Marek PILSKI[1]
ORCID: 0000-0003-2362-0416

[1] Siedlce University of Natural Sciences and Humanities
Faculty of Exact and Natural Sciences
Institute of Computer Science
ul. 3 Maja 54, 08-110 Siedlce, Poland

Methods to acquisition digital evidence for computer forensics

DOI: 10.34739/si.2022.26.05

Abstract. Computer forensics is a key science and competency in meeting the growing risks of cybercrime, as well as for criminal investigation generally. In order to provide irrefutable evidence of a potential crime, a specialist in the incident response team (e.g. an IT forensics specialist) must secure the digital evidence in accordance with the correct procedure. There are no strict guidelines on how to do this. It is known that the authenticity and fidelity of data must be preserved. This article will collect good practices developed by specialists in the field of computer forensics. The process of securing the evidence material from a digital data sources for later analysis will be presented.

Keywords. Securing evidence material, acquisition, digital evidence, computer forensics

1. Introduction

When working on a computer, users leave behind, consciously or less consciously, a lot of traces of their activities. These traces can then be used to analyze their activities and determine with a high degree of probability what they were doing on the computer at any given time [10]. Some of these users (thankfully a small number) have bad intentions. However, their actions are very dangerous and costly to the victim. The author works as an academic teacher. Among

other things, he teaches students of computer forensics. Based on practical experience and acquired knowledge, he collected and presented in this article good practices.

1.1. Computer forensics

The process of computer forensics, in the simplest case, can be broken down into three categories of activity: acquisition, analysis, and presentation [3].

Acquisition refers to the collection of digital media to be examined. Depending on the type of examination, these can be physical hard drives, CD disks, DVD disks, SD cards, mobile phones, chips from embedded devices, or any files. The acquisition process should consist of creating a duplicate of the original media (binary copy) and documenting all activities performed on the original medium [2].

Analysis refers to the proper analysis of the contents of binary media copies obtained in the first phase of the process and includes the identification, analysis and interpretation of data.

Presentation is the process by which an investigator shares the results of data analysis with other parties involved in an investigation. The presentation phase includes the preparation of a report describing the activities undertaken by the analyst, a list of acquired artifacts and their significance and connections. The report should be prepared in accordance with the legal system of a given country.

At the first Digital Forensics Research Workshop (DFRWS) in 2001, the term **computer forensics** was **defined as** follows: Digital Forensic: "*The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations*" [9].

Computer forensics is often described as a field of knowledge bordering on science and art. In [7] the authors argue that in certain situations, the computer forensics specialist conducting the investigation is a sort of digital archaeologist, and sometimes even digital geologist: "*Digital archaeology is about the direct effects from user activity, such as file contents, file access time stamps, information from deleted files, and network flow logs. ... Digital geology is about autonomous processes that users have no direct control over, such as the allocation and recycling of disk blocks, file ID numbers, memory pages or process ID numbers*".

In this article, the focus will be on the acquisition phase.

1.2. Adverse events and incidents

The Computer Security Resource Center (CSRC) at the US National Institute of Standards and Technology (NIST) defines events and incidents in a special publication 800-61 [12]. "*An **event** is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt".* In contrast, events unwanted by organizations are defined as *"**Adverse events** are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data".* It is worth noting that the document defines adverse events related to computer security and not caused by natural disasters, power failures, etc. This publication also defines the concept of an incident. "*A **computer security incident** is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices*." Such adverse events related to security incidents are usually associated with potentially high costs.

1.3. Cost of cybercrime

A cost of cybercrime can cover a very wide spectrum of areas. This cost may include expenses related to: detection, investigation, recovery and incident response management, costs that are related to post-fact activities and efforts to reduce disruption to operations, restore systems operation, etc.

