ISSUES OF CREDIBILITY IN DIGITAL EVIDENCE*

ปัญหาความน่าเชื่อถือในพยานหลักฐานดิจิทัล

Visitsak Nueangnong
วิศิษศักดิ์ เนืองนอง
Puvadol Damsanit
ภูวดล ดำสนิท
Rambhai Barni Rajabhat University, Thailand
มหาวิทยาลัยราชภัฏรำไพพรรณี
E-mail: not_tyman@hotmail.com

Abstract

Currently, Thailand and other countries worldwide have developed into the digital age, not just for communication. Even the transactions, lifestyle, and work of most people now need electronic devices involved. When making transactions and doing things, it's easier and more convenient, and access to information Collecting and forwarding is much easier and faster. Therefore, it is another channel for criminals to use those channels to commit crimes.

Digital evidence is unique in that it can be easily altered. And that editing can cause damage to various data. Therefore, dealing with digital evidence requires a standardized, universally accepted and reliable process. Digital evidence is unique in that it can be easily altered. And that editing can cause damage to various data. Therefore, dealing with digital evidence requires a standardized, universally accepted and reliable process. In particular, there are technical guidelines for dealing with digital evidence so that digital evidence remains credible and listenable in judicial and judicial processes.

While digital evidence plays a massive role in judicial processes worldwide, it is challenging to build digital evidence's credibility, confidence,

* Received 24 October 2019; Revised 28 November 2019; Accepted 24 December 2019

and security. When it has to be used in a trial or used in the judicial process of the courts, due to technical issues, expert personnel, and methods for dealing with digital evidence. These are essential problems in building trust in digital evidence because technology evolves day by day or second. It inevitably leads to sometimes making the old or previously practised methods unsuitable for what is new. It is challenging to cope with what is known as unpredictability or the inability to plan.

Learning of digital evidence and the processes involved in digital forensics to gain a deeper understanding, including empowering various aspects of the process of dealing with digital forensics. Therefore, it is essential to develop and create a digital evidence-related method to determine the direction and function that ensures credibility and usability in the judicial process.

Keywords: Technology, Digital Evidence, Trial, Judicial Process

บทคัดย่อ

ปัจจุบันประเทศไทยและประเทศอื่น ๆ ทั่วโลกได้พัฒนาเข้าไปสู่ยุคดิจิทัล ไม่ใช่เพียงการติดต่อสื่อสารแต่การทำธุรกรรมต่างๆ การดำเนินชีวิตและการทำงานของคนส่วนใหญ่ต้องมีเครื่องมืออิเล็กทรอนิกส์เข้ามาเกี่ยวข้อง เมื่อการทำธุรกรรมง่ายและสะดวกขึ้น การเข้าถึงข้อมูลต่างๆ ในการเก็บและส่งต่อง่ายและรวดเร็วขึ้น จึงเป็นอีกช่องทางหนึ่งที่ทำให้มิจฉาชีพใช้ในการกระทำความผิด

พยานหลักฐานดิจิทัลมีลักษณะเฉพาะคือสามารถถูกเปลี่ยนแปลงแก้ไขได้ง่าย การแก้ไขอาจทำให้เกิดความเสียหายต่อข้อมูลต่าง ๆ การดำเนินการกับพยานหลักฐานดิจิทัลจึงจำเป็นต้องมีกระบวนการที่ได้มาตรฐานที่เป็นที่ยอมรับและเชื่อถือได้ในระดับสากล โดยเฉพาะอย่างยิ่งแนวปฏิบัติทางด้านเทคนิคต่าง ๆ เพื่อให้พยานหลักฐานดิจิทัลคงไว้ซึ่งความน่าเชื่อถือและสามารถรับฟังได้ในกระบวนการพิจารณาคดี

ปัจจุบันพยานหลักฐานดิจิทัลเข้ามามีบทบาทอย่างมากในกระบวนการยุติธรรมต่างๆ ทั่วโลก แต่ก็ถือเป็นการยากอย่างยิ่งที่จะสร้างความน่าเชื่อถือ มั่นใจ และปลอดภัยแก่

