UDC: 343.983:004

POSSIBILITIES OF AUTOPSY TOOL USE FOR FORENSIC PURPOSES

Dragan Ranđelović[1]
Academy of Criminalistic and Police Studies, Belgrade
Dragan Stojković[2]
Ministry of Interior of the Republic of Serbia,
Security Directorate for VIP Persons and Objects

Abstract: The rapid development and widespread use of information technology has brought dramatic changes in all spheres of human activity. At the present time it is difficult to imagine how the world functioned without these technologies. However, despite all the advantages that it brings, information technology has opened various opportunities for misuse. This has caused the development of a new scientific discipline called digital forensics, which deals with the collection, preservation, analysis and presentation of digital evidence. Since digital evidence is very sensitive (easy to delete, modify, etc.), it cannot usually be detected and seen with the classic tools. Therefore, for this purpose, the use of specialized forensic tools is required, that can successfully identify such evidence. There are a number of forensic tools, commercial and non-commercial, which can be found on the market. Some of them are used for each step in the process of digital forensic investigations, and some are multi-functional. When talking about the differences between commercial and non-commercial tools, a frequently asked question is which tools are better, more reliable, faster, more functional, etc. This paper will describe the use of Autopsy, one of the most famous non-commercial forensic tools, and compare its properties with the commercial tool FTK (Forensic Toolkit).

Keywords: digital forensics, forensic tools, digital evidence, Autopsy, FTK.

1 Prof. dr Dragan Ranđelović, Kriminalističko-policijska akademija, e-mail: dragan.randjelovic@kpa.edu.rs
2 Dragan Stojković, Uprava za obezbeđenje određenih ličnosti i objekata, MUP Republike Srbije, e-mail: drstojkovic83@yahoo.com

1. Introduction

We are witnessing a growing number of computer crimes, and it is safe to say that this trend will continue, in parallel with the development of technology. It is becoming increasingly obvious that we are more often the victims of a new type of crime, the modalities and the "modus operandi" develop with a hitherto unseen dynamics. To successfully oppose this type of crime, it is necessary to implement a comprehensive prevention, and if it does not produce the desired results, a key role in the discovery of the perpetrator and collection of evidence of his guilt is now played by a relatively young discipline of forensics - digital forensics.

In the literature pertaining to the field of digital forensics you may find different names of the discipline, such as computer forensics, computer forensics, digital forensics, computer forensics, "cyber" forensics, etc. Likewise, you may see various attempts to define, we can say, the youngest discipline of forensics. Computer forensics uses digital technology to develop and provide evidence in court and prove or disprove a claim (Newman, 2007). A slightly different definition is given by John Vacca, and in his opinion, computer forensics involves the preservation, identification, extraction and documentation of evidence stored on digital computer (Vacca, 2005). It is interesting that in some cases, digital forensics is also seen as a science and as an art using IT knowledge and skills to assist in the resolution of any legal process (Brown, 2010). Simply put, digital forensics is the process of collecting, preserving, analyzing and presenting digital evidence. In most cases, the terms "computer forensics" and "digital forensics" are regarded as synonymous, but there is still some difference between them. Unlike computer forensics relating to the collection of digital evidence stored on a computer (PC), digital forensics is a more general term and refers to all the devices that can carry digital data. In addition to the computer, these can include: digital photo cameras[3], digital cameras, mobile phones, smart phones, PDAs[4], and various other audio/video playback devices. Simply, we can say that digital forensics upgrades computer forensics, due to the development of information technology and the emergence of various digital data carriers.

When an incident occurs, the process of digital forensic investigations starts. Digital forensics is crucial for the successful detection and prosecution of criminals in the area of "computer crime." When you start this procedure, its duration must be conducted in accordance with the law, because only in this way evidence gathered in this process may be valid in court. Also, it is very important that this process is performed in a strictly determined order and not skipping any of the phases. The evidence, contained in a digital form, are very sensitive and can be easily modified or destroyed. Every mistake that you make in this process can be a big problem because digital forensics thus loses its fundamental meaning. If there is no credible evidence that has been collected in accordance with legal procedures, then you cannot get to punish the perpetrator. When we talk about the process of digital forensic investigations, in the literature generally there is agreement on the sequence of procedures, but there are different opinions on the number of phases. In most cases, we talk about four stages, although there are cases

3 Digital photo camera, as opposed to analogue, receives, stores, processes and transmits data in binary form. It takes a picture and stores it in a digital format on a memory card in the form of ones and zeros, and takes a photo to analogue "film" by highlighting different intensities. Digital data in binary form (1 and 0) become the subject of digital forensics.

4 PDA is the abbreviation of "Personal Digital Assistant." The device is a miniature computer that can fit in the palm of your hand, and whose main purpose is daily data storage, exchanging e-mails, file transfers, multimedia playback, etc.

where this number is three, five or even seven stages. The process of digital forensic investigation consists of the following stages:

- Acquisition,
- Searching,
- Analysis, and
- Presentation.