In October 2013 the Ponemon Institute published for the first time the results of research on the costs incurred by various organizations due to cybercrime. The results were appalling the, average annual cost of cybersecurity was $7.2 dollar. Two years later, in 2017, Ponemon Institute published a second report in which these costs were at the level of 17 million [4]. The results presented in the report concerned only 2647 cases from 355 companies, from 11 countries, including Australia, France, Germany, Italy, Japan, Great Britain and the United States. The next report from 2019 shows a cost of $13 million [5]. The current report in 2021 has not been published yet, work is probably still underway. Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015 [6]. This represents the greatest transfer of economic wealth in history. However, the cost to the affected organization is not enough, because the damage that criminals will do using stolen information is very difficult to quantify and can only be determined over time or may never be discovered.

2. Principles and good practices related to the protection of digital evidence material

One of the features necessary to obtain the features and required when securing the material is the authenticity and fidelity of the data. Authenticity ensures that the origin of the material is absolutely indisputable. On the other hand, fidelity (or identity) guarantees the possibility of determining whether a given evidence material has not been changed intentionally or by mistake during subsequent activities of data analysis in terms of, for example, a committed crime. In order to maintain the authenticity and fidelity of the evidence, the following rules should be adhered to. A secure digital medium should be kept in its frozen state where it was found by a member of the incident response (IR) team. All activities along with time performed by an IR member should be described in detail in a protocol. The evidence material should be properly and unequivocally marked [1], sealed and described in the protocol. Create a binary copy (so-called clone), created on an equal basis with the original.

The process of creating a binary copy should be performed with the use of available software or hardware techniques, which make it impossible to make any changes to the data on the original data carrier. So-called blockers are used for this, which work with the original medium in read-only mode. Calculate the check sum MD5, SHA1, SHA2 or CRC32 [3] [13] of the carrier, which will uniquely enable the authentication of the material. Evidence analysis should be performed only and exclusively in a binary copy, it will protect the specialist against e.g. unintentional data change.

Such an operation on a binary copy makes it possible to perform multiple analyzes on the same evidence material. When securing the evidence, it is worth remembering to preventing bystanders from destroying traces and evidence. For this purpose, it is necessary to isolate the computers and prevent access to the computers by persons in the searched room. Before securing electronic evidence, a fingerprint examination should be performed on the discovered computer and network equipment. If it is necessary for procedural reasons, examine the keyboard, mouse and remove fingerprints. This will allow the identification of at least the last physical user.

3. Securing a hard drive from a desktop computer – case study

The task is to secure the evidence in the form of computer hardware. As a member of the incident response team (e.g. IT forensics specialist), you take part in securing a desktop computer located in a workroom. The task is to secure the data carrier in accordance with good

practices [8] so that the evidence cannot be rejected during legal action. Suppose the computer is turned off.

Step 1. If the computer is turned off - do not turn it on, because it will overwrite data in the system and on the disk. Turning on the computer will change the information stored in it and exclude it as evidence in the case.

Step 2. Do not touch the device.

Step 3. Make a photo documentation. Take a picture of the computer. Take a picture of the surroundings, connected devices, input sockets, labels. Take a picture of connections to other devices. Describe in the protocol how the individual parts of the computer station are connected with each other.

Step 4. Label the individual ports and the cables that are connected to them in order to reconnect the cables after performing the steps. Label all wires and connections.

Step 5. If printing is in progress, do not turn off the printer until printing is complete.

Step 6. In order to reduce the potential of electric charges before securing your computer, you must discharge the electric charge from your body.

Step 7. To avoid accidentally starting the computer, disconnect the power plug from the back of the computer case, not from a wall socket or power strip. Disconnecting the cable from the computer case rather than from the wall socket (you can unplug the wrong device) ensures that the computer is not receiving power.

Step 8. Pull out any other cables for external devices connected to the computer.

Step 9. If the computer is connected to a modem or telephone line, note the telephone number and disconnection time.

Step 10. Remove the external devices connected to the USB sockets, such as an external disk.

Step 11. Seal each drive's openings with a special tape.

