International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 48-76
The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012)

Digital Forensic Trends and Future

Farhood Norouzizadeh Dezfoli, Ali Dehghantanha, Ramlan Mahmoud, Nor Fazlida Binti Mohd Sani, Farid Daryabar
Faculty of Computer Science and Information Technology
University Putra Malaysia
{Farhood1990, farid0fx} @gmail.com
{alid, ramlan, fazlida} @fsktm.upm.edu.my

ABSTRACT

Nowadays, rapid evolution of computers and mobile phones has caused these devices to be used in criminal activities. Providing appropriate and sufficient security measures is a difficult job due to complexity of devices which makes investigating crimes involving these devices even harder. Digital forensic is the procedure of investigating computer crimes in the cyber world. Many researches have been done in this area to help forensic investigation to resolve existing challenges. This paper attempts to look into trends of applications of digital forensics and security at hand in various aspects and provide some estimations about future research trends in this area.

KEYWORDS

Digital forensics, Image, Memory, Security, Identification, Recovery, Investigation, Intrusion, Validation.

1 INTRODUCTION

Digital forensics process involves collection, preservation, analysis and presentation of evidence from digital sources. With the rise of challenges in the field of forensic investigations, problems that are more interesting are looming on the horizon for both victims and investigators. As computers become smaller, faster and cheaper, computers are increasingly being embedded inside other larger systems which allow information to be created, stored, processed, analyzed and communicated in ways that are unpredicted. Once we gathered digital evidence from monolithic, stand-alone mainframes whereas today we have PCs, supercomputers, distributed client-server networks, laptops and smart phones, and LANs and WANs to convey information across the world, each of which is a potential source of digital evidence. Evidences stored in a computer is not unique with regard to relevancy and materiality, but because it can be easily duplicated and modified, often without leaving any traces and is readily available to a miscreant using another computer half a world away and hence, should be constrained by evolving legal standards and constraints to defend privacy issues.

In general, privacy means allowing or disallowing access to information. The code of ethics requires the forensics professionals to maintain the privacy of the client. In the event of proper investigation of cases, depending on the sensitivity of the issue and the requirement of the result, the privacy of the client may need to be compromised.

But it is also possible the victim organization might lose out the trust over forensics team. Moreover there are organizations where in any slight leakage of the issue may attract huge media attention resulting in endangering the reputation and finally the business of organization.In such situations, privacy rights and law enforcement's need to search and seize digital evidence during digital forensic belong together.It may also be possible that the forensics expert may not share the information with any third party but takes the advantage of the confidential information of the client himself, which is also a case of violation of right to privacy. That is why, it is the policy maker's responsibility to see the impact of forensics in the broader context of business goals and make the hard decisions that trade off forensics capabilities with issues of privacy and, correspondingly, morale.

Key strategies for digital forensics in order to protect privacy are selective revelation, strong audit and rule processing technologies. In the present situation, the dilemmas are How to monitor digital forensics while keeping search information secret? How do we keep private information from being improperly disclosed in the name of forensics?

This paper comprises of 3 Sections and will be presented as such: Section 2 narrate the data collection procedure for this review as well as the limitations of the collected data. Section 3 discusses all the collected papers and analyses the result of each paper. Finally, section 4 concludes the paper and summarizes the overall development of technology in digital forensic.

2 CURRENT TRENDS IN DIGITAL FORENSIC

This section identifies the limitation of this work and explains the procedure of data collection.

2.1 Limitations of the Study

It is unlikely that this approach will capture the true picture of privacy protection in current digital forensic landscape, as they are delicate in each research specimen. The papers read are more interested to discuss exploiting security mechanism and framework rather than privacy protection techniques. The numbers of papers provided are also too few to adequately sustain very significant research value. Most of the papers reviewed are too specific in their corresponding research field and purpose; it is difficult to generalize the specimen into statistical data with higher accuracy. The research nature and scenarios used cannot be fully depended upon as they are not necessarily applicable in another similar scenario. Since the publications go through a lengthy peer review process that adds a long time lag to the publication route, they are not so responsive to the current security trends and issues. Hence, they tend to be a following rather than a leading indicator of information security trends. We also realize that almost all specimens are from the Elsevier journal platform, and thus there is a limitation on the availability of more related research publications in other sources. We also identified another limitation, which is the lack of graphical statistical data, as most of the papers researched do not necessarily belong to statistically based research. It is not practical to add statistical assumptions depending on the given articles only rather it has the

unavoidable possibility to divert the accurate picture of the research.

2.2 Data Collection Procedure

In this research, a passive data collection procedure is executed in three phases depending on 97 articles from 31 journals. We focus on statistical analysis based on trends not older than 2008 to obtain a view of recent interests in the arena of digital forensics. A wide range of well-established journals is chosen that have digital forensics as its primary focus fulfilling both academic & business purposes.

Phase 1: Keyword Analysis. The data collection process started with keyword analysis in order to identify the focus of each article studied. We found out that the keywords used by authors do not necessarily reflect the picture of techniques and theories that are being emphasized within the timeframe of a paper. At the same time, some keywords are too generic and may not bring any significant research value unless paired with other keywords.

Figure 1 summarizes the frequency of the keywords in all the articles included for this survey. It is rather evident that the current focus of forensics is now more towards computer, multimedia and network forensics with 31, 24 & 22 papers focusing on those areas respectively. 14 articles explaining present & future forensic tools and applications also receive significant focus, as these are the foundation of many digital security solutions. With the rapid development of image processing techniques, tampering with digital images without leaving any obvious traces is becoming easier and thus, image forensics evolved quickly during the last few years and has been studied in 12 papers.

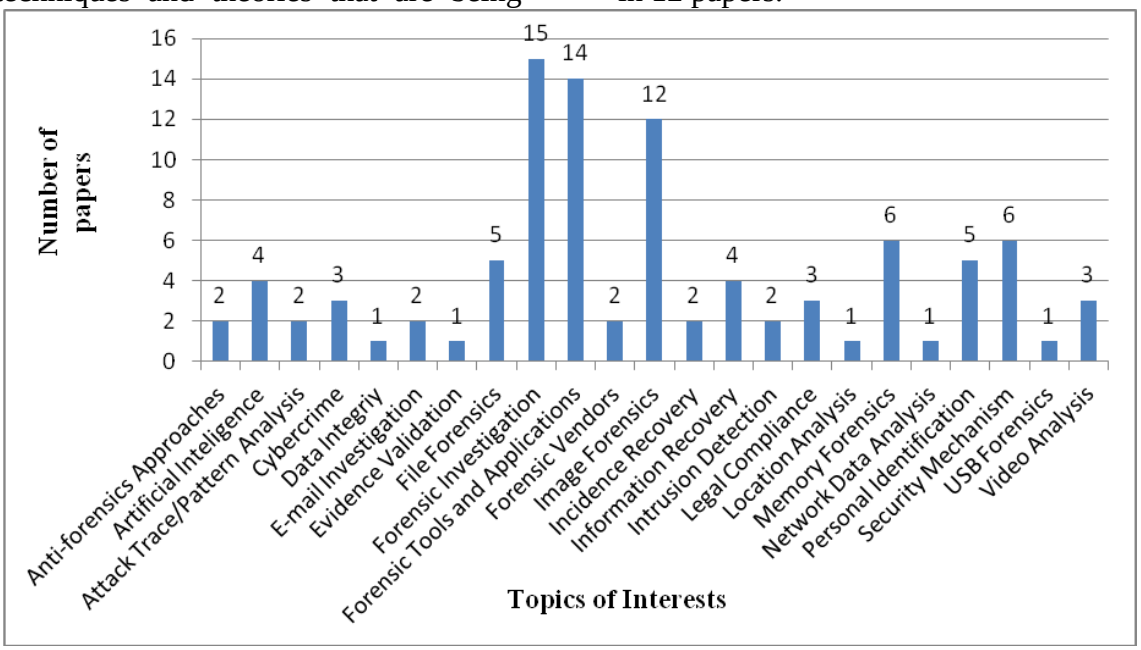

Figure 1. Coverage of topics in journal papers

Phase 2: Topics Covered in the Journals. The collected keywords were then grouped into broad category topics based on their representation to

accommodate most of the topics identified in recent digital forensics, as shown in table-1. For example, articles containing keywords like image splicing detection, edge detection, image tampering, JPEG compression, image segmentation were grouped as image forensics and fell into a broader category of multimedia forensics. Articles, grouped in one category, can actually fit into multiple broader categories, such as articles with paired-keyword 'memory' & 'windows registry' and 'memory' & 'mobile phone' were both categorized as memory forensics, but the former is more suitable to computer forensics whereas the latter is appropriate in mobile device forensics. The same strategy applies to all the other broad topics. All the topics that appear not to be part of any of the broad topics were categorized as other. This category included topics like: Forensic Psychiatry, Microelectronics Reliability, Evidence Validation and Anti-forensics Approaches to name just a few.

Table 1. Keyword categories.

Categories	Computer Forensics	Mobile Device Forensics	Network Forensics	Database Forensics	Multimedia Forensics	Cloud Forensics	Other	Total
Forensic Investigation	2	1	5	2	2	2	1	15
Forensic Tools and Applications	9	2	1		2			14
Image Forensics					12			12
Security Mechanism	2	1	1		2			6
Memory Forensics	5	1						6
Personal Identification	1		1		1		2	5
File Forensics	5							5
Artificial Intelligence	4							4
Information Recovery	3				1			4
Video Analysis	1				2			3
Cybercrime	1		2					3
Legal Compliance			1				2	3
Intrusion Detection			2					2
Attack Trace/Pattern Analysis	1		1					2
E-mail Investigation	1		1					2
Incidence Response			2					2
Forensic vendors							2	2
Anti-forensic Approaches							2	2
Network Data Analysis			1					1
Data Integrity						1		1
USB Forensics	1							1
Evidence Validation							1	1

Location Analysis							1	1
	36	5	18	2	22	3	11	97

Phase 3: Results Obtained from the Journal. Individual analytic platform is conducted as a final data collection. This is done by picking up a summary of each paper and giving a brief explanation of what the paper is trying to prove and possible benefits from the publications.

