Comparative analysis on integrated digital forensic tools for digital forensic investigation

Jae-ung Lee, Woo-young Soh
Department of Computer Engineering, Hannam University Republic of Korea
leejaeung1990@gmail.com, wsoh@hnu.kr

Abstract. As a variety of digital devices have recently become widely commercialized, digital forensics, a process where electronic information stored in digital devices is accurately identified, collected, preserved and analysed and the information is submitted to the court as evidence, is gaining enormous popularity. This paper analyses characteristics, applications, limitations of digital forensic tools and compare the tool with others in terms of ease of use, thereby helping investigators to adopt integrated digital forensic tools in their investigation.

1. Introduction
Recently, the assassination of the Saudi dissident Jamal Khashoggi has drawn enormous attention from all over the world. To figure out what actually happened in his disappearance, investigators paid attention to the Apple Watch on his wrist. That is because the Apple Watch allegedly recorded the killing of Khashoggi and was connected to other devices. As a variety of digital devices have recently become widely commercialized, digital forensics, a process where electronic information stored in digital devices is accurately identified, collected, preserved and analyzed and the information is submitted to the court as evidence, is gaining enormous popularity. A comprehensive digital forensic tool integrates various functions such as analysis tools and reporting tools into one model. This paper will examine the characteristics, applications and limitations of these integrated digital forensic tools and further compares their ease of use with other tools, which will help investigators adopt the integrated digital forensic tools.

2. Relevant research
Digital forensics has traditionally been utilized in forensic science. In other words, it was used in fields such as fingerprinting, hair and DNA analysis and autopsies. However, with the advent of various digital devices, the concept of forensics has been expanded to include electronic evidence stored in digital devices, not to mention physical forms of evidence. Thus, digital forensics refers to the process of accurately identifying and collecting electronic information stored in digital devices, preserving and analyzing the information and submitting to the court as evidence. Depending on the subject of analysis, digital forensics includes disk forensics, system forensics, network forensics, Internet forensics, mobile forensics, database forensics, and cryptographic forensics.

2.1. Disk Forensics
Disk forensics is the science of extracting forensic information from physical digital storage media like hard disks, Floppy disks, CDs, USB devices etc.
2.2. System Forensics
System forensics is a branch of digital forensics that extracts forensic information by analysing computer operating systems, application programs or computer processes. It is important to understand file system of various operating systems.

2.3. Network Forensics
Network forensics collects evidence by analysing data or password transmitted via network or network configurations. Most of the networks provide tracking tools for monitoring purposes.

2.4. Internet Forensics
Internet forensics collects information that uses internet protocols such as WWW or FTP.

2.5. Mobile Device Forensics
Mobile device forensics is a branch of digital forensics that extracts digital evidence or data from a mobile device. Given data from small handheld devices are easily concealable, mobile device forensics requires high level accuracy.

2.6. Database Forensics
Database forensics is a branch of digital forensics that collects and analyses information from databases. Considering companies store all their data in their databases, it can serve as a useful tool to secure evidence.

2.7. Password Forensics
It is a type of digital forensics that recovers password of files or systems. Files or systems are often encrypted in order to block access from unauthorized entities. Password forensics is used in such cases.

3. Integrated digital forensic tool comparative analysis
A digital forensic tool refers to a tool designed for digital investigation. Specifically, Integrated Digital Forensics combines functions such as analysis tools or reporting tools into one tool. Thus, it is classified into integrated analysis in dataset creation strategies that performs interpreting and search functions of the program interface. It can also be categorized as detailed analysis that performs analysis and carving for smart devices of which tool performance may vary.

3.1. EnCase
EnCase is an integrated digital forensic tool developed by Guidance Software and is available for about $2,995. Major functions include Triage, Collect, Process, Search, Analyse, and Report. The recommend systems settings for a computer’s hardware and operating system is a CPU that is a quad core or higher, 16 GB RAM or higher, and Windows OS in 32-bit or 64-bit environment. It provides a wide range of features, including the operating system installation drive, installation images, portable data medium, physical memory and MacOSX analysis, as well as file restoration, extraction and reporting functions.

Thus, it can be widely used for digital forensics. Also, it is highly scalable, given that features that are not supported by the program can be dealt with by script programming. However, diverse functions of the tool make it complicated to handle. Therefore, it is necessary to fully familiarize oneself with EnCase before using it. It would be highly useful if an investigator who uses the tool to be familiar with it and capable of utilizing various functions of the tool.

3.2. FTK (Forensic Tool Kit)
Forensic Tool Kit (FTK) is an integrated digital forensic tool which is developed by AccessData and sold for about $5,144. Quad-core or higher CPU or Xeon-class CPUs, 32 GB of RAM, and a 64-bit Windows OS are recommended. Two available operating environments are server and desktop. FTK supports a wide range of analysis as well as operating installation drive and installation image,
portable storage medium, physical memory and encrypted disk volume. It uses collected artifacts for a database called Postgre to refine and select data. In addition, since it uses Tab, it is relatively easy to familiarize oneself with the tool. However, since dependency problems such as installation of database occur when the tool is installed, it is necessary to establish an investigation-friendly environment beforehand.

