# Towards Fact-Based Digital Forensic Evidence Collection Methodology

Nik Zulkarnaen Khidzir, Shekh Abdullah-Al-Musa Ahmed
*Faculty of Creative Technology and Heritage / Global Entrepreneurship Research and Innovation Centre, Faculty of Creative Technology and Heritage, Universiti Malaysia Kelantan, Malaysia*

## Abstract

*Digital Forensic is the fundamental property of information system security. It plays an important role to find out digital crime in the cyber world. A key aspect of digital forensic is how to collect the evidence and represent it in court for legal action. A primary concern of digital forensic evidence is to make it as a scientific evidence. So whenever verify the evidence it will give the same result. Since Forensic Science is an integrate science. Therefore, medical evidence is an integral part of forensic methodical research. Using the forensic methodical research such as collecting information and present it on the courtroom. So, this is of proof technology symbolizing the knowledge of collection information by establish methodical research. For example, to make a DNA profile, going after the establish standard protocol to produce a DNA account. So, by evaluating it thousand time it is going to supply the same result. This can be a establish guide of science. Whenever we apply this guideline in the courtroom it'll called scientific Evidence. Evidence is whatever demonstrates, clarifies or shows the reality of an undeniable fact or point involved. Traditionally there's been amount of resistance to the approval of new varieties of proof that emerge because of this of changing technology. Many countries on the globe have started using digital proof including Malaysia. The amendment to Evidence Act 1950 (Amendment 2012) 90A, 90B and 90C in 1993 has provided for the admissibility of 'computer-generated documents' in both civil and criminal proceedings. However, these rapid changes of technology are having a serious effect on digital forensics to explore the Improvement of Digital forensics from various aspect, legal concern of digital crime and the way to get and analysis the digital fact-based substantiation. And suggesting the digital evidence which is admissible to court that treat as scientific evidence. Due to the changing of technology we suggest digital evidence collection methodology.*

## 1. Introduction

A primary concern of Computer forensics involves the preservation, identification, extraction, records, and interpretation of computer media for evidentiary and root cause analysis. Digital proof might be required for a variety of computer criminal offenses and misuses. The United Kingdom (UK) Police and Criminal Evidence Code identifies digital proof as "all information contained in a computer". Forensic science is an incorporate science. Technological information is a part of forensic science. By simply using the forensic scientific research collecting information and present it on the judge. Therefore, the meaning of evidence of science symbolizing the understanding of collection information by establish scientific research. For example, to create a DNA profile, pursuing the establish protocol to generate a DNA report. So, by testing it thousand time it will give the same result. This is the establish rule of science. When we apply this rule in the court then it will be called scientific Evidence. Regarding to Eoghan Casey, “Handbook of Digital Forensics and Investigation”, he identified-the definition of digital forensics was formerly used as a synonym for computer forensics but has extended to cover investigation of all devices capable of storing digital data. With roots in the personal computing revolution of the late 1970s and early on 1980s, the discipline developed in a haphazard manner throughout the 1990s, and it had not been until the early on 21st century that countrywide policies emerged. Before the 1980s crimes involving computer systems were dealt with using existing laws. As well as identifying direct proof of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements and determine purpose identify sources or authenticate documents [1].

## 2. Literature Review

The first computer crimes were recognized in the 1978 Florida Computer Crimes Act, which included legislation against the unauthorized modification or deletion of information on a computer system. Above the years to come the range of computer crimes being committed increased, and laws were approved to manage issues of copyright laws, privacy/harassment such as internet bullying, cyber stalking and online predators. It was not before the nineteen eighties that federal laws commenced to incorporate computer accidents. Canada was the first country to pass legal guidelines in 1983. This was

 

followed by the US Federal Computer Fraud and Abuse Act in 1986, Australian amendments to their crimes acts in 1989 and the British Computer system Misuse Act in 1990. According to Daniel J. Ryan; Gal Shpantzer.” Legal Aspect of Digital Forensics” they described - When used in a court digital evidence comes under the same legal guidelines but other varieties of evidence, courts do not usually require more rigid guidelines [2]. Whereas in computer science, data is nearly anything in an application well suited for use with some type of computer. Data is often distinguished from programs. A program is a set of instructions that detail a process for the computer to accomplish. In this sense, data is thus everything that is not program code. Generally, in addition to science, data is a gathered body of facts. Some specialists and publishers, cognizant of the word data that come from Latin origins and as the form of "datum”. Others take the view that since "datum" is rarely used, it is more natural to take care of "data" as a singular form. Data security refers to protective digital privacy measures that are applied to not authorized access to computers, data source and websites [10]. Data security also protects data from corruption. Data security is the key priority for organizations of each and every size and genre. Instances of data security systems include software or hardware disk security, backups, data masking and data erasure. A key data security technology solution is scrambling, where digital data, software or hardware, and hard drives are scrambled and rendered unreadable to not authorized users and hackers. The attack in the history were commonly conducted over phone lines during the 1980s, however in the modern era are usually spread over the Internet.

