital investigations.

And lastly Triaging [36, 37, 38, 39, and 40] has been proposed as a solution to systematically prioritize the acquisition and analysis of digital evidence.

Parallelization research could also provide benefits, the area identified in [7] are the imaging and carving process, and the development of user history timelines, including those based on multiple data sources. In addition, approaches that combine data imaging and evidence identification in parallel could also be beneficial, allowing an investigator to potentially direct the data acquisition process based on real-time results to acquire the most promising data sources during the initial phase of analysis.

3.4 Mobile and Embedded Devices

There have been major advances in the field as Computer Forensics has evolved into Digital Forensics. This change of name indicates the wide range of digital devices that are often part of an investigation. However, while devices such as cell phones, smartphones, including iPhone, Android and Blackberry, digital media players and game consoles may contain useful information, the law enforcement and forensics investigators have struggled to effectively manage digital evidence obtained from these devices. Some of the reasons include [51 and 52]:

- 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.
- File systems that are contained in mobile devices operate from volatile memory or computer memory that requires power to maintain stored information.
- 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.
- Pertinent data such as call histories are stored in proprietary formats in locations that will alter that data according to phone model. Even the cable used to access the mobile device’s memory will vary according to manufacturer and model.
- Different formats of information stored on mobile phones.

There are many devices that are cheaply manufactured in China and are very difficult to perform forensics by examiners. The primary reason is that inexpensive Chinese cell phones are unbranded, meaning they have no International Mobile Equipment Identity (IMEI) number and therefore, cannot be traced. Furthermore, forensics tools often cannot handle new or less commonly encountered devices, leaving an investigator to either develop custom tools, or lose the opportunity to examine the device. In addition to the number of incompatible devices of a particular type, the number of device types, especially integrated devices, is also growing rapidly.

3.5 Live acquisition

Traditional digital forensics has focused on static analysis—that is, the analysis of non-volatile data from a halted computer system. This approach maximizes result reproducibility, but it misses dynamic state Information, such as processes and network connections, memory-resident malware, unlocked file system decryption keys, or data in output buffers that isn’t yet written to file. In “Live Analysis: Progress and Challenges,” Brian Hay, Matt Bishop, and Kara Nance [31] explore the challenges and opportunities of live analysis—that is, the analysis of data gathered while a system is operating. The most significant challenge here is how to gather data without introducing distortions, especially when you must rely on the running system’s integrity to execute the data collection software correctly. Even live data collection using specialized hardware comes with opportunities for introducing distortion. Virtual computing presents new challenges and opportunities. On one hand, it enables continuous recordings of a virtual machine’s complete state, without running data-gathering software inside the virtual machine itself; on the other, it doesn’t entirely eliminate the possibility of distortion or detection by an opponent.

Sasa Mrdovic, Alvin Huseinovic and Ernedin Zajko [32] propose combination of static and live analysis. Virtualization is used to bring static data to life. Volatile memory dump is used to enable offline analysis of live data. Using data from memory dump, virtual machine created from static data can be adjusted to provide better picture of the live system at the time when the dump was made. Investigator can have interactive session with virtual machine without violating evidence integrity.

The research area identified in live acquisition are RAM analysis, methods for interrupting the execution for live acquisition, and methods for performing live analysis on systems without interrupting the execution sequences.[7] Live analysis gives less assurance and is less clear in compare to static analysis, as action taken by the investigator may change the state of the target system , and the dynamic state observed may not be reproducible, repeated analysis of the same state is not possible. As a result, there is certainly integrity, trustworthiness, and legal admissibility must be considered as a part of the research effort into the live analysis.

3.6 Anti- Forensics

Anti-Forensics is a set of techniques used as countermeasures to forensic analysis. It 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. In "Forensics Is So 'Yesterday,'" Michael A. Caloyannides [41] explains that computer forensics isn't effective against anti-forensic techniques and thus won't be useful for catching sophisticated criminals and agents. Instead, computer forensics will catch naive crooks who don't know how to hide their tracks and innocent people who don't know how to protect their systems. Liu and Brown identified four primary goals for anti-forensics [42]:

- Avoiding detection that some kind of event has taken place.
- Disrupting the collection of information.
- Increasing the time that an examiner needs to spend on a case.
- Casting doubt on a forensic report or testimony.

Anti-forensics methods are often broken down into several sub-categories: data hiding (encryption, steganography), artifact wiping, trail obfuscation and attacks against the computer forensics processes and tools (evidence elimination tools).

A number of research works has been done on this area such as [41, 42, 3 and 43] examining how to define and control the anti-forensics problem and [44, 45, 46and 47] has worked to identify and detect the availability of anti-forensics.

4. Conclusions

Resent advances in the field provide both challenges and opportunities. Advancements in information technology such as cloud computing, social media, personal devices such as smart phones; BlackBerrys, web 2.0 etc. is on one side represent an opportunity and benefits to the organisation and on other side have posed new challenges for those policing cybercrimes. The current forensics tools and processes are unable to provide reliable results in this new environment. This paper summarizes current research directions and major research areas in the digital forensics field. The major categories described in this paper are framework, network forensics, data volume, mobile and embedded devices, live acquisition and anti-forensics.