The acquisition is the first phase in the process of digital forensic investigations. This phase is analogous to taking photographs, fingerprints or traces of blood in the "traditional" forensic investigation. Since from the beginning it does not mean that all data will be used as digital evidence, the objective of this phase is to preserve all digital values. Therefore, during the acquisitions made, there is so-called bit-by-bit copy of data. In fact, it is a process when with the help of proper forensic tools (software, hardware or a combination) a copy of the original device (HDD, CD, USB memory, etc.) is made. This copy is called a forensic copy of the disk, a disk image, or simply "images." A forensic copy is not an ordinary logical backup, because it includes not only the visible data currently on the disk already but it contains the data that have been previously deleted.

In the searching phase, copies (images) are "started up" on computer that is used for the analysis. After that, the searching starts. It is essential to use time effectively, because sometimes it is a resource which is not available in the required quantity. It is a good first step in eliminating files that are known not to represent the potential of digital evidence (explore.exe, iexplore.exe, winword.exe, etc.). Also, if you know what you are looking for, your search may be conducted by keyword (keyword analysis). In this way, it performs filtering files based on a given word, and it is much easier a search.

In the analysis phase, it comes to the interpretation of digital evidence collected in the previous phase. The analysis aims to detect and display all the circumstances relating to particular incident. This stage requires the most skill and creativity, some of which directly depend on clarifying and verifying specific criminal activity.

Presentation of the results obtained from the previous phase, represents the last, i.e. final phase in the process of digital forensic investigations. The results of the forensic investigation are presented or given to the use of those organs that requested investigation. The results shall be such that at any moment they could be repeated and that someone else can also get to the same results.

The main objective of the investigation, when it comes to a "computer" incident, as in the case of classic crime, is to collect irrefutable and solid evidence of guilt or release the suspect. In the case of "traditional" crimes, such as murder, the irrefutable evidence is firearms located in the hands of murderers. Or, in the case of theft, evidence may be the money that was found on a person who has committed a theft. In computer crime, such an obvious and direct evidence is almost impossible to obtain, but it is possible to build a solid, irrefutable digital evidence without the so-called cracks, a series of circumstantial digital evidence, such as in nature all the digital data stored or generated in a computer system. Also, in contrast to the classical investigations, in the beginning of digital forensic investigation it cannot be known where all the evidence can be found. There are no obvious places to find evidence such as the classic crime, for example, a bullet hole, blood stains, messed things, etc. Also, it is very difficult to preserve a place where there are digital evidence from a variety of effects that can destroy or alter evidence. For example, if it rains on the footprints found in the dust, forensic scientist has the ability to cover the area and later to continue the investigation. All this indicates that digital evidence is very sensitive and forensic experts must have vast knowledge and experience in order to successfully carry out the process of digital forensic investigation and collect the necessary evidence.

In literature it is possible to find various definitions of digital evidence. According to one of them, digital evidence is defined as any information that is stored or transmitted using a computer and that supports or refutes the theory of how the offense was performed and who was its executor (Casey, 2004). Also, they can be defined as the data and information that is of relevance to the investigation, which is stored or transmitted by an electronic device in digital form (Newman, 2007). Simply put, digital evidence is any information in digital format (consisting of 1 and 0), which is relevant to the legal proceedings (Randjelovic, 2009), (Randjelovic, 2011). These can be various patterns of texts, images, sound clips, video clips, or any combinations thereof.

Digital evidence is stored within a computer system, so it is impossible to see the content without the help of appropriate forensic tools. There are a number of tools. Some of them are used for one purpose, while others have a much greater range of options. The choice of tools depends on the specifics of the investigation. It is desirable to always choose the tool that will contribute to the most reliable way of achieving the objective for which it is used. Forensic tools can be divided into several groups, but it should be noted that, according to the functions they perform, they may not strictly belong to only a particular group to which they belong. In literature, in most cases, the tools are classified into commercial and non-commercial tools, i.e. those which are licensed and those that are open source.

Commercial tools are made mainly for the Windows platform. These tools have many modules integrated into a single program, so they generally cover more areas of the process of digital forensic investigations. What appears as a problem with these tools is that they are paid and are costly. Non-commercial tools are not paid, they are running on Linux, and they usually incorporate all aspects of the process of digital forensic investigations. What is important for these tools is that they can make a full investigation, i.e., provide all the features as the expensive commercial tools. In the "open source" tools, source code is available for consideration and further customization. That is what makes them very functional (Altheide & Carvey, 2011).