## 3. Challenges Collecting The Digital Proof

Many countries on the globe have started using digital proof including Malaysia. Section 3 of the Evidence Act 1950 (Amendment 2012) defines evidence as:(a) all statements which the court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry, such statements are called oral evidence; (b) all documents produced for the inspection of court, such documents are called documentary evidence. The amendment to Evidence Act 1950 (Amendment 2012) 90A, 90B and 90C in 1993 has provided for the admissibility of 'computer-generated documents' in both civil and criminal proceedings [3]. Digital evidence is undoubtedly documentary proof as described in Section 3 Interpretation of Evidence Act 1950 (Amendment 2012), ‘document’ means any subject expressed, explained, or as a matter of symbolized, after any product, materials, thing or article. Thus, many kind of digital information play an important and useful role in a variety of civil and criminal court cases. In Malaysia, digital evidence is admissible as documentary proof and primary evidence or facts. The admissibility of digital end result is set up under sections 90A, 90B and 90C of the Evidence Act 1950 (amendment 2012). Digital proof is any probative information stored or sent in digital form to get together to a courtroom case and might use during trials. An excellent digital details management system must adhere to MS ISO 6175-2:2012, Part 2: Recommendations and practical requirements for digital documents management systems which illustrate the requirements for software systems used to control records. Regarding to MS ISO 16175-2:2012, Part 2, digital documents management systems must have the following characteristics that seek to ensure that key information characteristics are preserved:

- creating and acquiring records in framework
- controlling and maintaining information control
- maintaining details for so long as they required
- implementing documents disposition
- the management of details management metadata

According to Sarah Mocas (February 2004) - "Building theoretical underpinnings for digital forensics research". Identified the examination of digital media is covered by national and international legal guidelines. For civil investigations, in particular, laws may limit the skills of experts to undertake examinations. Constraints against network monitoring or reading of personal marketing and sales communications often exist [4]. Evidence from computer forensics investigations is usually put through the same guidelines and practices of other digital proof. This has been used in many of high-profile circumstances which is becoming widely accepted as reliable within U.S. and European court systems.

Multiple methods of discovering data on computer system recovering deleted, protected, or damaged file. Data monitoring live activity discovering violations of corporate plan, information collected assists in arrests, prosecution, termination of employment, and protecting against future against the law activity.

## 4. The Phenomena of Digital Crime

Regarding to Debarati Halder and K. Jaishankar in their book “ Cyber – crime and the Victimization of Woman : Laws , Rights , and Regulation ” cybercrime from the perspective of gender and defined 'cybercrime against women' as Crimes targeted against women with a motive to

 

intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones. Throughout the world both governmental and non-state actors participate in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one country state is sometimes known as cyberwarfare [6]. Most information which guides or publications on cybercrime that get started by understanding the conditions "computer crime" and "Digital Crime". Just before providing an overview of the debate and analyzing the approaches, it is useful to look for the relationship between "Digital Crime" and "computerrelated crimes". Without going into fine detail at this stage, the definition of "cybercrime" is narrower than computer related crimes as it has to require a computer network. Computer-related crimes cover even those offences that bear no relation to a network, but only affect stand-alone computer systems.

During the 10th United Nations Congress on the Prevention Criminal offense and the Treatment of Offenders, two definitions were developed in a related workshop. In that case Digital Crime in a narrow sense of computer crime that covers any illegitimate behavior directed by way of electronic digital functions that target the safety of computer systems and the information processed by them. Digital Crime in a broader sense of computer-related crimes covers any illegitimate behavior committed by means of, or in connection to a computer system or network, including such criminal offenses as illegitimate possession and offering or distributing information by means of a computer or network.

