Comparative study of Digital forensic tools

Siang Lee Khaw
P-COM0023/19
CDS523 Forensic Analytics and Digital Investigations
School of Computer Sciences
University Science Malaysia
Penang, Malaysia
sianglee.khaw@student.usm.my

***Abstract*— In recent years, there are a tremendous increase in cybercrime such as credit card theft, online banking fraud, intellectual property theft, child pornography, unauthorized intrusion, identity theft, digital piracy, money laundering, etc. Laptops, desktops, smartphones, tablets, smartwatches, and GPS devices can be used to aid in crime. All digital devices leave behind a digital footprint. Because of this, digital forensic tools used in acquisition, recovery, analysis, and being able to present the evidence in court are very important. In this paper, I will perform a comparative study on the Digital forensic tools namely Autopsy, Encase, Forensic Toolkit (FTK) based on their features and ability of acquisition, recovery, analysis, and presentation.**

Keywords—Digital forensics, Autopsy, Encase, FTK.

I. Introduction

With the increasing use of digital appliances for online transactions, medical records, and personal information, there is an increase in cybercrime committed with digital devices. Digital forensics is a new demanding field in Computer sciences to recreate the crime event with the preserved data which was collected in the crime scene by a trained investigator. The evidence must be handled properly and maintained in its original condition so that it can be used in court. Hence, comprehensive processes are needed to be in place to handle the collecting, preserving, recovering, analyzing, and presenting.

II. Digital Forensic Investigation

The digital forensic investigation comprises of four major processes:

1. Acquisition

The goal for this step is to obtain the evidence device physically or remotely without tampering or modifying the content or crime scene. Each acquisition step should be documented as much as possible. Before the acquisition, the investigator will need to verify if a warrant is needed or if the incident is under the investigator's jurisdiction also the kind of system under siege, and does it need to be kept running for live state backup. Digital forensic tools are used to perform bit-by-bit backup copies of the digital evidence to a trusted device. The replications are then hashed and documented to maintain the integrity of the backup.

2. Recovery

Most file-system only delete the entries of the files or directory so after acquiring the image of the storage device, the investigator will try to recover files that may be deleted by the suspect. Unless the complete sector had been overwritten by other content, recovery tools can recover from slack space. Slack space is an unallocated sector in the file system or unused space at the end of files or unused space in the file system. The suspect may conceal suspected data in other data or files, so as part of the recovery process, the investigator will use forensic tools to decode the steganographic data. Recovery may also involve decryption of data, after identifying an encrypted file, the suspect will be obliged by law to reveal the key to decrypt them. Some files may be completely deleted or too fragmented to be recovered, the investigator can recover the cache files, temporary directory/files created while accessed files by the suspect, swap files, hibernated backup files, etc. to help for analyzing process.

3. Analysis

Depending on the nature of the incident, the investigator is limited to locating specific files specified in the search warrant and whether the existing or recovered files are illegal. Investigator will also determine whether the system had been compromised and the rightful owner of the illegal files. Analysis plays an important role because the result will help the investigator reconstruct the event and find the cause of the incident. The investigator can be assured that the evidence found after the analysis phase is effective and justifiable to be present in court.

4. Presenting

The investigator may have to be present in court as an except witness for the case. The result of the analysis will be documented thoroughly that the judge or top management of the organization can understand. The forensic examination report will list out the forensic tools used in the process of digital forensic investigation, list of devices confiscated from the crime scene, list of software used and their versions, the hash results, all storage media numbers, model, make.[2]

III. Related Work

Varsha Karbhari Sanap, Vanita Mane, Comparative Study and Simulation of Digital Forensic Tools, the paper discusses the need for digital forensics, digital forensic process, digital evidence, and digital data. Three digital forensic tools WinHex, Active file recovery, ProDiscover Basic have been compared.[2]

Neelam Maurya, Jyoti Awasthi, Raghvendra Pratap Singh, Dr. Abhishek Vaish, Analysis of Open Source and Proprietary Source Digital Forensic Tools. The author performed a comparison matrix that provides an overview of each tool based on the functionalities.[3]