2. Autopsy

The Autopsy Forensic Browser is an HTML based graphical interface to the command line tools in the Sleuth Kit. Together, the Sleuth Kit and Autopsy Forensic Browser provide many of the same features found in commercial digital forensics tools for the analysis of Windows and UNIX file systems. Autopsy runs as a web server, and can be accessed using an HTML browser.

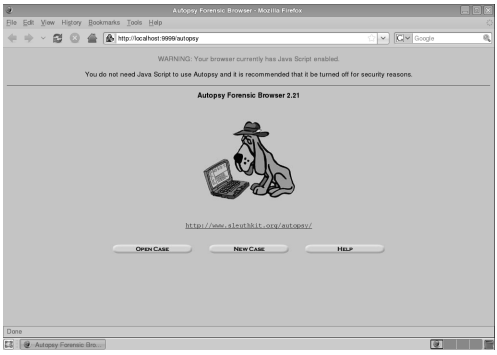

Figure 1: *Autopsy Forensic Browser*

This tool offers two of analysis modes. First, the "dead analysis" is performed when an extensive analysis of past events on the suspected system is required. In this mode, Autopsy and Sleuth Kit are run in a trusted environment, usually in a laboratory. Second, the "live analysis" occurs when the suspect system is being analyzed while it is running. In this mode, these tools are typically run from the CD. This method is usually used when you need an answer at the time when the incident happened.

Autopsy provides the ability case management, integrity checking image, search by keywords and other automated operations. This tool is used:

- To analyze the contents of folders, including deleted files,
- To analyze the contents of files (in ASCII or hex format, it is possible to extract parts of files),
- To monitor the time sequence of events based on time of access and changes to the facility,
- For content search based on regular expressions,
- For metadata analysis,
- For recovery of deleted content,
- For reporting of activities, etc.

File Analysis mode allows the analysis performed from the perspective of files and directories, in order to investigate the desired content, and collect potential evidence. In this mode, it also displays the removed contents, which is of particular importance for the investigation. Basic binary analysis can be performed by extracting the ASCII strings from binary files. Also, if we want to, we can sort files by any field. In this mode, in the left side there are four options to assist in the analysis and the right side displays the contents (figure 2).

Figure 2: *File Analysis*

Directory Seek is an option that helps faster and easier finding of the desired directory. You just have to enter in the text box the name of the directory that is subject to search.

File Name Search helps find a particular file or file categories. For the categories of files (pictures, documents, etc.), it is necessary to enter only the correct extension (".jpg", ". doc", etc.) in the text box.

Hide/Expand Directories helps find the directory that contains the contents allocated. Show All Deleted Files is an option that helps extract only the deleted files.

In this mode, two colours are used for files and folders, which greatly facilitates the analysis. Directories and files that are marked with blue are those that have been allocated, i.e., those which are not deleted and can be seen. They are not our main interest. Red indicates those contents that have been deleted, and they are the files and directories that are important to us and which may contain the potential digital evidence.

Keyword Search is a mode that allows you to search based on the given expression, i.e., based on keywords. This greatly reduces the time required for the search. For a given term, the search will be conducted in the unallocated files, which is important to find a deleted file. When selecting the desired expression and when the search is completed, a list of files containing a given term appears on the left side. Also, in addition to its content, we can see their status, i.e., whether or not they have been allocated and the location at which they are placed. To search using "grep" command that is built into most UNIX systems. To find the key word examine the entire file system, including the structure of metadata, allocated space, unallocated space and "slack" space. However, "grep" does not know anything about the file system structure so that the strings cross the "border" of the file system are also identified by the "grep." In this case false positive results can be shown. This occurs when a part of the string was requested at the end of the file and continued to the beginning of the next file.

File Category Type Analysis is file mode which facilitates the analysis process by allowing sorting of files based on file type, as well as the exclusion of known files (i.e., reducing their number). The tool we use for this sort is "Sorter." It processes the image and classifies files based on their type. There are two main operations performed by this tool, including: sorting by file and confirmation extension.

Image Details is a mode that displays general details about the image content and therefore the contents will vary depending on the file system type.

Metadata Analysis is a mode that allows viewing details about the structure of the metadata. The metadata structures are the on-disk structures that contain the details of a file, such as times and pointers to the allocated data units. To see the contents of the structure, the address can be entered in the text box on the left side or, more simply, it can be accessed directly from the regime, "File Analysis." Usually, the structure of the metadata does not have file name which the structure has shown, but there is an option to apply this name to be found (Search for File Name). This is because this process with the FAT file system is very slow, so it does not mean its exercise. The structure can be seen and the file type, which is the result of a "file" tool.

Data Unit Analysis is a mode that allows viewing the contents of an individual data unit. Data unit is a generic term used to describe the areas on the disks that are used to store data. Also, this mode is useful when recovering and analyzing deleted data. After the unit address has been entered, the contents are displayed on the right side. Filters can be used to view the data in the desired format (strings, hex dump, ASCII). To save the content locally, it is necessary to choose "Export Contents" option. "Add Note" option provides the ability to add comments about a given data unit, so that the latter can be found easily.

