THE ANNALS OF “DUNĂREA DE JOS” UNIVERSITY OF GALATI
FASCICLE III, 2019, VOL. 42, NO.1, ISSN 2344-4738, ISSN-L 1221-454X
ELECTROTECHNICS, ELECTRONICS, AUTOMATIC CONTROL, INFORMATICS
Article DOI: https://doi.org/10.35219/eeaci.2019.1.05

DIGITAL FORENSICS – A LITERATURE REVIEW

Cătălin Anghel

Faculty of Automation, Computers, Electrical Engineering and Electronics, Department of Computer Science and Information Technology, University "Dunărea de Jos" of Galati – Romania, 2 Științei, 800146 Galati, Romania, e-mail: catalin.anghel@ugal.ro

Abstract: Digital Forensics is a branch of forensic science that is aimed to retrieve, collect and examine the digital evidence of materials found in digital devices, in relation to computer crimes. This paper contains a brief review of the literature aimed to identify the relevant pieces of knowledge in the digital forensics field.

Keywords: digital forensics, digital forensic science, computer forensics, network forensics.

INTRODUCTION

In our days, all digital devices such as cell phones, tablets, laptops and desktop computers can be used for criminal activities such as fraud, drug trafficking, homicide, hacking, forgery, terrorism, etc (Mithileysh. Sathiyanarayanan, 2016). To fight against these criminal activities, digital forensics is used to help investigate cybercrimes and to identify the device-assisted crime and the authors of it (Mithileysh. Sathiyanarayanan, 2016).

There are many definitions of digital forensics but, the one that describe it properly is “*Digital forensics is the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law”* (National Cybersecurity and Communications Integration Center – NCCIC).

PRINCIPLES OF DIGITAL FORENSICS

Digital forensics is a scientific process, a relatively new science, which has to be studied, described and investigate its phenomena continuously due to changes and evolution of the software and hardware.

A flowchart representation of the scientific process is presented in fig.1 (Greg Gogolin, 2013).

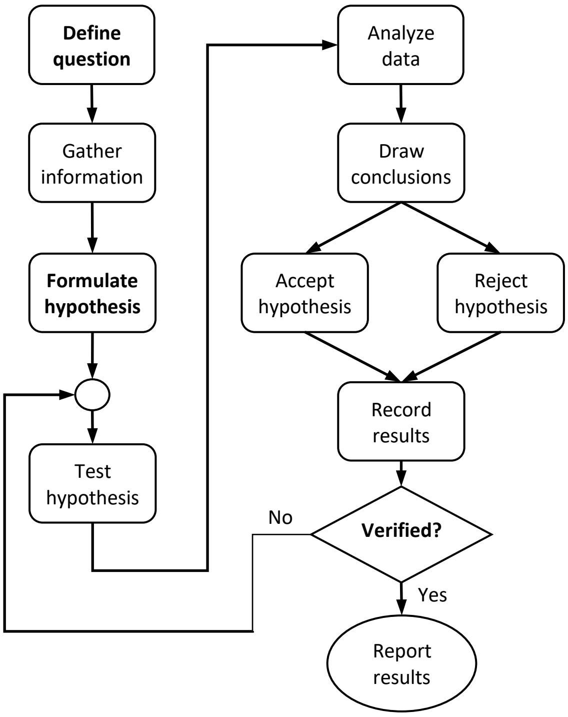

Fig. 1. The scientific process of digital forensics

Digital forensics scientific process has three main stages: define question, formulate hypothesis and verification of results.

The first stage is to exactly define the question or what we are looking for on that device. The second stage is to formulate the hypothesis or what was that device used for. The third stage is verification of results or test the results on a controlled environment (Greg Gogolin, 2013).

CHARACTERISTICS OF DIGITAL FORENSICS

Digital forensics can be divided in five steps: policy and procedure, evidence assessment, evidence acquisition, evidence examination and evidence documenting and reporting (U.S. Department of Justice, https://www.ncjrs.gov), as described below.

Policy and procedure

In order to be efficient undeniable and accurate a forensic unit must have and use good policies and procedures. These procedures must describe step by step instructions that the forensic unit have to do in a digital forensic investigation.

The development process of the procedures must include: problem identification, possible solutions, testing solutions on a control sample, evaluation of the results and procedure validation.

Evidence assessment

Digital evidence should be analyzed from the perspective of the case in order to know how to act and witch actions to make.

The evidence assessment process must include: evidence prioritization, evidence documentation, storage location, packaging and transportation.

Evidence acquisition

Digital evidence is very delicate and can be altered, corrupted, or even destroyed by improper handling or examination.