According to Daniel J. Ryan , Gal Shpantzer in their Article “Legal Aspects of Digital Forensics” . They described the digital proof is nearly never in a format readable by humans, requiring additional steps to include digital documents as evidence such as printing out the material. This has been argued that this change of format may mean digital proof does not qualify under the "best evidence. Nevertheless, the "Federal Rules of Evidence" rule 1001(3) states that "if data are stored in a computer, any printout or other outcome readable by sight, shown to reflect the data accurately, is an 'original’ [7][8]. The term "Digital Crime" can be used to describe a range of offences including traditional computer crimes, as well as network crimes. Since these crimes differ in many ways, there is no single criterion that could include all functions mentioned in the several local and international legal methods to address the issue, even though excluding traditional crimes that are just facilitated by using hardware [9]. The simple fact that there is not one definition of "Digital Crime" does not need to be important, as long as the term is not used as the best term [10].

## 5. Digital Forensics Investigation Methodology

A digital forensic investigation commonly consists of three stages: acquisition or imaging of exhibits, analysis, and reporting. Ideally acquisition involves capturing an image of the computer's volatile memory (RAM) and creating an exact sector level duplicate (or "forensic duplicate") of the media, often using a write blocking device to prevent modification of the original. However, the growth in size of storage media and developments such as cloud computing have led to more use of 'live' acquisitions whereby a 'logical' copy of the data is acquired rather than a complete image of the physical storage device. So, based of the three stages this paper oraganized eight phase of collecting digital evidence collection technique. According to the National Institute of Justice, “Digital evidence should be examined only by those trained specifically for that purpose.” So that proposing this phase are very effective for collecting digital evidence. The nobelity of this method is that representing the step of phases.The goal of these 8 steps is to answer systematically to digital forensic investigations and determine the analysis methodology. An identical process is accessible and was made by Integrating Forensics Technique into Incident Response (pub. #: 800-86) published in 2006. Since technology is always changing, here in this article proposing the new methodology steps.

| No. of Phase | Digital Evidence Collection Methodology |
|---|---|
| Phase 1 | Confirmation |
| Phase 2 | System Explanation |
| Phase 3 | Proof Acquisation |
| Phase 4 | Timeline Evaluation |
| Phase 5 | Mass Media Artifact Evaluation |
| Phase 6 | Sting Byte Search |
| Phase 7 | Data Collection |
| Phase 8 | Reporting Result |

Figure 1. Showing the Different Phase of Digital Evidence Collection Methodology

### 5.1. Confirmation

Normally the computer forensics analysis will be achieved within an event response scenario, consequently the first step ought to be to verify an

 

incident has occurred. Determine the breadth and opportunity of the event, evaluate the situation. What is the specific situation, the type of the circumstance and its details [11], [12]. This primary step is important because it can help to deciding the characteristics of the event and determining the best method of identify, maintain and gather information. It could also help justify to companies to have a system offline.

### 5.2. System Explanation

Then it comes after the step where gathering data about the precise incident. Starting by firmly taking notes and explaining the system heading to investigate, where is the machine being acquired, the machine role in the business and in the network [13]. Outline the operating-system and its standards settings such as drive format, amount of ram memory and the positioning of the data [14].

### 5.3. Proof Acquisition

Identify possible resources of data, acquire volatile and non-volatile data, check the integrity of the info and ensure string of guardianship. When in uncertainty of what things to accumulate be on the safe area and is way better to rather accumulate too much than not [15], [16]. In this step is also important that prioritize facts collection and participate the business enterprise owners to look for the execution and business impact of chosen strategies. Because volatile data changes as time passes, the order where data is accumulated is important [17]. One recommended order where volatile data should be obtained is network cable connections, ARP cache, login periods, running processes, available documents and the material of ram memory and other relevant data – we have to be aware that this data should be accumulated using respected binaries rather than the methods from the impacted system. After collecting this volatile data go into the next thing of collecting non-volatile data including the hard drive. To assemble data from the hard drive with regards to the case there are usually three ways of do a little bit stream image, by using a hardware device just like a write blocker in the event can take the machine offline and take away the hard drive; using an event response and forensic toolkit such as Autopsy which will be used on top of that the machine[18], [19]. Using live system acquisition (locally or remotely) that could be used when interacting with encrypted systems or systems that can't be used offline or only accessible remotely. After acquiring data, ensure and confirm its integrity. And really should also have the ability to obviously describe the way the proof was found, how it was dealt with and exactly what took place to it i.e. chain of custody.

### 5.4. Timeline Evaluation

Following the evidence acquisition begins doing analysis and evaluation in forensics laboratory. Start by performing a timeline analysis. That is an essential step and incredibly useful since it includes information such as when documents were modified, utilized, transformed and created in a human being readable format[20]. The info is gathered by using a variety of tools which is extracted from the metadata covering of the document system. Timelines of memory space artifacts can even be very helpful in reconstructing what happen. The finish goal is to create a snapshot of the experience done in the machine including its time frame, action and source. The creation is a fairly easy process however the interpretation is hard. Through the interpretation it can help to be careful and perseverance and it helps if comprehensive document systems and operating-system artifacts knowledge [21].

