International Journal of Cyber-Security and Digital Forensics (IJCSDF) 3(4): 209-234
The Society of Digital Information and Wireless Communications, 2014 (ISSN: 2305-0012)

A Survey on Digital Forensics Trends

[1]Mohsen Damshenas, [2*]Ali Dehghantanha, [3]Ramlan Mahmoud
[1, 2, 3] *Faculty of Computer Science and Information Technology, University Putra Malaysia*
**Corresponding Author*
mohsen@zhoenix.com, {alid, ramlan}@upm.edu.my

1. ABSTRACT
Digital forensic has evolved from addressing minor computer crimes to investigation of complex international cases with massive effect on the world. This paper studies the evolution of the digital forensic; its origins, its current position and its future directions. This paper sets the scene with exploring past literature on digital forensic approaches followed by the assessment and analysis of current state of art in both industrial and academic digital forensics research. The obtained results are compared and analyzed to provide a comprehensive view of the current digital forensics landscape. Furthermore, this paper highlights critical digital forensic issues that are being overlooked and not being addressed as deserved. The paper finally concludes with offering future research directions in this area.

Keywords
Digital Forensic, Mobile Device Forensic, Forensic Framework, Network Forensic, String Analysis

2. INTRODUCTION
The term computer crime, first used in 1976 in a book by Donn Parker titled "crime in computer" [1],[2] stepped into the legal system by Florida Computer Crimes Act 1978 dealing with unauthorized deletion or modification of data in a computer system [3]. However, the first actual computer analysis and response team was established by FBI in 1984 to conduct advanced digital forensic investigation of the crime scenes [4].
One of the first complicated digital forensic investigation cases was performed in 1986, pursuing a hacker named Markus Hess [5]. Hess had gained unauthorized access to Lawrence Berkeley National Laboratory (LBL) and was detected and investigated by Mr. Clifford Stoll. At the time of the incident, there was not any standard digital forensic investigation framework in place so Clifford had to do the investigation on his own. As Clifford's objective was discovering the identity of the hacker, he did not change anything in the system and only collect the possible traces. By tracking the hacker for months using so called alarms which send notification when the attacker was active, he finally managed to discover the identity and location of the attacker by cooperation with the FBI and the Telco Company. Since the case was involved different military, academic and individual bodies in U.S and Germany the jurisdiction of the case became a big issue [6].
The day by day improvement of digital devices makes digital crime way more complicated than it was back in 1986. Nowadays crimes are happening over cloud which mandates cross national forensic investigation. It is therefore an essential demand for the security experts to realize their strengths in investigation of complex digital crimes via studying the history and current trends in the field. Specialists need to understand that digital forensics is not about looking at the past because of having an attack history; neither looking at the present in fear of being attacked; nor about looking at the future with uncertainty about what might befall us but about to being ready all the times for the moving target.
This survey offers a critical review and investigation over:

- Origins of digital forensics
- its evolvement to its current the current position
- And its future trends and directions

Vividly, using a map without knowing the current position is difficult; realizing the future can only be possible if the current and the past are clear. Hence, section 2 of this paper rectifies history of events and researches in the field in

the period of 2002 to 2007 while section 3 concentrates only on recent research works in the period of 2008 and 2013 and offers categorization of major fields and a statistical comparison between industrial and academic in the field. Finally, we look into overlooked issues and offer several future research directions in the field.

3. DIGITAL FORENSICS: THEN

The formal beginning of academic community research in the area of digital forensic investigation was in 2002 with an article called "Network Forensics Analysis" authored by Corey et al. [7] who studied Network Forensic Analysis Tool (NFAT) and highlighted its benefits in regard to traffic capture, traffic analysis and security issues.

In 2004, Stevens [8] illuminated the issue of comparing and correlating time stamps between different time sources and proposed a clock model to address these timing issues by simulating the behavior of each independent time stamp (A.K.A independent clock). This model can be used to remove the expected clock errors from time stamps and develop a more accurate timeline analysis of the events. Forte [9] studied tools and techniques which were widely used for digital forensic investigation namely "GLIMPSE" and "GREP" and explained their syntax and applications. GREP as one of the most popular text search tool was covered comprehensively in this article. Carrier and Grand [10] studied the essential requirements for volatile memory acquisition and proposed a hardware based method to acquire memory data with the least possible changes. This method employed a hardware expansion card (PCI slot card) to create a forensic image of volatile memory with the push of a button. However, this technique required pre-installation of the card on the victim machine. Mocas [11] identified basic properties and abstractions of digital forensic investigation process and proposed a comprehensive framework for unifying all characteristics of digital forensic. Vaughan [12] presented a methodology for evaluating the evidential value of an Xbox game console system. Moreover, he proposed a methodology for evidence extraction and examination from a suspect Xbox system. Nikkel [13] outlined the forensic investigation analysis of IP networks and domain names. This article defined point of concerns of a presence which automatically collects evidences related to the Internet presences, time-stamped these evidences, store the evidences in a neat manner, generate the integrity hash checksum of the evidence and finally produced an official report of the discovered information. Buchholz and Spafford [14] studied the effects of metadata on digital forensics to find out which information can be useful in a computer forensic investigation. Moreover, they demonstrated potentials of metadata in computer forensic investigation and analyzed issues in obtaining and storing these data.

In 2005, Francia and Clinton [15] outlined the required resources and procedures to establish a forensic lab and presented a cost efficient Computer Security and Forensic Analysis (CSFA) experimental lab design and implementation. Nikkel [16] discussed forensic investigation challenges in file and contents recovery of magnetic tape data acquisition and analysis and proposed a methodology for determination of tapes content. Jansen and Ayers [17] provided an overview of the available forensic investigation tools for Personal Digital Assistants (PDA) devices and PDAs software and hardware. They utilized some basic scenarios to evaluate those tools in a simulated environment using simulated evidentiary situations and offered a snapshot of how these tools work under provided situations. Bedford [18] explained the forensic investigation challenges of Host Protected Area (HPA) in IDE drives. The HPA is a part of a hard drive that is hidden from the operating system and the user whichis often used to hide sensitive data and as such is a good source of evidence.

In 2006, Harrison [19] described a project for explaining real-life issues in digital forensic investigation and utilized a group-based project for practicing computer investigation in academic environments. Laurie [20] studied well-known Bluetooth security flaws and available techniques and tools to exploit those flaws; and then discussed the effects of these attacks on common digital forensic investigation practices. Nikkel [21] described concepts of distributed network-based evidences, forensic

techniques of evidence acquisition over the network and the weaknesses of these techniques. In addition, he suggested some improvements to conquer challenges in network data collection. Ieong [22] highlighted major principles of digital forensic investigation and outlined eight roles with their responsibilities in common digital investigation frameworks. The paper proposed a framework named FORZA which is based on Zachman's framework [23]. Harris [24] studied and analyzed several anti-forensic techniques and classified them to achieve a standard method for addressing anti-forensics issues and then outlined general strategies to preserve forensic integrity during investigation. Garfinkel [25] proposed Forensic Feature Extraction (FFE) and Cross Drive Analysis (CDA) techniques to analyze large data sets of disk images and other types of forensic data. These two methods were used for prioritizing and systematically identifying social networks usage in the suspect's system. Schuster [26] explored the structure of memory containing processes' data and then proposed a search pattern to scan the whole memory dump for traces of physical memory objects independent of kernel's list of memory objects. As a proof of concept, an implementation of the technique successfully revealed some hidden and terminated processes and threads even after rebooting the system. Jeyaraman and Atallah [27] proposed an approach to examine the accuracy and effectiveness of automated event reconstruction techniques based on their capabilities to identify relations between case entities. They then quantified the rate of false positives and false negatives and scalability in terms of both computational burden and memory-usage. Alink et. al., [28] introduced a novel XML based approach for storing and retrieving forensic traces derived from digital evidences which was implemented in a prototype system called XIRAF. This system runs the available forensic analysis tools against the evidence file and then exports the result in an XML database. Johnston and Reust [29] outlined procedures for investigation of an attack which includes compromising of several systems with sensitive data and discussed challenges involved in this process. Mead [30] studied the National Software Reference Library (NSRL) repository of known software, file profiles, and file signatures by examining the uniqueness of the signatures produced in NSLR repository. This repository is essentially vital for digital forensic investigators to improve the speed of data analysis by omitting the file analysis of trusted files according to the retrieved hash checksum from NSRL. Nikkel [31] presented a forensic evidence collector tool using promiscuous packet capture on an embedded hardware using open source software. This tool operates as a standalone tool in different modesandcan be pre-configured by the investigator.

In 2007, Wang et al. [32] analyzed methods and applications of cryptography in digital forensic investigation, and highlighted differences between these methods. Afterwards, the authors discussed the weaknesses of SHA-1 and approaches to crack SHA-1 in order to highlight the issue of potential clashes in checksum verification and possible effects on related applications. Peisert et al. [33] presented the importance of examining the order of function calls for forensic analysis and showed its usefulness in isolating the causes and effects of the attack through intrusion detection systems. This analysis, not only detects unexpected events in the order of function calls, but also detects absence of expected events. Castiglione et al. [34] investigated the issues of hidden metadata in compound documents that use opaque format and could be exploited by any third party. The authors proposed a steganography system for Microsoft Office documentsand introduced FTA and StegOle as tools to improve the forensic analysis of Microsoft Office documents. Murphey [35] proposed a method to automatically recover, repair and analyze Windows NT5 (XP and 2003) events logs. Authors implemented a proof of concept code to repair common corruptions of multiple event logs in one simple step without any manual user intervention. Spruill and Pavan [36] studied the U3 technology for portable applications and illustrated different artifacts left behind from a committed crime through a portable application. This research also investigated some of the common applications used on U3 drives. Turner [37] questioned usefulness of the common digital forensic investigation approaches in live incident

investigation and demonstrated the applications of Digital Evidence Bag (DEB) storage format in dynamic environments. Richard et al. [38] explained Data Evidence Container (DEC) format to bundle arbitrary metadata associated with evidence along with the actual evidences. Authors then explored the challenges of utilizing this container and proposed Forensic Discovery Auditing Module (FDAM) as a complementary mechanism Nikkel [39] demonstrated digital forensic investigation principles for IPv6 networks and discussed about IPv6 addressing, packet structure, supported protocols and information collection from public registrars such as WHOIS. They finally presented some IPv6 tools for collection and analysis of network traffic and investigation of remote IPv6 nodes. Masters and Turner [40] demonstrated techniques of magnetic swipe card data manipulation in different types of devices and proposed the application of Digital Evidence Bag (DEB) as a suitable format for bulking the evidences obtained from a magnetic swipe card. Lyle and Wozar [41] studied challenges in making a forensic image of a hard disk and addressed practical problems like resolving some faulty sectors causing difficulties in imaging process. Arasteh et al. [42] proposed a formal model checking technique for forensic analysis of system logs and provided a proof of concept system using tableau-based proof checking algorithm. Arasteh and Debbabi [43] presented a forensic analysis method to extract threads history by using threads stack. The technique used a process model to retrieve data from a thread stack and then compared against an assembly model to verify extracted properties. Schatz [44] proposed a technique for obtaining volatile memory from arbitrary operating systems and provide a “point in time” snapshot of the volatile memory. Body Snatcher, an implementation of this method was used for presenting the proof of concept of the proposed technique. Barik et al. [45] studied the issues of Ex2 file system in terms of authenticity of the OS created timestamps andproposed a solution to preserve authentic date and time stamp for the studied issues using Loadable Kernel Modules (LKMs).