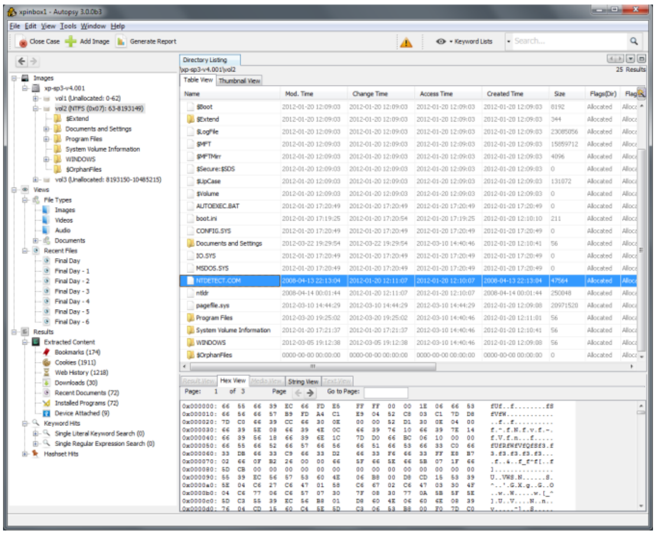
Mayank Lovanshi, Pratosh Bansal, Comparative Study of Digital Forensic Tools. The paper provides a comparative study between forensics application tools and a set of parameters. This approach is useful for forensics experts and investigators to select the best possible forensic tool based on their requirements.[4]

Nilakshi Jain, Dr. Dhananjay R Kalbande, A Comparative Study based Digital Forensic Tool: Complete Automated Tool Cloudera Distribution. The main object of the study was to determine whether the complete proposed digital forensic framework can be implemented in digital forensic tools with automated report generation. [5]

IV. Forensic Tools Overview

A. *Autopsy version 4*

Autopsy is an easy-to-use, GUI-based program that allows users to efficiently analyze hard drives and smartphones. It is available in Windows, Linux, and OSX. Autopsy was designed to be intuitive and approachable so that it can be effectively used by non-technical investigators. Autopsy provides a vast forensic analysis module and is also extensible through a plug-in module by a third party. Autopsy runs background tasks in parallel using multiple cores and presents results to the user as soon as they are found. Autopsy is free and Autopsy v4 source code is distributed under Apache 2 license. [11]



Name	Mod. Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
$Boot	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	8192	Allocated	Alloc
$Extend	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	344	Allocated	Alloc
$LogFile	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	23085056	Allocated	Alloc
$MFT	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	15859712	Allocated	Alloc
$MFTMirr	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	4096	Allocated	Alloc
$Secure:$SDS	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Alloc
$UpCase	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	131072	Allocated	Alloc
$Volume	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Alloc
AUTOEXEC.BAT	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloc
boot.ini	2012-01-20 17:19:25	2012-01-20 17:20:54	2012-01-20 17:19:25	2012-01-20 12:10:10	211	Allocated	Alloc
CONFIG.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloc
Documents and Settings	2012-03-22 19:29:54	2012-03-22 19:29:54	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Alloc
IO.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloc
MSDOS.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloc
NTDETECT.COM	2008-04-13 22:13:04	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-13 22:13:04	47564	Allocated	Alloc
ntldr	2008-04-14 00:01:44	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-14 00:01:44	250048	Allocated	Alloc
pagefile.sys	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-01-20 12:09:08	20971520	Allocated	Alloc
Program Files	2012-03-20 19:25:02	2012-03-20 19:25:02	2012-03-10 14:40:46	2012-01-20 12:11:01	56	Allocated	Alloc
System Volume Information	2012-01-20 17:21:37	2012-01-20 17:21:37	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Alloc
WINDOWS	2012-03-05 19:12:38	2012-03-05 19:12:38	2012-03-10 14:40:46	2012-01-20 12:09:08	56	Allocated	Alloc
$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Alloc

```
0x000000: 66 55 66 39 EC 66 FD E5  FF FF 00 00 1E 06 66 53  fUf..f........fS
0x000010: 66 56 66 57 B9 FD A4 C1  E9 04 52 C8 03 C1 7D D8  fVfW............
0x000020: 7D C0 66 39 CC 66 30 0E  00 00 52 D1 30 0E 04 00  ..f..f..........
0x000030: 66 39 5E 08 66 39 4E 0C  66 39 76 10 66 39 7E 14  f.^.f.N.f.v.f.~.
0x000040: 66 39 56 18 66 39 6E 1C  7D D0 66 BC 06 10 00 00  f.V.f.n...f.....
0x000050: 66 55 66 52 66 57 66 56  66 51 66 53 66 33 C0 66  fUfRfWfVfQfSf3.f
0x000060: 33 DB 66 33 C9 66 33 D2  66 33 F6 66 33 FF E8 B7  3.f3.f3.f3.f3...
0x000070: 02 66 0F B2 26 00 00 66  5F 66 5E 66 5B 07 1F 66  .f..&..f_f^f[..f
0x000080: 5D CB 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ]...............
0x000090: 55 39 EC 56 57 53 60 4E  06 B8 00 D8 CD 16 53 39  U..VWS.N......S.
0x0000a0: 5E 04 C6 27 C6 47 01 58  C6 67 02 C6 47 03 30 4F  ^..'.G.X.g..G..O
0x0000b0: 04 C6 77 06 C6 57 07 30  7F 08 30 77 0A 5B 5F 5E  ..w..W.....w.[_^
0x0000c0: 5D C3 55 39 EC 56 B8 01  D8 60 4E 06 60 6E 08 39  ].U..V....N..n..
0x0000d0: 76 04 CD 15 60 C4 5E 5D  C3 06 53 B8 00 F0 7D C0  v.....^]..S.....
```