2.3 Comparing Journal Result with Existing Survey-Reports

A survey was conducted among the experienced researchers and practitioners in the computer forensics field in 2008 during the Digital Forensics Research Workshop. Nine volunteers from the digital forensics practitioner group within the United States participated and were asked to describe the type of cases that are involved in their investigations [98]. The result is shown in Figure 2.

The most common digital forensic investigation cases, 77.8% of overall cases, are those that deal with single personal computer (PCs). Surprisingly, the second-most common digital forensic investigation cases, 55.6% of overall cases, involve mobile media. The third-most common digital forensic investigation cases, 44.4% of overall cases, involve networks, hacking, and multimedia. Only a small number of cases, i.e., 11.1% of overall cases, are concerned with stenography and other sophisticated computer techniques. Note that the total percentage is over 100% because some cases may involve multiple devices. For example, a cell phone, PDA, as well as desktop PCs, laptops, etc. may be part of the same case.

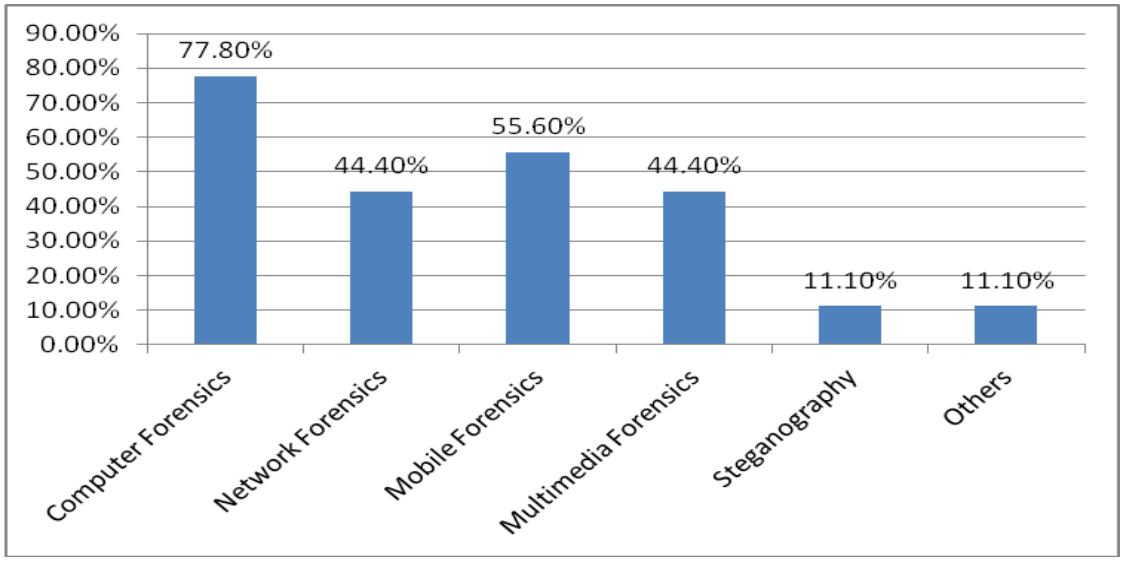

Figure 2. The percentage of Different digital forensics investigation cases [98]

3 DISCUSSION AND ANALYSIS OF RESULTS

Digital Forensic Investigation is a rapidly growing field involved in Information Technology era emergent. It indicates the numerous techniques how the crime in a computer system is handled which occupied from the very lowest part end user to the highest level. In this paper, our summarization is based on every part of keywords mention in the Introduction section. We believe all the methods are not synchronous. We compare all compiled methods which have been used for ages ago to the newest techniques respectively. Part of the summary, we enclosed with the future work that we believed would be significantly important to the further research onward.

3.1 Forensic Investigation

In a computer system, Forensic Investigation (F.I) is a practice to establishing the evidence and facts to be presented in court. It may involve in multiple number of system layer. Different network architecture would demand different F.I approach and different level of difficulties. In [7], the author discusses the issue that makes the F.I. in cloud computing system more complex when it comes to the decentralized authority issue. The provider of cloud computing differentiated by location and the location and some of them will encrypt the data before delivered to the public network.

The usage of the peer-to-peer software may cause to complexity of F.I recovery. As it capable of searching and downloading files from or to any node/computer, it also becomes a factor of exposing company private data to any attack. In peer-to-peer (P2P) F.I, the analyst have to determine the configuration parameter; password, username, log time, installation time and etc [9]. They also advocate the LANGuard software application to monitor P2P activities within the network.

As mobilephones become more advance nowadays, the more vulnerable they are to attack. More users of Smartphone are doing the personal private activities through Smartphone; online banking transaction or e-commerce. The misuse of mobile application involves obtaining and spreading confidential information, fraud, theft, money laundering, copyright infringement and indecent image [6]. The author emphasizes the digital acquisition method on the Subscriber Identity Module (SIM), memory card and flash memory by applying bit-to-bit copy. On the other hand, copying acquisition is also discussed by the author in [80] using the hash verification process. The author proposes a new software Chain of Custody (CoC) which is able to print, custody and transfer any piece of evidence recorded.

During F.I. process, it is important to maintain the privacy of honest users while the system is under investigation. In [47], the author proposes the Enhanced-Respect Private Information Not Abuser (E-RPINA) to provide privacy of honest user yet accountability to the attacker.

In cloud computing system, it potentially involves great data exposure to the security threat and privacy breach. In addition, the users activity can be traced out using the audit trail process [51]. The forensic analyst has to handle the

information carefully or otherwise it might fall into the wrong hand.

The data can be either software or hardware encrypted in order to keep it private and confidential. High demands to protect user's personal data and files led to the introduction of encrypted disk. In [86] the author reveals an open source encryption software known as TruCrypt. It is freely available and able to encrypt the whole partition contain of operating system file.

Nowadays, it takes more consideration upon attack prevention process and technique. The monitoring and visualization of network activities are a crucial mechanism within an organization's network. In [66] the author exposes the development of Enterprise Network Activities Visualizations (ENAVis) as an aid to network administrator to manage and monitor network activities.

Nevertheless, still the computer systems are potentially exposed to attack with the minimal information given. It affects the privacy of user when suing the encrypted traffic and believed they are securely protected. In [97] the author demonstrates the attacking method on Secure Shell (SSH) and Skype software.

3.2 Forensic Tools and Applications

To run a F.I, the correct tools and software play important role as aiding to the efficiency and effectiveness of the investigation. As P2P is widely used for sharing illicit material, the author discusses a tool to extract information from binary evidence based on Java Object Serialization (JOS) as implemented in P2P [67]. Based on the JOS specification, personal information about users can be extracted using a tool known as AScan. However, this tool only available for the law enforcement community. On the other hand, another great tool is used to render back the HTML file through the tcpdump program, which is known as PyFlag. Any recorder network can be capture and replicate the content. The same goes to Flash Memory in the Smartphone, the application can be used to determine any related application logs and multimedia file upon a user [42]. The author develops a Mobile Internal Acquisition Tool (MIAT) in order to target the Symbian OS. However, because of the conflict issue regarding the user privacy information, the software is not to be released under open source license.

There are special forensic tool involves in different operating system (OS) respectively. The introduction of Macintosh Evidence Gathering and Analysis (MEGA) describes how the implementation of system analysis works in Mac OSX [72]. It has great capabilities in manage and monitor the network and even can handle Mac FileVault encrypted home directory. Nevertheless in the Linux OS, the author in [92] mentioned about the uses of Forensic Automated Correlation Engine (FACE) as an image analyzer of the Linux partition. It may obtain any personal information of victim for forensic investigator or unauthorized personnel.

3.3 Image Forensic

Image analysis is used in image forensic to expose the information using the image support machine with decision fusion techniques [4]. The author proposes a model that identifies the source model or device of an image by using the support vector machine approach along with decision fusion

techniques. The paper considers feature selection algorithms as features in optimal subsets are generated in a series of inclusion and exclusion steps and count based aggregation as the algorithm of decision fusion. The algorithm selects the top λ features from 43 features in order to get the highest identification rate and the SVM trained model is built where test images is fed into the trained model to predict the camera source model. The flowchart of the model is illustrated in Figure 3.

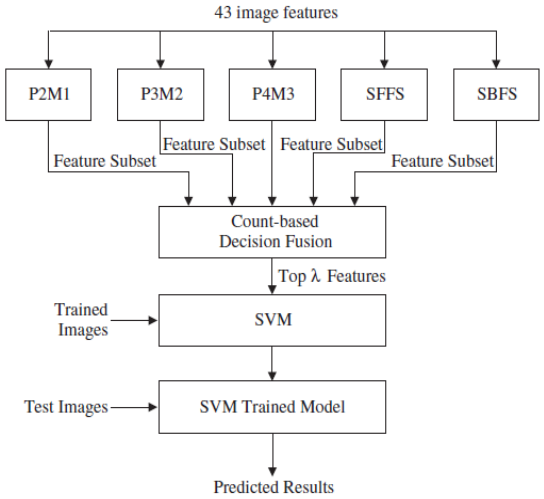

Figure 3. Flow Chart [4]

In [56] the author introduces image meta-description approach suitable for different image inference applications named as progressive randomization (PR). This technique is based on perturbations on the values of the Least Significant Bits of images that makes it different from the state-of-the-art algorithms.

