International Journal of Advances in Image Processing Techniques
Volume 3 : Issue 2 *[ISSN 2372-3998]*
Publication Date : 31 August, 2016

Software and Hardware Tools used in Digital Forensic Data Analysis

Erhan AKBAL, Şengül DOĞAN

Abstract*—Crimes committed though information technology increase day by day. The resources subject to cybercrime is varies. Investigation requests from the forensic authorities are collected specific groups. In this context, data analysis, voice analysis and image analysis processes is the basis of the forensic investigation. For better research and investigation, investigator uses many forensics hardware and software tools. The use of these tools to perform an accurate analysis is very important. These computer forensics software tools can also be classified into open source and with licensed. Software tools according to used Operating System, hardware tools according to the mobile and not mobile can be classified. This study represents digital forensic analyses software and hardware tools. Also tools are examined according to using purpose. *(Abstract)

Keywords*—digital forensic, data analysis, forensic tools. *(key words)

I. Introduction

Digital forensics include collecting data on digital resources, making evidence and reporting processes. Digital forensics experts use so many software and hardware devices. So many different data can be presented on digital devices. There can be so many file types, such as sound, video, image, document and text etc. Different specialty information is required to make examination on different file types. Experts must use various software and hardware devices to reveal crime factor at the end of examination [1,2]. In order that examination results as an evidence are succeeded, intended results are required to be gotten that digital resources from legal authorities are analyzed with examination devices. The type of resource that will be examined and data types in, determine how to examination process. In general, the hardware that will be examined are divided into mobile and non-mobile. Especially hardware devices that will be used in the examination vary by mobile and non-mobile devices. In order to analyze mobile devices, hardware devices that are specific to the device are used. Software devices that will be used in the examination are divided into open source software and closed source software. Examination centers and experts try to reach to the result by using all the devices that can reveal the evidence. Using correct software makes the evidence examine correctly.

Erhan AKBAL
University of Firat, Department of Digital Forensics Engineering
Turkey
erhanakbal@gmail.com

Şengül DOĞAN
University of Firat, Department of Digital Forensics Engineering
Turkey
senguldgn@gmail.com

II. Digital Forensics Analysis

Primary aim of digital forensics examinations is to transfer correct results to legal authorities by defining, analyzing, providing data integrity of the obtained digital evidence related to crime and correct reporting [1]. With the examination of digital evidences, the results which are computer attacks, unauthorized use, pornography, suspected computer detection, correspondences containing crime element and voice records and keeping illegal data can be revealed. The content varies by the file types, which has crime concept. Legal digital forensics generally contain three basic stages [2]. The structure of legal examination process is shown in Figure 1.

These are 1. Evidence Acquisition, 2. Analysis, 3. Reporting and presentation processes [1]. Examination tools are also required in all the stated processes.

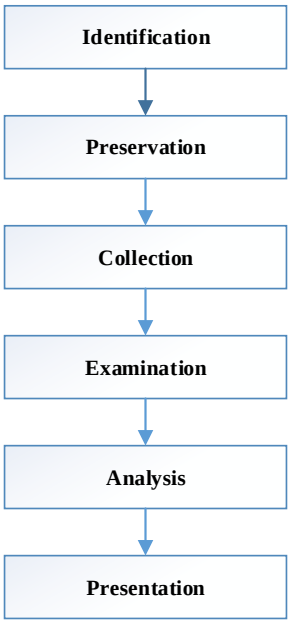

Figure 1. Digital Investigation Process [2]

A. *Evidence Acquisition Process*

It includes obtaining the digital sources that will be analyzed with a correct method from crime scene. Taking its image and own digital source related to crime from crime scene correctly according to legal procedures is directly related to next stages. Hardware tools vary by mobile or non-mobile type of digital source. In this stage, hardware tools are required to be used.

B. Analysis Process

It is the level which digital sources obtained from crime scene are examined and searched for evidence. Examination of evidences are done according to demand from legal authority.

Examination of what information, time intervals, and file types related to crime element are different from the demand [3]. In addition, examination processes vary by manipulation, contradiction and validity related to the evidence. In the analysis stage, software and hardware tools should be used together. Analysis process consists of basic three stages. These are pre-analysis, analyiss and last analysis.