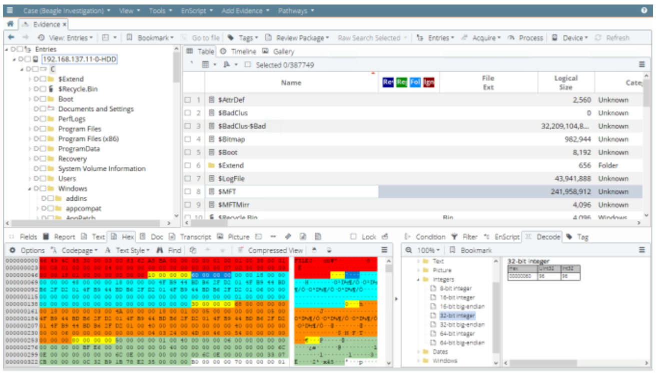
Figure 1. Autopsy interface

Below are feature list of Autopsy: [12]

- Multi-User Cases: Collaborate with fellow examiners on large cases.
- Timeline Analysis: Displays system events in a graphical interface to help identify activity.
- Keyword Search: Text extraction and index searched modules enable you to find files that mention specific terms and find regular expression patterns.
- Web Artifacts: Extracts web activity from common browsers to help identify user activity.
- Registry Analysis: Uses RegRipper to identify recently accessed documents and USB devices.
- LNK File Analysis: Identifies shortcuts and accessed documents
- Email Analysis: Parses MBOX format messages, such as Thunderbird.
- EXIF: Extracts geolocation and camera information from JPEG files.
- File Type Sorting: Group files by their type to find all images or documents.
- Media Playback: View videos and images in the application and do not require an external viewer.
- Thumbnail viewer: Displays thumbnail of images to help quick view pictures.
- Robust File System Analysis: Support for common file systems, including NTFS, FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2, and UFS from The Sleuth Kit.
- Hash Set Filtering: Filter out known good files using NSRL and flag known bad files using custom hash sets in HashKeeper, md5sum, and EnCase formats.
- Tags: Tag files with arbitrary tag names, such as 'bookmark' or 'suspicious', and add comments.
- Unicode Strings Extraction: Extracts strings from unallocated space and unknown file types in many languages (Arabic, Chinese, Japanese, etc.).
- File Type Detection based on signatures and extension mismatch detection.
- Interesting Files Module will flag files and folders based on name and path.
- Android Support: Extracts data from SMS, call logs, contacts, Tango, Words with Friends, and more
- Input format: analyzes disk images, local drives, or a folder of local files. Disk images can be in either raw/dd or E01 format.
- Reporting: HTML, XLS, and Body file reports are available. An investigator can generate more than one report at a time and either edit one of the existing or create a new reporting module to customize the behavior for their specific needs.