As the imaging analysis being enhanced, [55] contributes reviewing the state-of-the-art image registration methods that lays the foundations on evolutionary computation and analyzes the 3D modelling of forensic objects. The paper includes different evolutionary approaches in order to represent the wide variety of techniques within the EC paradigm and an IR method based on the classical ICP algorithm proposed by Liu. The paper reveals that the majority of the EIR methods following a parameter-based approach achieve the best and the most robust performance and the poor performance obtained by the matching-based methods.

With the highly advanced application, the forensic tool is able to differentiate between the fake and real image. By using multi resolution decomposition and higher order local autocorrelations *(HLACs*) image features are extracted and determine if it is real or fake [23]. They are used and as by right of the inner product lemma of higher order autocorrelation, the feature extraction and SVM are joined and the computation complexity is decreased significantly. The paper suggests Two dimensional discrete wavelet transformation (2D-DWT), a powerful multi resolution analysis tool. The signal characteristics in detail can be localized in different position, orientation and scale and multi resolution decomposition contains many intrinsic characteristics of natural images and fake images.

As Noise degradation causes failure to blind forgery detection methods, in [9] the author proposes a model that divides a suspected image into different partitions with homogenous noise levels. However, the authentic images also can contain various isolated regions with very different variations, which make the proposed method a supplement to other forgery detection methods rather than a standalone forgery detector. The proposed method is not able to find the corrupted regions, when the noise degradation is very small ($\sigma < 2$). The proposed method can be achieved by omitting the blocks merging step.

In image analysis, the image can be detected and located the duplicate regions with rotation, using an efficient and robust passive authentication method [64] .It uses circle block and the Hu moments for detection and location. In this method Gaussian pyramid is used for decomposition and to overcome the possible distortion caused by JPEG compression and noise contamination, produced sub-image in low frequency is chosen. The sub-image is divided into many circle blocks overlapping each other and from them the features of Hu moments are extracted. Here, the circle-block mode and the Hu moments are able to eliminate the effect of rotation. We believe that the new rotation-invariant features should be constructed directly on the circle region. The corresponding robust detection method will be investigated for other intermediate processing such as resizing, cropping etc.

In order to detect image splicing the common form of image tampering, the author in [33] proposes an approximate run length based scheme. Proposed scheme only computes run lengths on the edge pixels and what makes it better is that splicing normally introduces extra edges to the image. This method introduces to a threshold t. If the absolute value of the difference of two neighboring pixels' grayscale value is not greater than the threshold t, the two pixels are considered as they are in an approximate run. We believe further research should be done on the fluctuation of grayscale values of consecutive pixels that tends to be more dramatic in an image with complex texture. Hence makes the authentic images and the spliced one less distinguishable.

The exposure to a new extraction algorithm as proposed by the author in [25] is able to extract the block artifacts grids (BAG) and then abnormal BAGs due to interpolate or concealing objects can be detected with a marking procedure by copy–paste operations. The author suggests that with extracting weak horizontal and vertical edges with periodicity of 8 separately and then combining them the BAGs are found. The image tampering applications like image cropping, painting and copy-paste operation can be detected by BAG using mismatching phenomena.

In order to detect image forgery, it does not require any other prior information about the image, for detecting image forgery [20]. This paper includes all the existing surveys and references that directly deal with blind image forensics.

Nevertheless**,** this method only implies that leaving the "ideal" lab conditions and applying the existing methods to real-life applications, higher rate of false positives are considered than reported. Lack of automation is another drawback of existing methods. To localize the forgery, existing methods need to have knowledge of various modification regions containing some inconsistencies. Many of the existing methods deals only with JPEG and compression properties.

Ideally the method to prove the authenticity of a picture in legal proceedings is not straightforward, an easier approach would be matching an image back to the type of device that last modified it, either hardware or software. [71] explains how quantization tables, which is generally used for JPEG compression, can be used for image source identification since it can identify if images have been processed by software or not, thus can benefit forensic examiner to only consider the unaltered

ones from a large volume of given pictures. For this, the author classified quantization tables into several categories used by the JPEG images that vary by different camera models and software program. A software library developed known as *Calvin* to identify the type of quantization tables used by the existing images that the library contains. For excellent solution of image forensic, we are recommending that the knowledge of JPEG quantization table combining with image factor EXIF data, signature program or color signature for real skin may produce an excellent work of image analysis.

The image of computer generated and real image can be distinguished based on human visual system. In [38] it describes a series of psychophysical experiments that used images of varying resolution, JPEG compression, and color to explore the ability of observers. From the experiments conducted, it reveals that the image is in fact photographic when an observer believes it to be photographic that can be expressed as the following conditional probability,

P (I = photo | R = photo) where R denotes the user response and I the image category.

By replacing "photo" with "CG", the conditional probability that an image is CG if an observer says it is CG,

P (I = CG | R = CG)

However, the accuracies reported in the paper are a lower bound on human performance, unlike time rendering technologies; observer performance can likely be improved.

To identify the source camera-model of a digital image, [99] utilizes traces of demosaicing operation in digital cameras and employing two methods and defining a set of image characteristics which are used as features in designing classifiers that distinguish between digital camera models. the paper identifies demosaicing artifacts associated with different camera-models. By determining the differences in the image formation pipeline, e.g., processing techniques and component technologies, the first method in this paper tries to detect the source camera-model of the image. Two methods namely Expectation–Maximization algorithm that analyzes the correlation of each pixel value to its neighbors and analysis of inter-pixel differences are used to detect and classify the traces of interpolation operation in images. Experiment proposes to feed the images to the classifier to verify the consistency of *demosaicing* artifacts. Hence, the final decision is made by the classifier. It is expected that the use of combined method would eliminate some of the false-positives due to mismatch of the reference pattern.

3.4 Security Mechanism

In [81]**,** author confers the importance of computer forensics as a standard for electronic crime investigations and the expertise required. As the computer forensic field is growing, the field of operation and the number and complexity of the managed cases determine required tools or equipments. Computer forensics, in this paper is termed as mechanism of prevention, compliance and assurance rather than investigation and response.

[26] proposes information hiding techniques as an alternative to encryption. This paper uses the FAT file system as a proof-of-concept example of a covert communication medium. In simple approach, the information to be hidden is embedded in the arrangement

of the clusters of a file. In an alternative approach, the distribution of the cover file clusters can be used to create a covert channel. The approach proposed is undetectable of encrypted or random data.

[43] reveals the fact that Portable Document Format is not impervious from some privacy related issues. Two issues, how changes made to PDF documents handled and interactive features of PDF, are investigated in this paper. This paper shows while trigger events like opening or closing of documents takes place, other programs might be executed or external link might be resolved without user awareness.

[57] emphasis on building up of technological advancement for fraud. It marks phone specially Smartphone as a modern threat to confidentiality. This paper states that Smartphones have a 'dual personality' - one that is loyal to the employer's exchange server, VPN and security systems, the other which can operate on public WiFi, alternative SIM cards and other seemingly anonymous networks, as described in Figure 4.

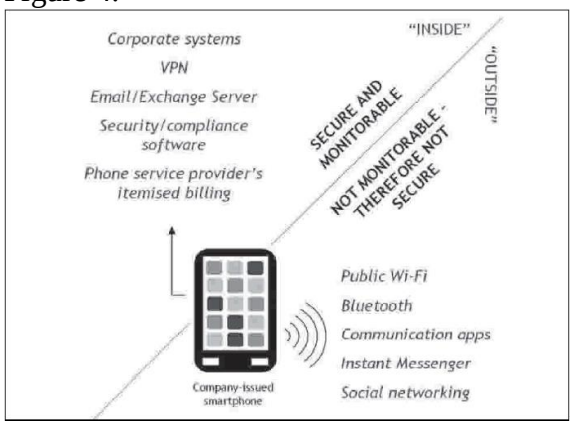

Figure 4. The Dual Personality of Smart Phones [57]

[42] proposes a highly robust protection algorithm that is based on an information hiding technique known as Steganography. Embedding the secret message in the first level 2D Haar DWT with the Symmetric-padding mode is the elementary concept of this paper. Fourier transform (FFT) together with the output of Hash Algorithm 1 (SHA-1) forms a strong image encryption setting Moreover, using DWT gives advantage of the possibility of converting the document into compressed formats without losing details.

[33] discusses the implementation of robust watermarking with the EXIF metadata of images and integrated error-control codes for copyright protection. The proposed algorithm is DCT-based watermarking techniques with necessary modifications for integrating with the BCH-protected EXIF metadata. For verification of the algorithm, attacks are performed by JPEG compression, low-pass filtering (LPF), and median filtering (MF).

These papers discuss methods and algorithms to secure information and increase in digital privacy in sharing information.

3.5 Memory Forensic

Memory forensics examines the information captured from memory at the time the computer is seized. As less focus has been paid to extracting information from Windows drivers, developing a methodology to minimize the effort of analyzing these drivers. [17] first describes a general methodology for reverse code engineering of Windows drivers' memory structures. Proposed process for reconnaissance and analysis is shown in Figure 5.

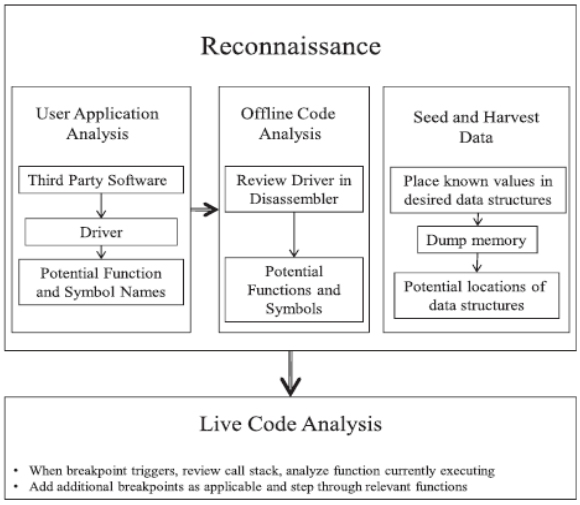

Figure 5. Methodology for reversing drivers [17]

As modern Windows operating systems aggressively cache file data in memory. Current forensic tools and techniques, however, do not take mapped-file information into account.