พยานหลักฐานดิจิทัลเหล่านั้นเมื่อจะต้องมีการนำมาใช้ในการพิจารณาคดี หรือใช้ในกระบวนการยุติธรรม เนื่องจากปัญหาทางเทคโนโลยี บุคคลกรที่เชี่ยวชาญ และกระบวนการในการปฏิบัติต่อพยานหลักฐานดิจิทัล สิ่งเหล่านี้ล้วนเป็นสิ่งสำคัญและเป็นปัญหาหลักต่อการสร้างความเชื่อถือในพยานหลักฐานดิจิทัล เพราะเทคโนโลยีได้พัฒนาไปอย่างรวดเร็ว ทำให้วิธีการเดิมๆ หรือที่เคยปฏิบัติมาไม่เหมาะสมกับสิ่งที่เกิดขึ้นใหม่อยู่เสมอ ยากต่อการที่จะรับมือสิ่งเหล่านี้ ซึ่งเรียกได้เลยว่าเป็นสิ่งที่ไม่อาจคาดเดาได้หรือไม่สามารถที่จะวางแผนรับมือล่วงหน้าได้นั่นเอง

การเรียนรู้ถึงพยานหลักฐานดิจิทัลและกระบวนการต่าง ๆ ที่เกี่ยวกับพยานหลักฐานดิจิทัลให้เข้าใจอย่างถ่องแท้ รวมถึงการเสริมศักยภาพด้านต่าง ๆ ของกระบวนการปฏิบัติต่อพยานหลักฐานดิจิทัล จึงเป็นสิ่งสำคัญในการพัฒนาและการสร้างกระบวนการที่เกี่ยวกับพยานหลักฐานดิจิทัลซึ่งจะสามารถกำหนดทิศทางและการทำงานที่ทำให้เกิดความน่าเชื่อถือและสามารถนำมาใช้ในกระบวนการยุติธรรมได้อย่างแท้จริง

คำสำคัญ: พยานเทคโนโลยี, หลักฐานดิจิทัล, การพิจารณาคดี, กระบวนการยุติธรรม

Introduction

It is not only Thailand but all countries around the world that are interested in digital evidence. We cannot deny that our world has wholly entered the digital world and continues to evolve infinitely. Digital evidence, also known as electronic evidence, offers information/data of value to a forensics investigation team. Every piece of data/information present on the digital device is a source of digital evidence. This includes email, text messages, photos, graphic images, documents, files, video clips, audio clips, databases, Internet browsing history, etc.

Digital devices are everywhere in today's world, helping people communicate locally and globally with ease. Most people immediately think of computers, cell phones, and the Internet as the only sources for digital evidence, but any piece of technology that processes information can be used criminally. For example, hand-held games can carry encoded messages

between criminals, and even newer household appliances, such as a refrigerator with a built-in TV, could be used to store, view, and share illegal images. The critical thing to know is that responders

Digital evidence is defined as information and data of value to an investigation that is stored on, received, or transmitted by an electronic device (National Forensic Science Technology Center, 2008). This evidence can be acquired when electronic devices are seized and secured for examination. Digital evidence: Is latent (hidden), like fingerprints or DNA evidence, Crosses jurisdictional borders quickly and easily, Can be altered, damaged, or destroyed with little effort, and Can be time-sensitive.

With the dependence on electronic media and IoT devices, the risks and vulnerabilities associated with digital devices are also high. E.g., cybercriminals can launch a malware campaign by infecting a computer with a virus to further their malicious intent. Here, digital forensics experts' role in identifying and preserving evidence gathered from the digital device during a criminal investigation is paramount.

There are many sources of digital evidence, but for this publication, the topic is divided into three major forensic categories of devices where evidence can be found: Internet-based, stand-alone computers or devices, and mobile devices. These areas tend to have different evidence-gathering processes, tools, and concerns, and different types of crimes tend to lend themselves to one device or the other. The issue of credibility in digital evidence is the most critical issue for the justice system in the digital age. It thus creates various thought processes and proofs to build the credibility of such digital evidence.

What is Digital Evidence?

Digital evidence is best described as the data generated or found on any electronic device such as mobile phones, computers, smart TVs, etc. Every

electronic device combined with IoT technology is a potential source of digital evidence and is crucial to forensic investigations. Forensics experts gather, identify and preserve the evidence from these sources to track the perpetrators of the crime and present them in a court of law. Additionally, pieces of digital evidence help corroborate a timeline of events. A digital forensic examiner must consider a variety of types of evidence (National Forensic Science Technology Center, 2008) as follow.

1. Analogical Evidence can prove helpful in scenarios with limited information or credible evidence to present during the investigation. By drawing comparisons between two similar cases, analogical evidence can lend credibility during a formal argument; however, it cannot be shown in court as proof.

2. Anecdotal Evidence loosely translates to accounts or stories by people to a specific incident or event. However, such testimonies do not hold valid in a court but can be used as supporting theory to grasp better or analyze a situation.