B. *Encase Forensic version 8*

Encase is a commercial forensic tool developed by Guidance Software with its first release in 1998. OpenText™ (NASDAQ: OTEX) (TSX: OTEX), a global leader in Enterprise Information Management (EIM), has acquired Guidance Software in Sept 2017. Encase claimed to be a court-proven solution built for deep-level digital forensic investigation, powerful processing, and integrated investigation workflows with flexible reporting options. [13]



	Name	Re Re Fol Ign	File Ext	Logical Size	Cate
□ 1	$AttrDef			2,560	Unknown
□ 2	$BadClus			0	Unknown
□ 3	$BadClus·$Bad			32,209,104,8...	Unknown
□ 4	$Bitmap			982,944	Unknown
□ 5	$Boot			8,192	Unknown
□ 6	$Extend			656	Folder
□ 7	$LogFile			43,941,888	Unknown
□ 8	$MFT			241,958,912	Unknown
□ 9	$MFTMirr			4,096	Unknown
□ 10	$Recycle.Bin		Bin	4,096	Windows

Hex	UInt32	Int32
00000060	96	96

Figure 2. Encase Forensic acquires data from a wide variety of devices.

Below are feature list of Encase: [13]

- Enhanced indexing engine: Empowers investigators to conduct investigations with powerful processing speeds, advanced index searching, comprehensive language support, and optimized performance
- Easy reporting: Provides customizable templates to help examiners create compelling, easy to read, professional reports that can be shared for every case
- Extensibility: Offers extensibility through EnScripts, which are automated code commands that streamline and automate tasks and extend the capabilities of EnCase Forensic to help the examiners complete investigations more efficiently
- Workflow automation: Delivers automated investigation workflows so examiners can easily navigate through EnCase Forensic to enhance how they uncover evidence
- Updated encryption support: Provides encryption support for Microsoft® Windows® 10 Bitlocker XTS-AES, Dell® Data Protection 8.17 and Symantec™ PGP v10.3; investigators can acquire encrypted evidence without worry about data corruption, damage, or unnecessary delays
- Apple File System (APFS) support: Supports APFS, the file system used in the Apple High Sierra operating system (macOS® 10.13), helping investigators conduct targeted data collections from APFS and send the output as an EnCase logical evidence file
- Volume shadow copy capabilities: Examines Volume Shadow Snapshot (VSS) backups, also known as volume shadow copies, generated by Microsoft Windows, allowing investigators to recover deleted or modified files, as well as full volumes and learn what may have taken place on a system before the investigation

C. *Forensic Tool Kit (FTK) version 6*

FTK is a commercial forensic tool developed by Access Data. FTK can quickly locate evidence and forensically collect and analyzes any digital device from multiple devices. Known for its intuitive interface, email analysis, customizable data views, processing speeds, and stability. FTK manages massive data sets, separates critical data from trivial details, and protects digital information while complying with regulations. [14]