[49] describes a method for recovering files mapped in memory and to link mapped- file information process data. It discusses three methods for recovering files from memory-Allocated file-mapping structures; unallocated file-mapping structures and Unidentified file pages.

[5] proposes an automated system to support the mobile phone's live memory dynamic properties analysis on interactive based applications, as depicted by Figure 6. The paper describes the experiments and presents the results on identifying the memory region of a process where the message exchange can be observed, and investigating the cached data and the volatile evidence data persistency.

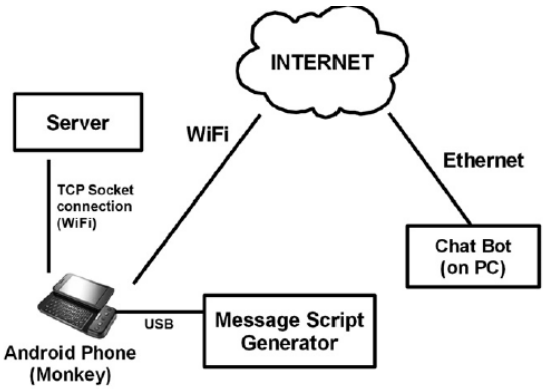

Figure 6. System Overview [5]

[54] analyzes the pool allocation mechanism of the Microsoft Windows operating system. It describes a test environment, which allows obtaining a time series of physical memory images and allocations from the non-paged pool.

[14] describes an algorithm to locate paging structures in a memory image of an x86 platform running either Linux or Windows XP that can be used to find potential processes. The first pass of the algorithm searches the potential page directory for kernel mappings. The second pass of the algorithm inspects the potential page directory by (0e767) entries.

[90] exhibits technique that enables full access to the registry data cached in memory and shows that there are attacks that cannot be detected without examining the registry in memory. To counter attacks, the paper recommends collecting registry data from both RAM and the hard drive.

The papers propose and analyze methods and techniques to extract data hidden in memory and investigation of attacks examining memory to strengthen digital privacy of data.

3.6 Personal Identification

[58] proposes a recognition scheme, different from traditional, starts with the

dynamic partition of the noise-free iris into disjoint regions from which MPEG-7 color and shape descriptors are extracted.

[18] presents an automated system for shoe model identification from outsole that can provide information in timely manner impressions taken directly from suspect's shoes. Once Maximally Stable Extremal Region is identified as being robust and having a high repeatability, it is detected as a match. After detection, the paper employs a feature descriptor Scale Invariant Feature Transform to code the appearance or properties of the local features.

[74] proposes a stochastic vision model based on a Markov Random Fields (MRF). The model employs a skin model and human affine-invariant geometric descriptor. For skin detection, the paper proposes the use of CIE-Lab due to its popularity in some real world application domains. In addition to the CIELabcolor space, the proposed skin model employs texture, another low-level.

[73] suggests that in developing technologies and internet era, it is problematic to prove an individual that is suspected of a crime based on technology beyond doubt. The paper looks for reasons that effected proof of identity and what makes it difficult for identifying a crime suspect. Diversity of devices has put increasing pressure on an already limited resource. Malicious software usage and vulnerability of authentication of credentials made it difficult for forensic investigator to determine who had breached a system.

[53] proposes Automated Impersonator Image Identification System (AIIIS) that allows investigators to track down impersonator attackers. AIIIS uses a combination of dynamic fingerprinting and spread spectrum data hiding.

These papers present system and techniques of personal identification for the authentication information protection and investigation of impersonation.

3.7 File Forenisc

As mentioned in [22], "in the file system FAT-32 the route table entry with the file name will point to the first cluster of the file, which in turn will point to the next cluster and so on until the last cluster of the file". When a file is deleted, only the file's entry is removed from the table not the actual content that located in several clusters in the storage device. It will recover the file from the unallocated space declared by the file system. In this paper, the authors mentioned that the main problem in to recover a file in digital forensic is file carver still fail to recover a fragmented file. In [19], the author compared two published techniques to recover a fragmented file, the Bifragment Gap Carving (BGC) and Parallel Unique Path (PUP) technique.

The author discussed the process of information concealment in [15]. The method described in this paper utilizes the trash sector space (slack space in allocated sectors) and empty space (unallocated sectors) of MS Office files. The author shows how to conceal information into the file based on the format. The author also demonstrates the detection of the concealed information in MS Word file. They create a C# program to detect the concealed information. The program detects the concealed information by analyzing the unknown relationship in the file.

[37] discusses about the method to perform forensic analysis. The issues

highlighted by the author discuss whether visual analysis of a file in forensic analysis is a new or old trend. The article mainly discusses about how we can identify the content of a file by looking into its graphical representation and how much time it can reduce for investigators who need to analyze a large number of files. The issues with privacy mentioned in this article is at a minimal level if the method is used by authorized persons.

[87] highlights the importance of visual forensics that may help investigator identify the important files in their list of evidences. The author describes how a single string embedded in an image only because light differences in the image brightness that may cause an investigator to exclude the image for further forensic analysis. The article also mentioned that with the help of different color to represent different behavior of http session log file content, a forensic investigator could easily identify the protocol used, destination and source of the packet.

In [93], the authors investigate two types of algorithm to predict the type of the fragmented file. The authors also illustrate the results of implementation of the two algorithms mentioned above. The paper demonstrates how the algorithms can be implemented as a proof of concept and not as practical application because there are some aspect that need to consider to implement the algorithm as practical application.

These papers help investigators with file forensics to face issues with digital privacy.

3.8 Artificial Intelligence

The objective of the author in [82] is to introduce an open source tool for analyzing file systems that allow investigators to work on the same shared cases reducing the workload and also expediting the results. GUI features, administrator options and main features of the system are discussed in the paper.

[69] discusses the applications of probabilistic graphical models and also focuses on the class of optimization methods that use probabilistic graphical models to organize the search on a search space. The paper proposes Estimation of distribution algorithms (EDAs) are evolutionary algorithms is based on the assumption that it is possible to build a probabilistic model of the search space that can be used to guide the search for the optimum where the construction of this probabilistic model is a crucial step.

The discussion of [2] involves the limitation of Classical forensic reporting that provides only ‘‘identification’’ or ‘‘exclusion/elimination’’ decisions and way around solution of the limitations. The analysis infers the identity of the probe, but it gives the likelihood ratio for the two competing hypotheses. In forensic engine likelihood ratio serves as an indicator of the discriminating power. Thus, it can be used in assessing authentication performance.

[95] describes the need for training in digital forensics and briefly describes a virtualized training platform for network defense and computer forensics, Cyber Defense Trainer (CYDEST) as shown in Figure 7.

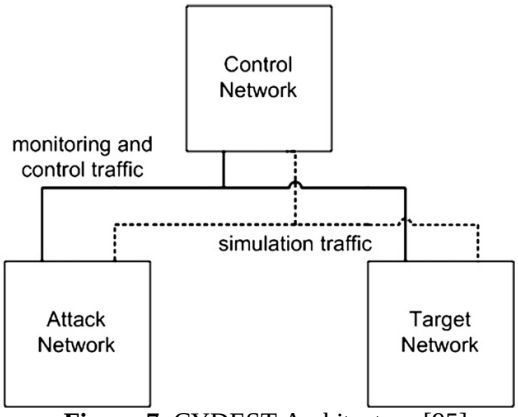

Figure 7. CYDEST Architecture [95]

It uses virtual machines to provide tactical level exercises for personnel such as network administrators, first responders, and digital forensics investigators.

These papers describe methods and techniques for virtualization of digital forensics to help prevent cyber attack.

3.9 Information Recovery

Information recovery is one of the important processes in digital forensics. Evidence of a crime may reside in a deleted email. So a proper technique should be used to recover the information back without changing the original content of the email. As mentioned by (John Shaw et al) the solution to recover the deleted email is by expose reverse engineering on how the email was deleted. The email may be manually deleted by the user or criminal to remove the evidences, or it might happen in some cases that the database is corrupted or hacked by unauthorized personnel. To recover the removed email, the recovery process will be performed from vendor site that can provide a backup plan, which is called as Cache Exchange mode. The data must be synchronized to the server. The deleted email will remain as deleted mail until someone tries to "up" it back, when the machines or servers get synchronize together. The second method is using parents and orphanage method which recover the email based on the type of file or software used, for example using Microsoft Outlook. The email can be recovered by looking at history of email for a particular period. This is due to the Windows method that delete the email depends on the 'flag'.

The second issue is to recover the password protected account or system in organization. Khawla et al discussed on the paper [53] how to generate individual- related electronic profile and recover the password –protected account or system and save time consuming. There are several methods that can be used to recover the password. It can be a complex method like recovering from Random Access Memory (RAM) or even use the social engineering method. Social engineering is proven to be an effective method to gain the password upon a password-protected system or machine. It utilizes the vulnerability of human factor to recover the password. The factor of an individual behavior also plays an important part in recovery password. Some people are sharing the same password with their colleagues for different machine Password also can be recovered back by using software like PRTK, John theRipper, L0phtCrack, Cain & Abel and Paraben's Decryption Collection. All these software also can be used in brute attack.

The privacy issues related to the topic is that the investigators who perform information recovery shall not hold the interesting data, which is not relevant to the case for their own agenda. For example, the recovered password, which has been used by the user, may be used to access different machine or accounts that used the same password. If the password has been used for the purpose

other than evidence recovery, it may violate the users' privacy.