3. FTK

FTK (Forensic Toolkit) is a commercial forensic tool that provides a complete and detailed forensic examination of the computer, made by AccessData. FTK features powerful file filtering and great functionality when performing searches; therefore it is

recognized as one of the leading forensic tools. FTK can automatically extract Microsoft Office documents, e-mail, Internet activity and much more. This tool is fully indexed data, so that keyword searches are almost instantaneous. This may not sound important, but the hard disk image that has multiple gigabytes where it is sometimes necessary for a few hours of search, clearly shows the functionality of the tool in this kind of analysis.

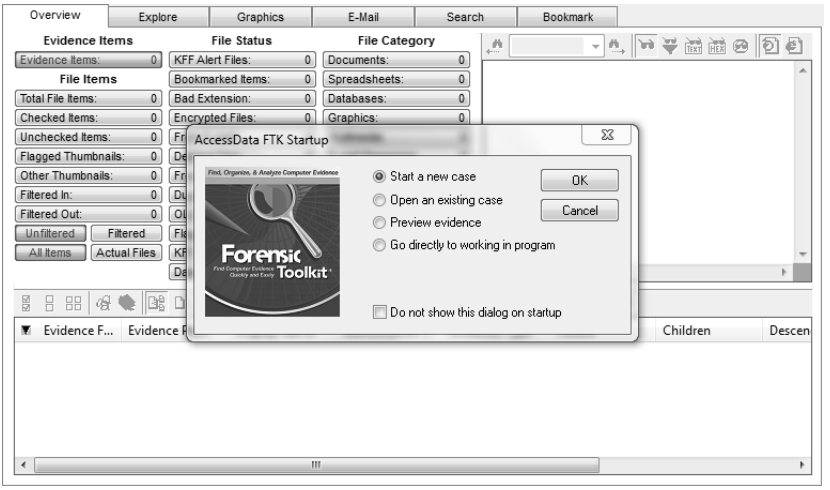

Figure 3: *Starting and opening a new case in FTK*

The basic steps to be taken during the process of computer forensic investigations using FTK and FTK Imager, include:

1. Collection and preservation of evidence,
2. Analyzing evidence,
3. Presentation of computer evidence, creating reports to document the evidence and findings of the investigation.

Collection and preservation of evidence: For the collected and stored digital evidence to be valid, they must be preserved in its original form. There are two ways to achieve this: by creating an image of the suspect disk drive using hardware devices or using software applications. FTK Imager is a software tool for collecting evidence. It can be used for fast evidence reviewing, and if the evidence is guaranteed to continue the investigation, to create forensic images on disk. To prevent accidental or deliberate manipulation of evidence, FTK Imager creates a bit-by-bit duplicate of the controlled media. A forensic image is identical to the original in every way, including empty files that are used as limiters and unallocated or free space.

Analyzing evidence: In order to analyze the evidence, FTK uses a variety of options, including hashing, the known files filter (KFF), databases, and search.

Hashing file or files is related to the process of creating unique value based on the file contents. Hash values are used to verify the integrity of files and to identify duplicate and known files. FTK and FTK Imager have two hash functions available: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1).

The known files filter (KFF) is a utility program that compares the size of the hash values in relation to the size of the hash value from the database of known files. KFF's purpose is to eliminate negligible files (such as the well-known system and program files) or a warning to known illicit or dangerous files. It also checks for duplicate files.

Files that contain other files, such as ZIP or e-mail files with attachments, called "container files." When KFF identifies a "container file" as negligible, FTK does not extract files stored in it. Using the KFF, the evidence is divided on negligible files (such as system files) and evidence is still under investigation. This allows a great saving of resources in research.

By searching we can search live (live search) or we can conduct an indexed search. "Live Search" is a lengthy process that includes checking the item-by-item in relation to a given search term. Indexed search uses the index file to find the search term. The index file contains all the separate words or numbers that belong to a string, which were found in the allocated and unallocated space. FTK uses dtSearch as a tool for an indexed search. DtSearch is one of the leading tools that is used for the search.

Presentation of evidence: FTK presents computer evidence creating a case report and case diary in order to document evidence and results of the investigation. This tool uses the Report Wizard to create and modify reports. In the report, you can add bookmarks (information that you choose during the test), customize graphics review, choose the file listings, etc. The report is generated in HTML format.

Diary of a case (case log) assists in documenting and recording activities during the investigation and analysis of the case. This information can be used as part of the report or as material to meet the person who is subsequently involved in the case, about the progress of the same. Diary of a case is automatically created by FTK and renamed ftk.log.