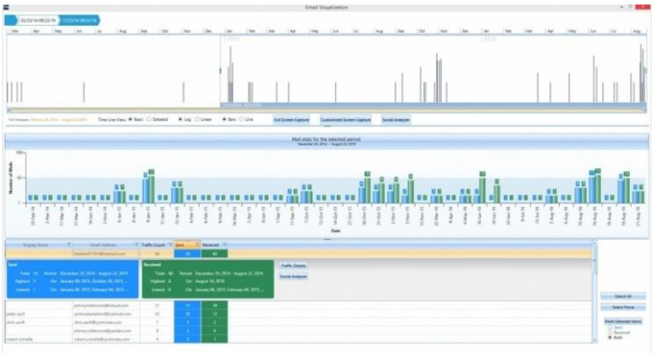


Figure 3. FTK Key Feature

- Database Driven: All digital evidence is stored in one case database, All data is stored securely and centrally, allowing your teams to use the same data. This reduces the cost and complexity of creating multiple data sets.
- Unmatched Processing Speed: provide the fastest, most accurate, and consistent processing with distributed processing.
- True multithread/multi-core processing: FTK used 100 percent of its hardware resources and is more reliable in the event of hardware or software glitches.
- Faster Searching with Consistent Results: Indexing is done upfront, so filtering and searching are faster. FTK offers the flexibility to perform multi-pass data review and change indexing options without reprocessing your data and a shared index file which eliminates the need to recreate or duplicate the file.
- Remote Machine Analysis: users can preview, acquire and analyze evidence remotely from computers on your network.
- Visualization: Automatically construct timelines and graphically illustrate relationships among parties of interest in a case.
- Internet Browser and Web-Based Email Evidence: Web browsing caches store records of sites a suspect has visited, web-based emails may help to prove intent or correlate other events and instant message conversations or social media sites can contain evidence.
- Password Cracking and Recovery: Unlock files when you don't know the password with market-leading decryption password cracking and recovery.
- Explicit Image Detection (EID): Image detection technology recognizes flesh tones and auto-identifies more than 30,000 potentially pornographic images.
- Malware Triage & Analysis: Cerberus is an automated malware triage platform solution designed to integrate with FTK.
- Third-Party Integrations: Gain access to nearly 200 mobile parsers with the Belkasoft® add-on connector. Using the C# API,

V. PROPOSE WORK

Below is a comparative analysis parameters map to four phases of the digital forensic process.

Phases	Comparative Parameters
Acquisition	Bitstream backup Hash calculation of backup copy Remote acquisition
Recovery	Identify deleted files Recover deleted files Identify encrypted file Decrypt file Decrypt file system Password recovery Email recovery

Phases	Comparative Parameters
Analysis	File Type Detection
	Timeline Analysis
	Keyword Search
	Web Artifacts
	Registry Analysis
	LNK File Analysis
	Email Analysis
	Extracts EXIF
	Media Playback
	Log of investigation activity
	Show file created time
	Show file modified time
	Show file accessed time
	Most recently used
	Identify registry file
	File Carving
	Search Unallocated Space
	Identify slack spaces
	Repeatability
	File System Analysis
	Apple File System Analysis
	Contraband image recognition
Presentation	Documentation
	Reporting
System	Support Windows OS
	Support Linux OS
	User friendly
	License
	Cost
	Multi-Thread
	Multi-user
	Extensible through plugin
	Forensic Process Workflow
	Remote Machine Analysis
	Distributed forensic in the cluster

Table 1. Comparative Parameters

VI. Explanation of Comparative Parameters

Parameters	Explanation
Bitstream backup	Backup of all areas of a computer hard disk drive or another type of storage media. Such a backup exactly replicates all sectors on a given storage device.
Hash calculation of backup copy	It is used for assuring the integrity of the evidence.
Remote acquisition	Remotely gathering digital evidence through a secure, verifiable client/server imaging architecture.
Identify deleted files	Whether the tool can identify the files which are deleted from the drive or the system?
Recover deleted files	Whether the tool able of recovering the files which were permanently deleted?
Identify encrypted file	Whether the tool able to identify the files which are encrypted?
Decrypt file	Whether the tool has a decryption engine to decrypt the encrypted file.
Decrypt file system	Whether the tool has a decryption engine to decrypt the encrypted file system.
Password recovery	Whether the tool able to automate password recovery?
Email recovery	Whether the tool able to recover email from Outlook/Thunderbolt
File Type Detection	Whether the tool able to identify file type correctly?
Timeline Analysis	Whether the tool able to provide a line graph for the activities happened recently in the evidence system?
Keyword Search	Whether the tool able to find files that mention specific terms and find regular expression patterns?
Web Artifacts	Whether the tool able to extract web activity from common browsers to help identify user activity?
Registry Analysis	Whether the tool able to identify recently accessed documents and USB devices?
LNK File Analysis	Whether the tool able to identify shortcuts and access documents?
Email Analysis	Whether the tool able to extract and analyze Outlook/Thunderbolt or any email client?
Extracts EXIF	Whether the tool able to extract geolocation and camera information from JPEG files?
Media Playback	Whether the tool able to view videos and images in the application and not require an external viewer?
Log of investigation activity	Whether the tool able to create and maintain the case logs of investigation activity?
Show file created time	Does the tool show the created time for any file?
Show file modified time	Does the tool show the modified time of any file?
Show file accessed time	Does the tool show the last accessed time for any file?
Most recently used	Does the tool show information about the tools and software which were run on the system recently?
Identify registry file	Does the tool identify and analyze the registry files for getting system information?
File Carving	Whether the tool able to search the file based on the content rather than the Metadata?
Search Unallocated Space	Whether the tool can locate the unallocated space?
Identify slack spaces	Whether the tool able to identify slack spaces in the given image?
Repeatability	Whether the tool able to provide similar results every time for the same data set and same working environment?

