Evaluation of Digital Forensics Tools on Data Recovery and Analysis

Ioannis Lazaridis, Theodoros Arampatzis, Sotirios Pouros
AMC Metropolitan College
14th El. Venizelou Str., 54624, Thessaloniki, Greece
jnlazaridis@gmail.com

ABSTRACT

This paper presents a comparison and evaluation of several digital forensics tools on data recovery scenarios. Modern tools have been tested and evaluated in order to provide evidence regarding their capabilities in qualitative analysis and recovery of deleted data from various file systems. Results derived from the comparisons, present the capability of each digital forensics tool. Based on variables and specifications, the tool with the best performance is considered the most suitable application for analysing and retrieving files. A comparison between digital forensics tools takes place as well, alongside conclusions.

KEYWORDS

Forensic analysis, Data Recovery, Encase, Autopsy, FTK imager, DFF, OSForensics, Recuva

1 INTRODUCTION

Digital forensics is the science which deals with the discovery, validation and interpretation of digital evidence found in electronic devices, often in accordance to a computer crime. The main goal is to recover and preserve digital evidences to its original form, since it might be used to support a legal case. [1-8]. There is a significant variety of digital evidence sources, including personal computers, servers, laptops, hard drives, flash drives, smartphones and networks. In most cases the digital evidence is a common file or it is stored in a file such as:

- Image/Video/Audio Files
- System/Server/Network Log Files
- Emails
- Browser History/Cache
- Document Files such as .doc/.txt/.xml/.pdf

Hard drives are likely to include an Operating System (or more than one), application programs and user data stored in files. Hard drives also provide additional storage for system information used by the processor if necessary (backing store) [9-15].

The hierarchy of files is divided in six levels:

- Level 0 (Regular Files): The information contained in the file system. It includes the file names, file attributes and file content. Can be accessed directly.
- Level 1 (Temporary Files): Temporary files, including printed files (print spooler), the cache of the browser and files in the Recycle Bin. Many users believe that the system will automatically delete this data or even worst, they don’t even know they exist.
- Level 2 (Deleted Files): When a file is deleted from the file system, most operating systems do not replace the blocks on the hard drive that the file is written - they simply remove the record reference from the containing directory. The blocks of the “erased” file are tagged as free for registration.

- Level 3 (Retained data blocks): Level 3 data include information of the virtual memory, slack space, backing store and level 2 data which are partially replaced and cannot be fully recovered.
- Level 4 (Vendor Hidden blocks): This layer consists of blocks of data that can be accessed only by using specific instructions provided by the manufacturer (Vendor). This level includes the control unit programs and data used for the block management.
- Level 5 (Overwritten data): It is believed by many experts that there is a possibility, data can be retrieved from a hard drive, even after the replacement (overwriting) of the blocks in which they were registered. Level 5 is reserved for such data [16].

Tools, techniques and methodologies for forensic investigation, collection and analysis of evidence are used worldwide. Besides recovering the evidences, it is important to maintain their integrity, throughout the investigation [17]. The modern digital forensic analysis tools are used to retrieve information and evidences from a hard disk. Thus, analysts can process hard drives regardless the operating system and file system, but also they can be sure that the integrity is maintained since tools analyse a virtual copy of the hard disk (disk image).

2 METHODOLOGY

The purpose of this paper is to provide practical results from data recovery scenarios, experimenting on different file systems and hard drive technologies, using several modern digital forensics tools. The tools are compared based on the number of deleted files detected and the percentage of their usability. Files such as photographs and videos that have been partially recovered, (e.g. miss some pixels), are considered a successful attempt, since those files can still be used as acceptable digital evidences. Continuing, the same tactic is used in specific experimental files (.zip .doc .jpeg .txt .avi) which have been written and deleted from from the digital devices.

2.1 Tools and evidences

The digital forensics tools that used were free, except Encase forensic software which was provided from AMC Metropolitan College as a part of the research. Specifically, the selected tools were Encase 7, Autopsy 3.1.2, OSForensics 2.2, FTK Imager 3.1.1.8 and Digital Forensics Framework (DFF). Finally, on that list of tools another one was added, (Recuva) which is not considered a digital forensic tool, but it can be used to recover deleted files.

- Windows 8.1 (NTFS) 640GB SATA III
- Windows 8.1 (NTFS) 128 GB SSD SATA III
- Kali Linux (ext4) 80GB SATA II Partition of 320GB
- Flash Drive (FAT32) 8GB

The list above includes all the discs that have been tested. Initially, it was necessary to ensure the integrity of the evidences. FTK Imager was used to create the E01 image files for each disc [20]. Recuva was used, from a third party laptop, since it doesn’t support image analysis.

