DIGITAL FORENSIC INVESTIGATION, COLLECTION AND PRESERVATION OF DIGITAL EVIDENCE

Vahidin Đaltur , Kemal Hajdarević,

Internacional Burch University, Faculty of Information Technlogy
71000 Sarajevo, Bosnia and Herzegovina
Vahidin.dzaltur@gmail.com

ABSTRACT

With computers, and other electronic devices being involved in an increasing number, and type, of crimes the electronic trace left on electronic media can be a vital part of the legal process. To ensure acceptance by courts, accepted processes and procedures need to be acquired and demonstrated which are not dissimilar to the issues surrounding traditional forensic investigations. Forensic technology makes it possible to: identify privacy issues; establish a chain of custody for provenance; employ write protection for capture and transfer; and detect forgery or manipulation. It can extract and mine relevant metadata and content; enable efficient indexing and searching by curators; and facilitate audit control and granular access privileges. In recent years, digital forensics has emerged as an essential source of tools and approaches for facilitating digital preservation and curation, specifically for protecting and investigating evidence from the past. Institutional repositories and professionals with responsibilities for personal archives can benefit from forensics in addressing digital authenticity, accountability and accessibility. Digital personal information must be handled with due sensitivity and security respecting available standards while demonstrably protecting its evidential value. A digital forensic investigation is a special case of a digital investigation where the procedures and techniques that are used will allow the results to be entered into a court of law. Computer forensics is a new and fast growing field that involves carefully collecting and examining electronic evidence that not only assesses the damage to a computer as a result of an electronic attack, but also to recover lost information from such systems to prosecute criminals. With the growing importance of computer security today and the seriousness of cyber-crime, it is important for computer professionals to understand the technology used in computer forensics.

Keywords: Computer forensics, image acquisition, digital preservation, data recovery

1. What Is Computer Forensics?

Computer forensics is the practice of collecting, analyzing and reporting on digital information in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. Computer forensics follows a similar process to other forensic disciplines, and faces similar issues. Purpose is to give answer to questions of a legal system related to computers. Any sort of legal issue, trial, some sort of civil court cases or any other legal processing that has computer involved.

"Computer forensics usually refers to the forensic examination of computer components and their contents such as hard drives, compact disks, and printers." (Eoghan Casey, 2011).

2. Preparing for an investigation

Before we start with forensic investigation, we want to be sure that we understand the scope of investigation. In order to understand what pieces of evidence we are looking for, what elements are in play, what will move case forward in order to understand the truth what happened? In understanding the scope of investigation we will get what evidence do we need to acquire and what evidence do we have authority to acquire. There are cases where we may find information that we don't actually have authority to acquire and obtain. After we determined scope of investigation, we must understand the type of investigation we are going to conduct.

- Live acquisition
  - Do we need what's in memory?
  - Do we need network state?

- Static acquisition
  - Files
  - Programs

The type of investigation is important so it has to be determined do we need that system up and running in order to do live acquisition, or we just need hard drive or other storage device in order to do static acquisition. Next step is to provide evidence storage in places, to store disk drives, USB stick, and any type of memory card or a PC. We must have a place where we can store them securely, with limited access or no access to other person at all. Also, we need place to store digital artifacts where we can store image files of evidence that can't be tampered with. Along with those lines we need to be sure how documentation will be look like. We must have a chain of evidence and evidence verification data (hash values). Ultimately we need to be able to control and document everything that was happening with evidence from the point that we required to the point that we handled off or presented testimony for the evidence.

3. Forensic Workstation

If we are doing a lot of a forensic investigation or forensic examination, we definitely want to have dedicated forensic work station. First we have to build a hardware configuration, chose different types of interfaces, USB, FireWire, SCSI and so on. Other decision we have to make is what operating system we are going to run on that working station. One of the choices is to run a "LIVE CD", because in this way we actually storing anything in primary hard drive, nothing is writable at that regard and we are not making any changes.

"Primary these live CD-s are mostly Linux based and there are several available for forensic workstation usage" (Christopher L.T. Brown, 2009).