Step 12. Make sure that all elements have been written down in the notebook and that the appropriate labels [1] and descriptions have been attached.

Step 13. Remove the hard drive from the computer.

Step 14. Take pictures of the hard drive labels in order to capture data such as: serial number, type, capacity, firmware, brand, etc. (see Fig. 1) and the interface, because sometimes a jumper on the pins is set (see Fig. 2).

Figure 1. A hard drive label (serial number, type of drive, model, capacity, brand, etc.). Own study. Photo taken with the POCO X3 Pro**.**

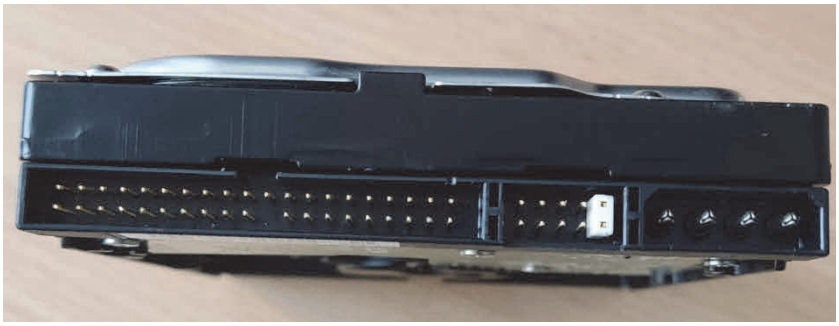

Figure 2. A hard drive interface with a jumper on pins. Own study. Photo taken with the POCO X3 Pro.

Step 15. Format the target hard disk on which the binary copy will be ripped.

Step 16. Connect the blocker (software or hardware) to the tested source disk with the write-protect technology, guaranteeing data integrity.

Step 17. Make a binary (bit-by-bit) copy of the source disk for later analysis onto a blank target disk. An example of this task will be presented in the section 3.1.

Step 18. Calculate a checksum (hash) of copies – authentication, which is a digital signature of copied data, guaranteeing their fidelity necessary in the evidentiary proceedings. An example of this task will be presented in the section 3.2.

Step 19. Secure and pack the hard disk with the binary copy (destination) in an anti-static bag (see Fig. 3) and protective box.

Figure 3. An antistatic bag. Own study. Photo taken with the POCO X3 Pro.

Step 20. Seal the antistatic bags and attach permanently the object labels, containing the device numbers, types, individual features and other data. Impress the company seal in the sealing wax on the labels. Place antistatic bags in protective boxes to prevent physical damage.

Step 21. Store packed disks away from magnets, any radio transmitters at room temperature and proper air humidity.

Step 22. Search the computer's surroundings to find notebooks, cards, notes, records, documentation which may contain, for example, access passwords.

Step 23. Perform complete documentation, protocol describing all performed steps.

Step 24. Require the user to show the license for the programs.

Step 25. Require the user to provide all parameters for access to programs in the form of any accounts, passwords, identifiers, etc.

3.1. Acquisition process - making a binary copy of a digital data carrier

This section will show you how to create a special DEFT Zero Live version on a USB drive using the LinuxLive USB Creator tool. Next, the commands for mounting external media in safe mode (read-only), data protection by creating bit copies of data (dd commands) and alternative tools with GUI DEFT Zero will be discussed.

The following open-source software will be used for this use case:

- **DEFT Zero Linux Live** (Digital Evidence & Forensic Toolkit) [14] is a specialized Linux distribution from Italy designed to analyze the contents of a computer in terms of forensic research (computer forensics and penetration tests). The system is built on a light Lubuntu distribution and is available for 64 bit machines in the form of a hybrid ISO DVD/USB image. It is an easy-to-use system that includes excellent hardware discovery and one of the best open source incident response and computer forensics applications.
- **dd** is a Unix program with command line interface for low-level copying and converting raw data. dd is used to copy a specified number of bytes or blocks of data, with the optional conversion of the copied data. dd can operate on partitions or entire disks, and is often used in digital evidence gathering where it is necessary to read the disk bit by bit. You can use tools with a GIU, such as GuyMager, which use the dd command.
- **LinuxLive USB Creator** [11] is a simple tool that allows the user to create bootable versions of Linux that can be run directly from a USB drive, such as a USB flash drive.