An overview of the above mentioned researches, as indicated in Figure 1, shows a smooth growth in the number of digital forensic investigation research articles published in main relevant journals namely "Digital Investigation", "Information Forensics and Security, IEEE Transactions on", "Computers & Security", "Computer Law & Security Review", "Multimedia Tools and Applications", "Computer Standards & Interfaces", "Computers & Mathematics with Applications", "Information Sciences", "Selected Areas in Communications, IEEE Journal on".

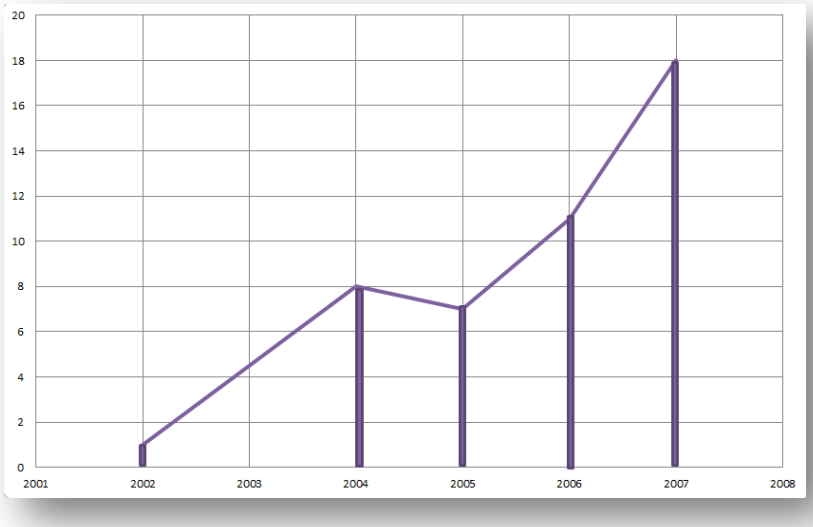

Figure 1: number of articles in digital forensics in the period of 2002 – 2008
(No articles matched our search criteria in 2003)

All the studied articles are extracted by searching the term "forensic" in the abstract of 4 main computer science indexing services known as Science Direct, Springer, IEEE and ACM; though the search was limited only to articles published in computer science during the period of 2002 – 2008.

4. NOW

From the very first days of digital forensic investigation's life up to now, there were vast improvements in digital forensics techniques ranging from recovering deleted evidences and searching the megabytes storage devices to deal with petabytes storage devices [46], cloud based investigations [47], mobile device examinations [48], wireless network investigations [49], and database forensics [50]. Generally, the current perspective of digital forensic investigation can be categorized into four main types namely Computer Forensic, Smart Device Forensic, Network Forensic and Database Forensic. Among mentioned categories, computer forensics has attracted the most attention of academicians and professionals. On the other hand, digital criminals and intruders are trying to minimize footprints of their actions utilizing anti-forensic techniques. Some of the common approaches of anti-forensics are using cryptography [51], steganography [52], meta-data tempering [53], program packing [54], generic data-hiding [52], and even disk sanitizing [55], [56].

In spite of all studies in the field of digital forensic investigation we are yet to have a comprehensive reliable study which offers analysis of related scientific research trends in the field. To address the aforementioned issue, we started this survey with searching in computer science research journals indexed by four main scientific database namely Science Direct, Springer, IEEE and ACM for papers published in the period of Jan 2008- Mar 2013 that include "forensic" as an author keyword or in the paper abstract. The result of the search contained articles published in main journals in the field namely "Digital Investigation", "Information Forensics and Security, IEEE Transactions on", "Computers & Security", "Computer Law & Security Review", "Multimedia Tools and Applications", "Computer Standards & Interfaces", "Computers & Mathematics with Applications", "Information Sciences", "Selected Areas in Communications, IEEE Journal on".

After several brainstorming sessions to identify main journals in the field, it was decided to keep our focus only on journals which published 2 or more papers in our searching period as shown in Table 1.

Table 1 – Final result of participated Journals with number of related papers in each

Journal Name	Number of Related Papers
Digital Investigation	117
IEEE Transactions on Information Forensics and Security	20
Computers & Security	9
Computer Law & Security Review	4
Multimedia Tools and Applications	3
ACM Computing Surveys	2
Computer Standards & Interfaces	2
Computers & Mathematics with Applications	2
Information Sciences	2
Personal and Ubiquitous Computing	2
IEEE Journal on Selected Areas in Communications	2

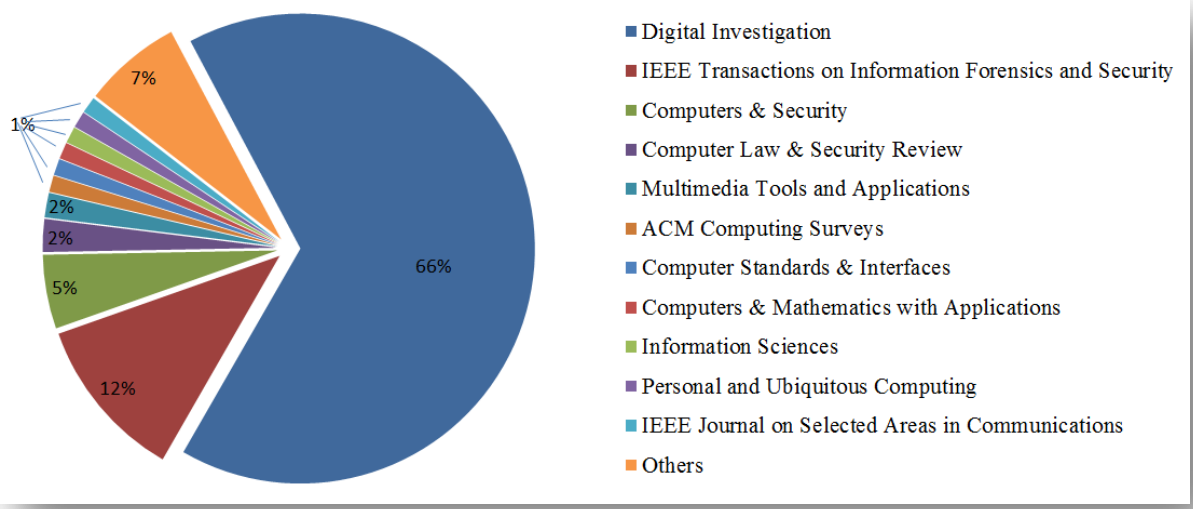

Figure 2 – Number of forensics relevant papers from Jan2008 –to Mar2013

Figure 2 offers a ratio of the position; "Digital Investigation" journal (indexed in "Science Direct") with 117 published articles (66% of total articles in the studied period) has the highest number of published articles followed by "IEEE Transactions on Information Forensics and Security" journal (indexed in "IEEE") with 20 published articles (12% of total articles in the studied period) and "Computers & Security" journal (indexed in "Science Direct") with 9 articles (5% of total articles in the studied period).

Not being an exception, this research faced some limitations. The main limitation of this study was to include all perspectives of digital forensic using trust worthy sources. The most important selection factor for us was creditability of our sources so we can provide a trustable review of current forensics landscape. As such, we just selected papers from reputable sources which indirectly implicates that we ignored possibly relevant papers which were not published in reputable sources. Selecting journals was not only based on the mere number of articles they published (2 or more) in a specific period (2008-2013), but to make sure only papers of very relevant journals which are reflecting realistic view of the field are selected. Moreover, to improve the reliability of the given perspective in addition to reputable academic sources some articles from the SANS reading room were included as the representative of the industrial research.

4.1. Results Obtained

The data collection process began with brainstorming among authors to identify major types of digital forensic investigation to classify and rank research papers appropriately. For example, all topics related to smartphone investigation, iPad data acquisition, GPS data analysis and similar subjects were categorized under mobile forensics. ISO9660 analysis, meta-data analysis, cluster and all investigations relevant to the science of file systems grouped as file system forensics. The same approach was taken for all other categories as well as shown in Figure 3. Finally, papers in topics like digital audio forensics, malware forensics [57], database forensic and cloud forensic which were not fall in previously mentioned categories and there were 5 or lesser papers in those topics were grouped as "Others" as shown in Figure 4. Identification of general categories was more difficult than it was expected as there were difficulties in categorizing inter-disciplinary papers or papers with wide range of focus. For example, papers under collecting volatile

memory of mobile phones could be categorized in both volatile memory acquisition and in mobile phones investigation category. Obviously, we could not count a paper multiple times and in such cases, the team carefully read the paper thoroughly to find out the major focus of the paper with specific attention to the paper abstract, keywords and conclusion. Afterwards, we categorized the paper in the most relevant category. It is notable that, the classification of this study is exclusively the opinion of the authors and although all relevant scientific and statistical techniques were employed to ensure correctness and comprehensiveness of the study but all conclusions are subjective to author's view-points only. Moreover, there were several publications contain news section or discussion that cannot be qualified to be called full article. Each of these papers were analyzed carefully and included in this survey if they offer valuable knowledge or results about the current state of the art in digital forensic.

When investigating each of the journals separately, it is interesting to note different topics emphasized in each journal. Table 2 lists the number of publications in each journal in each topic. Outstanding result indicates that the "Digital Image Forensic" topic took the lead with 20 articles, followed by "Mobile Device Forensic" with 14 articles, "forensic framework" at 12, "forensic tools" and "file system forensic" both at 9 that constitute the top six topics. In "IEEE Transactions on Information Forensics and Security", articles on anti-forensics were more than all other categories (3 articles), followed by "digital image forensic", "forensic tools" and "string analysis" with only 1.