One of the advantage for using Linux or UNIX like operating systems are number of tools that are built in. Also we have a lot of forensic programs that run only on a Windows. Some of the best free digital forensic investigation tools are:

- **ProDiscover Basic** is, indeed, a professional tool for consultants, system administrators and investigators, giving them the information required to build strong legal cases.
- **The Sleuth Kit** (+Autopsy), are open source digital investigation tools (a.k.a. digital forensic tools) that run on Windows, Linux, OS X, and other Unix systems. They can be used to analyze disk images and perform in-depth analysis of file systems (such as NTFS, FAT, HFS+, Ext3, and UFS) and several volume system types.
- **FTK Imager**, is a simple but concise tool. It saves an image of a hard disk in one file or in segments that may be later on reconstructed. It calculates MD5 hash values and confirms the integrity of the data before closing the files. The result is an image file(s) that can be saved in several formats including, DD raw.
- **DEFT (Linux LIVE CD)**, (acronym for Digital Evidence & Forensics Toolkit) is a distribution made for Computer Forensics, with the purpose of running live on systems without tampering or corrupting devices (hard disks, pen drives, etc…) connected to the PC where the boot process takes place.
- **CAIN**, Is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kinds of passwords by sniffing network, cracking encrypted passwords using dictionary, brute-force and cryptanalysis attack, recording VoIP conversation, decoding scrambled password, recovering wireless network keys.

4. Image Acquisition

Image format is the way that data from a hard drive or hard drive partitions is stored in the way they can be analyzed later on. There is a several way to acquire a disk image. Also, they are a couple a different ways to store that disk image once we are acquired a data so that they can be used without that actually having to use a hard drive. One of really important ways of storing that is advanced forensic format (AFF). It is able not only to store data from a hard drive, but also it can store some forensic Meta data along with them. AFF format is supported from most of the primary forensic tools like Sleuth Kit and FTK. Another image format used in Linux based OS is a RAW image. It's a bit for bit copy whether it is a hard drive or a particular partition, exactly the way it was on that physical media, but it's stored in the file.

"When collecting the bit-stream image to file, the investigator will essentially access the data through this method; stream the data sector by sector from the evidence media into a file or group of files residing elsewhere." (Christopher L.T. Brown, 2009).

4.1 Image Acquisition Under Linux

Under Linux, we have advantage of built in tools that will allows as to do image capture. Name of the tool which is most often in use is dd, and it's comes with majority of Linux distributions available today. It can be used for various digital forensic tasks such as:

- Creating a raw image file (a bit for bit) from drive or partition

  the basic syntax is:

  dd if=/dev/sdb1 of=/home/vahidin/newimage.dd bs=512 conv=noerror, sync

  where if = input file (in our case drive)

  of = output files

  bs = block size

  conv = conversion options

- Forensically wiping a drive or partition (zero out a drive)

  the basic syntax is:

  dd if=/dev/zero of=/dev/sdb1 bs=1024tem

  where if = input file

  of = output files

  bs = block size

We can find a modified version of dd such as dcfldd or dc3dd, with additional features that were added specifically for digital forensic acquisition tasks. The dd is a very powerful tool that can have devastating effects if not used with care. It is recommended that you experiment in a safe environment before using this tool in the real world.

4.2 Image Acquisition Under Windows

One of the most popular Windows imaging tools is "FTK Imager (Forensic Tool Kits)". FTK Imager is a data preview and imaging tool that allows as to examine files and folders on local hard drives, USB sticks, network drives, CDs/DVDs, or any other media card and review the content of forensic images or memory dumps. Using FTK Imager we can also create SHA1 or MD5 hashes of files, export files and folders from forensic images to disk, review and recover files that were deleted from the Recycle Bin (providing that their data blocks haven't been overwritten), and mount a forensic image to view its contents in Windows Explorer.

4.3 Volatile Information

As we are doing an investigation, sometimes we have use different systems which have to be up and running and is actively in use. Volatile system information's is capturing particular information from this system before its shutdown, because when its shutdown the system's all information will vanish or disappear. One type of volatile information is logon session where we can find information about user and services used at any given point of time. One of the commonly used software is named ProDiscover.

"Using ProDiscover's expanded live memory imaging and processed volatile data extraction, investigators can learn more about the target system's interaction within the running environment and find passwords and memory-only resident malware" (Harlan Carvey, 2012).