The minimum hardware and software resources are:

- USB memory stick with a capacity of at least 1 GB,
- ISO image of DEFT Zero Linux (deftZ-2017-1.iso),
- Linux Live USB Creator application, most conveniently in a portable version.

Next, you need to create a bootable USB predive with DEFT Zero Linux Live. The easiest way to use the portable version of Linux Live USB Creator. All you need to do is unpack the zip archive of the application to the location of your choice, enter the application directory and run the file called LiLi USB Creator.exe. Then connect the USB flash drive on which the DEFT Zero system will be installed to the computer and go through all the wizard's steps presented in the Linux Live USB Creator application window. The bootable USB drive process is as follows:

Step 1. Choose the USB flash drive.
- From the drop-down list, select the drive that corresponds to the USB drive on which Linux will be installed.

Step 2. Choose the source file.
- Press the "ISO / IMG / ZIP" button and select the location of the DEFT Zero image file (deftZ-2017-1.iso).
- The Linux Live USB Creator application will validate the system to be installed. You may find that this Linux distribution is not on the compatibility list. However, decide to follow the process of creating this system and go to the next step.

Step 3. Persistence.
- Here you should see "Live Mode" - select it.

Step 4. Options.
- Select all three options: (i) hide created files, (ii) format the USB drive to FAT32, (iii) activate LinuxLive booting on Windows.

Step 5. Create.
- If all lights are green, press the lightning bolt symbol to start the system build process.
- While the Linux Live USB Creator application is running, the progress status will be displayed.

Boot the target computer with Deft Zero. For this purpose, it may be necessary, for example, to change the drive order settings in the computer's BIOS in the BOOT section, or to activate a special boot menu by pressing the F12 button on a keyboard. This task must be performed when the computer starts up. Next, insert the USB stick with DEFT Zero into the USB socket of the computer. Restart the computer. When the computer turns on, press the F12 button and select the option to boot from the USB drive. DEFT Zero starts up on the computer.

After starting the DEFT system, you can work in the graphic mode. Now make a bit copy of the secured hard disk. The most convenient way is to insert a secured hard drive into a portable case (let's call it PSHDisk). Everything is ready, now a bit copy of PSHDisk will be created:

Step 1. Mount your computer's internal hard drive in write mode, as this will be the destination for the bit copy. You can use the File Manager PCManFM application for this purpose.

Step 2. Connect the PSHDisk to the computer via the USB port as a bit of copy source. Mount it in safe (read-only) mode in order not to interfere with the data stored there.

Step 3. Launch Guymager in order to create a PSHDisk bit copy.
- In the list of devices, locate and select the USB device (PSHDisk) for which you will perform the image. In this case it will be "*/dev/sdc*" (you can also use the disk size if you know it).
- From the device context menu, select the Acquire image option.
- In the "Acquire Image of */dev/sdc*" window set:
  - in the File format section, check the option: Linux dd raw image;
  - in the Destination section, set the location where you will save the image, i.e. in the Image directory field, select e.g. */media/root/your_hard_disk/images/copy*;
  - give a name to the file (bit copy), e.g. *pskdisk_image*;
  - press the Start button;

– in the Guymager window, you can watch the progress of the process.

Step 4. In the File Manager PCManFM application, locate the file that was created (pskdisk_image).