REFERENCES

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

[2] IC3, *2012 Internet Crime Report*. Federal Bureau of Investigation (FBI) and National White Collar Crime Center (NW3C).

[3] A S. Garfinkel (2007), "Anti-forensics: Techniques, detection and countermeasures," in 2nd International Conference on i-Warfare and Security, 2007, p. 77.

[4] S. L. Garfinkel (2010), "Digital forensics research: The next 10 years," Digital Investigation, vol. 7, pp. S64-S73, 2010.

[5] Dr. Richard Bassett, Linda Bass and Paul O'Brien (2006), "Computer Forensics: An Essential Ingredient for Cyber Security", Journal of Information Science and the Technology 2006, Volume: 3, Pages: 22-32.

[6] Palmer, G., 2001. A Road Map for Digital Forensic Research. DFRWS Technical Report.

[7] Nance Kara, Hay Brian and Bishop Matt (2009), "Digital forensics: defining a research agenda". In: Proceedings of the 42nd Hawaii international conference on system sciences; 2009.

[8] Beebe Nicole (2009), "Digital forensics research: the good, the bad, and the unaddressed". In: Fifth annual IFIP WG 11.9 international conference on digital forensics; January 2009.

[9] Walls RJ, Levine BN, Liberatore M and Shields C (2011). "Effective digital forensics research is investigator-centric". In: Proc. USENIX workshop on Hot Topics in Security (HotSec); 2011b.

[10] Simson Garfinkel (2012), "Lessons learned writing digital forensics tools and managing a 30TB digital evidence corpus", Digital Investigation 9 (2012) S80–S89.

[11] Mark Reith, Clint Carr and Gregg Gunsch (2002). " An Examination of Digital Forensic Models". International Journal of Digital Evidence, Volume 1, Issue 3.

[12] Brian Carrier and Eugene H. Spafford (2003)."Getting Physical with the Digital Investigation Process". International Journal of Digital Evidence , Volume 2, Issue 2

[13] Baryamureeba, V. and Tushabe, F. (2004). "The Enhanced Digital Investigation Process Model". Proceeding of Digital Forensic Research Workshop. Baltimore, MD.

[14] Séamus Ó Ciardhuáin (2004), "An Extended Model of Cybercrime Investigations ", International Journal of Digital Evidence, Volume 3, Issue1.

[15] A Beebe N. l. and Clark J. G. (2004). "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process". Proceedings of Digital Forensics Research Workshop. Baltimore, MD.

[16] Carrier B. and Spafford E. H. (2004). " An Event-based Digital Forensic Investigation Framework". Proceedings of 4th Digital Forensics Research Workshop. Baltimore, MD.

[17] Kohn M., Eloff J. and Oliver M. (2006). "Framework for a Digital Forensic Investigation". In Proceedings of Information Security South Africa (ISSA) 2006 from Insight to Foresight Conference.

[18] M. K. Rogers, J. Goldman, R. Mislan, T. wedge and S. Debrota (2006). "Computer Forensics Field Triage Process Model". Proceedings of Conference on Digital Forensics, Security and Law, (pp. 27-40).

[19] K. Kent, S. Chevalier, T. Grance, and H. Dang (2006), "Guide to Integrating Forensic Techniques into Incident Response," NIST Special Publication 800-86, 2006.

[20] R. S. C. Ieong (2006), "FORZA - Digital forensics investigation framework that incorporate legal issues," *Digital Investigation*, vol. 3, pp. 29-36, 2006.

[21] Jock Forrester and Barry Irwin (2006), "A Digital Forensic Investigative Model for Business Organisations", ISSA conference 2006. http://icsa.cs.up.ac.za/issa/2006/proceedings/research/57_

[22] Stephenson P. (2003)." A Comprehensive Approach to Digital Incident Investigation". Elsevier Information Security Technical Report. Elsevier Advanced Technology.

[23] Freiling F. C. and Schwittay B. (2007). "A Common Process Model for Incident Response and Computer Forensics". Proceedings of Conference on IT Incident Management and IT Forensics. Germany.

[24] Siti Rahayu Selamat, Robiah Yusof, and Shahrin Sahib (2008), "Mapping Process of Digital Forensic Investigation Framework". IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10.

[25] D. Billard (2009), "An Extended Model for E-Discovery Operations," IFIP*Int. Conf. Digital Forensics, volume 306 of IFIP Advances in Information and Communication Technology, page 277-287. Springer,* (*2009*).

[26] C. P. Grobler, C. P. Louwrens, and S. H. von Solms (2010), "A Multi-component View of Digital Forensics". 2010 international conference on Availability, Reliability, and Security, pp. 647-652, IEEE.