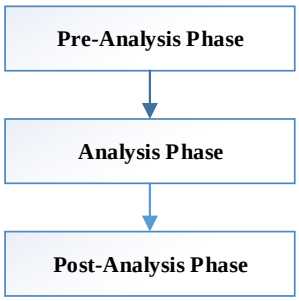

Figure 2. Common Proces Model for Analaysis [2]

C. Reports and Presentations

This is the level that creating the results obtained from analysis stage to be presented in relevant authorities. Those legal authorities analyze the results and decide criminal sentence in accordance with the result is directly related to correct reporting.

III. Software Tools

The tools used in collecting data are used to make take the data in examination area and crime scene from digital sources in accordance with legal processes [3,4]. The tools that are used, are mostly used to take the copy evidence. The tools that are used must protect accuracy and integrity of the evidence. For this purpose, there are so many software tools used. When categorizing tools, they are divided as Windows, Linux, Mac-based and open source. There are basic characteristics that a legal digital forensics must have in below. [5].

- They should present a proper platform
- They should be in a form which can control data flow efficiently
- They should make digital evidence use in legal authorities by making identity authentication
- The tool should be in a form that can increase examination experts who will work in this area and their performances

A. Windows Based Tools

Most common tools used in digital forensics examinations work as Windows-based. Examination experts mostly use Windows-based tools [5,6]. In this part, Windows-based software tools most common used are presented.

MobilEdit is a software with license fee to control mobile phones produced by Compelson Laboratories [7]. With basic operations, it can be used to take data on phones and make a search on. Information like phone book, call history, notes and calendar can be analyzed. In addition, it can make information of IMEI and operating system, deleted information take and decipher PIN code and phone passwords.

Accessdata FTK Imager is a software used by so many experts in digital forensics examinations [8]. It is used to make copies of digital data in different formats. By showing an internal disc on the obtained evidence copies on operating system, it enables to make analyses on it.

Forensic Imager is a copying software used for taking legal copies of digital evidences developed by Guidance Company [9].

Encase Forensics is a digital forensics software produced by Guidance Software, which is most known and used. Software; can make so many analysis operations from taking shadow copy and keeping functions to searching word and data recovery in basic meaning in basic level in hard drive [10]. Encase Software is a shareware. Models like CD/DVD Examination, Writing-Protecting can be obtained for e fee.

Forensic Tool Kit mFTK Imager is a software produced by AccessData company [11]. Main purpose of the software is to image data collecting department and take a shadow copy. The efficiency of software in data recovery usually depends on the deleted time of data. The other characteristic of the software is to produce MD5 or SHA hash values of accessible Medias. In real terms, producing MD5 hash values is done to give guaranty of protecting original data integrity.

X-Ways Forensics is a licensed software used in digital forensics data examinations. It provides disc cloning, taking image, and finding deleted files [12]. It has a structure to operate on USB flash drive without installing X-ways software. Oracle data base installation is not needed. It takes a few seconds to make software useable.

Recovery My Files is a strong recovery software that enables the recovery of accidently or deliberately deleted files on your computer [13].

Internet Evidence Finder is a software with license fee produced by Magnet forensics company [14]. Personal computers are used in the process of examinations of smart phones and tablets by experts. With its different models, it presents the characteristics like examining internet TV series, analysis of traces obtained from mobile applications. It is used on Windows and MacOs operating systems.

Virtual Forensic Computing is a software with license fee produced by GetData company [15]. It is one of the software which experts have used to obtain data from digital evidences in recent years. It makes discs analyze safely by making images obtained from evidences boot and proving physical write protect.

Oxygen Forensic Suite is a software with license fee produced by Oxygen Forensic company [16]. It is the software that can make analytics of cell phones.

Forensic Explorer is a software with license fee produced by GetData company [17]. It has very fast ability

of making analysis. In addition, it makes the imaged obtained via application operate on storage and remain hash values of evidence unchanged.