3.2. Hash calculation

The hash of a block of data (e.g. a file) is a sequence of alphanumeric characters of fixed length calculated by a mathematical function. This mathematical function is mono-directional. It is impossible to reconstruct the block that has originated a hash sum. Any alteration of the data, albeit minimal, will result in a completely different hash. With Linux systems you can use one of the following applications to generate a hash sum: md5sum, sha1sum, md5, sha1, sha256 deep, dhash. For our case, let's choose the command **md5sum**. md5sum is a Unix program used to compute and verify hash functions with the MD5 algorithm. The checksum is a cryptographic algorithm that acts as a hash, generating from a data string of any length a 128-bit (in the case of MD5). The command syntax is as follows:

md5sum [options] file_name.

The MD5 sum calculation for the *pskdisk_image* file looks like this. Launch a terminal and execute the command:

md5sum /media/root/your_hard_disk/copies/pskdisk_image

Checksum calculation may take a while.

4. Summary

The way of acquisition of digital forensic evidence is very important. The evidence in this area is volatile and delicate. It should be noted that due to improper handling, the investigation may be disrupted. In other words, acquisition, storage, transmission, and the preservation of evidence require precise procedures. This article presents good practices and tips on how to do it properly. Sample software and how to use them are also indicated.

Beginners in this field ask: what investigative tools are taken into account by the court? The answer to this question is that any tool that works strictly according to certain rules, can be tested and reviewed, is generally accepted in the specialist community, and returns reproducible results with a known margin of error, can be approved. All the tools covered in this article have their own strengths and weaknesses. They are definitely simple, repeatable, and effective. So individual circumstances will be the biggest factor in deciding will you use them. Finally, this

is by no means an exhaustive list of imaging tools fit for the process described in this article. It is worth developing the ability to use other new tools, which are many on the market.

References

1. Appendix B - Incident Response Forms - Incident Response and Computer Forensics, 3rd Edition. Form 1 – Evidence Tag. Web site: https://ir3e.com/appendix-b/ [date of access: 01.03.2022]

2. Nikkel B.: Practical Forensic Imaging. Securing Digital Evidence with Linux Tools. No Starch Press, September 2016, 320 pp.

3. Altheide C., Harlan Carvey: Digital Forensics with Open Source Tools. Elsevier, 2011

4. Cost Of Cyber Crime Study. Ponemon Institute, 2017. https://www.accenture.com/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf [date of access: 01.03.2022]

5. Cost Of Cyber Crime Study. Ponemon Institute, 2019. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf [date of access: 01.03.2022]

6. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cyber Crime Magazine. Web site: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ [date of access: 01.03.2022]

7. Farmer D., Venema W.: Forensic Discovery. Chapter 1. The spirit of forensic Discovery. Web site: http://www.porcupine.org/forensics/forensic-discovery/chapter1.html [date of access: 01.03.2022]

8. Ekspert informatyki śledczej – Mediarecovery Web site: https://mediarecovery.pl/ekspert-informatyki-sledczej/ [date of access: 01.03.2022]

9. Group work: A Road Map for Digital Forensic Research. Procedings: The Digital Forensic Research Conference DFRWS 2001, Utica, New York, USA, August 7-8, 2001, 44 pp.

10. Mandia K., Pepe M., Jason T. Luttgens: Incident Response and Computer Forensics, Third Edition. McGraw-Hill Professional Publishing, 2014

11. LinuxLive USB Creator. Web site: https://www.linuxliveusb.com/ [date of access: 01.03.2022]

12. Cichonski P., Millar T., Grance T., Scarfone K.: Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. Special Publication 800-61 Revision 2, National Institute of Standards and Technology, August 2012

13. Kumar S., Gupta E. P.: A Comparative Analysis of SHA and MD5 Algorithm. International Journal of Information Technology and Computer Science 5(3), pp. 4492 - 4495, June 2014.

14. Fratepietro S., Rossetti A., Dal Checco P.: Deft 7 manual. Digital Evidence & Forensic Toolkit. https://paper.bobylive.com/System/EN-deft7.pdf [date of access: 01.03.2022]