3. Circumstantial Evidence is evidence not drawn from direct observation of a fact in issue. It depends on inferences from a series of attributes to conclude a connection with the crime. This evidence is indirect. For example, when investigators retrieve an audio clip about someone expressing their wish to commit a crime before a crime occurs, some inferences can be drawn from someone's search history on the web related to the crime. But this is not a direct observation of the crime as it is being committed.

4. Character Evidence is considered a testimony that validates a person's actions on a specific depending on that person's character. Character evidence is handy to prove intent, motive, or opportunity.

5. Digital Evidence has multiple sources, including email, text messages, hard drives, social media accounts, audio and video files, smart TVs, etc.

Therefore, digital data sourced from electronic media and Internet devices is an essential link in solving crimes.

Types of Digital Evidence or Proof

In a court of law, evidence is of supreme importance; it is crucial to establish facts. Data or relevant information from electronic devices is pulled from two types of sources. Volatile or non-persistent: Hard disks and removable devices are a few examples of explosive data devices, which means that data is not accessible when unplugged from the computer. Further, data can be deliberately erased or wiped from these devices to destroy evidence. Of course, Volatile also refers to memory that relies on power to store its contents, such as RAM chips. When the power is switched off, the memory contents are lost. Non-volatile, which is persistent: Persistent data is stored permanently in memory, and a loss in power doesn't erase its content. For example, data stored in flash memory, ROM (Read-only memory), CD/ DVD, or tape. (CISOMAG, n.d.)

Forensics investigation is incomplete without digital evidence. Digital data or information stored in electronic devices are associated with e-crime – another word for cybercrime. In the digitalization era, every Internet-enabled electronic device like a smartwatch, smart TV, video game console etc. It can be a crucial component in gathering information to crack a case. Additionally, the five rules of collecting digital evidence that every forensic expert should keep in mind are that digital evidence should be: admissible, authentic, complete, reliable, and believable. Hence, skilled individuals trained in this field need to handle digital evidence.

Challenges of Digital Evidence

Acquiring digital evidence is not free of challenges. Only experts with the appropriate skill set and training are qualified to collect digital evidence. It

is different from gathering physical evidence, and therefore, handling the digital acquisition of data is not free of risks. Data stored in electronic media is volatile and is subject to changes or modifications. For example, a software update can change the data in the phone, or suspects can delete their data from the cloud or use the wipe-clean feature on their phones to remove any evidence. (CISOMAG, n.d.)

Consequently, this can prove tricky for investigators in carrying out the investigation. Besides, examining the massive volumes of data extracted from electronic media or devices is also a tedious task and requires the expertise of a skilled expert. A forensic expert must be updated on the latest technological changes to analyze and document the evidence. With the changes in big data and the latest technology updates, forensic experts need to be skilled in extracting data from multiple sources without modifying them and preserving the basis of evidence for authenticity and integrity.

Objectives of computer forensics

The essential objective of using Computer forensics that helps to recover, analyze, and preserve computer and related materials in such a manner. It enables the investigation agency to present them as evidence in a court of law. It helps to postulate the motive behind the crime and the identity of the main culprit. Designing procedures at a suspected crime scene enables you to ensure that the digital evidence obtained is not corrupted. Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them. It helps you identify the evidence quickly and allows you to estimate the potential impact of the malicious activity on the victim. It produces a computer forensic report which offers complete information on the investigation process. Preserve the evidence by following the chain of custody.

Digital forensics entails the following steps: Identification Preservation Analysis Documentation and Presentation, as follows: Identification, Preservation, Analysis, Documentation, and Presentation.

Identification is the first step in the forensic process. The identification process mainly includes what evidence is present, where it is stored, and how it is stored (in which format). Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

Preservation, in this phase, data is isolated, secured, and preserved. It includes preventing people from using digital devices so that digital evidence is not tampered with.

Analysis, in this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.

Documentation, in this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

Presentation, in this last step, the process of summarization and explanation of conclusions is done. However, it should be written in a layperson's terms using abstracted terminologies, and all abstracted terminologies should reference specific details.

Types of Digital Forensics

There are many types of digital forensics are:

1. Disk Forensics: It deals with extracting data from storage media by searching active, modified, or deleted files.

2. Network Forensics: It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.

3. Wireless Forensics: It is a division of network forensics. The main aim of wireless forensics is to offer the tools needed to collect and analyze the data from wireless network traffic.

4. Database Forensics: It is a branch of digital forensics relating to the study and examination of databases and their related metadata.