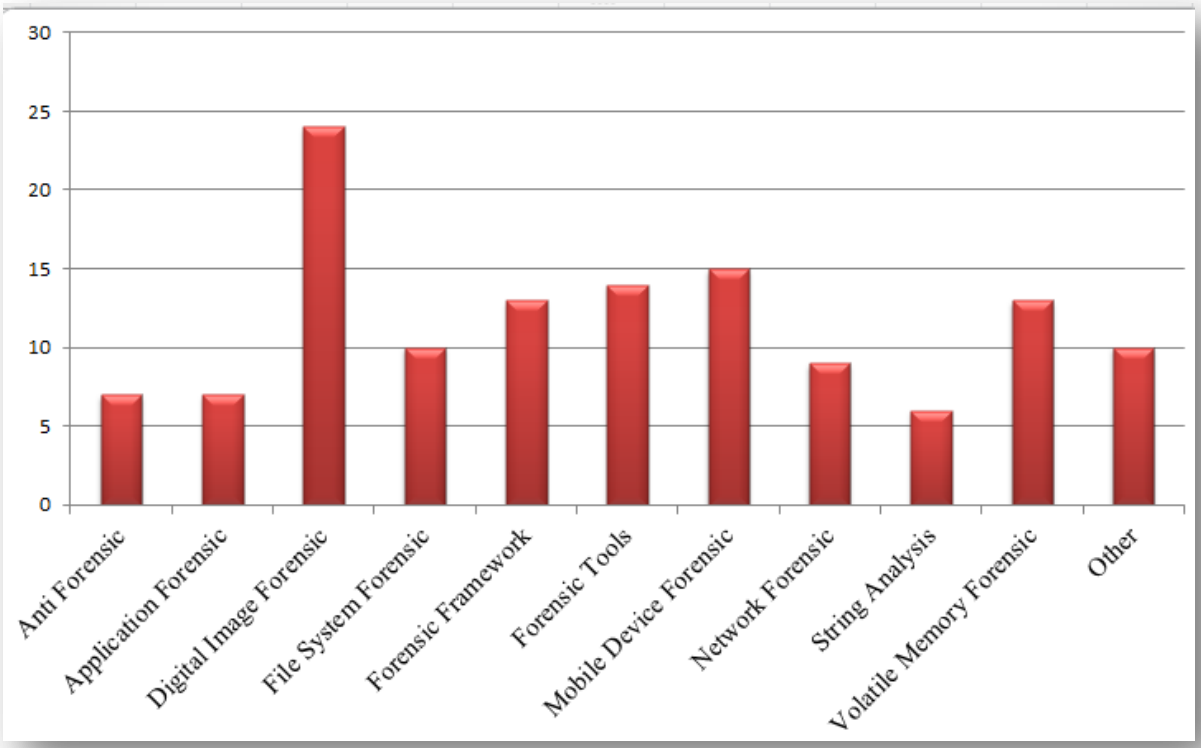

Figure 3 – Digital forensic investigation categories in period of 2008 - 2013

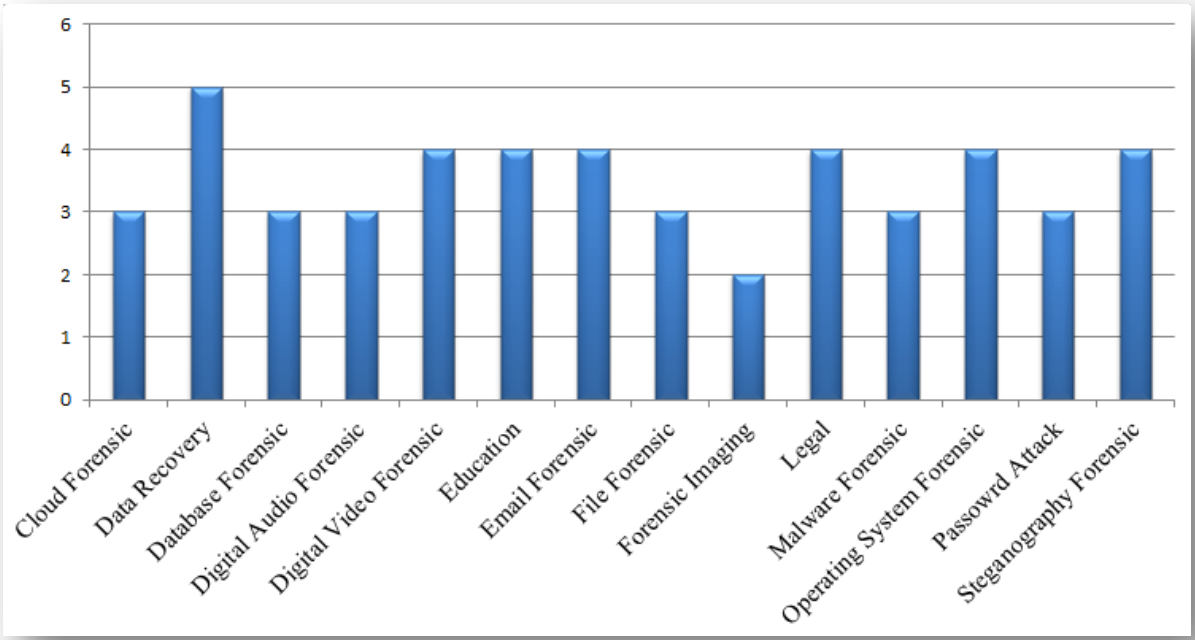

Figure 4 – Digital forensic investigation topics with less than 5 papers ("Other" category)

Table 2 – List of journals and number of published articles grouped by the category

Topics VS Journals	Digital Investigation	IEEE Transactions on Information Forensics and Security	Computers & Security	Computer Law & Security Review	Multimedia Tools and Applications	ACM Computing Surveys	Computer Standards & Interfaces	Computers & Mathematics with Applications	Information Sciences	IEEE Journal on Selected Areas in Communications	Personal and Ubiquitous Computing
Anti Forensic	2	3	1					1			
Application Forensic	7										
Digital Image Forensic	20	1	1	1					1		
File System Forensic	9									1	
Forensic Framework	12							1			
Forensic Tools	9	1	2								
Mobile Device Forensic	14		1								
Network Forensic	5				2						1
String Analysis	1	1					1		1		
Volatile Memory Forensic	10										

4.1.1. Topics covered by SANS

This subsection of the study analyzes articles published in the SANS reading room as a well-established organization known as a pioneer in non-academic digital forensic investigation research. SANS papers are considered as a reliable source for studying industrial digital forensic research trends. However, the quantitiy of SANS forensics articles is just a few in compare to the academic journals as publication is not included in the main duties of the forensics practitioners.

We have identified 24 papers in SANS reading room and categorize them similar to the academic papers. The outcome includes "File Forensic", "File System investigation", "Forensic Framework Development", "Forensic Tools Investigation", "Legal Aspects of Digital Forensics", "Mobile Device Investigation", "Operation System Investigation", "Database Investigation", "Network Investigation", "Steganography" and "String Analysis" categories as shown in Figure 5.

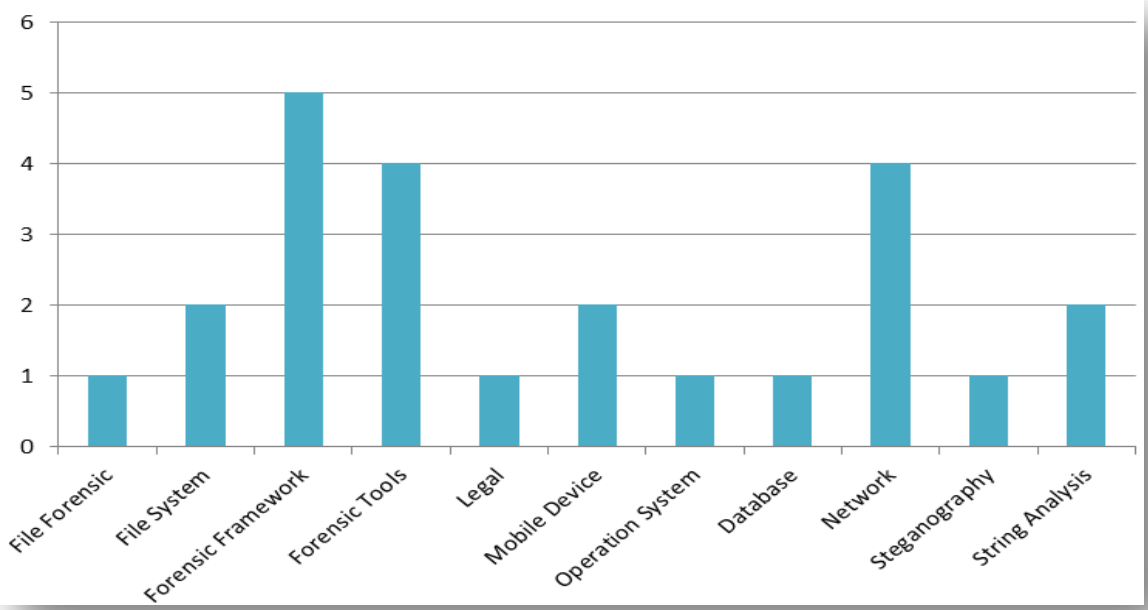

Figure 5 – Categories of SANS articles

The further analysis of the SANS articles indicates the differences between academic and industrial research trends. The results show that the share of forensic framework, network forensic and forensic tools from overall SANS articles is %21, %17 and %17; while they have only %8, %5 and %8 of academic journals. On the other hand, in academic environment, digital image forensic, mobile device forensic and forensic tools were the leading topics.

Figure 6 is the result of comparing the common topics between SANS and academic journals while the SANS topics lacks some of the topics covered in academic environments. Figure 7 clearly indicate the results by providing the share of each topic in SANS and academic journals.

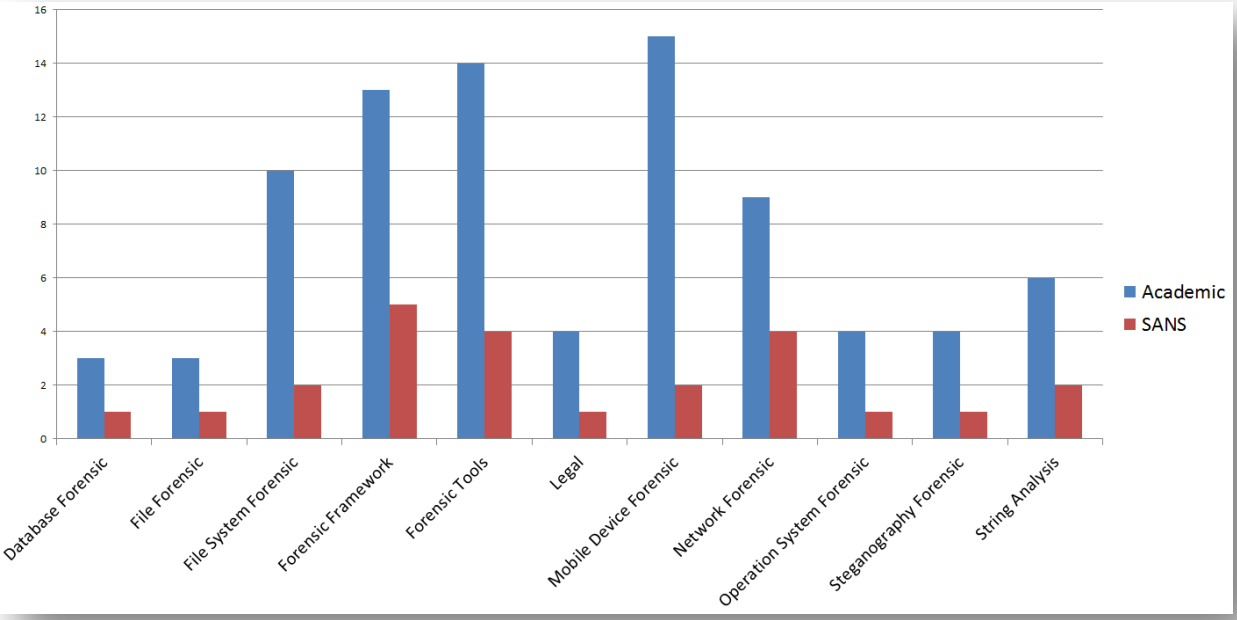

Figure 6 – Comparison of common categories in academic and SANS publications in term of number of articles

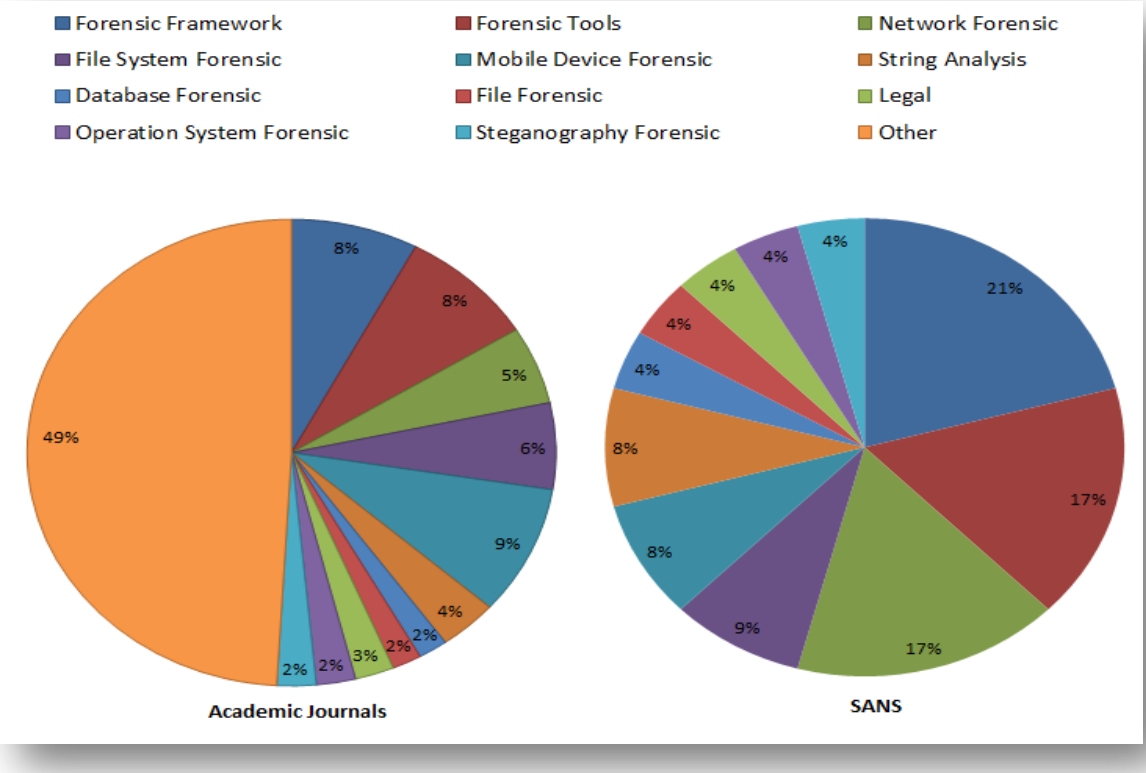

Figure 7 – SANS vs. Academic Journals (the "Other" in academic journals indicates the topics which were not covered in SANS articles)

4.2. Discussion and Analysis

In this section, we offer detailed analysis of each of 10 most categories identified in the previous sections namely digital image forensic, mobile device forensic, forensic tools, volatile memory forensics, network forensics, anti-forensic, data recovery, application forensics, file system forensics and forensic frameworks. We critically analyze trends and current state of the art in each category and rectify possible future trends.