Parameters	Explanation
File System Analysis	Whether the tool able to analyze common File Systems e.g. FAT 12, FAT 16, FAT 32, NTFS, EXT2, EXT 3?
Apple File System Analysis	Whether the tool able to analyze Apple File System?
Contraband image recognition	Whether the tool able to recognize contraband images?
Documentation	Whether the tool record forensic activity in the document?
Reporting	Whether the tool produce a presentable report that can be used in court?
Support Windows OS	Whether the tool able to run in Windows OS?
Support Linux OS	Whether the tool able to run in Linux OS?
User friendly	Whether the tool is user-friendly, the GUI is intuitive?
License	Whether the tool requires a license to install or use?
Cost	How much does it cost to own the tool?
Multi-Thread	Does the tool able to process in multi-thread mode?
Multi-user	Whether the tool support concurrent user to access and perform the forensic analysis?
Extensible through plugin	Whether the tool is extensible through the third-party module and has API?
Forensic Process Workflow	Whether the tool provides an easy wizard workflow for each digital forensic process?
Remote Machine Analysis	Whether the investigators can preview, acquire and analyze evidence remotely from computers on your network?
Distributed forensic in the cloud cluster	Whether the tool able to perform forensics processing tasks in parallel in the cloud environment?

Table 2. Comparative Parameters

VII. Comparisons Between Forensic Tools

Comparison base on above comparative analysis parameters.

● – fully support, ▲ – partial support, ○ – no support

Comparative Parameters	Autopsy	Encase	FTK
Bitstream backup	●	●	●
Hash calculation of backup copy	●	●	●
Remote acquisition	▲ Partial support using dd	●	●
Identify deleted files	●	●	●
Recover deleted files	●	●	●
Identify encrypted file	●	●	●
Decrypt file	▲	●	●
Decrypt file system	▲	●	●
Password recovery	▲	●	●
Email recovery	●	●	●
File Type Detection	●	●	●
Timeline Analysis	●	●	●
Keyword Search	●	●	●
Web Artifacts	●	●	●
Registry Analysis	●	●	●
LNK File Analysis	●	●	●
Email Analysis	●	●	●
Extracts EXIF	●	●	●
Media Playback	●	●	○
Log of investigation activity	●	●	●
Show file created time	●	●	●
Show file modified time	●	●	●
Show file accessed time	●	●	●
Most recently used	●	●	●
Identify registry file	●	●	●
File Carving	●	●	●
Search Unallocated Space	●	●	●
Identify slack spaces	●	●	●
Repeatability	●	●	●
File System Analysis	●	●	●
Apple File System Analysis	○	●	○
Contraband image recognition	●	●	●
Documentation	●	●	●
Reporting	●	●	●
Support Windows OS	●	●	●
Support Linux OS	●	○	●
User friendly	●	●	●
License	Open-source	Propriety	Propriety
Cost	Free	High	High
Multi-Thread	●	●	●
Multi-user	●	○	●
Extensible through plugin	●	●	●
Forensic Process Workflow	●	●	●
Remote Machine Analysis	●	●	●

Comparative Parameters	Autopsy	Encase	FTK
Distributed forensic in the cluster	●	○	○

Table 3. Comparison between Forensic Tools

VIII. Discussion

Encase Forensic offers the most complete digital forensic tool in one single package, with its ability to support Apple File System analysis will benefit the investigator to analyze more suspected devices as pieces of evidence of justice. Investigators can gather more encrypted evidence for analysis with Encase Forensic extensive encryption support to decrypt the encrypted file system. EnCase has maintained its reputation as the gold standard in criminal investigations and was named the Best Computer Forensic Solution for eight consecutive years by SC Magazine.[16] I would recommend Encase Forensic for public investigation which covers the broader type of acquisition devices and their reputation in acceptance in court.