It should be noted that FTK Imager and DFF are not included in the first three scenarios for each image. That is because they don’t include an image analysis feature which makes it impossible to calculate the total number of deleted/recovered files.

3 RESULTS

It should be mentioned that the research doesn’t give a general assessment of each tool and all its features, but it compares the tools based on their capabilities in analysing and recovering of deleted files.

3.1 Windows 8.1 (NTFS) 640 GB

Table 1. Number of deleted files detected and recovered by each tool.

Encase	Autopsy	OSForensics	Recuva
281.924	27.953	9.354	19.046

The results in Table 1 indicate Encase's superiority compared to the other tools. Autopsy coming in the second place with almost 90% less detected files from Encase. Recuva comes in the third place with 19.046 files, with OSForensics coming last. The number of deleted files found by Recuva exceeds the number of OSForensics, which is offered as a digital forensics tool rather than as a simple file recovery tool.

Table 2. Percentage of file usability after restoration.

Encase	Autopsy	OSForensics	Recuva
60%	70%	60%	20%

While observing the results of Table 2 we understand that a large percentage of files identified by the Recuva is useless.

Table 3. Time required for disk analysis.

Encase	Autopsy	OSForensics	Recuva
7:38:00	3:12:00	0:00:50	0:00:07

Table 3 presents process time, which obviously differs between tools. Encase required more than 7 hours and Autopsy approximaterly 3 hours.

All of the tools were able to find an retrieve the experimental files, except Recuva which found four out of five. One of the retrieved files was useless in OSForensics, DFF and Recuva.

3.2 Windows 8.1 (NTFS) SSD 128 GB

Table 4. Number of deleted files detected and recovered by each tool.

Encase	Autopsy	OSForensics	Recuva
502.373	100.303	51.507	62.295

Table 4 illustrates that Encase managed to detect five times more files compared to Autopsy. The results are more or less same as the previous measurements (HDD), but the number of detected files for all the tools has been multiplied.

Table 5. Percentage of file usability after restoration.

Encase	Autopsy	OSForensics	Recuva
60%	70%	60%	20%

The percentage of the restored files usability, from the SSD image, is impresive, as shown in Table 5.

Table 6. Time required for disk analysis.

Encase	Autopsy	OSForensics	Recuva
5:22:34	1:18:00	0:00:45	0:00:17

Table 6 indicates the process time needed for each tool to analyse the evidence. The process time differs, especially with Encase and Autopsy, from the previous results (Table 3).

All tools, but Recuva, were able to locate and succesfully recover the experimental files.

From the results on the SSD image is clear that the number of deleted files found is almost double compared to HDD's results. It should be stated that TRIM was enabled on the SSD, before the E01 image was taken.

3.3 Linux Ubuntu Image E01 (ext4) 80GB

Table 7. Number of deleted files detected and recovered by each tool.

Encase	Autopsy	OSForensics
537.898	62.012	77

Regarding the Linux image, once again it is noticeable that Encase comes first with more than 500.000 files, followed by Autopsy which detected 62.000, while OSForensics managed to detect only 77 files. The results are presented in Table 7.

Table 8. Percentage of file usability after restoration.

Encase	Autopsy	OSForensics
15%	20%	16%

In Table 8 it can be noticed that most of the files detected were useless, they had been partially replaced, since most of them were system files which have been altered from several distribution updates.

Table 9. Time required for disk analysis.

Encase	Autopsy	OSForensics
3:52:00	3:08:00	0:00:57

Table 9 indicates that Autopsy required the same process time to analyse an 80GB ext image with a 640GB NTFS image.

Encase, Autopsy and FTK Imager were able to detect and recover all five experimental files. DFF detected three and recovered successfully two, while OSForensics recovered only one.

Recuva was excluded from these measurements, since it doesn’t support any ext file systems.

3.4 USB Stick (FAT32) 8GB

Table 10. Number of deleted files detected and recovered by each tool.

Encase	Autopsy	OSForensics	Recuva
12.757	7.817	3.156	12

Table 10 illustrates that Encase was able to detect the most files, unlike Recuva which identified only 12.

Table 11. Percentage of file usability after restoration.

Encase	Autopsy	OSForensics	Recuva
55%	66%	60%	10%

From these initial results in Table 11, we may tell that the usability of the restored files was great since all of the tools were able to restore successfully at least 50% of the files, except Recuva which partially restored only one.

Table 12. Time required for disk analysis.