4.2.1. Digital Image Forensics

Since the wild increase in usage of digital images, the crimes involving digital images such as image forgery are increased consequently and detection of the image tampering brought many difficulties to forensic investigators and forensic researchers. The major detectable research topics in digital image forensics are image authenticity, image correction, steganography, image processing and source detection.

Image authenticity as the most popular topic in Digital Image Forensic category concerns about the reliability of the evidence. Amerini et al. [58] proposed a SIFT based algorithm to detect multiple copy-move attacks on an image. This technique extracts and matches the image features to identify similar local region on the image and then makes a hierarchical cluster of the extracted features to identify the cloned areas. In case the image is classified as unauthentic, the geometrical transformation will be identified to discover the original area and the copy-moved area. Gou et al. [59] introduced a source identification technique with the ability of recognizing various post-processing operations on scanned image. Utilizing the noise analyses through wavelet analysis, neighborhood detection and image de-noising, made this approach capable of detecting the model of scanner used to scan the image and type of the image source (scanner, digital camera or computer generated). Chen et al. [60] introduced a source digital camera identification technique with integrity verification capability based on Photo Response Non-uniformity Noise (PRNU) imaging sensor fingerprint. The PRNU is generated through the maximum likelihood principle derived from normalized model of the sensor output and then compare to a pre-generated experimental dataset. Yuan [61] introduced a novel method for detection of median filtering in digital images. The key points of this method were the capability of median filtering detection for low resolution, JPEG compressed images, and tampering detection in case a median-filtered part is inserted in a non-median-filtered image and vice versa. Mahdian and Saic [62] studied the addition of locally random noise to tampered image regions for anti-forensic purposes and introduced a segmentation technique for dividing the digital image into various partitions based on homogenous noise levels. Their novel approach utilized tiling the high pass wavelet coefficients at the highest resolution with non-overlapping blocks, to estimate the local noise level and median based method to estimate the standard noise level of the image. Farid and Bravo [63] introduced a novel methodology for computer aided differentiation of photorealistic computer generated images and photographic image of people using images with different resolution, JPEG compression, and color mixture of the image. Kornblum [64] studied the quantization tables in JPEG compression and explained how quantization tables can be used for differentiating between images processed by software and intact images. Authors utilized other factors such as the presence or absence of EXIF data, signatures of known programs, and color signatures of real skin to increase the success rate of the detections. Mahalakshmi et al. [65] proposed an approach for detection of image manipulations through available interpolation related spectral signature method. This method could detect common forgeries like re-sampling (rotation, rescaling), contrast enhancement and histogram equalization. Moreover, a set of techniques were introduced for detection of global and local contrast enhancement and histogram equalization.

Source detection explicitly tries to identify the source device with which the image is taken or edited. Tsai et al. [66], the author employed support vector machines and decision fusion to identify the camera source model of an image. The evaluation result of the proposed model indicates 91.66% accuracy for images take by 26 cameras. Choi et al. [67] proposed a new approach for color laser printer identification of

an unknown printed image, based on the noisy texture analysis and support vector machine. This method identifies the invisible noises of the schema according to wiener-filter and the 2D Discrete Wavelet Transform (DWT) filter and then the texture of the noise is analyzed via gray level co-occurrence matrix (GLCM).

Image processing involves the analysis of the image to find specific patterns for variety of purposes. Islam et al. [68] proposed a framework for detection of children skin in images which utilized a novel vision model based on the Markov Random Fields (MRF) prior by employing a skin model and human affine-invariant geometric descriptor to identify skin regions containing pornographic. Steel and Lu [69] proposed a system called Automated Impersonator Image Identification System (AIIIS), which tracks the used image in impersonation attack back to the original source by employing digital watermarking technique. This technique it encoded access details of the image (like IP address, server and the download date-time) and download them to the image. In [70], the author utilized demosaicing artifacts to identify the digital camera model. The process includes estimating demosaicing parameters, extracting periodicity features of the image for the purpose of detecting simple forms of demosaicing and finally defining a set of image characteristics as features to be used for designing classifiers that distinguish between digital cameras.

Image correction as another hot topic in image forensic, mainly intends to ease the analysis of the image. Tang et al. [71] developed a Knowledge Based (KB) approach to remove JPEG blocking artifacts in skin images. The approach utilized a Markov model based algorithm and a one-pass algorithm to implement the inference; plus a block synthesis algorithm for handling the cases with no prior record in dataset. Moreover, in order to reduce the search time in the dataset, the author proposed a multi-dimension indexing algorithm. Lin et al. [72] introduced a method for detecting the image source encoder alongside the estimation of all coding parameters based on the intrinsic fingerprints of the image source encoder. The evaluation of this approach indicated the success rate of more than 90% for transform-based encoders, sub-band encoders, and DPCM encoders when PSNR is higher than 36dB.

Steganography as one of anti-forensic techniques in digital images plays a significant role for identification of the evidence. Huang [73] provided a solution for detection of double JPEG compression using the “proper” randomly perturbed ratio. This approach is highly dependent on finding the correct ratio; thus a novel random perturbation strategy is utilized on the JPEG coefficients of the recompressed image. Kirchner and Bohme [74] challenged the current image tampering detection techniques by presenting types of image transformation operation that cannot be detected using the available resampling detection tools. Among these attacks, resampling with edge-modulated geometric distortion and the dual-path approach are nearly impossible to be detected.

4.2.2. Mobile Device Forensics

Due to the wild incline in usage of mobile devices such as smart phones, tablets and GPS devices, investigation of such devices is significantly vital; thus obtaining and analyzing the evidence from mobile devices has a great value. In continue Mobile live memory, Mobile forensic framework, Mobile forensic tools and Mobile on-scene triage topics are discussed.

Mobile live memory concerns about imaging and analyzing mobile devices volatile memory. In [75] the authors presented a novel approach to obtain forensic image of an Apple iPad device through iPad camera connection kit and a USB storage device. The results of the evaluation indicated that this method can obtain image up to 30 times faster than acquiring image through the usual method utilizing Wi-Fi channel. Thing et al. [76] proposed a system for real-time digital forensic analysis of mobile memory with focusing on dynamic properties of memory. The system evaluation consists of investigation of different communication variables (i.e. message length, message interval, dump interval, key-press interval) which resulted in 95.6% and 97.8% for dump intervals of 40 and 60 seconds. Sylve et al. [77] illustrated the process of live memory collection of the android devices, the new memory dump module (named DMD or LiME (Linux Memory Extractor)) and the challenges of device independent memory

acquisition; it then proposed a memory collection method which can dump memory to SD card or network storage. The proposed method operates via "rooting" the android device with methods like "Rage against the Cage" and other privilege escalation techniques.
Depends on the type of device, utilizing the right mobile forensic tool always plays a noteworthy role. In [78] authors enriched their previously published methodology for smartphone evidence acquisition (Mobile Internal Acquisition Tool) in term of improvements and assessments. The MIAT can be executed from a memory card like MMC and explores recursively the file system tree and copy each entry to a backup volume. The behavior of MIAT is also evaluated by comparing to Paraben Device Seizure as a well-known tool. Vidas et al. [79] illustrated the digital forensics collection method of Android device via a modified boot loader from recovery bootimg. The advantage of this method is mainly because it only slightly changes the recovery partition and no user or system partition is affected during the collection stage of the investigation unlike normal approaches which "root" the android device for image acquisition.
Mobile forensic framework discusses different procedures and frameworks for mobile device forensics. In [80], the authors investigated the use of mobile phone flash boxes in a forensic framework and proposed a validation procedure to ensure the integrity of the acquired evidence in this new method. Unfortunately using mobile phone flash boxes do not provide forensically sound evidence; even though this proposed method increased the percentage of the reliability of the evidence, it still lacks the sufficient evidence integrity proof and demand to be lifted up by further research. Owen and Thomas [81] studied the available framework for mobile forensic investigations and highlighted the lacks and strength of each in comparison with the common digital forensic investigation practices of hard disk drives. Grispos et al. [82] compared the available mobile forensic toolkit for discovering to what extend these tools can operate and how much they are reliable. The result of this comparison indicated the limitations of using file carvers for information recovery, conflicts of diverse methods of information recovery, several differences between the documented capabilities of the CUFED and its actual performance, and the fragility of existing mobile forensic toolkits when recovering data from partially corrupted file system images.
Mobile on-scene triage determines the priority of evidence collection in mobile devices. In [48], the author presented a methodology for obtaining and analyzing evidences in webOS system partition; the article provides solution for obtaining different types of evidence (i.e. Call logs, contacts, calendar events and etc.). The article also provided approaches for recovering deleted files from a webOS operating system. Eijk and Roeloffs [83] discussed the challenges of obtaining evidence from TomTom GPS device and approaches to acquire volatile memory of the device via either JTAG signals or loading a small Linux distribution to the GPS memory. The article described the structure of data on GPS device and technique for analyzing the obtained data. In [84] the author studied the available framework for forensic investigation of windows mobile equipped mobile phones and showed the similarities of windows mobile investigation with normal windows investigation on PC systems. This work demonstrated that Windows mobile phone investigation obeys the common digital forensic investigation framework and the analysis of collected data is very much similar to windows operating system. Mislan et al. [85] studied the on-scene triage of mobile devices and compare its requirements with common digital forensic investigation requirements; it formalized the on-scene triage process and provides guidelines for standardization of the process. At the end, it defined the basic requirements of an automated on-scene triage.

4.2.3. Forensic Tools

Employing different tools in the process of digital forensic is inevitable for the investigator, yet choosing the most suitable tool can affect the result of the investigation. The identified research topics of this category would be as forensic formats, new forensic tools, and forensic tools examination.
This topic, new forensic tools, reviews novel tools discussed in forensic articles. In [86] authors presented a forensic investigation tool

named Cyber Forensic Time Lab which help the investigator to sort all evidences according to their time variables for generating Temporal analysis of the crime. Klaver [87] introduced the forensic application of available tools on Windows CE (Windows Mobile) after studying the typical hardware information and software components. The author explained the usage of current tools for forensic investigation of Windows CE mobile phones. Joyce et al. [88] discussed the Mac OS x forensic investigation approaches and introduced MEGA, a comprehensive tool for analyzing Mac OS x files from an image. MEGA offers ease of access to Spotlight metadata, content search and FileVault encrypted home directories. In [89], authors described their novel techniques to develop a memory analysis tool for variety of operating systems. Inoue et al. [90] provided a new tool for volatile memory imaging of the Mac OS x and then compared it using four metrics of completeness, correctness, speed and interference. Moreover, a visualization method called the density plot is introduced for indicating the density of repeated pages in an image.