4. Comparison of Characteristics of Autopsy and ftk

One way to look at the possibilities of a non-commercial tool is to compare it to commercial tools by the most important characteristics. In this case, we show a practical example of the differences that appear when using FTK and Autopsy. For the purposes of this example, on the USB memory of 4 GB, we inserted two files in the folder "Analiza." The first file, where there is no message, we called "Prazan.doc," a second file that contains the secret message with a picture, we deleted.

First of all, when comparing non-commercial and commercial tools, we should emphasize the difference in price performances. Specifically, non-commercial tools are completely free, i.e., they can be easily downloaded from the internet. These are the open source tool, which means that they can adapt to different needs. Although these tools usually do not incorporate all the steps in the process of digital forensic investigations, several of them can be linked to a single software package, which creates an excellent multifunctional tool that can satisfy the most diverse requirements in digital forensics. Unlike these tools, commercial tools are very expensive. The advantage of commercial tools is that they typically integrate all the steps in the process of digital forensic investigation and they are used in many countries as the official tools, thereby proving their reliability. The choice of a forensic tool depends on the needs and possibilities. It would be ideal to use some of the commercial tools, but keep in mind that non-commercial tools can be used as an excellent free alternative.

In what follows we compare certain characteristics of FTK and Autopsy, such as: acquisition speed, image loading speed, speed of analysis and "live analysis" speed.

Before we begin the analysis, it is necessary to perform image acquisition. This is the initial step, if not to take "live analysis."

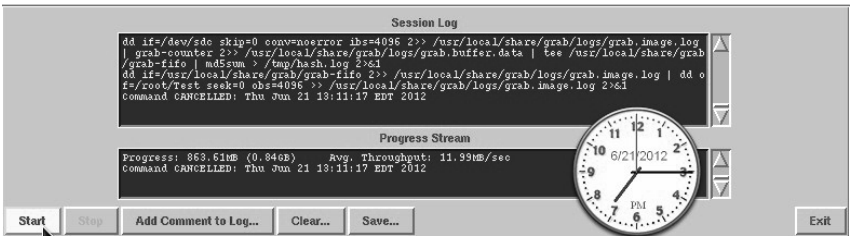

Figure 4: *Start of acquisition at Autopsy*

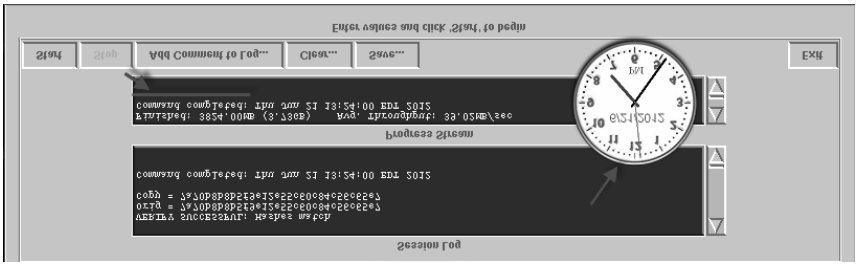

Figure 5: *Completion of the acquisition process at Autopsy*

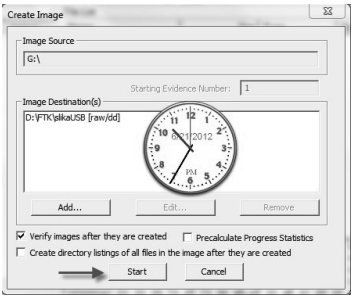

Figure 6: *Start of acquisition at FTK*

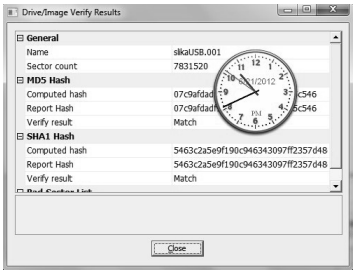

Figure 7: *Completion of the acquisition process at FTK*

As it can be seen, the time required for the acquisition at Autopsy is 9 minutes and 01 seconds, and at FTK 5 minutes and 51 seconds. FTK has done this operation for more than three minutes faster.

After the acquisition, tools need to load the recorded image disc.