Another interesting thing is processes that are running at any given time on a system. This information is usually retained in memory while the system is operating and tends to disappear when the system is shut down. Volatile information generally consists of:

System time, Logged on user(s), Process information, Network connections, Network status, Clipboard contents, Command history, Service/driver information.

5. Data Recovery

Data recovery is the process of restoring data that has been lost, corrupted or made inaccessible for any reason or accidentally deleted.

"In general, when a file is deleted, the data it contained actually remain on a disk for a time and can be recovered" (Fred Cohen, 2009).

There are several reasons for data recovery; it's possible that has been a deliberate attempt's to destroy a hard drive or partitions, or at least a data on them. We can find very handful tools available for different platforms in order to recover the data. Depending on the file system, we know that each operating system treats differently deleted files. For example:

- Windows FAT, marks file directory as unused and destroy allocation information.
- Windows NTFS, marks file entry as unused, then it deletes record from directory and mark a disk space as unused.
- Linux file system destroys a file descriptor and sets a disk as free. (File location info, file size, type of the file etc.)

This mean that *data will remain* there *until* the operating system reuses the space for new *data.*

5.1 Tools for Data Recovery

Whether we want to recover a deleted files and folders or to recover data from damaged media our chances to save those data at safe location are depending at circumstances in which way they are missing. In order to achieve this, we will use one of available data recovery software, but we must pay attention from which file system, are we trying to recover the data.

Let as introduce some of them:

- **VirtualLab Data Recovery**, besides supporting the NTFS, FAT and FAT-32, file systems, it supports Mac HFS / HFS+ and even NFS. In addition, it supports data recovery on devices such as memory card or USB drives. It has ability to make sector-by-sector copy of a failing drive.
- **EaseUS Data Recovery Wizard**, have a three recovery modules
    - Complete Recovery, used to recover data from formatted hard drive, corrupted or displayed as a RAW
    - Deleted File Recovery, used when your data are deleted and emptied from Recycle Bin.
    - Partition Recovery, used to recover data from hard drive when the partition is deleted, invisible or lost.
- **Stellar Pheonix**, recover data from Windows PC hard drive, memory card and USB sticks. Hi can restore archive, databases, documents and different type of multimedia files.

Beside these, we can find a several other programs with better or almost the same functions, depends on whether they are licensed or free of charge.

6. Conclusion

As is the case with all evidence, it's very important to maintain a chain of custody for computer evidence. Each person who handled evidence may be required to testify that the evidence presented in court is the same as when it was processed during the investigation. Although it may not be necessary to produce at trial every individual who handled the evidence, it is best to keep the number to a minimum and maintain documentation to demonstrate that digital evidence has not been altered since it was collected. **Forensic investigators** must do everything possible to preserve the integrity of the digital evidence. Any mistakes in the process call the evidence into question and rendering it worthless. The way we handle integrity issues are numerous and include the way we seize, label, transport copy, analyze and finally present the results at court trials.

REFERENCES

[1] Christopher L.T. Brown, (2009). *Computer Evidence, Second Edition: Collection & Preservation.*

[2] Eoghan Casey, (2011). *Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computer and Internet.*

[3] Harlan Carvey**,** (2012). Windows Forensic Analysis Toolkit, Third Edition: Advanced Analysis Techniques for Windows 7.

[4] Fred Cohen**,** (2009). *Digital Forensic Evidence Examination.*

[5] John Sammons, (2012). *The Basic of Digital Forensics, The primer For Getting Started in Digital Forensics.*

[6] Michael G. Solomon, K Rudolph, Ed Tittel and Neil Broom, (2011). Computer Forensics JumpStart **,** *Second Edition.*

[7] LIVE CD - BackTrack Linux - Penetration Testing Distribution. (2012). Retrieved Jan 27, 2014, from http://www.backtrack-linux.org/

[8] Sleuth Kit – Open Source Digital Investigation Tools. (2014). Retrived Feb 15, 2014 from http://www.sleuthkit.org/

[9] FTK – Forensic Toolkit 5. (2014). Retrived Feb 23, 2014 from http://www.accessdata.com/products/digital-forensics/ftk