There is always a demand for testing approaches to examine the performance and accuracy of the tools. In [91] the first generation of computer forensic tools is challenged by the authors as they have limitations and flaws in processing speed, data design, auditability, task analysis, automation and data abstraction; and then the second generation tools requirements is discussed and some available tools is suggested for handling each deficiency. Pan and Batten [92] presented a performance testing approach for digital forensic tools offering testing with good quality via a limited number of observations. The proposed method is specially designed for forensic tool testing and claimed of being the best available software among forensic tool performance testers.

Choosing the forensic format of the evidence has an important role in the forensic investigation process; in continue four novel forensic formats are proposed by different authors. In [46], the author introduced a redesign of the Advanced Forensic Format (AFF) based on the ZIP file format specification. This file format support full compatibility with previous versions of AFF while it offers the capability of storing multiple type of evidence from various devices in one archive and an improved separation between the underlying storage mechanism and forensic software. Garfinkel [93] studied the Digital Forensic XML (DFXML) language and discussed motivations, design and utilization of this language in processing forensic investigation information. Levine and Liberatore [94] introduced DEX, an XML format for recording digital evidence provenance, which enable investigators to use the raw image file and reproduced the evidence by other tools with same functionality. Conti et al. [95] studied automated tools of mapping large binary objects like physical memory, disk image and hibernation files via classifying of regions using a multi-dimensional, information-theoretic technique.

4.2.4. Volatile Memory Forensics

Extracting potential evidences from volatile memories is another challenge for forensic investigators as the basic requirements of knowing the structure of memory is not satisfied. The detectable volatile memory forensic topics are data extraction from volatile memory, volatile memory mapping and forensic imaging of volatile memory.

Data extraction from volatile memory involves utilizing different tools and techniques to analyze and obtain available evidences. In [96], authors studied the tools and techniques of extracting Windows registry data directly from physical memory dump and then presented an attack against on-disk registry analysis techniques by modifying the cashed registry values in physical memory. Maartmann-Moe et al. [51] proposed a novel technique for identification of cryptographic keys stored in volatile memory and support the method by a proof of concept, Interrogate, which can identify AES, Serpent and Twofish cryptography keys. Baar et al. [97] described a novel approach for identifying and recovering files mapped in physical memory to recognize the source of the data and the usage of them via three different algorithms (carving allocated file-mapping structures, unallocated file-mapping structures and unidentified file pages). Schuster [98] studied nonpaged pool area of the physical memory and its potential in containing massive

amount of information about the cunning and even closed processes. In continue the author demonstrated the Microsoft Windows operating system pool allocation technique.

Volatile memory mapping is an essential research area as it is the primary requirement for volatile memory analysis and data extraction. In [99], the author described an algorithm for detecting paging structure of processes in physical memory dump; this method is based on hardware layer and works on both Windows and Linux with minor tweaking. Stevens and Casey [100] introduced a methodology for recognizing and extracting user command line history in Microsoft Windows operating system after studying the structure of command line data on physical memory dumps. At the end authors provided a proof of concept tool for Microsoft Windows XP. Hejazi et al. [101] introduced a unique technique for collecting case-sensitive information from extracted memory content based on analyzing the call stack and security sensitive APIs. The method is limited to Microsoft Windows XP (SP1, SP2). In [102], authors explained the debugging structures in physical memory and Microsoft Program's Database (PDB) to extract configurations, network activities and processes information from any Windows NT family operating system. J. Okolica and Peterson [103] demonstrated the significance of the clipboard information in digital forensic investigation and described the structure and the procedure of retrieving copy/paste information from Microsoft Windows XP, Vista, and 7. This technique can obtain information from the software which the data have copied from (i.e. Notepad or WordPad). J. Okolica and Peterson [104] proposed a novel efficient methodology for reverse engineering the Windows drivers and dynamic link libraries. In addition, the authors have revealed the network connection information structure on physical memory which eases the analysis part of the investigation.

Even though there is a lack of scientific forensic imaging technique for volatile memories, there is only one research found in the scope of this survey. Rabaiotti and Hargreaves [105] presented a novel method for obtaining forensic image of an embedded device by exploiting a buffer overflow vulnerability and execute customized code for creating the image of the console memory. The current work only covered Microsoft Xbox gaming console while the idea is applicable to any type of embedded device.

4.2.5. Network Forensics

Obtaining evidences from network traffics is a great challenge for investigators mainly due to the live characteristic of network packets. Beverly et al. [106] showed that IP packets, Ethernet frames and other network related data is available in physical memory and these data can be retrieved from hibernation files or memory images. Additionally, the authors proposed the network carving algorithm, techniques and essential tools to identify and extract the information. Thonnard and Dacier [107] presented an analysis framework for extracting known attack patterns from massive amount of honeynet data sets. This method allows the analyst to select different feature vectors and appropriate similarity metrics for creating clusters. Shebaro and Crandall [108] described the privacy related challenges of network flow recording for different purposes and then introduced a network flow recording technique by utilizing identity based cryptography and privacy preserving semantics. Zhu [109] introduced an iterative algorithm to discover network based attack patterns via network traffic logs; this method used a unique feedback mechanism to propagate the chance of being under attack or suspicious score and then pass it to the next iteration without any dependency to human supervision (i.e. defining threshold).

Tracking the source of traffic in networks is another challenge when network address translation and other types of network services interfere in the communication. In [110], the author studied the forensic investigation challenges of Network Address Translation (NAT) service enabled networks and proposed a model and algorithm for discovering of observed traffic into the source behind the NAT; the model used specific correlation of NAT gateway artifacts left overs to identify the source. Takahashi et al. [49] focused on reviewing IEEE 802.11 wireless network characteristics based on the traffic pattern of nodes; in order to recognize user fingerprints, rogue access points and media access control protocol missuses. Hsu et al.

[111] proposed a forensic approach for identifying the voice over IP (VoIP) call source via network operators (NWO) and service providers (SvP) without depending on routers logs.

4.2.6. Anti-Forensic

The procedure of forensic investigation can be affected by the criminals via anti-forensic action; researchers challenge the integrity of forensic process by demonstrating new types of anti-forensic method. Evidence collection and common attacks are two identified topics in this area. Distefano et al. [112] analyzed anti-forensic attacks on mobile devices and presented some fully automated examples of these attacks. The authors then examined the effectiveness and strength of the implementations, by using them against cursory examination of the device and tools for obtaining the internal memory image. Sun et al. [113] proposed two anti-forensic steganography approaches based on exploiting modification direction (EMD) technique for storing and extracting data in image. The highlight of EMD (HoEMD) and the adaptive EMD (AdEMD) are high efficient and high quality methods introduced in this work. Stamm and Liu [114] introduced anti-forensic approaches for removing forensically important indicators of compression such as image compression history from an image. This technique utilized a novel approach to identify and omit the compression fingerprints of an image's transform coefficients. Khan et al. [115] presented a novel approach to hide data in a deniable way (to use plausible deniability) by storing sensitive data on a cluster based filesystem; to do so, a covert channel encodes the data via altering the fragmentation pattern in the cluster distribution of the secret file.

Rekhis and Boudriga [116] studied the digital forensic investigation techniques of anti-forensic attacks and then characterized secure evidence, provable and non-provable attacks. As the main contribution of this research, the authors developed an anti-forensic attack aware forensic approach using a state-based logic. Casey et al. [117] explained the challenges of full disk encryption (FDE) for digital forensic investigators and provided a guidance to take necessary items from the crime scene, to ease the access to encrypted data or live forensic acquisition of the running system. The provided measures can help obtaining evidences in an unencrypted state or finding the encryption key or passphrase.

4.2.7. Data Recovery

As one of the most essential stage of evidence identification and collection, data recovery can be affected by different variables like file system type; below some of the data recovery techniques are reviewed. In [118], the author analyzed the main properties of the Firefox SQLite database and its use in forensic investigation. Moreover, a novel algorithm is proposed to recover deleted records from unallocated space based on the fact that Firefox utilizes temporary transaction files. Jang et al. (Jang et al., 2012) described the integrity issue of forensic image corruption after acquisition and provided a novel algorithm for recovering and protecting the evidence image using recovery blocks. The recovery process is applicable when data blocks (generate by recovery blocks) are damaged. Yoo et al. [119] highlighted the challenges of multimedia file carving and NTFS compressed file carving; and proposed solutions for these challenges. The solution for multimedia file carvings is based on the characteristics of AVI, WAV and MP3 files.

In [120], the author discussed the structure of Windows registry data and the behavior of Windows in deleting the registry records. In continue a technique is developed for identifying the deleted Windows registry records and recovery of deleted keys, values and other attributes of records. Garfinkel et al. [121] studied the usage of cryptographic hashes of data blocks for finding data in sectors and introduced the concept of "distinct disk sector". Moreover it provided some approaches for better detection of JPEG, MPEG and other compressed data files. Chivers and Hargreaves [122] explored the structure of Windows search database and the challenge of recovering the deleted records after the file is deleted; it then proposed a novel record carving approach for identifying and recovering the deleted database records from database unused space or filesystem. King and Vidas [123] compared the solid state disk (SSD) with normal HDD and proved the TRIM command can affect the investigation process. The analysis from 16

different disks shows that TRIM enabled disks has almost 0% recoverable data while the SSDs with disabled TRIM has the average of %100 success rate.

4.2.8. Application Forensics

The forensic investigation of applications is quite advantageous as these applications usually store specific evidences. Identifying and collecting these evidences demands for prior research on the application behavior. In [124], the authors studied Internet Download Manager (IDM) activities recorded and effects on different files such as log files, Windows registry and history from artifacts point of view. This study demonstrated approaches and told to detect different attributes of download requests like URL, download time and login credentials. Garfinkel (Garfinkel, 2012b) shared the experience of construction a Korean Reference Data Set (KRDS) based on National Software Reference Library RDS (NSRL RDS) and developed a model for both effective importing of NSRL data sets and adding Korean specific data sets. Lallie and Briggs [125] explored three well-known peer-to-peer network clients (BitTorrent, µTorrent and Vuze) and analyzed their artifacts on Windows registry using the effects created by installation and working with these clients.

In [126], the authors outlined the significance of web browsers in forensic investigation and proposed a methodology for evidence collection and analysis from web browsers log files. Lewthwaite and Smith [127] looked into the Limewire artifacts remained in Windows registry and other log files. It also has developed a tool, AScan, to identify and recover evidences from unallocated spaces and slack spaces of hard disk drives. Fellows [128] described the significance of recovering the WinRAR temporary files and studied the behavior of WinRAR in creating these temporary files. The results of this research indicated that there is a chance to detect and recover the evidence file from deleted temporary folders while the original file is protected by cryptographic solutions.

4.2.9. File System Forensics

Conducting research on file systems structures and attributes is extremely important mainly due to the need to extract evidence from these file system which can be failed in case of unknown file systems. In [53], the authors studied the structure of file time attributes in the NTFS file system and analyzed the modifications in access, modification and creation time attributes of files/folders by the user under different operating system. Grier [129] proposed a methodology for examining filesystems and detecting emergent patterns unique to copying via stochastically modeling filesystem behavior through routine activity and emergent patterns in MAC timestamps. Beebe et al. [130] explained the functionality, architecture and disk layout of ZFS file system and then discussed the forensic investigation methods available for ZFS. This work also brought some of the forensic challenges of ZFS to light. Carrier [131] investigated the credibility of ISO9660 file system in forensic investigation and the fact that this file system can be used for data hiding. The details of data hiding process is studied and then used to create an image with hidden data for examining the available forensic toolkits.