The evidence acquisition process has to be done in a manner that protects and preserves the evidence and must include following actions:

- Digital evidence has to be secured accordingly to forensic unit policies;
- Crime computer case has to be disassembled in order have access to storage devices;
- Storage devices that need to be acquired have to be identified and documented;
- Hardware configuration has to be documented;
- In order to prevent alteration or damage of data, storage devices must be disconnected
- Configuration information from boot sequence has to be acquired thru a controlled boot.
- Storage devices from suspect's computer have to be removed in order to perform the acquisition.
- Geometry storage devices have to be investigated in order to ensure that all space is accounted, including host-protected data areas.
- Digital evidence has to be acquired using the appropriate software and hardware tools.
- Acquisition has to be verified by doing a sector-by-sector comparison of the original to the copy.

Evidence examination

Digital examination should not be performed on original evidence and consists of extracting and analyzing the data. Extraction is recovery of data from the suspect's media and analysis refers to the interpretation of the recovered data.

There are two different types of extraction, physical and logical. Physical extraction recovers data from the entire physical drive. Logical extraction recovers data based on the installed operating system, file system, and application.

The evidence examination must be conducted by computer forensic specialists and has following steps:

- A working directory on a separate media must be prepared for extraction and/or recovery of evidentiary files and data.

- A physical extraction of the data from the drive must be performed and applied the following methods: keyword searching, file carving, and extraction of the unused space on the physical drive.

- A logical extraction of the data from the drive, based on the file system of the drive, must be performed in order to investigate active files, deleted files, file slack, and unallocated file space.

- Data must be analyzed to determine their significance to the case. The analysis consist in timeframe analysis, data hiding analysis, application and file analysis and ownership and possession analysis.

- The final step in the examination process is to ensure that all results of the extraction and analysis processes are taken into consideration entirely.

Evidence documenting and reporting

Documentation is a continuous process that takes place throughout the entire digital investigation. All actions must be noted and correlated with the resulting evidence.

All results and conclusions must be must written in a report on the understanding of the investigators and prosecutors.

Digital forensics can also be split up into five branches: computer forensics, network forensics, mobile device forensic, memory forensics and email forensics (Kumari, N. et al., 2016).

Computer forensics is the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media (M. G. Noblett, 2010).

Network forensics is "The use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities" (Gary Palmer, 2001).

Mobile device forensics is a branch of digital forensics related to the recovery of digital evidence from mobile devices under forensically sound conditions using accepted methods (Kevin Curran, 2010).

Memory forensics is the examination of volatile data in a computer's memory dump. Volatile data includes the browsing history, clipboard contents, and chat messages present in the short-term memory storage. A memory dump is a capture of data through a random access memory or RAM (The Importance of Memory Forensics Tools, 2017).

Email forensics refers to studying the source and content of electronic mail as evidence, identifying the actual sender and recipient of a message and the date/time it was sent (Natarajan Meghanathan et al., 2009).

TOOLS USED IN DIGITAL FORENSICS

Digital forensics field is dealing with a tremendous amount of data that needs to be acquired, analyzed, interpreted and sorted according to each case of computer crime.

There are many multipurpose tools that helps investigators to acquire, analyze and sort the evidence related to a computer crime.

Software market offer a vast variety of tools which the investigators can use according to their respective fields: disk and data capture tools, file viewers, file analysis tools, registry analysis tools, internet analysis tools, email analysis tools, mobile devices analysis tools, network forensics tools and database forensics tools (Infosec, 2019).

Most popular forensics tools used in digital forensics investigations are presented as follow: (Infosec, 2019).

Digital Forensics Framework

DFF (Digital Forensics Framework) is an open source forensics framework used to investigate hard drives and volatile memory and create reports about users and system activities. DFF interface automatically guides the user through the main steps of a digital investigation to quickly and easily conduct a digital investigation and perform incident response. (https://github.com/arxsys/dff).

Open Computer Forensics Architecture

OCFA (Open Computer Forensics Architecture) is an open source computer forensics framework, built by the Dutch National Police Agency, for automating digital forensics process, created on Linux platform with postgreSQL database for storing data. (http://sourceforge.net/projects/ocfa/).

Computer Aided Investigative Environment

CAIN (Computer Aided Investigative Environment) is an Italian GNU/Linux live distribution that offers a complete forensic environment. CAIN has a user-friendly graphical interface and is created to integrate existing software tools as software modules. (http://www.caine-live.net/).

X-Ways Forensics

X-Ways Forensics is an advanced work environment for computer forensics investigations, is fully portable and runs off a USB stick on any given Windows system without installation. Some of the features of X-Ways Forensics are: disk cloning and imaging, automatic identification of lost/deleted partitions, access to logical memory of running processes, hard disk cleansing to produce forensically sterile media, gathering slack space, free space, inter-partition space, and generic text from drives and images. (http://www.x-ways.net/forensics/).