3.10 Video Analytics

There are many tools that can be applied to aid in the digital forensic analysis, whether it is a software tool or hardware tool. Some manufacture like Samsung providing the device like digital video recorder (DVR) to perform an analysis in imaging digital forensic [48]. The device designed with two separated hard disk to perform particular recording and testing. It is also for minimizing the error occurs during the video forensic investigation. This device is able to compress the video recorded in the form of MPEG-4 format and store in the video file. Furthermore, it is capable to transfer the video into a PC (Samsung 2005) in real-time connection.

The investigation of video recorded can refer to the time and date stated on the image display. The primary and secondary hard disks are divided into three partitions. The first partition is "ect" whixh is used to store event and system log file. The second partition is "bin" directory which contains operating system executable files. The third partition is "root" directory that is used for bookkeeping files for example ". db" and ".eve" files. Therefore, the history of logged files will be recorded in hard disks accordingly. In addition, Closed Circuit Television (CCTV) also an effective way in providing an image for digital forensics investigation [59]. The video data will be extracted before it can gain access to manufacturer's application software. The image will be stored on the CCTV disk as well as digital video recorder. However, the disk must not overload with data in order to provide the best result of the initial investigation.

The papers mentioned in this topic contain the related issues with privacy regarding the structure of the hard disk. The information about the structure may be a copyrighted information which should be available on the manufacturer side only and not for other parties. The history in the log file may reveal user activity that may be private to the user and should be accessible by other person.

3.11 Cybercrime

The author describes the method of Strategy of Triple-E (SeTO) in solving trojan defense in cyber crime in [28]. It is used to defend the computer from any risk of trojan effects on any matters. The trojans can be used to track the password of a machine. The result used in the log history and kept on the server cannot be trusted to keep the best data or information. The computer/cyber/IT forensic helps the examiner to investigate and undercover the data that may not be immediately obvious. The author express to use M-N method where M is the path, N is the period of login and logout. In evidential part, the collected data must be handled with care so that it will not cause any problem in the court. The company or organization must have a well structured for employment and email management. This may protect the company network from being attacked by intruders. If the email is saved on the computer, then the email comes together with the header details (date, sender, subject &etc). If the emails are investigated as a disciplinary measure, the organization/company should abide by that law.

3.12 Legal Compliance

Computer forensics investigation includes legal aspects of handling computer forensics as well as e-mail forensic investigation. This is including the creation of law or act implementation and the involvement of management in the relevance of computer forensic investigation. In [10] the author has discussed regarding the implementation of computer forensic and e-mail forensic investigation in United State. Generally, the aim of the computer forensic policy is to protect the organization with the private data and the employee.

A corporate computer policy should ideally cover the installation of unauthorized software within the employee machines, including the digital portable storage device and also the home use of the corporate network. The IT Manager should implement the policy precisely in order to allow or restrict which website can be accessed from internal network. There might be very hard to control and manage the portable storage device and home corporate network. However, the computer forensic policy should cover this level of application to ascertain the organization parameter during any misuse. Moreover, the sensitive company information can be at particular risk from home based computer or any portable device. The author declared that the security of home-based computer could be increased if the company policy might include the appropriate rule and standard like; changing the password regularly, disable USB port and use the office machine to prevent spyware.

In paper [11], it describes the legal actions towards an emails investigation approach. The email investigation activities gather all the information sent through an email conversation regarding a criminal activity. The forensic handler can gain the information about the event, the people or organization involved, that take a biggest evidence to bring to court. It also involve of email recovery method. Basically, there are two types of technique, which is employed in investigating email; content-based analysis and event-based analysis.

The content-based analysis requires the examiner to read the content of e-mail and figure out the critical information inside. It provides the rich information about the whole picture of crime. While the event-based analysis required the examiner to figure out about the time and date that the e-mail has been sent from a person to another. It can provide the pattern collection of who are the persons involved in the specific crime. These papers are providing a discussion about the boundaries in the view of legal aspect involved in a digital forensic area that also relate to the privacy of the users.

3.13 Intrusion Detection

Even though wireless communications are good in providing mobile internet access to the user, it is still vulnerable and easily exposed to interception of eavesdropper along the way of information transmission. The security mechanism such as Wired Equivalent Privacy (WEP) and WiFi Protected Access (WAP) are not sufficiently capable of providing a guaranteed security in wireless communication. The tools like clock skew and click print are able to provide the information of IP addresses or websites that the user browses the most. The user identity including the Medium Access Control (MAC) and IP address are not

sufficiently protected if they are using the wireless transmission medium. This information are captured by using tools like Wireshark and tcpdump, while the WiGLE.net tool is able to track the location of which the Access Point device is logging from.

On the other hand, the network traffic can be investigated through monitoring methodologies that are able to analyze and access to the network performance [12]. The monitoring mechanism can be either in wired or wireless techniques. The wired monitoring system is connected to a sniffer, which illegally accesses the network through a wired connection to any machine. It collects the information of network traffic. Furthermore, the network can be monitored using the Simple Network Management Protocol (SNMP) statistic. In a wireless network, the monitoring behavior is more sensitive to the physical information. It is deployed with portable mechanism, which is allowing users to access in mobile. The Access Point must be carefully organized with appropriate authorization by the network administrator. In order to detect any unauthorized AP in the network, an advanced monitoring fingerprint scheme is suggested in 4-tupple. Furthermore, the misbehavior of MAC Layer can be detected using compromise the protocol parameter. In conclusion, network traffic analysis can be diagnosed using the user fingerprinting technique. The intrusion detection system also might expose users' private information traveling on the network. In the hand of authorized person the privacy issues is not severe as if the system controlled by unethical person. The unethical person might use the private information available in a system that violates user's privacy.

3.14 Attack Trace/Pattern Analysis

Collecting a huge amount of data can be a tough procedure for a cyber forensic practitioner during the investigation. An appropriate framework of data collection is discussed in [50]. There are few methods to be implemented but one after all is graph-based clustering. The experiment applied by placing the 44 honeypot sensors in different locations using the different IP address. The graph or result illustration is using the Symbolic Aggregate Approximation (SAX). Based on the graph, it showed that the attack came in small traffic volume [53]. To be flexible in doing analysis, the analyst plugs into the machine with different application. The more flexible the machine, the more malicious attack can be investigated. The framework mentioned in the paper includes a certain flexibility that allows analysts to plug in different feature vectors and appropriate similarity metrics to be used in the clustering step, depending on the attack features they might find relevant to investigate. The contribution is being able to draw knowledge out of honeynet data by discovering attack patterns via attack trace similarity, rather than via a rigid signature.

The relationship between the topic and privacy issues that can be concluded is that, the investigator must maintain the ethical behavior while performing analysis of the patterns/traces in their collected data because some of the data contain private information that belongs to another user and not the attacker.

3.15 E-mail Investigation

In [56], the author described about the method to recover the data or email lost

in the digital forensic investigation. The fastest method is by using the reverse engineering from how the email is deleted (the exchange server is corrupted, the laptop is purposely crashed). The evidence of lost file in email said to be handled with care since the file can be very fragile. It is important to establish the authenticity of an electronic file or email in the organization. An incident handler is able to discover the evidence that is 'buried' within temporary files, replicated files, swap files, other system-created files or in a computer's unallocated space. The task is performed thorough searches of storage media relating to previous deleted or erased documents, parts of documents or drafts of documents. Parts of the document may consist of private data which irrelevant to the crime. Therefore, the investigator must differentiate and prioritize the content to avoid any privacy issue.

3.16 Incidence Response

Incident responder is the main body to recover the cyber forensic investigation of a company or organization. The level of complexity relies on the size and nature of a company. In paper [78] it discussed on the responsibilities of an incident responder who may carry out planning, preparing, management toward incident in network, system , mobile device or even in a cloud computing. Planning and preparing involves drafting the guideline and the development of training programs. Incident responder is the one who educating their internal workers upon the security on the network and regularly monitor whether the workers are continuously following the network security rules and approach. Educating might take throughout the email message or up to workshop program. Besides that, they should provide internal consultation regarding the technical nature. From time to time, they are responsible to execute the computer forensic tasks throughout the digital evidence management process**.** In order to have up-to-date point of vulnerabilities of hacking, the incident response team has to give support for analysis of IT company and network architecture [81].

The incident response can be handled using technological alternatives locally or remotely. The most important issue during an investigation is the availability of the media required. To resolve this kind of problem, some IT vendor implemented the agent-based architectural approach to allow access in multiple level or authenticity, from a most volatile data until to the most static data [88]. For the small cost forensic investigation, the remote forensic is applicable without requiring the agent-based analysis. The remote forensic cost is so low and currently it is available in ISCSI standard which allowing read-only access toward the targeted machine. The most application medium to run the remote-forensic is through VPN network. Some vendors develop the interesting agent-based architectural solution to allowing the multiple accesses to target machine. With highly concern demand in today network security implementation, an organization is hiring an incident responder to apply the best evidence collection and preservation practices. Therefore, the income of the incident responders should be justified with their responsibility to avoid any illegal action like gathering private data of the company or other employee that will lead to violation of the privacy issues.

3.17 Forensic Vendors

The author describes about the similarities and differences between Private Investigation (PI) and Digital Investigation (DI). Generally, PI is a profession regulated by state, federal or international law [79]. Both PI and DI investigator have to follow the code of ethic and technical guidelines. They also required to have professional insurance. Performing an investigation also considered to be properly authorized by a legal organization background. The violation of a simple rule could result in legal liability.

As an incident responder, they could be asked to perform a sort of wiretapping, eavesdropping and be specialized in electronic surveillance program. A PI and DI must maintain a behavior based on integrity and ethic. Otherwise, they might break the privacy of the data that should be handled by ethical people.