3.3. Forensic Explorer
Forensic Explorer is an integrated digital forensic tool developed by GetData and sold for about $1,247.95. Quad-core or higher CPU, a minimum of 8 GB of RAM, a 32-bit and 64-bit Windows OS are recommended.

Forensic Explorer supports operating system installation drive and image, portable storage medium and a script for analysis. But the script should be written with Pascal, so learning Pascal is required. However, compared to Encase or FTK, it offers distinctive benefits such as operability in low-end PCs and an intuitive interface. Thus, even those who are not familiar with the tool can easily utilize Forensic Explorer. This makes it possible for low-skilled investigators to use the tool without impairing efficiency of investigation.

3.4. X-Ways Forensics
X-Ways Forensics is an integrated digital forensic tool developed by X-Ways and sold for about €1199. Quad-core or better-functioning CPU, 4GB of RAM or more, and Windows OS in 32-bit and 64-bit environment are recommended. X-Ways Forensics can be used in most forensic environments from media imaging to physical memory analysis. Collecting and aggregating artifacts and providing reporting functions, X-Ways Forensics has the lowest drive environment specification requirement among all the integrated digital forensic tools. It can also be operated without installation. Although it can run on such low specification devices, it still provides with analysis of image files as well. However, the functions it provides are relatively limited. In addition, since it mainly focuses on Hex View, it requires highly-skilled tool exploitation.

3.5. BlackLight
BlackLight is an integrated digital forensic tool developed by BlackBag and sold for about $2,600. Quad-core or better-performing CPUs, 16GB of RAM or more, and a Window OS in 32-bit and 64-bit environment and MacOSX which has lower specification than Mavericks are recommended. BlackLight, analysing data with the use of user history in the MacOSX environment, provides multiple functions. It supports functions such as file system browsing and recovery functions for unallocated space as well as basic functions of Mac’s operating system such as interpreting email, internet, message, schedule, maps and notes. In addition, it is capable of interpreting disk image files when interpreting HFS file systems. As for EFS, it interprets file systems with the use of keychain file. However, its operation is unstable in the Window OS environment and relatively stable in Mac OS X.

Thus, it can serve as an additional tool for the investigator. Except BlackLight, which is specifically designed for Mac OS X, the best performing tool is Forensic Explorer. It uses an intuitive interface that categorizes tabs by type of artifacts collected, Forensic Explorer is more convenient than other tools. Also, it provides with most of the functions of FTK or EnCase. Also, in terms of registry analysis, it uses automatic parsing to support outputting important information such as user information, installation and external storage medium. Other tools cannot be utilized unless one fully understands how to uses those tools. In Linux/Unix or Mac OS X, most of those tools mentioned above can interpret EXT, HFS, HFS+partitions. Thus, investigators can extract artifacts and analyse them. BlackLight only analyses Mac OS X artifacts, and the supported partitions are limited to FAT partitions, HFS, and HFS + partitions. It automatically parses the key information of Mac OS X and outputs the result. The artifacts supported by the tool parse information such as user information, operating system information, Web history, e-mail, installation application, etc. and output the results. Thus, If one does not know the path of artifacts of Mac OS X or how to collect them, they can be expected to utilize BlackLight instead.
4. Conclusion

As a variety of digital devices have recently become widely commercialized, digital forensics, a process where electronic information stored in digital devices is accurately identified, collected, preserved and analysed and the information is submitted to the court as evidence, is gaining enormous popularity. The integrated digital forensic tool, a comprehensive tool that incorporates collection of digital evidence, reporting and analysis, offers various functions, which can help reduce the amount of time spent for analysis. In addition, you can get uniform results, given that it is capable of producing results of many artifacts in the form of a report. However, it requires high-end PCs for investigative purposes and offers numerous functions which are hard to be familiar with. Also, since that most of them are commercial software, their license is quite costly. This paper will examine the characteristics, applications and limitations of these integrated digital forensic tools and further compares their ease of use with other tools, which will help investigators better adopt integrated digital forensic tools.

References

[1] Lovanshi M and Bansal P 2019 Comparative Study of Digital Forensic Tools Engineering and Applications pp 195-204
[2] Yagnik S.B and Panchal E.P 2019 AEACFE System—An Intelligent Digital Forensic System Third International Congress on Information and Communication Technology 797 pp 409-416
[3] Paul Joseph D and Norman J 2019 An Analysis of Digital Forensics in Cyber Security First International Conference on Artificial Intelligence and Cognitive Computing 815 pp 701-708
[4] Panchal E.P, Yagnik S.B and Sharma B.K 2019 Use of Machine Learning Algorithm on File Metadata for Digital Forensic Investigation Process Third International Congress on Information and Communication Technology 797 pp 401-408
[5] Mane D and Shibe K 2019 Big Data Forensic Analytics Data Management, Analytics and Innovation 839 pp 113-129
[6] Hemdan E.ED and Manjaiah D.H 2019 Digital Forensic Approach for Investigation of Cybercrimes in Private Cloud Environment Recent Findings in Intelligent Computing Techniques 707 pp 25-33