5. Malware Forensics: This branch identifies malicious code to study their payload, viruses, worms, etc.

6. Email Forensics: Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.

7. Memory Forensics: It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from the Raw dump.

8. Mobile Phone Forensics: It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

Challenges faced by Digital Forensics

The major challenges faced by the Digital Forensic: (1) The increase of PC's and extensive use of internet access, (2) Easy availability of hacking tools, (3) Lack of physical evidence makes prosecution difficult, (4) A large amount of storage space into Terabytes that makes this investigation job difficult, (5) Any technological changes require an upgrade or changes to solutions.

In recent times, commercial organizations have used digital forensics in the following a type of cases: Intellectual Property theft, Industrial espionage, Employment disputes, Fraud investigations, Inappropriate use of the Internet

and email in the workplace, Forgeries related matters, Bankruptcy investigations, Issues concern with the regulatory compliance.

Advantages of Digital forensics, which have many advantages this Digital forensics. It ensures the integrity of the computer system. It produces evidence in the court, which can lead to the punishment of the culprit. It helps the companies to capture important information if their computer systems or networks are compromised. It efficiently tracks down cybercriminals from anywhere in the world. It helps to protect the organization's money and valuable time. It allows to extract, process, and interpretation the factual evidence, so it proves the cybercriminal action's in the court.

Disadvantages of Digital Forensics that is Digital evidence accepted into court. However, it is must be proved that there is no tampering; producing electronic records and storing them is a highly costly affair. Legal practitioners must have extensive computer knowledge, and it needs to produce authentic and convincing evidence. If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice. Lack of technical knowledge by the investigating officer might not offer the desired result.

The Issues Associated with the Acceptance of Digital Evidence as Scientific Evidence

Several aspects are considered which could conflict with the formal recognition of digital forensics as a sound and scientific discipline. Notably, these issues constitute the most probable reasons for the lack of appropriate standard testing and verification of forensic methods. Eventually, the shortage of empirical validation will adversely affect the acceptance of digital evidence as legally sound and reliable scientific evidence.

1 Standard Data Sets

Scientific research can be performed with or without a standard and with the same data sets. The choice of data sets highly depends upon the nature of the work. Some studies, such as intrusion detection, require access to Malware samples. Likewise, in a facial recognition system, the demand for images of human faces are needed, but for encryption schemes, certain data sets may not be required. Moreover, the same input sources are essential for comparing two different techniques used for a similar purpose, i.e., intrusion detection. Comparable data sets are also necessary to test the proposed improvements in an existing approach. Therefore, researchers must use identical data sets to evaluate and try new techniques or re-implement other methods to assess and check their own (proprietary) data sets. The latter process requires full access to the specifications or requirements for the new technique or proposed recent changes plus the implementation plan or strategy of the person's work. Thus, evaluating the results on identical data sets is the preferred choice, saving considerable time and effort.

2 Establishing Error Rate

In a recent study of 100 random digital forensics lawsuits, 10 of these cases claimed errors in data collection and analysis with only two of these cases reversed. (Cole K. A. et al., 2015) Incorrect output and a wrong timestamp were blamed on the forensic software being at fault. Furthermore, the contamination of evidence during examination was cited. Another 13 cases appealed for miscalculation in sentences and sentence enhancement, and from among these claims, six were proven to be valid in court. In this regard, the State of Florida v. Casey Anthony (2011), the murder trial of a 2-year-old girl, is an example where false forensic evidence was offered. The forensic software used to search for the term "Chloroform" reported that the word was cited 84 times by the primary suspect while it was only once (Eckelberry A. et

al., 2007) mentioned, with the erroneous data, proving to be a severe setback for the prosecution.

3 Standardization Issues

Digital forensics deals with a vast assortment of electronic devices and information formats which are further proprieties of a diverse group of software developers and device manufacturers. Indeed, creating standards, for such a large and varied group of stakeholders, is a challenging task. Also, complicating matters further, the participants are reluctant to agree to certain standards and rules and often resulting in potential conflicts of interest with one another (Bennett D., 2012). The academic community and practitioners have always complained about the shortage of SOPs in digital forensics and have strongly voiced the requirement of having systematic and sound methods for forensic investigations. Still, very few partially productive standards and procedures are available within the domain.