FTK is more robust when dealing with a big investigation with a lot of digital evidence because all evidence is stored in a centralized database where a team of investigators can work on the same dataset at the same time without recreating new digital evidence. FTK forensic features match closely with Encase forensic, except for Apple file system analysis where Encase has the advantage. I would recommend FTK forensic for public and private investigation because of stability and robustness in recovery and analysis.

I would recommend Autopsy for private investigation because of cost concerns. The intuitive GUI and simple digital forensic process workflow will benefit investigators. There is a lot of open-source ingest module available to further enhance Autopsy capability in forensic analysis.

IX. Conclusion

With the rapid rising in cybercrime, and more digital devices being involved in the crime, acquisition of all digital evidence become a time-consuming task.

Although all three forensic tools have the four digital forensic processes built in their software. They have slights different in their product offering.

Future work may include acquisition in a crime scene that real-time stream capture and analysis can cut short the time to acquire all the one by one. Also, utilizing distributed computing to perform digital forensics using a cloud platform which will reduce processing time and storage costs.

X. References

[1] Bill Nelson, Amelia Phillips,Christopher Steuart, Guide to Computer Forensics and Investigations: Processing Digital Evidence, Fifth Edition

[2] Varsha Karbhari Sanap, Vanita Mane, Comparative Study and Simulation of Digital Forensic Tools – International Journal of Computer Applications (0975 – 8887).

[3] Neelam Maurya, Jyoti Awasthi, Raghvendra Pratap Singh, Dr. Abhishek Vaish, Analysis of Open Source and Proprietary Source Digital Forensic Tools, International Journal of Advanced Engineering and Global Technology, Vol-03, Issue-07, July 2015.

[4] Mayank Lovanshi, Pratosh Bansal, Comparative Study of Digital Forensic Tools, Springer Nature Singapore Pte Ltd. 2019. https://doi.org/10.1007/978-981-13-6351-1_15

[5] Nilakshi Jain, Dr. Dhananjay R Kalbande, A Comparative Study based Digital Forensic Tool: Complete Automated Tool, DOI: 10.5769/J201401003 or http://dx.doi.org/10.5769/J201401003.

[6] K.K. Arthur, H.S. Venter, AN INVESTIGATION INTO COMPUTER FORENSIC TOOLS, Information and Computer Security Architectures (ICSA) Research Group.

[7] Megh Shah, David Paradise, Tool Comparison, http://www.lcdi.champlin.edu/.

[8] Adam Cervellone, Robert Price Jr., Joshua Brunty, Terry Fenger, A Comparison of Computer Forensic Tools: An Open-Source Evaluation, https://www.marshall.edu/forensics/files/CERVELLONEADAM_FinalResearchPaper-8-7-2015_-1.pdf.

[9] Michael Hendrik Sonnekus, A COMPARISON OF OPEN SOURCE AND PROPRIETARY DIGITAL FORENSIC SOFTWARE, https://research.ict.ru.ac.za/SNRG/Theses/Sonnekus%202014.pdf

[10] Autopsy, https://www.sleuthkit.org/index.php

[11] Autopsy intuitive, https://www.sleuthkit.org/autopsy/intuitive.php

[12] Autopsy features, https://www.sleuthkit.org/autopsy/features.php

[13] OpenText EnCase Forensic Product overview, https://www.guidancesoftware.com/docs/default-source/document-library/product-brief/encase-forensic-product-overview.pdf?sfvrsn=761867a2_38

[14] FTK overview, https://accessdata.com/assets/pdfs/FTK-6.3-WEB.pdf

[15] Forensic Tool kit | AccessData, https://accessdata.com/products-services/forensic-toolkit-ftk