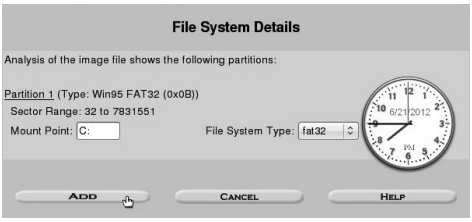

Figure 8: *Start of loading the disk image at Autopsy*

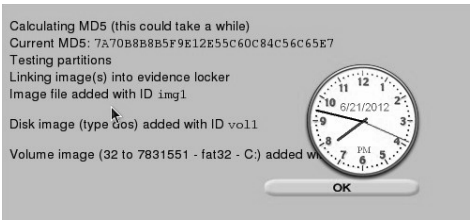

Figure 9: *Completion of loading the disk image at Autopsy*

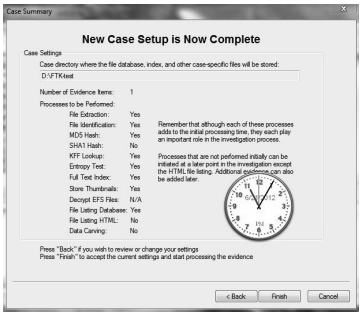

Figure 10: *Start of loading the disk image at FTK*

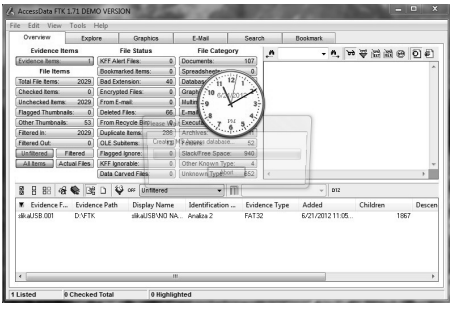

Figure 11: *Completion of loading the disk image at FTK*

The time required to load the disk image at Autopsy is 2 minutes and 19 seconds, and at FTK is 5 minutes and 02 seconds. Although Autopsy-in takes more time for image acquisition, this operation is done faster than FTK. However, the advantage is achieved here Autopsy pointless in the process analysis, that follows after loading the disk image.

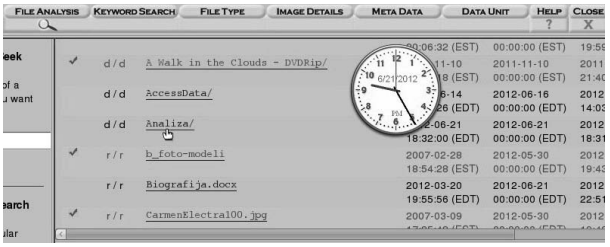

Figure 12: *Start of File Analysis at Autopsy*

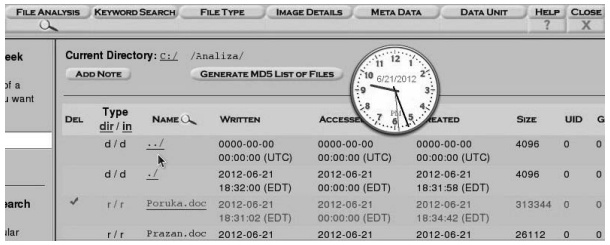

Figure 13: *Completion of File Analysis at Autopsy*

Figure 14: *Start of Keyword Search at Autopsy*

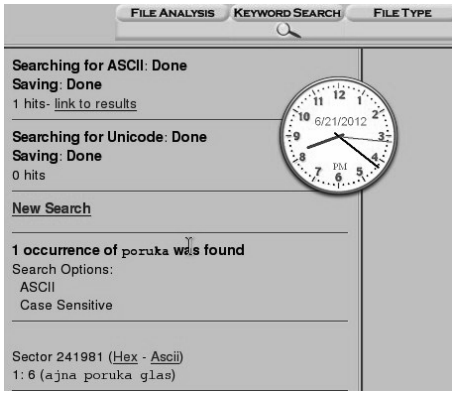

Figure 15: *Completion of Keyword Search at Autopsy*

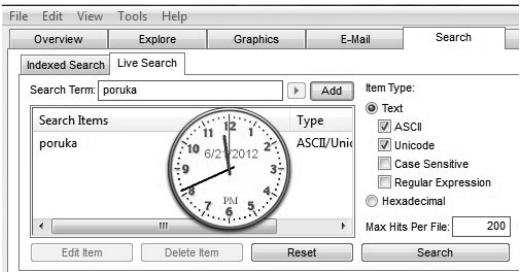

Figure 16: *Start of Live Search at FTK*

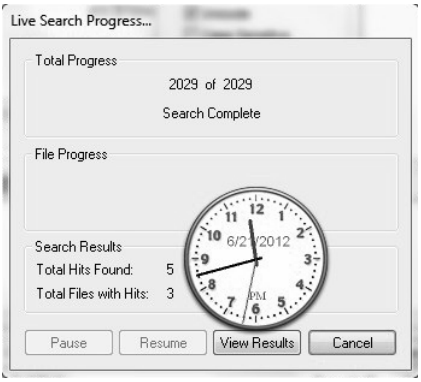

Figure 17: *Completion of Live Search at FTK*

The most significant advantage of FTK in relation to Autopsy can be seen in the analysis process (File Analysis and Keyword Search). The time required for File Analysis at Autopsy is 1 minute and 29 seconds, and Keyword Search is 6 minutes and 15 seconds. Unlike Autopsy, FTK performs this analysis instantly. However, as already mentioned, FTK has two ways to search, Indexed Search and Live Search. Indexed search is performed instantly, while Live Search is performed for 1 minute and 32 seconds.