4 Anti-Forensic Techniques & Tools

In general, any attempt or methodology used to modify, upset, refute or restrict a valid scientific forensic investigation is considered as being anti-forensics (AF). AF still does not have any agreed-upon definition (Harris R., 2006), despite several efforts to provide a standard description as presented in. Concealment and evasive behaviors are universal in all criminal disciplines. Sometimes criminals will intentionally perform these behaviors to mislead an analysis or examination, and often merely exist due to common factors. The inability to identify these evasive behaviors during an inquiry will severely compromise the integrity of the extracted evidence. Moreover, AF procedures directly affect the reliability of digital evidence if the trustworthiness of the evidence is successfully challenged in court and creates significant doubt; the evidence would be deemed useless.

Reliability crisis in digital forensics?

In the legal domain, several issues with unreliable forensic evidence are reported and discussed at length. Several reports have concluded that false confessions and inconsistent forensic science evidence are factors in wrongful convictions. Moreover, academics argue about systematic overestimation of the weight of expert evidence (Edmond G., 2016). In most jurisdictions, judges continue to be provided with no accurate guidance on determining evidential reliability, leading to unequal treatment of suspects and defendants. Arguably, the outlined "classical" problems with all forensic sciences in adjudication are deepened in digital forensics given some specifics in digital forensics practice, not typical for other forensic disciplines.

(Doyle S., 2019) conducted extensive research on the quality management of forensic science and its relation to fairness and concluded that the major challenges faced currently in all forensic fields are: the premature use of novel science and technology which lies outside a quality standards framework, lack of standardization and harmonization, lack of resources, and accountability.

Interpol further emphasized these issues as severe challenges in the digital evidence domain and the UK National Digital forensics Strategy. Digital forensics practitioners and academics expressed concerns about the lack of scientific validation in digital forensics. At the same time, the reproducibility crisis in the field was commented on by standardization and governmental bodies worldwide. Several legal scholars called for digital forensics expert accreditation and discussed the absence of clear legal rules for evidence reliability assessment to the disadvantage of suspects and defendants. The rapid scientific advances in computer-assisted forensic science render a lot of existing validation schemas outdated, side-track reproducibility, disturb accuracy testing in digital forensics and the subsequent court evaluation. The lack of

resources to deal with these continues to grow data volumes, complexity, digital evidence dynamics, and data is often used to argue for not implementing quality standards (Horsman G., 2019)

Conclusion

Various agencies have continually studied and developed digital evidence, resulting in learning and understanding the processes of digital evidence. It was developing judicial forms and methods to make digital evidence credible in international standards, also known as reasonable, to gain acceptance in the judicial process. It's not an easy matter, as technology and crime go hand in hand, with patterns evolving and changing over time. It's not just a matter of process and technology, but various parties, whether a skilled operator or a researcher, play an essential role in developing these systems. This is a complex problem to solve and extremely difficult to deal with.

Due to the relentless development of technology, obsolescence happens not only every day but every second that goes forward. In addition, the opinions of various personnel inevitably conflict in different thought processes and development systems. But these can be seen as a challenge for the justice system and academics to find ways and means to make digital evidence the prime evidence in the judicial process.

Therefore, it is interesting to find a way to manage and standardize what is known as a truly international standard for digital evidence. Will it be able to truly achieve the spirit of establishing an international standard of digital evidence? Will it create undisputed credibility and confidence in digital evidence in the judicial process? If it can be done, that will surely answer the plaintiff for the digital world that needs trust and security in various transactions and lifestyles in this era and the future.

Reference

Bennett D. (2012). The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations. Information Security Journal: A Global Perspective, 21(3), 159-168.

CISOMAG. (n.d.). What Is Digital Evidence and Why Is It Important. Retrieved from https://www.firstlegal.com/what-is-digital-forensics-and-why-is-it-important/

Cole K. A. et al. (2015). A review of recent case law related to digital forensics: the current issues. Proceedings of the Conference on Digital Forensics Security and Law, 95-103.

Doyle S. (2019). Quality Management in Forensic Science. California: Academic Press.

Eckelberry A. et al. (2007). Technical review of the trial testimony State of Connecticut vs. Julie Amero. Retrieved from http://dfir.com.br/wp-content/uploads/2014/02/julieamerosummary.pdf

Edmond G. (2016). Legal versus non-legal approaches to forensic science evidence. International Journal of Evidence and Proof, 20(1), 3-28.

Harris R. (2006). Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem. Digital Investigation, 3, 44-49.

Horsman G. (2019). Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework. Digital Investigation, 28, 146–151.

National Forensic Science Technology Center. (2008). A Simplified Guide To Digital Evidence. Retrieved from http://www.forensicsciencesimplified.org/digital/DigitalEvidence.pdf