Global Scientific JOURNALS

GSJ: Volume 9, Issue 3, March 2021, Online: ISSN 2320-9186
www.globalscientificjournal.com

The Evaluation of the Encase and FTK Forensic for effective evidence extraction

By

Abubakar Abdulkadir
And
Ahmad Ahmad
And
Badamasi Ja afar

Abstract

The paper present features of ETK and encase forensic tool and encase strength, advantages, similarities and discusses area of their strength, also proposes a general frame work that will take care of their weakness.

INTRODUCTION

Around the world, the standard in computer forensics as based on the software tools. The court-accepted digital investigations platform is built for speed, analytics and enterprise-class scalability. The Known features for software tools are intuitive interface, email analysis, customizable data views and stability. In this report, the FTK and Encase forensic tools are described and analyzed in terms of the Features similarity, Advantages or strength, Limitations or area of improvements.

THE FEATURES SIMILARITIES BETWEEN FTK AND ENCASE FORENSIC TOOLS

In this section, the features of two forensic tools are justified and discussed with their similarities as following:

2.1 FKT Features

FTK features powerful file filtering and search functionality and are recognized as the leading forensic tool for e-mail analysis. The Forensic toolkit can parse a number of file

systems, including FAT, NTFS, NTFS Compressed, Ext2, and Ext3. It can use image files created by AFF, EnCase, SMART, Snapback, some versions of Safe back. The program allows users to search with keywords or take advantage of drive indexing using the DTSearch algorithm [4]. Where things get really interesting is when you consider the advantages of employing all of the other tools in the suite. File carving, string searching (with hits tied to a specific running process), fuzzy hashing, and dumping strings in memory to feed into a password cracking dictionary are all possible within the FTK interface. The Dongle Access Data provides a parallel or USB dongle with FTK. The dongle is a security compliance device that you insert into the parallel or USB port during installation [4]. It maintains your FTK licensing and subscription information and is required to use FTK.

EnCase Features

Encase forensic, contains many features that made it fit in many different platforms in digital device forensic, right from the earlier released version 6.3.However, another features are also being added beside the previous version feature after the release of version 7, the feature are as follows:

- The most important advantage that made Encase tool widely popular is the breadth of operating systems and file systems. This tool previously was operable on 32 bit systems only but currently it can operate both in windows 32, 64. In addition to other operating systems such as Linux and Unix. This tool can also be used to perform investigation remotely where it can operate and control remote machines easily.(It can support remote system).
- In Encase also contains complex graphical user interface GUI and incorporate features for browsing, searching, displaying devices, file system and data file. However, the search features of encase allow investigator to search through different

internet and email artifact across machines these internet and email search finds different mail formats such as hotmail, outlook, lotus notes, yahoo etc. and internet artefact from internet explorer[5].

In Encase also incorporate its own programming language named Enscript almost look like other higher level programming languages e.g. java and C++[5].

A new Encase user interface (GUI) that combine functionalities of the tool and make the navigation easier[6].

- Encase are made to be more reliable through speeding up case reaction and ability to access information from new evidence processor (Evidence processor)
- Another higher performance indexing engine is added to the software, the indexing search engine make search more easier and has the ability to display search result across multiple file types this mitigate the defect come with the Encase previous version 6.3[6].
- Encase scalability is increase with efficient caching (efficient caching) means file system email and other compound structures are cached to disk. This will rationally reduced the time and system resource needed to re-examine already processed data (system overhead) also this mitigate the defect of the previous Encase tool version 6.3[4].
- Encase employ or has threading concept e.g. email and conversation threading, this give the Encase capability to review chain of conversations.
- Powerful hashing concept is introduce for message preservations and along with easy and customizable graphical user interface for managing hashing sets and hash libraries [4].

- User customizable tags can be defined to filter data and generate report (user customizable tags)[5].
- Some Encase features contribute to its strengths which includes: provision of recovery operations in case of file damage or folder, signature to preserved file contents, hash analysis etc[4].
- Encase has decryption suite (EDS): this feature enables the tool to decrypt supported full disk and volume encryption and encrypted registry entries[4].
- Encase has physical disk emulator (PDE) Module: it allow virtual physical disk to be created on the computer where deleted as well as evidence file are moved
- Encase has Virtual file system (VFS) module: evidence file are kept as offline network share in windows operating system.
- Encase has integrated Fast Bloc software Edition (SE): Software to deny writes operations to a removable device during preview or acquisition [7].