### 5.5. Mass media and Artifact Evaluation

In this task which will be overwhelmed with the quantity of information that might be looking at. Can answer questions such as what programs were carried out, which documents were downloaded, which documents were clicked on, which web directories were opened up, which documents were erased, where did an individual browsed to and many more. One technique found in order to lessen the data set in place is to recognize files regarded as good and those that are regarded as bad. Should understanding of file systems registry artifacts to consider benefitting of this system that will certainly reduce the quantity of data to be examined [22], [23]. Other things which will be looking is proof account utilization, browser usage, document downloads, file starting or creation, program execution. Memory space evaluation is another key evaluation part of order to analyze rogue processes, networking connections, proof code injections, process paths and many more. Avoiding anti-forensic techniques such as steganography or data alteration and damage, that will effect on investigation evaluation and conclusions.

### 5.6. String or Byte search

This task will comprise into using tools that will search the reduced level fresh images. If knowing what exactly are looking then may use this technique to think it is. In this task that use tools and techniques that can look for byte signatures of know documents known as the special cookies. Additionally, it is in this task that doing string queries using regular expressions. The strings or byte signatures which will be looking for will be the ones

 

that are highly relevant to the situation are interacting with.

### 5.7. Data Restoration

This is actually the step which will be looking at restore data from the data file system. A number of the tools that will assist in this task that will be the ones available in the FTK to investigate the data file system, data coating and metadata covering. Examining the slack space, unallocated space and in-depth data file system evaluation is part of the step and discover files appealing[24][25]. Carving data files from the fresh images predicated on document headers using tools like most important is another strategy to further gather proof.

### 5.8. Reporting Results

The ultimate phase involves confirming the results of the evaluation, which might include explaining the activities performed, identifying how many other actions have to be performed, and suggesting improvements to regulations, guidelines, methods, tools, and other areas of the forensic process. Confirming the results is an integral part of any analysis [26]. Consider writing in a manner that reflects the use of methodical methods and facts that can demonstrate. Adapt the confirming style with regards to the audience and become well prepared for the accountable to be utilized as information for legal or administrative purposes [27], [28].

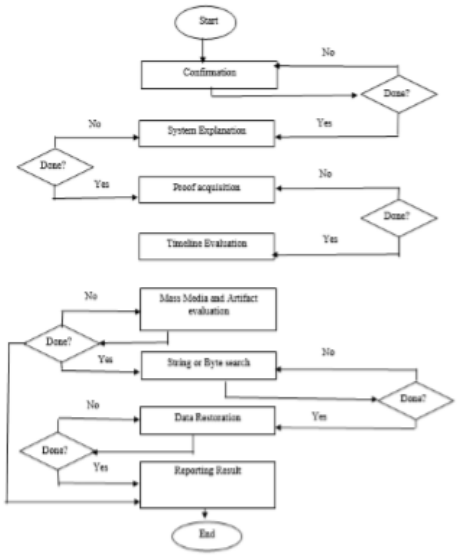


Figure 2. Showing the flowchart diagram of digital evidence collection methodology

## 6. Conclusion

The purpose of the paper is to determine the methodology of digital evidence collection process by digital forensic investigation. Forensic science is an incorporate science. Therefore, scientific evidence is a part of forensic scientific research. Utilizing the forensic scientific research such as collecting information and present it on the courtroom. So, this is of evidence of science symbolizing the understanding of collection information by establish scientific research. For instance, to create a DNA profile, pursuing the establish protocol to make a DNA profile. So, by testing it thousand time it will eventually give the same result. This is actually the establish guideline of science. When we apply this rule in the court it will be called scientific Evidence. In Bangladesh, the majority of time it is seen that judiciary process is be based upon hearsay evidence based. Justice in the lower court does not be based upon Digital forensic rather be based upon Confession based. The explanation of document is given in Section 3 at Evidence Act, 1872 and it is amended by ICT Act 2006 by Section 87, it is said that creating record, file and doc by electronic is also a document. So, any picture or video or audio tracks are electronic document is a document. The authors Reith, Carr and Gunsch [8] in their article "An examination of digital forensic models" described the actual process of examination can vary between research but common methodologies include conducting keyword searches across the digital media (within files as well as unallocated and slack space), recovering deleted files and extraction of registry information (for example to list user accounts, or fastened USB devices). During the analysis phase an examiner recovers evidence material utilizing a few different strategies and tools [29].

