Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2020, 7(4):160-164**

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Digital Evidence

M. N. O. Sadiku[1], S. R. Nelatury[2], S.M. Musa[1]

[1]College of Engineering, Prairie View A&M University, Prairie View, TX 77446
Email: mnsadiku, smmusa @pvamu.edu
[2]School of Engineering and Engineering Technology, Pennsylvania State University, Erie, PA 16563-1701
Email: srn3@psu.edu

Abstract Digital evidence refers to any reliable information or data generated by digital devices that may be relied on in the court of law. Such evidence is important in investigating computer crimes and other crimes. Digital evidence is usually examined only by those trained specifically for that purpose, i.e. digital evidence experts. This paper provides a brief introduction to digital evidence.

Keywords digital evidence, electronic evidence, IT evidence, computer evidence, digital investigation

Introduction

Digital devices such as computers, Internet, and mobile phones are everywhere in today's world, enabling people communicate with ease. For this reason, we are depending more and more on digital devices. But digital devices are now used in committing crime, and law enforcement now uses digital technology to fight crime through the science of digital evidence forensics. Cyber-crimes are increasingly being committed on the Internet and social media because the digital media allow criminals to remain relatively anonymous. Such crimes include credit card fraud, theft, money laundering, murder, street crime, dissemination of copyrighted materials, and pornographic images. To prosecute these cyber-crimes, relevant, complete, and admissible evidence is required.

Digital evidence (DE) is produced by digital devices or media and takes digital form such as email, digital video, digital photos, digital camera, mobile phone, flash memory sources, compact discs (CDs), digital versatile discs (DVDs), personal digital assistant (PDA), GPS locators, text messages, or word processing documents. Compared with traditional evidence (such as paper-based evidence), digital evidence tends to be more readily available, more mobile, easier to modify or duplicate, easier to tamper with, more difficult to destroy, and can be located in other nations [1]. Whereas paper-based documents can be read by humans unaided by any device, data stored can only be read with the assistance of a computer. Digital evidence is used in different applications such as business disputes, e-government applications, and criminal investigations. The volume of digital evidence continues to grow as the majority of crimes now continue to have a digital component. Figure 1 shows some sources of digital evidence [2].

Acquisition of DE

Traditional tools (fingerprints, DNA analysis, interrogations, etc.) for handling evidence are very robust but insufficient for the new challenges posed by digital technologies. Digital evidence is identified, captured, analyzed, and stored to ensure the integrity, provenance, and traceability of the proof [2]. Acquiring digital evidence involves the following steps [3], [4]:

- **Collection:** This is the initial stage of the investigation and it involves finding the potential traces of evidences from their digital sources such as laptops and smart phones. It is essential to know where information is stored, what format it is, and how to access it. This must deal with the diverse range of devices that contain the information.

- **Preservation:** Once information is collected from the digital devices, it is very important to maintain it and preserve it until the investigation is concluded. Preservation of digital evidence is important for deciding its admissibility and authenticity in the court of law.
- **Analysis:** This involves applying forensic tools and software to analyze the acquired evidences. Different kinds of cases and media may require different methods of analysis (filesystem analysis, memory analysis, network analysis, etc.). Visualization can be used for displaying big amounts of data at once.
- **Reporting:** In this final stage, the examiner is responsible for reporting the findings and results of the analysis. Documentation should be regarded as an ongoing process throughout the examination.

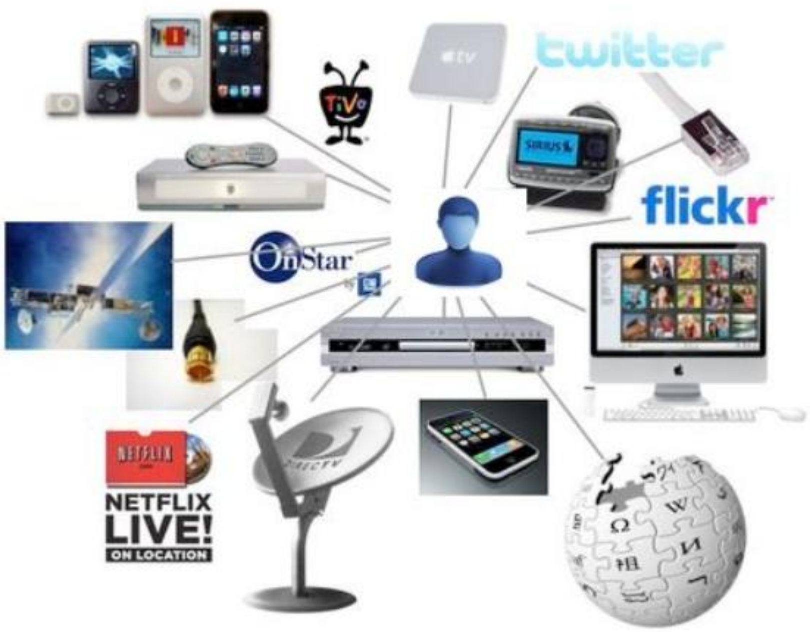

Figure 1: Sources of digital evidence [2]

Digital Evidence Tools

Proper digital forensic tools are required for the effective investigations. Vast data are available for digital evidence for cyber forensics but it is difficult to find out a single process which is compatible with all the digital devices. Considering various digital devices/applications, digital forensics can be divided into five branches [5]and each branch uses specific tools/technologies for recovery of digital evidence. Table-1 shows the various forensic branches and tools for each branch.