In [132], authors presented a novel approach to identify the disk cluster size without relying on meta data of file system; instead, by detecting the difference between the entropy difference distributions of the non-cluster boundaries and cluster boundaries. Kavallaris and Katos [133] introduced a technique for identification of past pod slurping type of attacks using information stored in filesystem time stamp. This technique infers a file's transfer rate from access time attribute and correlate it to the common rate of the suspicious USB (obtained from Windows registry) to identify the victim USB device.

4.2.10. Forensic Frameworks

Obviously, the forensic frameworks are the basis of the forensic process and developing new frameworks can guarantee the adaptation of forensic science with new technologies. In [134], authors made an extensive survey of available network forensic framework implementations and proposed a generic digital forensic investigation model with comparison to the available models. Finally, the implementation techniques of the proposed model are discussed. Beckett and Slay [135] highlighted the demand for adapting the new technologies with the science of forensic investigation so the digital forensics becomes a

true forensic science. This article examined the roots of scientific methods to establish principles of digital forensic as a science.

In [136], authors discussed the lack of standardized data sets, corpora, as a necessary requirement of forensic research; and presented a taxonomy for defining several available corpora. Guo et al. [137] studied the scientific description of computer forensic characteristics via identifying the basic functionalities of computer forensic investigation procedure; and introduced a functionality oriented validation and verification framework for digital forensic tools by using function mapping approach. Shields et al. [138] proposed PROOFS, a continuous forensic evidence collection tool, which utilizes data retrieval methods on file system forensic. PROOFS generate and save signature for files that are copied, deleted or altered6 over the network.

In [139], the authors analyzed the possible effects of a fictitious P2P model on committing a copyright violation crime while dealing with the illegal distribution of digital contents. Cohen et al. [140] introduced an open-source enterprise forensic investigation tool that provides remote access to memory and raw disk on multiple platforms. In continue, it described the architecture of the tool and how it performs enterprise forensic investigation regularly. Kahvedžić and Kechadi [141] presented a novel digital investigation ontology (DIALOG) for the management, reuse and analysis of digital investigation knowledge via creating a general vocabulary capable of describing the investigation at any level. Case et al. [142] explained the issue of correlation between digital investigation tools and then proposed a framework for automatic evidence identification with support of different targets. The implemented prototype presents the integrated analysis of configuration log file, memory image, disk image and network traffic captures.

In [143], the author shared the experience of forensic investigation of a commercial closed circuit television digital video recorder by using raw disk analysis of the storage disk. The result of investigation showed that with extra effort on processing the raw video data, it might be possible to extract the evidence in cases where the recording device is not functional. Kao et al. [144] proposed three analytical tools for clarifying forensic investigation issues of cybercrime using three strategies: Multi-faceted Digital Forensics Analysis (MDFA), Ideal Log and M-N model; in same order, they covered the basic elements of cyber-crime using new definitions of the forensic investigation, traceable elements of the evidence, and finally the ISP log records. Serrano et al. [145] designed a multi-agent system (MAS) debugging framework for developing a forensic analysis (in cases where MASs indicate complex tissues of connection among agents) by utilizing the pathfinder networks (PFNETs).

4.3. Critical overlooked issues

Privacy issues caused by digital forensic investigation is one of the topics which deserves more research in future as the issue rises where the investigation can threat the secrecy of unrelated data. The same challenge became even more complicated when the cloud computing and massive shared resources get involved. Neglect in conducting effective researches may lead to a direct conflict with citizens` right of privacy can cause the digital forensic face a deadlock where the law enforcers cannot differentiate between potential evidences and other private data. Studying the available works in users right of privacy shows that the solution can be in successful identification of related evidence objects based on existing privacy policies. The current feasible solution is using formal method to tag pieces if data according to the privacy policy and only then start collecting evidences [146], [147].

Thanks to cloud computing concept, many conflicts introduced to the digital forensic investigation [148]–[150]. The jurisdiction of the data is one of the most challenging topics which seem to be overlooked. The digital forensic community should realize that this conflict will cause massive obstacle in legal aspects of the investigation. Developing a suitable cross national low is one of the solution which has been working on in the past couple of years but it demands much more affords to be feasible [151], [152].

Moreover, only a few articles discuss digital forensic investigation science and digital forensic awareness. It is utterly vital to

understand that the bests of forensic frameworks may have conflicts with the true nature of forensic science; the majority of these conflicts end up affecting the integrity of precious evidence. As an instance, imaging the physical memory in a forensic manner is one of the challenges which did not attract much of the researchers` attention. It is for this reason that forensic science has emerged as a significant aspect of digital forensics. A well-conducted awareness campaign can help teach and make digital investigators and forensic researchers aware of these challenges. This may also help to update the investigators about the latest technologies and their new conflicts with forensic investigation disciplines on a regular bases; not only a once-off exercise.

5. CONCLUSION AND FUTURE WORKS

Digital crime is a moving target, from the era of telephone hackers up to the current state of the complex malware intrusions. With new developments and innovations, new types of crime came along. This survey result has shown that as we entered the twenty-first century, the scope of digital forensic investigation has widened and its focus is fast shifting toward mobile device and cloud based investigations. Digital forensics now requires a more coordinated and focused effort from the national and international society, governments and the private sector. It is no coincidence that the study shows a shift towards mobile device and cloud forensic while the true nature of forensic science becomes the essence of investigation frameworks. This survey results have also shown that most of today's forensic challenges are to a greater extent in direct conflict with common digital forensic practices. All indicators points to a scientific approach in the future development of the digital forensic discipline. However, as we move forward to address the new challenges it is also critical that we continue strengthening the technologies. Finally, New research efforts is required that minimize the gap between regulatory issues and technical implementations.

6. REFERENCES

[1] M. Pollitt, "A History of Digital Forensics," in *Advances in Digital Forensics VI*, vol. 337, K.-P. Chow and S. Shenoi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 3–15.

[2] D. B. Parker, *Crime by computer*. Scribner, 1976.

[3] E. Casey, *Digital Evidence and Computer Crime*. Academic Press, 2004.

[4] P. Sommer, "The future for the policing of cybercrime," *Computer Fraud & Security*, vol. 2004, no. 1, pp. 8–12, Jan. 2004.

[5] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation*, vol. 7, Supplement, pp. S64 – S73, 2010.

[6] C. Stoll, "Stalking the wily hacker," *Communications of the ACM*, vol. 31, no. 5, pp. 484–497, May 1988.

[7] V. Corey, C. Peterman, S. Shearin, M. S. Greenberg, and J. Van Bokkelen, "Network forensics analysis," *IEEE Internet Computing*, vol. 6, no. 6, pp. 60 – 66, Dec. 2002.

[8] M. W. Stevens, "Unification of relative time frames for digital forensics," *Digital Investigation*, vol. 1, no. 3, pp. 225–239, Sep. 2004.

[9] D. Forte, "The importance of text searches in digital forensics," *Network Security*, vol. 2004, no. 4, pp. 13–15, Apr. 2004.

[10] B. D. Carrier and J. Grand, "A hardware-based memory acquisition procedure for digital investigations," *Digital Investigation*, vol. 1, no. 1, pp. 50–60, Feb. 2004.

[11] S. Mocas, "Building theoretical underpinnings for digital forensics research," *Digital Investigation*, vol. 1, no. 1, pp. 61–68, Feb. 2004.

[12] C. Vaughan, "Xbox security issues and forensic recovery methodology (utilising Linux)," *Digital Investigation*, vol. 1, no. 3, pp. 165–172, Sep. 2004.

[13] B. J. Nikkel, "Domain name forensics: a systematic approach to investigating an internet presence," *Digital Investigation*, vol. 1, no. 4, pp. 247–255, Dec. 2004.

[14] F. Buchholz and E. Spafford, "On the role of file system metadata in digital

forensics," *Digital Investigation*, vol. 1, no. 4, pp. 298–309, Dec. 2004.

[15] G. A. Francia and K. Clinton, "Computer forensics laboratory and tools," *Journal of Computing Sciences in Colleges*, vol. 20, no. 6, pp. 143–150, Jun. 2005.

[16] B. J. Nikkel, "Forensic acquisition and analysis of magnetic tapes," *Digital Investigation*, vol. 2, no. 1, pp. 8–18, Feb. 2005.

[17] W. Jansen and R. Ayers, "An overview and analysis of PDA forensic tools," *Digital Investigation*, vol. 2, no. 2, pp. 120–132, Jun. 2005.

[18] M. Bedford, "Methods of discovery and exploitation of Host Protected Areas on IDE storage devices that conform to ATAPI-4," *Digital Investigation*, vol. 2, no. 4, pp. 268–275, Dec. 2005.

[19] W. Harrison, "A term project for a course on computer forensics," *Journal on Educational Resources in Computing*, vol. 6, no. 3, p. 6–es, Sep. 2006.

[20] A. Laurie, "Digital detective – Bluetooth," *Digital Investigation*, vol. 3, no. 1, pp. 17–19, Mar. 2006.

[21] B. J. Nikkel, "Improving evidence acquisition from live network sources," *Digital Investigation*, vol. 3, no. 2, pp. 89–96, Jun. 2006.

[22] R. S. C. Ieong, "FORZA–Digital forensics investigation framework that incorporate legal issues," *digital investigation*, vol. 3, pp. 29–36, 2006.

[23] J. P. Zachman, "The Zachman Framework™ Evolution," *EA Articles (page intentionally left blank)*, 2009.

[24] R. Harris, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem," *Digital Investigation*, vol. 3, Supplement, pp. 44–49, Sep. 2006.

[25] S. L. Garfinkel, "Forensic feature extraction and cross-drive analysis," *Digital Investigation*, vol. 3, Supplement, pp. 71–81, Sep. 2006.

[26] A. Schuster, "Searching for processes and threads in Microsoft Windows memory dumps," *Digital Investigation*, vol. 3, Supplement, pp. 10–16, Sep. 2006.

[27] S. Jeyaraman and M. J. Atallah, "An empirical study of automatic event reconstruction systems," *Digital Investigation*, vol. 3, Supplement, pp. 108–115, Sep. 2006.

[28] W. Alink, R. A. F. Bhoedjang, P. A. Boncz, and A. P. de Vries, "XIRAF – XML-based indexing and querying for digital forensics," *Digital Investigation*, vol. 3, Supplement, pp. 50–58, Sep. 2006.

[29] A. Johnston and J. Reust, "Network intrusion investigation – Preparation and challenges," *Digital Investigation*, vol. 3, no. 3, pp. 118–126, Sep. 2006.

[30] S. Mead, "Unique file identification in the National Software Reference Library," *Digital Investigation*, vol. 3, no. 3, pp. 138–150, Sep. 2006.

[31] B. J. Nikkel, "A portable network forensic evidence collector," *Digital Investigation*, vol. 3, no. 3, pp. 127–135, Sep. 2006.

[32] S.-J. Wang, H.-J. Ke, J.-H. Huang, and C.-L. Chan, "Concerns about Hash Cracking Aftereffect on Authentication Procedures in Applications of Cyberspace," *IEEE Aerospace and Electronic Systems Magazine*, vol. 22, no. 1, pp. 3 –7, Jan. 2007.

[33] S. Peisert, M. Bishop, S. Karin, and K. Marzullo, "Analysis of Computer Intrusions Using Sequences of Function Calls," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 2, pp. 137 –150, Jun. 2007.