Both of these tools have the ability for "live analysis." It is performed when a response at the moment of the incident is happening. In this situation it does not make a forensic copy of the disk, but directly accesses the system.

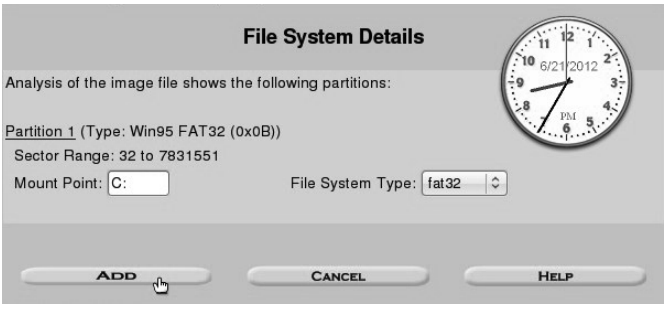

Figure 18: *Start of loading media for "live analysis" at Autopsy*

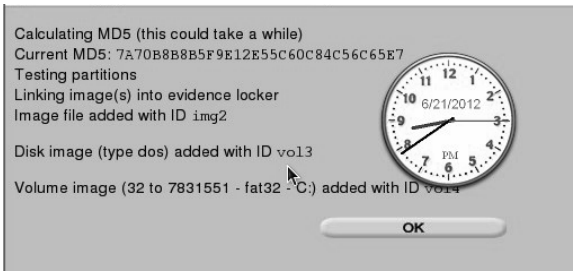

Figure 19: *Completion of loading media for "live analysis" at Autopsy*

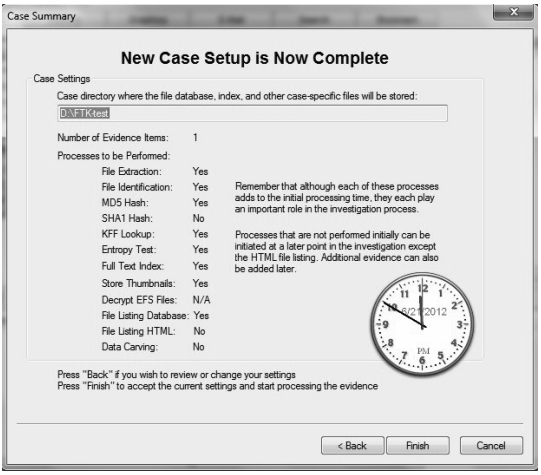

Figure 20: *Start of loading media for "live analysis" at FTK*

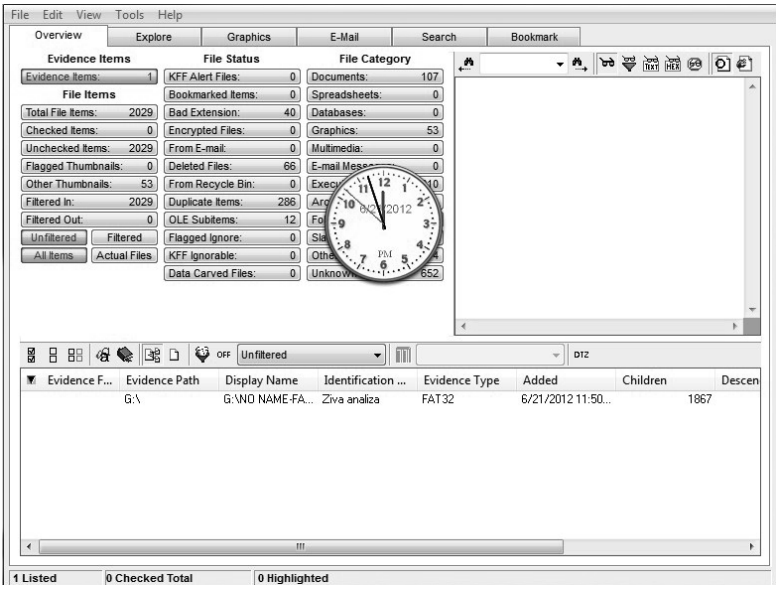

Figure 21: *Completion of loading media for "live analysis" at FTK*

As it can be seen, this action of Autopsy was done for 4 minutes and 15 seconds, and of FTK for 6 minutes and 47 seconds. In the same way as when loading a disk image, Autopsy has certain advantages in speed, but when it starts the process of analysis FTK achieved tremendous advantage.