Encase	Autopsy	OSForensics	Recuva
0:36:00	0:22:00	0:00:54	0:00:11

It must be noted that the tools were not able to recover the image (jpeg), except Recuva which even failed to detect it.

Table 13. Number of deleted files detected and recovered by each tool.

Encase	Autopsy	OSForensics	Recuva
436	23	14	14

Results after formatting and installing Kali Linux into the USB are impressive. Table 13 presents that Encase managed to detect only 436 files from 12.700. Autopsy detected only 23 (from 7817), while OSForensics and Recuva recovered only 14.

Table 14. Percentage of file usability after restoration.

Encase	Autopsy	OSForensics	Recuva
15%	20%	16%	8%

Table 14 depicts that the usability of the detected files has been plummeted, since all of the tools could only partially recover files.

Table 15. Time required for disk analysis.

Encase	Autopsy	OSForensics	Recuva
0:24:00	0:09:00	0:00:25	0:00:09

As it is illustrated in Table 15 the time required for the image analysis, was slightly less, compared to the previous results in the USB image (Table 12).

None of the tools was able to detect or recover any of the experimental files.

4 FUTURE WORK

The next step would be to acquire product licenses from companies such as Paraben, AccessData, Belkasoft, TechPathways and X-ways, which would allow the implementation of high-level comparison scenarios based on the high end digital forensics tools. The tools could also be evaluated based on the system resources required such as CPU and RAM consumption.

5 CONCLUSIONS

Analysing the results for each image the conclusion derived is that among tools that have been compared, Encase, followed by Autopsy, can be considered the most appropriate and reliable tool for data recovering in a professional level [19]. It should be borne in mind that all tools failed to recover the prerequisite number of digital evidences in the USB stick, since they are operating in the second level (Deleted Files) of the hierarchy of evidences, as mentioned in introduction [18]. It can be concluded, from the USB stick results, where all disk blocks have replaced their content, that it is impossible to properly recover files. It should be noted that there are different methods/tools which can be used in order to (partially) recover overwritten data.

6 REFERENCES

[1] A Yasinsac, R. E., 2003. Computer forensics education . From: s.l.:IEEE, pp. 15-23.

[2] ACPO, 2012. Good Practice Guide for Computer-Based Electronic Evidence, s.l.: ACPO.

[3] Akhgar, B., 2014. Cyber Crime and Cyber Terrorism Investigator's Handbook. s.l.: Syngress.

[4] Arpaci-Dusseau, R. H. A. C., 2014. File System Implementation.

[5] Bhanu Prakash Battula, B. K. R. R. S. P. T. S., n.d. Techniques in Computer Forensics: A Recovery Perspective. s.l.:s.n.

[6] Brenner, S. W., 2010. Cybercrime: Criminal Threats from Cyberspace.

[7] Buse, J. W., 2013. linux.org. Available at: http://www.linux.org/threads/ext-file-system.4365/[Accessed on 10 04 2016].

[8] Casey, E., 2009. Handbook of Digital Forensics and Investigation. From: s.l.:s.n., p. 567.

[9] Eoghan, C., 2004. Digital Evidence and Computer Crime. Second Edition επιμ. s.l.:Elsevier.

[10] GL Palmer, I. S. H. V., 2002. Forensic analysis in the digital world. International Journal of Digital Evidence.

[11] Horenbeeck, M. V., 2008. Mobile forensics. From: Technology Crime Investigation. s.l.:s.n.

[12] Jean-Loup, R., 2013. From Young Hackers to Crackers. International Journal of Technology and Human Interaction.

[13] John, J. L., 2012. Digital Forensics and Preservation. s.l.:DPC Technology Watch Report.

[14] Jones, K. J., 2005. Real Digital Forensics: Computer Security and Incident Response. s.l.:s.n.

[15] K.K. Arthur, H. V., 2007. AN INVESTIGATION INTO COMPUTER FORENSIC TOOLS. Pretoria: University of Pretoria.

[16] A Yasinsac, R. E., 2003. Computer forensics education . From: s.l.:IEEE, pp. 15-23.

[17] ACPO, 2012. Good Practice Guide for Computer-Based Electronic Evidence, s.l.: ACPO.

[18] Akhgar, B., 2014. Cyber Crime and Cyber Terrorism Investigator's Handbook. s.l.: Syngress.

[19] Sommer, P., 2004. The future for the policing of cybercrime. *Computer Fraud & Security 2004*, pp. 8 - 12.

[20] Welch, T., 1999. Handbook of information Security Management. s.l.:CRC Press LLC