[34] A. Castiglione, A. De Santis, and C. Soriente, "Taking advantages of a disadvantage: Digital forensics and steganography using document metadata," *Journal of Systems and Software*, vol. 80, no. 5, pp. 750–764, May 2007.

[35] R. Murphey, "Automated Windows event log forensics," *Digital Investigation*, vol. 4, Supplement, pp. 92–100, Sep. 2007.

[36] A. Spruill and C. Pavan, "Tackling the U3 trend with computer forensics," *Digital Investigation*, vol. 4, no. 1, pp. 7–12, Mar. 2007.

[37] P. Turner, "Applying a forensic approach to incident response, network investigation and system administration using Digital Evidence Bags," *Digital Investigation*, vol. 4, no. 1, pp. 30–35, Mar. 2007.

[38] G. G. Richard, V. Roussev, and L. Marziale, "Forensic discovery auditing of digital evidence containers," *Digital Investigation*, vol. 4, no. 2, pp. 88–97, Jun. 2007.

[39] B. J. Nikkel, "An introduction to investigating IPv6 networks," *Digital Investigation*, vol. 4, no. 2, pp. 59–67, Jun. 2007.

[40] G. Masters and P. Turner, "Forensic data recovery and examination of magnetic swipe card cloning devices," *Digital Investigation*, vol. 4, Supplement, pp. 16–22, Sep. 2007.

[41] J. R. Lyle and M. Wozar, "Issues with imaging drives containing faulty sectors," *Digital Investigation*, vol. 4, Supplement, pp. 13–15, Sep. 2007.

[42] A. R. Arasteh, M. Debbabi, A. Sakha, and M. Saleh, "Analyzing multiple logs for forensic evidence," *Digital Investigation*, vol. 4, Supplement, pp. 82–91, Sep. 2007.

[43] A. R. Arasteh and M. Debbabi, "Forensic memory analysis: From stack and code to execution history," *Digital Investigation*, vol. 4, Supplement, pp. 114–125, Sep. 2007.

[44] B. Schatz, "BodySnatcher: Towards reliable volatile memory acquisition by software," *Digital Investigation*, vol. 4, Supplement, pp. 126–134, Sep. 2007.

[45] M. S. Barik, G. Gupta, S. Sinha, A. Mishra, and C. Mazumdar, "An efficient technique for enhancing forensic capabilities of Ext2 file system," *Digital Investigation*, vol. 4, Supplement, pp. 55–61, Sep. 2007.

[46] M. Cohen, S. Garfinkel, and B. Schatz, "Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow," *Digital Investigation*, vol. 6, Supplement, pp. S57 – S68, 2009.

[47] M. Taylor, J. Haggerty, D. Gresty, and D. Lamb, "Forensic investigation of cloud computing systems," *Network Security*, vol. 2011, no. 3, pp. 4 – 10, 2011.

[48] E. Casey, A. Cheval, J. Y. Lee, D. Oxley, and Y. J. Song, "Forensic acquisition and analysis of palm webOS on mobile devices," *Digital Investigation*, vol. 8, no. 1, pp. 37 – 47, 2011.

[49] D. Takahashi, Y. Xiao, Y. Zhang, P. Chatzimisios, and H.-H. Chen, "IEEE 802.11 user fingerprinting and its applications for intrusion detection," *Computers & Mathematics with Applications*, vol. 60, no. 2, pp. 307 – 318, 2010.

[50] M. S. Olivier, "On metadata context in Database Forensics," *Digital Investigation*, vol. 5, no. 3–4, pp. 115 – 123, 2009.

[51] C. Maartmann-Moe, S. E. Thorkildsen, and A. Årnes, "The persistence of memory: Forensic identification and extraction of cryptographic keys," *Digital Investigation*, vol. 6, Supplement, pp. S132 – S140, 2009.

[52] B. R. Mallio, "Message hiding using steganography, and forensic approaches for discovery," *J. Comput. Sci. Coll.*, vol. 23, no. 3, pp. 6–6, Jan. 2008.

[53] J. Bang, B. Yoo, and S. Lee, "Analysis of changes in file time attributes with file manipulation," *Digital Investigation*, vol. 7, no. 3–4, pp. 135 – 144, 2011.

[54] V. G. Cerf, "Defense against the Dark Arts," *IEEE Internet Computing*, vol. 16, no. 1, p. 96, Feb. 2012.

[55] A. Savoldi, M. Piccinelli, and P. Gubian, "A statistical method for detecting on-disk wiped areas," *Digital Investigation*, vol. 8, no. 3–4, pp. 194 – 214, 2012.

[56] F. N. Dezfoli, A. Dehghantanha, R. Mahmoud, N. F. B. M. Sani, and F. Daryabar, "DIGITAL FORENSIC TRENDS AND FUTURE," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 2, no. 2, pp. 48–76, 2013.

[57] M. Damshenas, A. Dehghantanha, and R. Mahmoud, "A SURVEY ON MALWARE PROPAGATION,

ANALYSIS, AND DETECTION," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 2, no. 4, pp. 10–29, 2013.

[58] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 1099–1110, 2011.

[59] H. Gou, A. Swaminathan, and M. Wu, "Intrinsic sensor noise features for forensic analysis on scanners and scanned images," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 3, pp. 476–491, 2009.

[60] M. Chen, J. Fridrich, M. Goljan, and J. Lukás, "Determining image origin and integrity using sensor noise," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 1, pp. 74–90, 2008.

[61] H. D. Yuan, "Blind forensics of median filtering in digital images," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 4, pp. 1335–1345, 2011.

[62] B. Mahdian and S. Saic, "Using noise inconsistencies for blind image forensics," *Image and Vision Computing*, vol. 27, no. 10, pp. 1497 – 1503, 2009.

[63] H. Farid and M. J. Bravo, "Perceptual discrimination of computer generated and photographic faces," *Digital Investigation*, vol. 8, no. 3–4, pp. 226 – 235, 2012.

[64] J. D. Kornblum, "Using JPEG quantization tables to identify imagery processed by software," *Digital Investigation*, vol. 5, Supplement, pp. S21 – S25, 2008.

[65] S. D. Mahalakshmi, K. Vijayalakshmi, and S. Priyadharsini, "Digital image forgery detection and estimation by exploring basic image manipulations," *Digital Investigation*, vol. 8, no. 3–4, pp. 215 – 225, 2012.

[66] M.-J. Tsai, C.-S. Wang, J. Liu, and J.-S. Yin, "Using decision fusion of feature selection in digital forensics for camera source model identification," *Computer Standards & Interfaces*, vol. 34, no. 3, pp. 292 – 304, 2012.

[67] J. H. Choi, H. Y. Lee, and H. K. Lee, "Color laser printer forensic based on noisy feature and support vector machine classifier," *Multimedia Tools and Applications*, pp. 1–20, 2011.

[68] M. Islam, P. A. Watters, and J. Yearwood, "Real-time detection of children's skin on social networking sites using Markov random field modelling," *Information Security Technical Report*, vol. 16, no. 2, pp. 51 – 58, 2011.

[69] C. M. S. Steel and C.-T. Lu, "Impersonator identification through dynamic fingerprinting," *Digital Investigation*, vol. 5, no. 1–2, pp. 60 – 70, 2008.

[70] S. Bayram, H. T. Sencar, and N. Memon, "Classification of digital camera-models based on demosaicing artifacts," *Digital Investigation*, vol. 5, no. 1–2, pp. 49 – 59, 2008.

[71] C. Tang, A. W. K. Kong, and N. Craft, "Using a Knowledge-Based Approach to Remove Blocking Artifacts in Skin Images for Forensic Analysis," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 1038–1049, 2011.

[72] W. S. Lin, S. K. Tjoa, H. V. Zhao, and K. J. R. Liu, "Digital image source coder forensics via intrinsic fingerprints," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 3, pp. 460–475, 2009.

[73] F. Huang, J. Huang, and Y. Q. Shi, "Detecting double JPEG compression with the same quantization matrix," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 4, pp. 848–856, 2010.

[74] M. Kirchner and R. Bohme, "Hiding traces of resampling in digital images," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 4, pp. 582–592, 2008.

[75] L. Miralles and J. Moreno, "Versatile iPad forensic acquisition using the Apple Camera Connection Kit," *Computers*

& Mathematics with Applications, vol. 63, no. 2, pp. 544 – 553, 2012.

[76] V. L. L. Thing, K.-Y. Ng, and E.-C. Chang, "Live memory forensics of mobile phones," *Digital Investigation*, vol. 7, Supplement, pp. S74 – S82, 2010.

[77] J. Sylve, A. Case, L. Marziale, and G. G. Richard, "Acquisition and analysis of volatile memory from android devices," *Digital Investigation*, vol. 8, no. 3–4, pp. 175 – 184, 2012.

[78] A. Distefano and G. Me, "An overall assessment of Mobile Internal Acquisition Tool," *Digital Investigation*, vol. 5, Supplement, pp. S121 – S127, 2008.

[79] T. Vidas, C. Zhang, and N. Christin, "Toward a general collection methodology for Android devices," *Digital Investigation*, vol. 8, Supplement, pp. S14 – S24, 2011.

[80] K. Jonkers, "The forensic use of mobile phone flasher boxes," *Digital Investigation*, vol. 6, no. 3–4, pp. 168 – 178, 2010.

[81] P. Owen and P. Thomas, "An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO & NIST guidelines," *Digital Investigation*, vol. 8, no. 2, pp. 135 – 140, 2011.

[82] G. Grispos, T. Storer, and W. B. Glisson, "A comparison of forensic evidence recovery techniques for a windows mobile smart phone," *Digital Investigation*, vol. 8, no. 1, pp. 23 – 36, 2011.

[83] O. van Eijk and M. Roeloffs, "Forensic acquisition and analysis of the Random Access Memory of TomTom GPS navigation systems," *Digital Investigation*, vol. 6, no. 3–4, pp. 179 – 188, 2010.

[84] F. Rehault, "Windows mobile advanced forensics: An alternative to existing tools," *Digital Investigation*, vol. 7, no. 1–2, pp. 38 – 47, 2010.

[85] R. P. Mislan, E. Casey, and G. C. Kessler, "The growing need for on-scene triage of mobile devices," *Digital Investigation*, vol. 6, no. 3–4, pp. 112 – 124, 2010.

[86] J. Olsson and M. Boldt, "Computer forensic timeline visualization tool," *Digital Investigation*, vol. 6, Supplement, pp. S78 – S87, 2009.

[87] C. Klaver, "Windows Mobile advanced forensics," *Digital Investigation*, vol. 6, no. 3–4, pp. 147 – 167, 2010.

[88] R. A. Joyce, J. Powers, and F. Adelstein, "MEGA: A tool for Mac OS X operating system and application forensics," *Digital Investigation*, vol. 5, Supplement, pp. S83 – S90, 2008.

[89] A. Case, L. Marziale, and G. G. R. III, "Dynamic recreation of kernel data structures for live forensics," *Digital Investigation*, vol. 7, Supplement, pp. S32 – S40, 2010.

[90] H. Inoue, F. Adelstein, and R. A. Joyce, "Visualization in testing a volatile memory forensic tool," *Digital Investigation*, vol. 8, Supplement, pp. S42 – S51, 2011.

[91] D. Ayers, "A second generation computer forensic analysis system," *Digital Investigation*, vol. 6, Supplement, pp. S34 – S42, 2009.

[92] L. Pan and L. M. Batten, "Robust performance testing for digital forensic tools," *Digital Investigation*, vol. 6, no. 1–2, pp. 71 – 81, 2009.

[93] S. Garfinkel, "Digital forensics XML and the DFXML toolset," *Digital Investigation*, vol. 8, no. 3–4, pp. 161 – 174, 2012.