The (FKT, Encase) Features Similarities

Three common software packages in this category are Encase, Pro Discover and Forensics Tool Kit (\FTK"). Encase is the market leader and the most proprietary of the three. All three software packages allow you to image hard drives or to import a raw image. The actual use of each software package is unique and complex requiring practice. FTK uses DTSearch to build full text indices for searching (an option) whereas EnCase performs a "Live Search" every time you want to change your keywords. To explain this, EnCase will search through every document in your selected location every time you execute a search. The Live Search can take hours, depending on the size of your image drive - even on superior hardware.

According to DTSearch, if you do not have any experience with it, is the brains behind most high end search engines available commercially. They have a nice API that is very affordable, which makes it an easy choice for developers who need to parse tons of text in Windows.

ADVANTAGES AND STRENGTH

3.1 FTK Advantages and Strength:

FTK provides you the following advantages:

Simple Users' Interface

FTK makes evidence and easy to analyze. Our database architecture sorts and categorizes all graphics, e-mails, bad extensions, and encrypted files more quickly and simply.

Email Display

Most forensic software requires yet another utility to allow the investigator to view emails in readable HTML format. FTK allows you to view e-mail in a user-friendly HTML. You can view native formats such as AOL IP addresses, POP3 servers, and view attachments. You can also document them in HTML reports[4].

Fast Searching

Full-text indexing makes searching for keywords instantaneous. The index file is the case evidence. The indexed search uses the index file to find the search term. Evidence items may be indexed when they are first added to the case. Full-text indexing makes searching much more efficient.

KFF Database

The Known File Filter (KFF) is an FTK utility that compares file hashes of your evidence against a database of hashes from files known to be irrelevant (such as known system and program files). It also checks for duplicate files.

EFS Decryption

Forensic Toolkit (FTK) can break the file or folder encryption so that additional evidence can be uncovered. When evidence is added to a case and Decrypt EFS Files is selected in the New Case Wizard, FTK launches PRTK and decrypts EFS files. Additionally, FTK can recover encrypted instant messaging chat logs and additional information such as buddy lists.

Bookmarking

The end result of a successful investigation is a list of bookmarked data to be used as evidence.

Reporting

After you complete the case investigation, you can create a report that summarizes the relevant evidence of the case.

Password Dictionary Creation

FTK uses the full-text index for instantaneous keyword results. It can also be exported for use as a dictionary for password recovery processes in the Password Recovery Toolkit (PRTK).

3.2 Encase Advantages and Strength

FTK and Encase tools are the market leader in computer forensic field and they are the most popular and commonly used forensic tools globally [2]. This is due to the various strengths that they possess in investigating computer-related crimes. Some of those strengths or features are explained below:

1. Encase tool is known of its higher performance and faster data processing. Encase tools has been developed in chains or subsequent versions. The latest version of Encase tool which is currently available is version 7.03. This version is faster 3 times then the previous version, version 7.01 and 2 times than any other competitor similar products such as forensic tool kit (FTK). Distributed processing in FTK tool allows you to leverage up to 3 additional computers to dramatically reduce processing time and tackle massive data sets[2].

2. Encase and FTK tools are known of performing deep forensic Analysis. They have the ability to expose evidence that may go unnoticed if analyzed with other tools. They also support the analysis of EXT4 and HFSX file systems, Office 2010 files, encrypted drives, and IOS physical images [2].
3. Extra investigation support is done by Encase and FTK tools such as email investigations. The new email investigation platform makes performing email investigations as easy as reviewing emails in an inbox which enables examiners can perform succinct email investigations faster than ever before[3].
4. Encase and FTK tools facilitate tracking back former investigation operation through its built in archiving capability. This will ensure examiners have everything they need when a case needs to be reviewed in the future.
5. Encase has more advanced searching capabilities than other tools like 1) Boolean searches, (2) fuzzy logic, (3) context searching, and (4) methods involving mathematical probabilities. It performs the search based on predefined keywords. It also has the ability to enter optional characters in the keyword string such as "A-E" to indicate the character can be A, B, C, D, or E to match the keyword. On the contrary, FTK uses indexed search which uses the index file to find the search term.
6. Via the usage of such reliable tools, evidence is completely conserved and kept totally save and uncompromised. With Encase Forensic, examiners can be confident that the integrity of the evidence will not be compromised or tampered with. This is because all the file formats of evidences captured with Encase Forensic tool are widely accepted as the de facto standard evidence containers.