Table 1: Digital tools for various forensic branches

Forensic Branch	**Example of Digital Tools**
Computer Forensics	Helix, Winhex, Encase, FTK, CAT DETECT, Timelab Tool, Encase, Zeitline, CFT
Network Forensics	QRadar, Wireshark, E-detective, CapAnalysis, Chkrootkit
Mobile Device Forensics	Encase, PDA Seizure, Pilot-Link, OXYGEN Forensic Kit,
Memory Forensics	Hard Card
Email Forensics	DigLA (Digsby Log Analyzer)

Computer forensic tools are used to collect and analyze digital evidence by checking and extracting files on the system and reading the hard disk. The tools are designed to examine digital evidence of any level and are capable of creating disk images, recovering deleted files. The tools can generate existing and deleted files along with the timestamp, size, hash value, allocated cluster. Example of available tools for these are Helix [5] and Winhex [6] can search specific disk for text, file or the hexadecimal value. CAT Detect tool [7] has ability to find temporal inconsistency in the digital evidence and capable of removing inconsistencies in the time line. Another tool, Cyberforensic Timelab tool [8] also investigates time line issues and logs events orderly. There are other available tools in the market such as the Encase, FTK, Zeitline and CFT deal with time line and create time stamps for various processes [5-8].

Email is a key medium of communication in this time of era and becoming a crucial filed of digital forensic. Lots of information can be reviled through email hacking. Finding the digital evidence of hacking is one key aspect of Email forensic. DigLA (Disby Log Analyzer) is capable of collecting digital evidences for analysis from different location in the system. This identifies traces involved with chats, emails, message, file and folder of the system. This tool can also analyze system-RAM and find the login credentials [9].

For mobile, digital evidence is gathered using commercial tools such as Encase (palm OS, Andrioid) and PDA Seizure (pocket PC, palm OS). Oxygen tool is another one which can be used to extract and analyze data from the hand-sets [10], [11], [12].

Memory forensic is another important forensic branch. The content of the main memory is imaged and analyzed to find the digital evidence. Tools for this memory forensics are categorized in main memory and volatile memory. PTFinder and Forensic toolkit can be used to investigate the contents of the main memory [13], [14]. MAC memory reader can be used to map physical memory to evaluate the data. Belkasoft RAM Capturer [15], WindowsSCOPE [16], OSForensics [17] and Volatility [18] are volatile memory acquisition tools.

In today’s world, everything is connected to network and network forensic is a highly critical branch. Breaching network by various malwares is very common and a critical issue for small to large and non-government to government systems. There are various off-the-shelf products, such as the QRadar [19], Wireshark [20], E-detective [21], CapAnalysis [22], and chkrootkit [23] provide network/packet monitoring, network forensics, auditing and Lawful Interception solutions.

Issues with DE

As with any new concept, there are issues that must be addressed in order to expand the applicability of that concept. DE investigators are hindered by a wide range of independently developed, proprietary and incompatible formats used in storing digital evidence. The lack of standard or generally accepted format is hindering the development of DE. The Common Digital Evidence Storage Format (www.dfrws.org/CDESF) working group is defining an open data format for storing DE [24].

Digital evidence investigations require large volumes of data to be processed. As a result, current forensic tools are being stretched past the limit. Techniques such as data mining can be used to automate the searching process for digital evidence. When examining digital evidence, the digital privacy of witnesses and victims of cyber-crimes should be protected. There are the potential difficulties with prosecutors’ not fully understanding digital evidence, but they are likely to catch up quickly. Judges need to be educated to better understand using digital evidence in the courtroom. Sometimes law enforcement officers need to obtain information from providers located out of state or nation and may need an Internet service provider (ISP) to comply with an extraterritorial search warrant. International cooperation is sometimes required in digital investigations. Some cloud computing systems may store digital data in different jurisdictions and encrypt them before they enter the cloud. Identifying digital evidence in such a cloud computing environment is usually more complex, error-prone, and time consuming [25].

Conclusion

Digital evidence is increasingly being used in legal proceedings due to the increase of IT based systems and IT supported processes. It has emerged as a discipline that plays an ever-increasing role in local, state, and federal courts in the U.S. in both civil and criminal cases. However, only certified professionals can examine digital evidence. They are investigators who have the training and experience to properly examine sensitive or privilege evidence.