EnCase Forensic

EnCase is another popular multi-purpose forensic platform with many tools for several areas of the digital forensic process, used by many law enforcement agencies around the world (Garber Lee, 2001). EnCase can quickly search, identify, and prioritize potential evidence, in computers and mobile devices, to determine whether further investigation is warranted. (https://www.guidancesoftware.com/encase-forensic)

XRY

XRY is a mobile forensics tool used to analyze and recover crucial information from mobile devices. XRY has a hardware device that connects mobile phones to PC and the software performs the analysis of the device and extract data.

(https://www.msab.com/products/xry/).

HELIX3

HELIX3 is a live CD-based digital forensic suite created to be used in incident response. It comes with many open source digital forensics tools including hex editors, data carving and password cracking tools. HELIX3 can collect data from physical memory, network connections, user accounts, executing processes and services, scheduled jobs, windows registry, chat logs, screen captures, SAM files, applications, drivers, environment variables and internet history. (http://www.e-fense.com/h3-enterprise.php).

CONCLUSION

This paper, is a literature review of digital forensics science. Digital forensics is a rapidly changing field that has many challenges for investigators. These challenges become more and more complex because criminals also learn to hide evidences or have advanced computers knowledge.

Digital forensics processes involved in the cybercrime investigation have to be done in a manner that is accepted in a court of law and also digital evidence has to be presented in a form accepted in court of law.

Digital forensics is a multi-disciplinary and inter-disciplinary field encompassing diverse disciplines such as criminology, law, ethics, computer engineering, and information and communication technology (ICT), computer science, and forensic science, as shown in fig.2 (M.N.O. Sadiku et al., 2017).

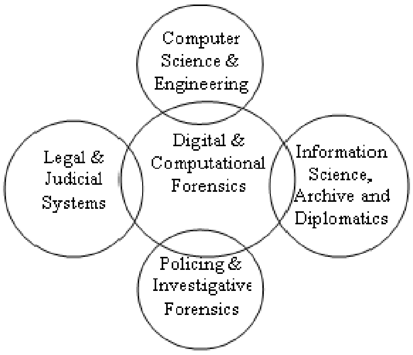
Computer Science & Engineering
Legal & Judicial Systems
Digital & Computational Forensics
Information Science, Archive and Diplomatics
Policing & Investigative Forensics

Fig. 2 Multiple domains of digital forensics (M. Lasavio et al., 2016)

REFERENCES

Computer Forensics US-CERT. https://www.us-cert.gov/security-publications/computer-forensics, National Cybersecurity and Communications Integration Center – NCCIC, US.

Greg Gogolin, Digital Forensics Explained, 2013, by Taylor & Francis Group, LLC.

U.S. Department of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, https://www.ncjrs.gov/.

Nikita Rana1, Gunjan Sansanwal, Kiran Khatter1, Sukhdev Singh, Taxonomy of Digital Forensics: Investigation Tools and Challenges, 2017, https://arxiv.org.

Mithileysh Sathiyanarayanan, Introduction to Digital Forensics, 2016.

N. Kumari and A. K. Mohapatra, An insight into digital forensics branches and tools, Proceedings of the International Conference on Computational Techniques in Information and Communication Technologies, 2016.

Gary Palmer, A Road Map for Digital Forensic Research, Report from DFRWS 2001, First Digital Forensic Research Workshop, Utica, New York, August 7 – 8, 2001, Page(s) 27–30.

Michael G. Noblett, Mark M. Pollitt, Lawrence A. Presley. Recovering and examining computer forensic evidence, 2010.

Curran K., Robinson A., Peacocke S., Cassidy S., Mobile Phone Forensic Analysis, International Journal of Digital Crime and Forensics, Vol. 2, No. 2, 2010.

The Importance of Memory Forensics Tools, https://lifars.com/2017/06/memory-forensics-tools/, 2017.

Natarajan Meghanathan, Sumanth Reddy Allam and Loretta A. Moore, International Journal of Network Security & Its Applications (IJNSA), Vol .1, No.1, 2009.

Infosec, https://resources.infosecinstitute.com/computer-forensics-tools/, 2019.

Garber Lee, Encase: A case study in computer forensic technology, IEEE Computer Magazine, 2001.

Matthew N. O. Sadiku, Mahamadou Tembely, Sarhan M. Musa, Digital Forensics, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 4, 2017.

M. Losavio, K. C. Seigfried-Spellar, J. J. Sloan III, Why digital forensics is not a profession and how it can become one, Criminal Justice Studies, vol. 29, no. 2, pp.143-162, 2016.