[27] Soltan Alharbi, Jens Weber-Jahnke, and Issa Traore (2011)."The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review", International Journal of Security and Its Applications Vol. 5 No. 4,

[28] Siti Rahayu Selamat, Robiah Yusof, Shahrin Sahib, and Irda Roslan, (2011)." Adapting Traceability in Digital Forensic Investigation Process". In proceeding of

Malaysian Technical Universities International Conference on Engineering & Technology (MUiCET 2011)

[29] A. Orebaugh (2006). "Proactive forensics," Journal of Digital Forensic Practice, vol. 1, p. 37, 2006.

[30] R. Ieong and HC. Leung (2007). ”Deriving, Cse-specific Live forensics Investigation procedures from FORZA”. Proceedings of the 2007 ACM symposium on Applied computing Pages 175-180.

[31] Brian Hay, Matt Bishop, and Kara Nance (2009). “Live Analysis: Progress and Challenges,” IEEE Computing in Science and Engineering Volume 7 Issue 2, March 2009 Pages 30-37.

[32] Sasa Medevac, Alvin Huseinovic and Ernedin Zajko (2009). “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.

[33] Erin E. Kenneally and Christopher L. T. Brown (2005). “Risk sensitive digital evidence collection”, Digital Investigation: The International Journal of Digital Forensics & Incident Response Volume 2 Issue 2, June, 2005 Pages 101-119.

[34] Brian Jones, Syd Pleno and Michael Wilkinson (2012) “The use of random sampling in investigations involving child abuse Material”, Digital Investigation 9 (2012) S99–S107.

[35] Nicole Beebe and Jan Clark (2005). “Dealing with Terabyte Data Sets in Digital Investigations”, IFIP — The International Federation for Information Processing Volume 194, 2005, pp 3-16.

[36] Adrian Shaw and Alan Browne (2013). “A practical and robust approach to coping with large volumes of data submitted for digital forensic examination”, Digital Investigation, Volume 10, Issue 2, 2013, Pages 116-128

[37] Stavros Shiaeles, Anargyros Chryssanthou and Vasilios Katos (2013). “On-scene triage open source forensic tool chests: Are they effective?” Digital Investigation Volume 10, Issue 2, September 2013, Pages 99–115.

[38] Andreas Moser and Michael I. Cohen (2013). “Hunting in the enterprise: Forensic triage and incident response”, Digital Investigation Volume 10, Issue 2, September 2013, Pages 89–98.

[39] Martin B. Koopmansaand Joshua I. Jamesb (2013). “Automated network triage”, Digital Investigation Volume 10, Issue 2, September 2013, Pages 129–137.

[40] Ilyoung Honga, Hyeon Yua, Sangjin Leeaand Kyungho Leea (2013). “A new triage model conforming to the needs of selective search and seizure of electronic evidence”, Digital Investigation Volume 10, Issue 2, September 2013, Pages 175–192.

[41] Michael A. Caloyannides (2009).” Forensics Is So "Yesterday"”, IEEE security and privacy 2009 (vol. 7 no. 2) pp. 18-25.

[42] Liu and Brown (2006), “Bleeding-Edge Anti-Forensics”, Infosec world conference and Expo, MIS training institute.

[43] Ryan Harris (2006). “Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem”, Digital Investigation Volume 3, Supplement, September 2006, Pages 44–49.

[44] G Valenzise, V Nobile, M Tagliasacchi and S .Tubaro (2011).” Countering JPEG anti-forensics”, Image Processing (ICIP), 2011 18th IEEE International Conference.

[45] Ioana Sporea, Benjamin Aziz and Zak McIntyre (2012). ” On the Availability of Anti-Forensic Tools for Smartphones”, International Journal of Security (IJS), Volume (6) : Issue (4) : 2012

[46] Bill Blunden and Below Gotham (2009). “Anti - Forensics: The Rootkit Connection”, Conference proceeding Black Hat USA 2009.

[47] Johannes Stüttgen and Michael Cohen (2013). “Anti-forensic resilient memory acquisition”, Digital Investigation 10 (2013) S105–S115.

[48] J. Broadway, B. Turnbull, and J. Slay (2008). “Improving the Analysis of Lawfully Intercepted Network Packet Data Captured for Forensic Analysis,” Proc. 3rd Int’l Conf. Availability, Reliability, and Security (ARES 08), IEEE CS, 2008, pp. 1361-1368.

[49] K. Ruan (2012). “Cloud Forensics: An Overview,” Proc. 7th IFIP Conf. Cloud Computing, Centre for Cybercrime Investigation, Univ. College Dublin, 2012.

[50] H.V. Zhao (2009). “Behavior Modeling and Forensics for Multimedia Social Networks: A Case Study in Multimedia Fingerprinting,” IEEE Signal Processing Magazine, Jan.2009, pp. 118-139.

[51] Michael Losavio, Dr. Deborah Wilson, and Dr. Adel Elmaghra by (2006). “Phone Digital Evidence Prevalence, Use, and Evidentiary Issues of Digital Evidence of Cellular Telephone Consumer and Small-Scale Digital Devices”, Journal of Digital Forensic Practice, 1: 291–296, 2006.

[52] David Bennett (2012). “The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations”, Information Security Journal: A Global Perspective, 21:159–168, 2012.