3.18 Anti-Forensic Approaches

The paper [89], discuss about the vulnerabilities involve in digital forensic software. As widely marketed, the forensic software may lead to defenseless state which might expose the collected information to the third party. The level of vulnerabilities is unlimited and can be exploited through software architecture, type of file, level of patching and etc. Thus, it is crucial to practice the administrative and authentication policy in IT system. As explained in [92] there will be no software is completely crash proof, as there will be an abnormality that involves of disfigure the data.

3.19 Network Data Analysis

Nowadays, the demand for IT gadget become rapidly increasing. The issues of networking become crucial in providing a connection between users. Besides providing the unlimited access to internet application and able to communicate between each other, the reliability of other IT gadget networking lies on how effective they can correspond to another device. In [45], the communication among those gadgets depends on lower-layer binary network signature like socket and packet data structure. In order to carve the network, the open source forensic tool is developed called as "scan_net". On network ground truth data, the data is securely erased and the Windows is installed with a virgin copy of the OS. The machine then connected to multiple numbers of servers, run the file transfer process and the packet entering and leaving the network is monitored using the promiscuous recorder. The tool carves the network on a specific level accordingly; IP address, Socket Structure, Windows and Ethernet level. On IP address carves, the potential IP address will be checked either in TCP or UDP protocol. Once it is possible, the IP address checksum will be performed in order to validate the correct IP address. On Socket Structure carving, the correct socket and port will be identified.

3.20 Data Integrity

The popularity of cloud storage services (CSS) grows rapidly in recent years. The cloud storage services provide lower cost to the data owner and it does not depend on a specific location for the data owner to consider. The client or the data

owner also does not have to perform storage management process and maintenance. The key concern in [1] is how to perform efficient audit services. The purpose of audit service is to check on data integrity and its availability of the outsourced data to the client when they need it. Because of this issue, the Third Party Auditor (TPA) gain benefit from the situation. Some of the clients themselves are not formidable enough to perform the audit service on their own. The cost of the audit service also caused the data owner to hire TPA to perform the audit service.

The authors propose their cryptographic interactive audit scheme in the paper. The proposed approach in the paper help to reduce the workload on the storage server as well as maintaining the capability to detect the server's abnormal behavior at a higher probability rate as mentioned in the paper. The paper also intends to cater the problem in privacy issues in their proposed approach. In the paper, they try to preserve the privacy of the data in the cloud storage services as part of their proposed approach. In the approach, the TPA unable to derive the user's data based on the information gathered during the audit service processes that preserve the users' privacy.

3.21 USB Forensic

Universal Serial Bus (USB) is widely used for their capacity and mobility capability. USB normally equipped with security function using the USB controller command. Because the USB is easily used, it tends to be used for USB memory – related crime. The USB controller command provides vulnerabilities during the user certification process which allows it to be bypassed. The paper, [27], explains on how to secure USB type, bypassing plan, certification method and the implementation of tools for USB security. USB provides an IP address tracking to allow only authentic user to have access. The paper compared the security method implemented by manufacturer in providing a secure USB usage in different type of USB. In order to enhance the security in USB application, some manufacturers implement USB controller demand. The tool mentioned in the paper can provide an image of data obtained in a user friendly interface and supply with the report of data received.

As a conclusion, as the USB memory increases its capacity and capability, this means that it has greater opportunity in providing information to digital forensics. By applying these tools, unlimited evidence are potential to be figured out. Privacy issues that can relate to the USB forensics is that with the usage of the tools, among the unlimited evidence that can be carved out of the USB storage, there might be private information that should not be accessed by unauthorized persons.

3.22 Evidence Validation

In [7], the paper reveals the method discussed by author to recover the lost files in the cloud computing system. Finding the evidence in cloud computing system may be very complex. The public cloud computing system is a publicly accessible remote interface for managing and transferring data. Some organization will encrypt the data before transfer it to cloud computing system. Unless a cloud computing application provides an audit trail, it may be difficult to extract digital evidence in an admissible manner from

such applications, and in some cases, there may be little evidence available to extract. This might lead to either legislation requiring cloud computing service providers to keep audit trails (or similar records of user activity), or that prosecution cases may need to be based upon evidence gained mainly from the user's computer, rather than from computing equipment within the cloud. So the process of evidence validating in cloud computing is quite complex as compared to the evidence validation in traditional computing. The investigation done on cloud computing may relate to the privacy issues of the other users in the cloud system.

3.23 Location Analysis

The TomTom navigation system is particularly divided into 3 main segments; SD Card, internal hardware device and flash memory [61]. The data can be saved in TomTom flash memory and keep the data as history until the power been turned off. The data will be saved in the setting.dat, temporary.iti and MapSetting.cfg file format. Besides directly connecting to the satellite upon navigation purpose, the TomTom system allows user to connect to computer using USB port. However, there are limitation of memory that will be erased when the device is turned off. It will delete or 'forget' about the last destination visited if the memory card is removed, the battery is less or the USB connection from the device is disconnected.

The new product released called as TomTology. It provides with huge capabilities which is not available previously like, type of record, (home, favorite, start of the last calculated route, POI, location entered by address or by lookup, as outlined earlier in this article). The tool can also interpret the structure of the .cfg file to identify how many locations of each type are stored in the.cfg file, identify recent destinations in the order they were entered, show details of the last entered journey and identify the last recorded GPS fix. It will carve out deleted.cfg files, if possible, so providing context for the deleted locations. The process of carving the files in the product might jeopardize users' privacy. It is because it able pinpoint where the user travel from deleted .cfg files. When using the product for digital forensic analysis, any act that leads to the violation of users' privacy must be avoided.

In addition there were several works on malware investigation [99,100], analysis of cloud and virtualized environments [101-103], privacy issues that may arise during forensics investigation[104-113], mobile device investigation [114-116], Voice over IP (VoIP) forensics investigation [117], greening digital forensics process [118], SCADA Systems [119] and securing forensic logs [120].

4 CONCLUSION AND FUTURE RESEARCH

As we can see in this paper, more and more tools are available or developed to facilitate the digital forensic investigators to acquire the digital evidence from the devices. Some of the tools are very powerful to extract the information from and reduce the duration of evidence analysis. Besides the advancement in the digital forensic investigation tools, the methodologies or techniques developed to obtain the information also become more advanced.

One of the key factors of the situation is contributed by the way computing technology evolves. The rapid development of computing devices requires new methods or tools to be used by the digital forensic investigators to obtain the evidences as a legally acquired evidence to be presented in the court. For example, as mentioned in [39] the paper demonstrates the development of Mobile Internal Acquisition Tool (MIAT). This tool executed from the removable memory card inserted into a Smartphone. This tool works in a different method from traditional evidence acquisition method, wherein the traditional method some data cables are required to transfer the evidence from the investigated device to the investigator's workstation.

The advancement in communication device also contributes to the following situation. Nowadays, mobile phones do not only transfer voice and text message, they have become a multipurpose device that can transfer multimedia files, perform video streaming, internet browsing and other operation that relates to data transfer. Thanks to the advancement in networking speed, the user can transfer their data easily with their mobile device. Even though this is a great situation for the user, it may lead them to the become a target of privacy invasion. Their personal data that reside in their mobile are valueable and might attract unauthorized attacker to gain their information for illegal purposes. As the computing technology evolves, the way computer user use or transfer the data in their environment also different from traditional computing system.

As discussed in [7-9], the digital evidence acquisition methodologies need to adapt the new environment like cloud computing and peer-to-peer networking environment. It differs from traditional computing system, where normally a single user uses the device and the application and user's data reside in their devices only. Unlike traditional computing environment the evidences or the data might not reside on single device but may be scattered around several devices. This requires the investigator to be extra careful with the data acquisition process because they might invade other users' private information that resides in that type of network. So with the complexity of networking, computing environment and the advancement of mobile devices, the digital forensic investigators also need to be advanced in their tools and methodologies to obtain the evidences legally without affecting the user's privacy to the court.

As we discuss throughout this paper, there are many tools and methodologies newly developed to assist digital forensic investigators in the digital evidence acquisition process and analyze the evidences. As we reviewed, some of the tools used by digital forensic investigators will be released under open source license. It means that the tools are available for public access. It comes to our mind that what if the tools fall into the hand unethical person. How severe the damage caused by the tools if the tools was used for illegal purpose and how to control the distribution of the tools if it is publicly available. These are the questions that we think that we need study and able to provide the solutions or answers to in the future.

Apart from the above questions, we are also interested to continue with the research on effective method on privacy education. As an initial step to reduce the privacy issue, it is crucial to combat the problems at the root level. The root

level solution is in our mind. Educating the human mind to become an ethical person in their work is one of the key factors that we think will help to reduce the issues in privacy. It is crucial to educate different level of person not to invade into other person's private information and to educate on what to do if they accidentally found that type of information. The method to educate people on privacy need to be effective enough, as we are human tends to explore something new to us. So, regardless how powerful the above mentioned tools might evolve, in the hand of ethical person, the privacy of related parties can be preserved if we have successfully educated ourselves to not interfere with the information which is not for our eyes to see.

6 REFENCES

[1] Y. Zhu, H. Hu, G.-J.Ahn, and S. S. Yau, "Efficient audit service outsourcing for data integrity in clouds," *Journal of Systems and Software*, vol. 85, pp. 1083-1095, 2012.

[2] H. Wechsler, "Linguistics and face recognition," *Journal of Visual Languages & Computing*, vol. 20, pp. 145-155, 2009.

[3] 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, pp. 795-800, 2009.

[4] 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, pp. 292-304, 2012.

[5] 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.

[6] M. Taylor, G. Hughes, J. Haggerty, D. Gresty, and P. Almond, "Digital evidence from mobile telephone applications," *Computer Law & Security Review*, vol. 28, pp. 335-339, 2012.

[7] M. Taylor, J. Haggerty, D. Gresty, and R. Hegarty, "Digital evidence in cloud computing systems," *Computer Law & Security Review*, vol. 26, pp. 304-308, 2010.