7. A unique security feature in Encase tool is the new evidence files captured can be encrypted directly within Encase Forensic, adding another level of security to the most trusted evidence file format in the industry.

LIMITATIONS OR AREA OF IMPROVEMENTS

4.1 Processing Speed

Processing averaged volumes of the evidential data tend to take much time as such, forensics analysis has to give large amount of time in processing any evidential data even when the evidence presentation needs to urgent .However, this effect not only FTK forensic tool but also the encase tool needs to have processing speeds to take advantages of urgent evidence processing that might be required at the court of appeal [4].

4.2 File Format Standardization

File Format Standardization not only between FTK and Encase forensic too but also among all the forensic tools, this will allowed changes make to a particular format can also fit in other 3rd party tools or be compatible[2].

4.3 Language Deficiency

Both Encase and FTK has language deficiency they are only English language based software, good if they are made to be supporting more languages this is because of the following reason

1. **Non- based professionals**

Compatibility issues in different operating system graphic form e.g. Arabic, Malay, Chinese.

4.4 Ability to Distinguish Between False Positive and False Negative

Both of the tools can not differentiate between false positive and false negative information in case of dealing with log files and they don’t have the ability of finding obfuscated information.

4.5 Client/Server

The tool doesn't support both client and server application. Means extracted evidence cannot be send to the analysis server remotely via SSL channel.

4.6 Keyword Search Based

Encase tool's does not have the ability to weight keywords in the result files to identify the most likely document to view first.

4.7 Search Capability

FTK software doesn't support the following functionality that will ease the works of the investigator

FTK cannot open case if drive letter changed where case data is located

No progress bar

Multi- Tasking

5. PROPOSED CONCEPTUAL FRAMEWORK

Based on the extensive reviews and analysis we have done, both FTK and Encase forensic tools suffer several limitations and weaknesses that increases the need to develop a new forensic tool framework that is required to eliminate or overcome the limitations of existing tools. The first limitation that should be addressed in our new framework is enlarging the support of searching data represented in languages other than English language. There are roughly 6,500 spoken languages in the world today, but most of the existing tools support few languages only. This will create huge difficulties in investigating computer crimes committed via unsupported language. Another feature that needs to be supported in the proposed framework is enhancing the searching capabilities to support all possible words as key words [2].Some existing tools exclude some proximity words during the searching process while those words could be the clue and a step towards the solution [1]. The limited support of result file format is another obstacle to investigators where files created by a tool

can only be open using the same tool but there are situations that the investigation process requires fast access to files even in a machines that does not has such tools to open those files, thus file formats must be widely supported and easily opened by common applications such as Microsoft office applications [2].

CONCLUSION

Last but not least, to facilitate investigators job, the proposed tool should sort the result files according to the highest number of match of the key words found where the files with higher match should appear first[3]and a new frame work should be adopted to take care of the multilangaugistic bearier and different file format.

References

[1] Safecomputing.umich.edu/tools/download
[2] http/ww.cit.cornell.edu/computer/security/tools
[3] http://www.digitalintelligence.com/software/guidancesoftware/encase7/
[4] :http://encase-forensic-blog.guidancesoftware.com/2012/03/encase-forensic-development-perspective.html
http://www.forensicfocus.com/index.php?name=Forums&file=viewtopic&t=1542
[5] http://www.digitalintelligence.com/software/accessdata/forensictoolkit3/
[6] S.Haenchen, “Advanced Text Searching Of Electronic Information Related To Forensic Discovery”.
[7] www.guidancesoftware.comEnCase ®
[8] Forensic Version 7 Preview New Features