Information security personnel are expected to be versed in handling digital evidence. They should be familiar with legal and technical components of DE [26]. The American Society of Crime Laboratory Directors/Laboratory Accreditation Board's (ASCLD/LAB) began to offer accreditation in the Digital Evidence Discipline in 2003. Digital Evidence Discipline consists of four sub-disciplines: Audio Analysis, Computer Forensics, Digital Imaging Analysis, and Video Analysis [27]. More information about digital evidence can be found in the books in [28-30] and a related journal: *Digital Evidence and Electronic Signature Law Review.*

References

[1]. "Wikipedia," 2017. [Online]. Available: https://en.wikipedia.org/wiki/Digital_evidence. [Accessed 08 June 2017].

[2]. "Steps in processing digital evidence," http://www.cjump.com/bcc/t155t/Week02/W02_0030 _steps_in_processing_d.htm

[3]. E. Kalaimannan, "Smart device forensics - acquisition, analysis and interpretation of digital evidences," in Proceedings of International Conference on Computational Science and Computational Intelligence, 2015.

[4]. F. Granja and G. Rafael, "Preservation of digital evidence: application in criminal investigation," in Proceedings of Science and Information Conference, 2015.

[5]. W. Mohammad et al., "Hacktivism trends, digital forensic," in in Proc. IEEE Information & Communication, 2013.

[6]. C. Eoghan, "Tool review—WinHex," Digital Investigation, vol. 1, pp. 114-128, 2004.

[7]. M. Andrew et al., "CAT Detect (computer activity timeline detection): a Tool for Detecting Inconsistency in Computer Activity Timelines," Digital Investigation, vol. 8, pp. S52-S61, 2001.

[8]. O. Jens and M. Boldt, "Computer forensic timeline," Digital Investigation, vol. 6, pp. S78-S87, 2009.

[9]. M. Yasin and M. Abulaish, "DigLA–A Digsby log analysis tool to identify forensic artifacts," Digital Investigation, vol. 9, no. 3, pp. 222-234, 2013.

[10]. J. Wayne and R. Ayers, "An overview and analysis of PDA forensic tools," Digital Investigation, vol. 2, no. 2, pp. 120-132, 2005.

[11]. "Encase," [Online]. Available: https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r. [Accessed 08 06 2017].

[12]. "Oxygen-Forensic," [Online]. Available: https://www.oxygen-forensic.com/en/. [Accessed 08 06 2017].

[13]. I. Hajime, F. Adelstein and R. A. Joyc, "Visualization in testing a volatile memory forensic tool," Digital Investigation, vol. 8, pp. S42-S51, 2011.

[14]. V. Stefan and F. C. Freiling, "A survey of main memory acquisition and analysis techniques for the windows operating," Digital Investigation, vol. 8, no. 1, pp. 3-22, 2011.

[15]. "Belkasoft," [Online]. Available: https://belkasoft.com/ram-capturer. [Accessed 08 June 2017].

[16]. "WindowsScope," [Online]. Available: http://www.windowsscope.com. [Accessed 08 June 2017].

[17]. "OSFrensic," [Online]. Available: http://www.osforensics.com/. [Accessed 08 June 2017].

[18]. "Volatil," [Online]. Available: http://www.volatilityfoundation.org/. [Accessed 08 June 2017].

[19]. "QRadar," [Online]. Available: https://www.ibm.com/us-en/marketplace/ibm-qradar-siem. [Accessed 08 June 2017].

[20]. "WireShark," [Online]. Available: https://www.wireshark.org/. [Accessed 08 June 2017].

[21]. "Edetective," [Online]. Available: http://www.edecision4u.com/.

[22]. "CapAnalysis," [Online]. Available: http://www.capanalysis.net/ca/.

[23]. "CheckRoot," [Online]. Available: http://www.chkrootkit.org/.

[24]. T. C. D. E. S. F. W. Group, "Standardizing digital evidence storage," Communications of the ACM, vol. 49, no. 2, pp. 67-68, 2006.

[25]. M. Taylor et al., "Digital evidence in cloud computing systems," Law & Security Review vol. 26, vol. 26, pp. 304-308, 2010.

[26]. G. Manes and E. Downing, "What security professionals need to know about digital evidence," Information Security Journal: A Global Perspective, vol. 19, no. 3, pp. 124-131, 2010.

[27]. J. Barbara, "Digital evidence accreditation in the corporate and business environment," Digital Investigation, vol. 2, pp. 137-146, 2005.

[28]. E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press; 3rd edition, 2011.

[29]. M. Tunninello et al., Encyclopaedia of Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (4 Volumes). Koros Press Limited, 2015.

[30]. P. Reedy, Strategic Leadership in Digital Evidence. Academic Press, 2020.

About the Authors

Matthew N.O. Sadiku is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interest include computational electromagnetics and computer networks. He is a fellow of IEEE.

Sudarshan R. Nelatury is an associate professor at Penn State University, The Behrend College, Erie, Pennsylvania. His teaching and research interests lie in electromagnetics and signal processing.

Sarhan M. Musa is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Sprint and Boeing Welliver Fellow. His research interests include computer networks and computational electromagnetics.