[8] M. Taylor, J. Haggerty, D. Gresty, and P. Fergus, "Forensic investigation of peer-to-peer networks," *Network Security*, vol. 2010, pp. 12-15, 2010.

[9] M. Taylor, J. Haggerty, D. Gresty, and T. Berry, "Digital evidence from peer-to-peer networks," *Computer Law & Security Review*, vol. 27, pp. 647-652, 2011.

[10] M. Taylor, J. Haggerty, and D. Gresty, "The legal aspects of corporate computer usage policies," *Computer Law & Security Review*, vol. 26, pp. 72-76, 2010.

[11] M. Taylor, J. Haggerty, and D. Gresty, "The legal aspects of corporate e-mail investigations," *Computer Law & Security Review*, vol. 25, pp. 372-376, 2009.

[12] 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, pp. 307-318, 2010.

[13] E. Serrano, A. Quirin, J. Botia, and O. Cordón, "Debugging complex software systems by means of pathfinder networks," *Information Sciences*, vol. 180, pp. 561-583, 2010.

[14] K. Saur and J. B. Grizzard, "Locating ×86 paging structures in memory images," *Digital Investigation*, vol. 7, pp. 28-37, 2010.

[15] S. Rekhis and N. Boudriga, "Logic-based approach for digital forensic investigation in communication Networks," *Computers & Security*, vol. 30, pp. 376-396, 2011.

[16] V.-H. Pham and M. Dacier, "Honeypot trace forensics: The observation viewpoint matters," *Future Generation Computer Systems*, vol. 27, pp. 539-546, 2011.

[17] M. Pavlou and N. M. Allinson, "Automated encoding of footwear patterns for fast indexing," *Image and Vision Computing*, vol. 27, pp. 402-409, 2009.

[18] B. Park, J. Park, and S. Lee, "Data concealment and detection in Microsoft Office 2007 files," *Digital Investigation*, vol. 5, pp. 104-114, 2009.

[19] A. Pal, H. T. Sencar, and N. Memon, "Detecting file fragmentation point using sequential hypothesis testing," *Digital*

Investigation, vol. 5, Supplement, pp. S2-S13, 2008.

[20] J. S. Okolica and G. L. Peterson, "Windows driver memory analysis: A reverse engineering methodology," *Computers & Security*, vol. 30, pp. 770-779, 2011.

[21] B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," *Signal Processing: Image Communication*, vol. 25, pp. 389-399, 2010.

[22] B. Mahdian and S. Saic, "Using noise inconsistencies for blind image forensics," *Image and Vision Computing*, vol. 27, pp. 1497-1503, 2009.

[23] W. Lu, W. Sun, F.-L.Chung, and H. Lu, "Revealing digital fakery using multiresolution decomposition and higher order statistics," *Engineering Applications of Artificial Intelligence*, vol. 24, pp. 666-672, 2011.

[24] N. Liao, S. Tian, and T. Wang, "Network forensics based on fuzzy logic and expert system," *Computer Communications*, vol. 32, pp. 1881-1892, 2009.

[25] W. Li, Y. Yuan, and N. Yu, "Passive detection of doctored JPEG image via block artifact grid extraction," *Signal Processing*, vol. 89, pp. 1821-1829, 2009.

[26] 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, pp. 35-49, 2011.

[27] T. Kavallaris and V. Katos, "On the detection of pod slurping attacks," *Computers & Security*, vol. 29, pp. 680-685, 2010.

[28] D.-Y. Kao, S.-J. Wang, and F. Fu-Yuan Huang, "SoTE: Strategy of Triple-E on solving Trojan defense in Cyber-crime cases," *Computer Law & Security Review*, vol. 26, pp. 52-60, 2010.

[29] 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.

[30] N. Jailani, N. F. M. Yatim, Y. Yahya, A. Patel, and M. Othman, "Secure and auditable agent-based e-marketplace framework for mobile users," *Computer Standards & Interfaces*, vol. 30, pp. 237-252, 2008.

[31] O. Ibáñez, O. Cordón, S. Damas, and J. Santamaría, "An advanced scatter search design for skull-face overlay in craniofacial superimposition," *Expert Systems with Applications*, vol. 39, pp. 1459-1473, 2012.

[32] H.-C. Huang and W.-C.Fang, "Metadata-based image watermarking for copyright protection," *Simulation Modelling Practice and Theory*, vol. 18, pp. 436-445, 2010.

[33] Z. He, W. Sun, W. Lu, and H. Lu, "Digital image splicing detection based on approximate run length," *Pattern Recognition Letters*, vol. 32, pp. 1591-1597, 2011.

[34] L. Gómez-Miralles and J. Arnedo-Moreno, "Versatile iPad forensic acquisition using the Apple Camera Connection Kit," *Computers & Mathematics with Applications*, vol. 63, pp. 544-553, 2012.

[35] S. Geetha, N. Ishwarya, and N. Kamaraj, "Evolving decision tree rule based system for audio stego anomalies detection based on Hausdorff distance statistics," *Information Sciences*, vol. 180, pp. 2540-2559, 2010.

[36] S. Geetha, N. Ishwarya, and N. Kamaraj, "Audio steganalysis with Hausdorff distance higher order statistics using a rule based decision tree paradigm," *Expert Systems with Applications*, vol. 37, pp. 7469-7482, 2010.

[37] D. Forte, "Visual Forensics: new or old trend?," *Computer Fraud & Security*, vol. 2009, pp. 15-17, 2009.

[38] H. Farid and M. J. Bravo, "Perceptual discrimination of computer generated and photographic faces," *Digital Investigation*, vol. 8, pp. 226-235, 2012.

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

[40] F. Cohen, "A method for forensic analysis of control," *Computers & Security*, vol. 29, pp. 891-902, 2010.

[41] Y.-K. Chung, W. K. Fung, and Y.-Q.Hu, "Familial database search on two-person mixture," *Computational Statistics & Data Analysis*, vol. 54, pp. 2046-2051, 2010.

[42] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "A secure and improved self-embedding algorithm to combat digital document forgery," *Signal Processing*, vol. 89, pp. 2324-2332, 2009.

[43] A. Castiglione, A. De Santis, and C. Soriente, "Security and privacy issues in the Portable Document Format," *Journal of*

Systems and Software, vol. 83, pp. 1813-1822, 2010.

[44] D. Byers and N. Shahmehri, "Contagious errors: Understanding and avoiding issues with imaging drives containing faulty sectors," *Digital Investigation*, vol. 5, pp. 29-33, 2008.

[45] 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.

[46] G. Antoniou, L. Sterling, S. Gritzalis, and P. Udaya, "Privacy and forensics investigation process: The ERPINA protocol," *Computer Standards & Interfaces*, vol. 30, pp. 229-236, 2008.

[47] A. Veremme, É. Lefevre, G. Morvan, D. Dupont, and D. Jolly, "Evidential calibration process of multi-agent based system: An application to forensic entomology," *Expert Systems with Applications*, vol. 39, pp. 2361-2374, 2012.

[48] W. S. van Dongen, "Case study: Forensic analysis of a Samsung digital video recorder," *Digital Investigation*, vol. 5, pp. 19-28, 2008.

[49] 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.

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

[51] M. Taylor, J. Haggerty, D. Gresty, and D. Lamb, "Forensic investigation of cloud computing systems," *Network Security*, vol. 2011, pp. 4-10, 2011.

[52] C. M. S. Steel and C.-T.Lu, "Impersonator identification through dynamic fingerprinting," *Digital Investigation*, vol. 5, pp. 60-70, 2008.

[53] J. Shaw, "Speedy recovery: retrieving lost emails as part of an investigation," *Computer Fraud & Security*, vol. 2011, pp. 9-11, 2011.

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

[55] J. Santamaría, O. Cordón, and S. Damas, "A comparative study of state-of-the-art evolutionary image registration methods for 3D modeling," *Computer Vision and Image Understanding*, vol. 115, pp. 1340-1354, 2011.

[56] A. Rocha and S. Goldenstein, "Progressive randomization: Seeing the unseen," *Computer Vision and Image Understanding*, vol. 114, pp. 349-362, 2010.

[57] P. Ridley, "Outsmarting the smartphone fraudsters," *Network Security*, vol. 2010, pp. 7-9, 2010.

[58] H. Proença and G. Santos, "Fusing color and shape descriptors in the recognition of degraded iris images acquired at visible wavelengths," *Computer Vision and Image Understanding*, vol. 116, pp. 167-178, 2012.

[59] N. R. Poole, Q. Zhou, and P. Abatis, "Analysis of CCTV digital video recorder hard disk storage system," *Digital Investigation*, vol. 5, pp. 85-92, 2009.

[60] M. S. Olivier, "On metadata context in Database Forensics," *Digital Investigation*, vol. 5, pp. 115-123, 2009.

[61] B. Nutter, "Pinpointing TomTom location records: A forensic analysis," *Digital Investigation*, vol. 5, pp. 10-18, 2008.

[62] T. D. Morgan, "Recovering deleted data from the Windows registry," *Digital Investigation*, vol. 5, Supplement, pp. S33-S41, 2008.

[63] S. Mansfield-Devine, "Fighting forensics," *Computer Fraud & Security*, vol. 2010, pp. 17-20, 2010.

[64] G. Liu, J. Wang, S. Lian, and Z. Wang, "A passive image authentication scheme for detecting region-duplication forgery with rotation," *Journal of Network and Computer Applications*, vol. 34, pp. 1557-1565, 2011.

[65] H.-Y. Lin and W.-C. Fan-Chiang, "Reconstruction of shredded document based on image feature matching," *Expert Systems with Applications*, vol. 39, pp. 3324-3332, 2012.

[66] Q. Liao, A. Blaich, D. VanBruggen, and A. Striegel, "Managing networks through context: Graph visualization and exploration," *Computer Networks*, vol. 54, pp. 2809-2824, 2010.