Nuix Forensic Investigation Tools is a software developed by Nuix Company [18].

- It makes a fast review on data with large scale
- It supports so many file formats
- It can make relationship analysis between data.

ProDiscover: is a trade software developed by Pathways Company. It can use image format that can be created by itself [19]. It is quite successful on VMware systems.

Other: Blackthorn GPS Forensics, BringBack, Belkasoft Evidence Center, CD/DVD Inspector, Email Detective - Forensic Software Tool, Facebook Forensic Toolkit, HBGary Responder Professional, ILook Investigator, Mercury Indexer, OnlineDFS, OSForensics, Safeback, Proof Finder software tools are used in analysis stages but not commonly.

B. *Linux Based Tools*

LINRES is software tool designed to make studies on Linux systems and that can make examination by using minimum systems requirements prepared according to digital forensics standards [20].

- Temporary and permanent information on the system
- It is to obtain by using static-reviewed binary files without intervening all Meta data on the system.

SMART is a software tool that allows so many scenarios to use [21]. It makes

- remote image of system that will be examined or examine directly on it
- analysis of functionless systems, transform different evidence files and make tests.

Second Look Linux Memory Forensics tool can so many Linux-based operations [22].

- It can make analysis of different Linux types command line or user interface
- It can analyze Raw, slm, lime, vmware, virtual box, Libvirt storage images
- It is a significant software tool that can be used for storage analysis.

C. *Macintosh Based Tools*

BlackBag Mac Forensic Software tool are developed for Macintosh-based computers [23].

- Fast and correct data recovery
- To make multiple assignments at the same time
- To make examination by protecting all the characteristics of the original tool
- They have advanced reporting interfaces
- To make fast researches-target specific without searching irrelevant files and filtering files
- It uses SQL data base.

Recon for MAC OS X tool has characteristics, which are to make examination on live tool, make automatically table from Messages and Skype, form report files in different formats, and remove data from system temporary storage. Developed Timeline analysis [24].

IV. Hardware Tools

Hardware tools used in collecting evidence process are used to bring evidence from crime scene to analysis department or taking evidences from crime scene. In general, protection tools against write, media copier, secure deleting data tools, adapters, transporting tools and collecting data systems are used.

Taking Image Hardware: are done on their shadow copies not to any difference on the origin of all the examinations and analyses done in digital forensics. In the stage of shadow copy, in addition to software, private software is needed. Shadow copy means to take all the data on the evidence. There is various hardware used for this purpose in literature. These consist of;

- Tableau TD1 ve TD2
- CRU-Wiebetech Ditto
- DiskClon,
- Atola Insight
- Forensic RTX

etc. tools.

Protection Tools against Writing: Taking copy is required to connect the evidences used in legal review with write-protected. Hardware tools used for this purpose consist of;

- Forensic UltraDock,
- Forensic Notebook DriveDock,
- USB DriveDock,
- USB WriteBlocker,
- Media WriteBlocker

etc. tools.

Hardware Transporting Tools: are the tools used in the process of bringing legal evidences from crime scene to examination department. They are used to prevent electronic evidences from environmental effects. They are used to protect evidence from electromagnetic waves and against environmental signals. Transport tools, which are used commonly, consist of;

- 2.5,3.5 inc Disc Transporting BoxDisk,
- Faraday Bag,
- PhoneShield

Other: Signal and Power Cables, Accessories, charge cables, Adapter kits are also hardware tools used in digital forensic processes.

v. Conclusion

In this study, software and hardware tools used in digital forensics examinations have been shown. It has been dwelt on what tools need to be used in examination processes that will be made digital forensics. In addition to software tools that have different characteristics, various hardware that provide validity and acceptance of evidence by legal authorities are used. The hardware shown in the study have a great significance to use in obtaining evidences. Otherwise, the validness of the evidence might be lost.

All the software tool used have different characteristics. Examination of evidence must be provided by using different software in the examination stage. Thus, the validity of the analysis results related to the evidence and its acceptability can be increased.

References

[1] ENFSI, "Best Practice Manual for the Forensic Examination of Digital Technology," ENFSI-BPM-FIT-01,2015.