5. Conclusion

It is a permanent improvement in this area even to be able to successfully confront the dark side of the development and use of information technology. We have stepped further into digital age, and we can see that innovations in the functioning of society happen almost every day, i.e., we are ever more dependent on information technology (IT). In such an environment, familiarity with IT misuse becomes a necessary part of the general culture, and for some categories, such as the police, judiciary and prosecution, also of professional obligations. In Serbia, there are some forensic tools that are officially recognized and used in a digital forensic investigation as for example EnCase. This is a serious problem, because without such an investigation hard evidence cannot be provided that would make the judicial processing and finally result in the punishment of the offender in this area.

A lot of tools exist in the market that are used in digital forensics, commercial and those which are free (open source). It would be ideal to use a commercial tool, EnCase type, whose reliability has been proven in practice and that is used in many countries as the official forensic tool. However, there exist a lot of non-commercial tools that can serve as a great alternative. Autopsy is a forensic tool that has the same features that are found in commercial forensic tools for analysis with UNIX and Windows systems. Therefore, there are no obstacles to the tool findings in official use. In this study, we compared certain characteristics of Autopsy and FTK on the specific examples (Table 1).

Function	***Autopsy***	***FTK***
Acquisition Image	9 min and 01 sec	5 min and 51 sec
Loading Image	2 min and 19 sec	5 min and 02 sec
File Analysis	1 min and 29 sec	currently
Keyword Search	6 min and 15 sec	currently
„Live Search“	4 min and 15 sec	6 min and 47 sec

As it can be seen, there are some differences in the speed of performing certain functions for these two tools. When talking about the difference in speed, it should be noted that this study was done on the 4 GB USB memory, so the difference is not noticeable to a large extent. However, when analyzing the media from dozens of gigabytes, the difference would be more expressed.

Autopsy needed more time for image acquisition, but when you load the pictures this tool showed better results than the FTK. However, when you begin the process of analysis one can see all the advantages of commercial tools. FTK executes these processes almost instantly, which greatly saves time, and can sometimes be a resource that is not available in sufficient quantity.

In the end it raises a legitimate question, which tool should be given priority. It primarily depends on the needs and possibilities available to us. It is certainly better to use FTK, but in situations where there are not sufficient material resources, Autopsy can be a great alternative.

6. References

1. Altheide, C.; Carvey, H.: Digital Forensics with Open Source Tools. Massachusetts: Elsevier, 2011.
2. Brown, L. T. (2010). Computer Evidence: Collection and Preservation, Second Edition. Boston: Course Technology.
3. Casey, E. (2004). Digital Evidence and Computer Crime, Second Edition. London: Academic Press.
4. Carvey, H. (2009). Windows Forensics Analysis. USA: Syngress Publishing, Inc.
5. Garrison, C. (2010). Digital Forensics for Network, Internet, and Cloud Computing a forensic evidence guide for moving target and data. USA: Elsevier Inc.
6. Ignjatović, Đ. (1991). Pojmovno određenje kompjuterskog kriminaliteta. Beograd: Anali Pravnog fakulteta u Beogradu.
7. Jones, K. J., Shema, M., & Jonhson, B. C. (2003). Antihakerski alati. Čačak: Kompjuter Biblioteka.
8. Jones, K., Bejtlich, R., Curtis, W., & Rose, C. (2005). Real Digital Forensics. New York: Addison Wesley.
9. Lazarević, S. (2000). Hakeri. Beograd: Knjiga-komerc.
10. Milosavljević, M., & Grubor, G. (2009). Digitalna forenzika - udžbenik. Beograd: Univerzitet Singidunum.
11. Milosavljević, M., & Grubor, G. (2009). Istraga kompjuterskog kriminala. Beograd: Univerzitet Singidunum.
12. Newman, C. R. (2007). Computer Forensics: Evidence, Collection and Management. New York: Auerbach Publications.
13. Petrović, R. S. (2000). Kompjuterski kriminal. Beograd: Ministarstvo unutrašnjih poslova Republike Srbije.
14. Petrović, S., & Ćirić, V. (1986). Zaštita podataka u automatizovanim informacionim sistemima. Beograd: Naučna knjiga.
15. Ranđelović, D., & Bogdanović, T. (2010). Alati za digitalnu forenziku, NBP - Žurnal za kriminalistiku i pravo, Vol. XV, No. 2, 25-47.
16. Randjelović, D., Delija, D., Popović. B. (2009).EnCase forenzički alat,
17. Bezbednost 1-2, pp. 286-312.
18. Randjelović D., Đorđević V. (2011). A TEST SAMPLE APPLICATION IDS OPEN SOURSE AND COMMERCIAL SOURSE, NBP Vol. XIX ,No. 3, pp. 45-65.
19. Ruth, A., & Hudson, K. (2004). Security +, CET Computer Equipment and Trade.
20. Tanenbaum, A. (2005). Računarske mreže. Beograd: Mikro knjiga.
21. Vacca, R. J. (2005). Computer Forensics: Computer Crime Scene Investigation, Second Edition. Massachusetts: Charles River media.