[67] J. Lewthwaite and V. Smith, "Limewire examinations," *Digital Investigation*, vol. 5, Supplement, pp. S96-S104, 2008.

[68] J. Lee, S. Un, and D. Hong, "High-speed search using Tarari content processor in digital forensics," *Digital Investigation*, vol. 5, Supplement, pp. S91-S95, 2008.

[69] P. Larrañaga and S. Moral, "Probabilistic graphical models in artificial intelligence," *Applied Soft Computing*, vol. 11, pp. 1511-1528, 2011.
[70] P. Kumar, S. Roy, and A. Mittal, "OS-Guard: on-site signature based framework for multimedia surveillance data management," *Multimedia Tools and Applications*, vol. 59, pp. 363-382, 2012.
[71] J. D. Kornblum, "Using JPEG quantization tables to identify imagery processed by software," *Digital Investigation*, vol. 5, Supplement, pp. S21-S25, 2008.
[72] 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.
[73] A. Jones and T. Martin, "Digital forensics and the issues of identity," *Information Security Technical Report*, vol. 15, pp. 67-71, 2010.
[74] 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, pp. 51-58, 2011.
[75] F. Iqbal, R. Hadjidj, B. C. M. Fung, and M. Debbabi, "A novel approach of mining write-prints for authorship attribution in e-mail forensics," *Digital Investigation*, vol. 5, Supplement, pp. S42-S51, 2008.
[76] D. Horn, "Taking the right approach to digital forensics," *Computer Fraud & Security*, vol. 2008, pp. 16-17, 2008.
[77] F. Fusco, M. Vlachos, and M. P. Stoecklin, "Real-time creation of bitmap indexes on streaming network data," *The VLDB Journal*, vol. 21, pp. 287-307, 2012.
[78] D. V. Forte, "The responsibilities of an incident responder," *Network Security*, vol. 2010, pp. 18-19, 2010.
[79] D. V. Forte, "Are you going to be a forensic examiner or a private investigator?," *Computer Fraud & Security*, vol. 2010, pp. 15-17, 2010.
[80] D. V. Forte, "Volatile data vs. data at rest: the requirements of digital forensics," *Network Security*, vol. 2008, pp. 13-15, 2008.
[81] D. V. Forte, "Computer forensics: Are you qualified?," *Computer Fraud & Security*, vol. 2008, pp. 18-20, 2008.
[82] D. Forte, A. Cavallini, C. Maruti, L. Losio, T. Orlandi, and M. Zambelli, "PTK: An Alternative Advanced Interface for the Sleuth Kit", Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08." vol. 53, E. Corchado, R. Zunino, P. Gastaldo, and Á. Herrero, Eds., ed: Springer Berlin / Heidelberg, 2009, pp. 27-34.
[83] D. Forte, "Preventing and investigating hacking by auditing web applications," *Network Security*, vol. 2010, pp. 18-20, 2010.
[84] D. Forte, "The death of MD5," *Network Security*, vol. 2009, pp. 18-20, 2009.
[85] D. Forte, "Are you court validated?," *Network Security*, vol. 2009, pp. 6-8, 2009.
[86] D. Forte, "Do encrypted disks spell the end of forensics?," *Computer Fraud & Security*, vol. 2009, pp. 18-20, 2009.
[87] D. Forte, "Visual forensics in the field," *Computer Fraud & Security*, vol. 2009, pp. 18-20, 2009.
[88] D. Forte, "Technological alternatives in incident response," *Network Security*, vol. 2008, pp. 16-18, 2008.
[89] D. Forte, "Dealing with forensic software vulnerabilities: is anti-forensics a real danger?," *Network Security*, vol. 2008, pp. 18-20, 2008.
[90] B. Dolan-Gavitt, "Forensic analysis of the Windows registry in memory," *Digital Investigation*, vol. 5, Supplement, pp. S26-S32, 2008.
[91] M. I. Cohen, "PyFlag – An advanced network forensic framework," *Digital Investigation*, vol. 5, Supplement, pp. S112-S120, 2008.
[92] 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.
[93] W. C. Calhoun and D. Coles, "Predicting the types of file fragments," *Digital Investigation*, vol. 5, Supplement, pp. S14-S20, 2008.
[94] Y. Cai, "Video intelligence workshop (VI-2010)," *Procedia Computer Science*, vol. 1, p. 2509, 2010.
[95] S. Brueckner, D. Guaspari, F. Adelstein, and J. Weeks, "Automated computer forensics training in a virtualized environment," *Digital Investigation*, vol. 5, Supplement, pp. S105-S111, 2008.
[96] S. Bayram, H. T. Sencar, and N. Memon, "Classification of digital camera-models

based on demosaicing artifacts," *Digital Investigation*, vol. 5, pp. 49-59, 2008.

[97] R. Alshammari and A. N. Zincir-Heywood, "Can encrypted traffic be identified without port numbers, IP addresses and payload inspection?," *Computer Networks*, vol. 55, pp. 1326-1350, 2011.

[98] M. Tu, K. Cronin, D.Xu, S.Wira,"On the Development of Digital Forensics Curriculum", *http://www.dsu.edu/research/ia/documents/[6]-On-the-development-of-Digital-Forensics-Curriculum.*

[99] F. Daryabar, A. Dehghantanha, HG. Broujerdi, Investigation of Malware Defence and Detection Techniques," International Journal of Digital Information and Wireless Communications**(**IJDIWC**),** volume 1, issue 3, pp. 645-650, 2012.

[100] F. Daryabar, A. Dehghantanha, NI. Udzir, "Investigation of bypassing malware defences and malware detections," Conference on Information Assurance and Security (IAS), pp. 173-178, 2011.

[101] M. Damshenas, A. Dehghantanha, R. Mahmoud, S. Bin Shamsuddin, "Forensics investigation challenges in cloud computing environments," Cyber Warfare and Digital Forensics (CyberSec), pp. 190-194, 2012.

[102] F. Daryabar, A. Dehghantanha, F. Norouzi, F Mahmoodi, "Analysis of virtual honeynet and VLAN-based virtual networks," Science & Engineering Research (SHUSER), pp.73-70, 2011.

[103] S. H. Mohtasebi, A. Dehghantanha, "Defusing the Hazards of Social Network Services," International Journal of Digital Information, pp. 504-515, 2012.

[104] A. Aminnezhad, A.Dehghantanha, M.T. Abdullah, "A Survey on Privacy Issues in Digital Forensics," International Journal of Cyber-Security and Digital Forensics (IJCSDF)- Vol 1, Issue 4, pp. 311-323, 2013.

[105] A. Dehghantanha, N. I Udzir, R. Mahmod, "Towards a pervasive formal privacy language," Advanced Information Networking and Applications Workshops (WAINA), pp. 1085-1091, 2010.

[106] A. Dehghantanha, R. Mahmod, N. I Udzir, "A XML based, User-centered Privacy Model in Pervasive Computing Systems," International Journal of Computer Science and Networking Security, Vol.9, Issue 2, pp.167-173, 2009.

[107] A. Dehghantanha, R. Mahmod, N. I Udzir, Z.A. Zulkarnain, "User-centered Privacy and Trust Model in Cloud Computing Systems," Computer And Network Technology, pp. 326-332, 2009.

[108] A. Dehghantanha, "Xml-Based Privacy Model in Pervasive Computing," Master thesis- University Putra Malaysia 2008.

[109] C. Sagaran, A. Dehghantanha, R Ramli, "A User-Centered Context-sensitive Privacy Model in Pervasive Systems," Communication Software and Networks, pp. 78-82, 2010.

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

[111] A. Dehghantanha, R. Mahmod, "UPM: User-Centered Privacy Model in Pervasive Computing Systems," Future Computer and Communication, pp. 65-70, 2009.

[112] V.Ho, A.Dehghantanha, K.Shanmugam, "*A Guideline to Enforce Data Protection and Privacy Digital Laws in Malaysia*," Computer Research and Development, pp. 3-6, 2010.

[113] C Sagaran, A Dehghantanha, R Ramli, "A User-Centered Context-sensitive Privacy Model in Pervasive Systems," Communication Software and Networks, pp. 78-82, 2010.

[114] S. Parvez, A. Dehghantanha, HG. Broujerdi, "Framework of digital forensics for the Samsung Star Series phone," Electronics Computer Technology (ICECT), Volume 2, pp. 264-267, 2011.

[115] S. H. Mohtasebi, A. Dehghantanha, H. G. Broujerdi, "Smartphone Forensics: A Case Study with Nokia E5-00 Mobile Phone," International Journal of Digital Information and Wireless Communications (IJDIWC),volume 1, issue 3, pp. 651-655, 2012.

[116] F. N. Dezfouli, A. Dehghantanha, R. Mahmoud ,"Volatile memory acquisition using backup for forensic investigation," Cyber Warfare and Digital Foresnsic, pp. 186-189, 2012

[117] M. Ibrahim, MT. Abdullah, A. Dehghantanha , "*VoIP evidence model: A new forensic method for investigating VoIP malicious attacks*," Cyber Security, Cyber Warfare and Digital Forensic , pp. 201-206, 2012.

[118] Y. TzeTzuen, A. Dehghantanha, A. Seddon, "Greening Digital Forensics: Opportunities and Challenges," Signal Processing and Information Technology, pp. 114-119, 2012.

[119] F. Daryabar, A. Dehghantanha, N.I .Udzir, N.Fazlida, S.b.Shamsuddin, "Towards Secure Model for SCADA Systems," Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp. 60-64, 2012.

[120] N. Borhan, R. Mahmod, A. Dehghantanha, "A Framework of TPM, SVM and Boot Control for Securing Forensic Logs," International Journal of Computer Application, volume 50, Issue 13, pp. 65-70, 2009.