[2] Ritu Agarwal and Suvarna Kothari, "Review of Digital Forensic Investigation Frameworks", Lecture Notes in Electrical Engineering, 2015, pp:561-571.

[3] Nilakshi Jain and Dr.Dhananjay R Kalbande ,Digital Forensic Framework using Feedback and Case History Keeper ,International Conference on Communication ,Information & Computing Technology (ICCICT) 2015, pp 1-6.

[4] Nilakshi Jain and Dhananjay R Kalbande, Computer Forensic Tool using History and Feedback, International Conference on Infocom Technologies and Optimization (ICRITO),2015, pp.1-5.

[5] Dhwaniket Ramesh Kamble, Nilakshi Jain, Swati Deshpande, "Cybercrimes Solutions using Digital Forensic Tools," I.J. Wireless and Microwave Technologies, 2015, pp. 11–18.

[6] Vamshee Krishna Devendran, Hossain Shahriar, Victor Clincy, "A Comparative Study of Email Forensic Tools" , Journal of Information Security , 2015, vol. 6, pp:11-117.

[7] Compelsan Mobiledit Software. [Online]. Available: http://www.mobiledit.com/forensic, Accessed: January 2016.

[8] AccessData Forensic Toolkit, http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk, Accessed: January 2016.

[9] Guidance Software Forensic Imager. [Online]. Available: https://www2.guidancesoftware.com/products/Pages/, Accessed: December 2015.

[10] Guidance Software Encase search technology validated. [Online]. Available:https://www.guidancesoftware.com/products/Pages/encaseforensic/ overview.aspx?cmpid=nav , Accessed: January 2016

[11] AccessData FTK. [Online]. Available: http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk, Accessed: November 2015.

[12] X-Ways Forensic. [Online]. Available:http://www.x-ways.net/forensics/, Accessed: January 2016.

[13] GetData Recovery My Files. [Online]. Available: http://www.recovermyfiles.com/nist.php, Accessed: January 2016.

[14] Magnet Forensic IEF. [Online]. Available: https://www.magnetforensics.com/magnet-ief/, Accessed:January 2016.

[15] GetData Virtual Forensic Computing. [Online]. Available: http://www.virtualforensiccomputing.com/, Accessed: January 2016.

[16] Oxygen Forensics. [Online]. Available:http://www.oxygen-forensic.com/, Accessed: December 2015.

[17] Forensic Explorer. [Online].Available:http://www.forensicexplorer.com/, Accessed: January 2016.

[18] Nuix Forensic Investigation Kit. [Online].Available:http://www.nuix.com/investigation, Accessed: January 2016.

[19] ARC Prodiscover Forensic Edition. [Online]. Available:http://www.arcgroupny.com/products/prodiscover-forensic-edition/, Accessed: January 2016.

[20] Network Intelligence LINRES. [Online]. Available:http://www.niiconsulting.com/innovation/linres.html, Accessed: January 2016.

[21] ASRData Smart. [Online].Available: http://www.asrdata.com/forensic-software/smart-linux/, Accessed: January 2016.

[22] Second Look, Linux Memory Forensic. [Online].Available: http://secondlookforensics.com/, Accessed: January 2016.

[23] BlackBag Forensic Software. [Online].Available: https://www.blackbagtech.com/software-products.html, January 2016.

[24] Sumuri Forensics, Recon. [Online]. Available: https://www.sumuri.com/products/recon/, Accessed: January 2016.

About Author (s):

Erhan Akbal is currently working as an assistant professor at Digital Forensics Engineering Department of Firat University, He received his Ph. D. degree in electrical and electronics engineering in 2012, M.S. degree in computer engineering in 2007, from Firat University, Turkey. His research interests include computer network security, wireless sensor network, intrusion detection and digital forensics

Sengul DOGAN received her Ph.D degree in Electrical and Electronic Engineering from the University of Firat, Elazig, Turkey, in 2011. She is currently an Assistant Professor in the Digital Forensics Engineering Department of Firat University. Her research interests cover Data Hiding, Information Security, Image Processing and Optimization Techniques