[94] B. N. Levine and M. Liberatore, "DEX: Digital evidence provenance supporting reproducibility and comparison," *Digital Investigation*, vol. 6, Supplement, pp. S48 – S56, 2009.

[95] G. Conti, S. Bratus, A. Shubina, B. Sangster, R. Ragsdale, M. Supan, A. Lichtenberg, and R. Perez-Alemany, "Automated mapping of large binary objects using primitive fragment type classification," *Digital Investigation*, vol. 7, Supplement, pp. S3 – S12, 2010.

[96] B. Dolan-Gavitt, "Forensic analysis of the Windows registry in memory,"

Digital Investigation, vol. 5, Supplement, pp. S26 – S32, 2008.

[97] R. B. van Baar, W. Alink, and A. R. van Ballegooij, "Forensic memory analysis: Files mapped in memory," *Digital Investigation*, vol. 5, Supplement, pp. S52 – S57, 2008.

[98] A. Schuster, "The impact of Microsoft Windows pool allocation strategies on memory forensics," *Digital Investigation*, vol. 5, Supplement, pp. S58 – S64, 2008.

[99] K. Saur and J. B. Grizzard, "Locating ×86 paging structures in memory images," *Digital Investigation*, vol. 7, no. 1–2, pp. 28 – 37, 2010.

[100] R. M. Stevens and E. Casey, "Extracting Windows command line details from physical memory," *Digital Investigation*, vol. 7, Supplement, pp. S57 – S63, 2010.

[101] S. M. Hejazi, C. Talhi, and M. Debbabi, "Extraction of forensically sensitive information from windows physical memory," *Digital Investigation*, vol. 6, Supplement, pp. S121 – S131, 2009.

[102] J. Okolica and G. L. Peterson, "Windows operating systems agnostic memory analysis," *Digital Investigation*, vol. 7, Supplement, pp. S48 – S56, 2010.

[103] J. Okolica and G. L. Peterson, "Extracting the windows clipboard from physical memory," *Digital Investigation*, vol. 8, Supplement, pp. S118 – S124, 2011.

[104] J. S. Okolica and G. L. Peterson, "Windows driver memory analysis: A reverse engineering methodology," *Computers & Security*, vol. 30, no. 8, pp. 770 – 779, 2011.

[105] J. R. Rabaiotti and C. J. Hargreaves, "Using a software exploit to image RAM on an embedded system," *Digital Investigation*, vol. 6, no. 3–4, pp. 95 – 103, 2010.

[106] R. Beverly, S. Garfinkel, and G. Cardwell, "Forensic carving of network packets and associated data structures," *Digital Investigation*, vol. 8, Supplement, pp. S78 – S89, 2011.

[107] O. Thonnard and M. Dacier, "A framework for attack patterns' discovery in honeynet data," *Digital Investigation*, vol. 5, Supplement, pp. S128 – S139, 2008.

[108] B. Shebaro and J. R. Crandall, "Privacy-preserving network flow recording," *Digital Investigation*, vol. 8, Supplement, pp. S90 – S100, 2011.

[109] Y. Zhu, "Attack Pattern Discovery in Forensic Investigation of Network Attacks," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 7, pp. 1349–1357, 2011.

[110] M. I. Cohen, "Source attribution for network address translated forensic captures," *Digital Investigation*, vol. 5, no. 3–4, pp. 138 – 145, 2009.

[111] H.-M. Hsu, Y. S. Sun, and M. C. Chen, "Collaborative scheme for VoIP traceback," *Digital Investigation*, vol. 7, no. 3–4, pp. 185 – 195, 2011.

[112] A. Distefano, G. Me, and F. Pace, "Android anti-forensics through a local paradigm," *Digital Investigation*, vol. 7, Supplement, pp. S83 – S94, 2010.

[113] H. M. Sun, C. Y. Weng, C. F. Lee, and C. H. Yang, "Anti-forensics with steganographic data embedding in digital images," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 7, pp. 1392–1403, 2011.

[114] M. C. Stamm and K. J. R. Liu, "Anti-forensics of digital image compression," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 1050–1065, 2011.

[115] H. Khan, M. Javed, S. A. Khayam, and F. Mirza, "Designing a cluster-based covert channel to evade disk investigation and forensics," *Computers & Security*, vol. 30, no. 1, pp. 35 – 49, 2011.

[116] S. Rekhis and N. Boudriga, "A System for Formal Digital Forensic Investigation Aware of Anti-Forensic Attacks," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 2, pp. 635–650, 2012.

[117] E. Casey, G. Fellows, M. Geiger, and G. Stellatos, "The growing impact of full disk encryption on digital forensics," *Digital Investigation*, vol. 8, no. 2, pp. 129 – 134, 2011.

[118] M. T. Pereira, "Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records," *Digital Investigation*, vol. 5, no. 3–4, pp. 93 – 103, 2009.
[119] B. Yoo, J. Park, S. Lim, J. Bang, and S. Lee, "A study on multimedia file carving method," *Multimedia Tools and Applications*, pp. 1–19, 2012.
[120] T. D. Morgan, "Recovering deleted data from the Windows registry," *Digital Investigation*, vol. 5, Supplement, pp. S33 – S41, 2008.
[121] S. Garfinkel, A. Nelson, D. White, and V. Roussev, "Using purpose-built functions and block hashes to enable small block and sub-file forensics," *Digital Investigation*, vol. 7, Supplement, pp. S13 – S23, 2010.
[122] H. Chivers and C. Hargreaves, "Forensic data recovery from the Windows Search Database," *Digital Investigation*, vol. 7, no. 3–4, pp. 114 – 126, 2011.
[123] C. King and T. Vidas, "Empirical analysis of solid state disk data retention when used with contemporary operating systems," *Digital Investigation*, vol. 8, Supplement, pp. S111 – S117, 2011.
[124] M. Yasin, A. R. Cheema, and F. Kausar, "Analysis of Internet Download Manager for collection of digital forensic artefacts," *Digital Investigation*, vol. 7, no. 1–2, pp. 90 – 94, 2010.
[125] H. S. Lallie and P. J. Briggs, "Windows 7 registry forensic evidence created by three popular BitTorrent clients," *Digital Investigation*, vol. 7, no. 3–4, pp. 127 – 134, 2011.
[126] J. Oh, S. Lee, and S. Lee, "Advanced evidence collection and analysis of web browser activity," *Digital Investigation*, vol. 8, Supplement, pp. S62 – S70, 2011.
[127] J. Lewthwaite and V. Smith, "Limewire examinations," *Digital Investigation*, vol. 5, Supplement, pp. S96 – S104, 2008.
[128] G. Fellows, "WinRAR temporary folder artefacts," *Digital Investigation*, vol. 7, no. 1–2, pp. 9 – 13, 2010.
[129] J. Grier, "Detecting data theft using stochastic forensics," *Digital Investigation*, vol. 8, Supplement, pp. S71 – S77, 2011.
[130] N. L. Beebe, S. D. Stacy, and D. Stuckey, "Digital forensic implications of ZFS," *Digital Investigation*, vol. 6, Supplement, pp. S99 – S107, 2009.
[131] B. D. Carrier, "Different interpretations of ISO9660 file systems," *Digital Investigation*, vol. 7, Supplement, pp. S129 – S134, 2010.
[132] M. Xu, H.-R. Yang, J. Xu, Y. Xu, and N. Zheng, "An adaptive method to identify disk cluster size based on block content," *Digital Investigation*, vol. 7, no. 1–2, pp. 48 – 55, 2010.
[133] T. Kavallaris and V. Katos, "On the detection of pod slurping attacks," *Computers & Security*, vol. 29, no. 6, pp. 680 – 685, 2010.
[134] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *Digital Investigation*, vol. 7, no. 1–2, pp. 14 – 27, 2010.
[135] J. Beckett and J. Slay, "Scientific underpinnings and background to standards and accreditation in digital forensics," *Digital Investigation*, vol. 8, no. 2, pp. 114 – 121, 2011.
[136] S. Garfinkel, P. Farrell, V. Roussev, and G. Dinolt, "Bringing science to digital forensics with standardized forensic corpora," *Digital Investigation*, vol. 6, Supplement, pp. S2 – S11, 2009.
[137] Y. Guo, J. Slay, and J. Beckett, "Validation and verification of computer forensic software tools—Searching Function," *Digital Investigation*, vol. 6, Supplement, pp. S12 – S22, 2009.
[138] C. Shields, O. Frieder, and M. Maloof, "A system for the proactive, continuous, and efficient collection of digital forensic evidence," *Digital Investigation*, vol. 8, Supplement, pp. S3 – S13, 2011.
[139] S.-J. Wang, D.-Y. Kao, and F. F.-Y. Huang, "Procedure guidance for Internet forensics coping with copyright arguments of client-server-based P2P models," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 795–800, Jun. 2009.

[140] M. I. Cohen, D. Bilby, and G. Caronni, "Distributed forensics and incident response in the enterprise," *Digital Investigation*, vol. 8, Supplement, pp. S101 – S110, 2011.

[141] D. Kahvedžić and T. Kechadi, "DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge," *Digital Investigation*, vol. 6, Supplement, pp. S23 – S33, 2009.

[142] A. Case, A. Cristina, L. Marziale, G. G. Richard, and V. Roussev, "FACE: Automated digital evidence discovery and correlation," *Digital Investigation*, vol. 5, Supplement, pp. S65 – S75, 2008.

[143] N. R. Poole, Q. Zhou, and P. Abatis, "Analysis of CCTV digital video recorder hard disk storage system," *Digital Investigation*, vol. 5, no. 3–4, pp. 85 – 92, 2009.

[144] D.-Y. Kao, S.-J. Wang, and F. F.-Y. Huang, "SoTE: Strategy of Triple-E on solving Trojan defense in Cyber-crime cases," *Computer Law & Security Review*, vol. 26, no. 1, pp. 52 – 60, 2010.

[145] E. Serrano, A. Quirin, J. Botia, and O. Cordón, "Debugging complex software systems by means of pathfinder networks," *Information Sciences*, vol. 180, no. 5, pp. 561 – 583, 2010.

[146] A. Dehghantanha, N. Udzir, and R. Mahmod, "Evaluating user-centered privacy model (UPM) in pervasive computing systems," *Computational Intelligence in Security for Information Systems*, pp. 272–284, 2011.

[147] C. Sagaran, A. Dehghantanha, and R. Ramli, "A User-Centered Context-sensitive Privacy Model in Pervasive Systems," in *Communication Software and Networks, 2010. ICCSN'10. Second International Conference on*, 2010, pp. 78–82.

[148] S. Biggs and S. Vidalis, "Cloud Computing: The impact on digital forensic investigations," in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, 2009, pp. 1 –6.

[149] M. Damshenas and A. Dehghantanha, "Forensics Investigation Challenges in Cloud Computing Environments," presented at the The International Conference on Cyber Security, Cyber Warfare and Digital Forensic, Kuala Lumpur, Malaysia, 2012, pp. 190–194.

[150] F. Daryabar, A. Dehghantanha, N. I. Udzir, N. F. binti M. Sani, and S. bin Shamsuddin, "A REVIEW ON IMPACTS OF CLOUD COMPUTING ON DIGITAL FORENSICS," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 2, no. 2, pp. 77–94, 2013.

[151] T. Hasani and A. Dehghantanha, "A Guideline to Enforce Data Protection and Privacy Digital Laws in Iran," *Proceedings of International Conference on Software and Computer Applications (ICSCA 2011)*, pp. 3–6, 2011.

[152] P. Hunton, "The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation," *Computer Law & Security Review*, vol. 27, no. 1, pp. 61 – 67, 2011.