However, for digital proof-based solution this Article suggesting autopsy forensic tools, which will run on Kali Linux Forensic mode. It will eventually make a report paper and calculates MD5 hash principles and confirms the sincerity of the data before closing the files. Not really all computer offence we can called cybercrime, but if a person created forged certificate or take computer file, we might be called it as an electronic digital Crime. In real space, there are some physical force such as robber, theft and so on. But in Digital criminal offenses, there is absolutely no physical force, but doing the crime by technology. So, our content suggesting autopsy forensic tools, that will run on Kali Linux Forensic mode for digital proof-based consequence. The admissibility of digital evidence relies on the various tools and technique that is used to extract it. In the US, forensic tools are subjected to the Daubert standard, where the judge is accountable for ensuring that the procedures and software used

 

were acceptable. The author Brian Carrier and his Research article “Open Source Digital Forensics Tools: The Legal Argument”, argued that the Daubert guidelines required the code of forensic tools to be published and peer reviewed. He concluded that "open source tools may more clearly and comprehensively meet the guideline requirements than would close source tools [29].

## 7. References

[1] Casey, E., ed. Handbook of Digital Forensic and Investigation Academic Press. p. 567. ISBN 0-12-374267-6.

[2] Ryan, D.J., Shpantzer, G., “Legal Aspect of Digital Forensics” (PDF).

[3] Radhakrishna, G., (2012) “Digital evidence in Malaysia.”

[4] Mocas, S., (2004). "Building theoretical underpinnings for digital forensics research". Digital Investigation. 1 (1): 61–68. ISBN 1742-2876.

[5] Casey, E., (2004). Digital Evidence and Computer Crime, Second Edition ISBN 0-163104-4.

[6] Halder, D., & Jaishankar, K., (2011), Cyber – crime and the Victimization of Woman: Laws, Rights, and Regulation. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

[7] Clarke, R.A., Cyber War, HarperCollins (2010) ISBN 9780061962233.

[8] Reith, M., Carr, C., Gunsch, G., (2002). “An examination of digital forensic models”, International Journal of Digital Evidence.

[9] Ligh, M., Adair, S., Hartstein, B., (2010) “Malware analyst's cookbook and DVD: tools and techniques for fighting malicious code.”

[10] Kirschenbaum, M., Ovenden, R., (2010) “Digital forensics and born-digital content in cultural heritage collections.”

[11] Casey, E., (2011). “Digital evidence and computer crime: Forensic science, computers, and the internet.”

[12] Jones, K.J., Bejtlich, R., (2006) “Real digital forensics: computer security and incident response.”

[13] Wiles, J., Reyes, A., (2011) “The best damn cybercrime and digital forensics book period.”

[14] Farmer, D., Venema, W., (2009) “Forensic discovery.”

[15] Taylor, R.W., Fritsch, E.J., Liederbach, J., (2014) “Digital crime and digital terrorism.”

[16] Lillard, T.V., (2010) “Digital forensics for network, Internet, and cloud computing: A forensic evidence guide for moving targets and data.”

[17] Schweitzer, D., (2003) “Incident response: computer forensics toolkit.”

[18] Shinder, D.L., Tittel, E., (2002) “Scene of the cybercrime: Computer forensics handbook.”

[19] Walden, I., (2007) “Computer crimes and digital investigations.”

[20] Volonino, L., Anzaldua, R., Godwin, J., Kessler, G.C., (2007) “Computer forensics: principles and practices.”

[21] Marcella Jr, A., Menendez, D., (2007) “Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes.”

[22] Sammons, J., (2012) “The basics of digital forensics: the primer for getting started in digital forensics.”

[23] Altheide, C., Carvey, H., (2011) “Digital forensics with open source tools.”

[24] Nelson, B., Phillips, A., Steuart, C., (2014) “Guide to computer forensics and investigations.”

[25] Kruse II, W.G., Heiser, J.G., (2001) “Computer forensics: incident response essentials.”

[26] Dykstra, J., Sherman, A.T., (2011) “Understanding issues in cloud forensics: Two hypothetical case studies.”

[27] Dykstra, J., Sherman, A.T., (2012) “Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques.”

[28] Delmater, R., Hancock, M., (2001) “Data mining explained: a manager's guide to customer-centric business intelligence.”

[29] Carrier, B., (2002). Open Source Digital Forensics Tools: The Legal Argument (PDF). @stake Research Report.

 