International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Comparative Analysis of Digital Forensic Extraction Tools

Varun H M[1], Dr. Uma Rani Chellapandy[2], Srividya B G[1]

[1]Student, [2]Associate Professor,
[1,2]Department of MCA, Jain Deemed-to-be University, Bengaluru, Karnataka, India

ABSTRACT

Computer forensics: Process collecting and examining information present in digital format in civil, criminal, or administrative proceedings for use as evidence. It is also a from data recovery, which involves the recovery of data from a system that has been erased by error or lost during a server crash. Tools are designed to extract evidence from the computer and it is the role of the investigator to check whether the crime or policy violation has been committed by the suspect. Investigators use various kinds of tools based on the area or the kind of information which is lost such as digital data, network compromise, cyber breach, web data, email and many more.

How to cite this paper: Varun H M | Dr. Uma Rani Chellapandy | Srividya B G "Comparative Analysis of Digital Forensic Extraction Tools" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.487-489, URL: www.ijtsrd.com/papers/ijtsrd37980.pdf

IJTSRD37980

1. INTRODUCTION

A computer forensic analysis seeks to recover data from com puters confiscated in criminal investigations as evidence. Investigators follow a methodological approach to evaluate the evidence which might be used to raise a trial at the court. These steps include:

- **Acquisition:** First step of investigation where a copy of the original data is made in order to preserve the integrity and protect it from being damaged. The testing is not made on the original drive. There are many sub-functions such as physical data copy, logical data copy, data acquisition format, command-line acquisition, GUI acquisition, remote acquisition and verification.
- **Validation and discrimination:** Validation is ensuring the integrity of copied data. Discrimination which involves sorting and searching through all investigation data. The sub-functions under this process are hashing, filtering and analysing file headers.
- **Extraction:** Its function is the recovery task. Recovering data is the first step in analysing an investigation's data. The following sub-functions of extraction are used in investigations: Data viewing, keyword searching, decompressing, carving, decrypting and bookmarking
- **Reconstruction:** Process of re-creating a suspect drive to show what happened during a crime or an incident. These are the sub-functions of reconstruction: Disk-to-disk copy, Image-to-disk copy, Partition-to-partition copy and Image-to-partition copy
- **Reporting:** The final stage of investigation where all the details and findings is being documented. These are the sub-functions of the reporting function: Log reports and Report generator.

Forensic tools are available in many types, hence the exact tool choice relies on where, when and how it has to be used.

A comparison table of functions, sub-functions, and vendor items is useful for helping to decide which computer forensics device to purchase or use. Cross-reference functions and distributor product sub-functions make it easier to find the computer forensics device that better suits the investigators' needs.

In this paper different types of forensic tools are compared where description and features of each tool is explained followed by a comparison chart. The best tool among them can be selected by the user.

2. INVESTIGATION TOOLS

A. CAINE (COMPUTER AIDED INVESTIGATIVE ENVIRONMENT)

It is an open-source tool required to perform the digital forensic investigation. It is used by law authorization, corporate and military inspectors to examine the action which occurred on a PC. It is integrated with various digital forensic tool such as:

The Sleuth Kit	Fsstat	JpegView
Autopsy	MWSnap	QuickHash
Win Audit	Wireshark	NBTempoW
PhotoRec	Arsenal Image Mounter	USB Write Protector
RegRipper	FTK Imager	Windows File Analyzer
Tinfoleak	Hex Editor	Afflib

It is a user-friendly GUI interface
Supported platform: windows Linux Unix

Contains tools which performs digital forensic investigate process (preservation, collection, examination and analysis)

FEATURES:
- Acquire live image from a hard drive
- Perform data acquisition
- Analyse electronic evidence
- Write Blocker Technology: Device or disk is not compromised or damaged and ach host is mounted with a read-only software write blocker which can be unlocked using mounter
- Compatible with the caja web browser
- The "save as evidence" script: allows to store metadata about the device and investigator's comment can be enabled

B. X-WAYS FORENSICS

An application for law enforcement, intelligence agency and t he private sector to conduct investigations, document analysis and report generation.

Supported platform: windows

It is meant for investigators who are specialized in:
Accounting, construction rules, money laundering, corruption, murder and child pornography

Mainly used by:
Research analysts, officers, attorneys, paralegals, judges, internal and external auditors

FEATURES:
- Disk, file and RAM Editor
- Directory Browser for FAT, NTFS, Ext2/Ext3, ReiserFS, CDFS/ISO9660, UDF
- Disk Cloning
- Data and partition recovery
- Disk Wiping
- File Slack Capturing
- Unused Space Capturing
- Media Details Report
- Simultaneous Search
- PhotoDNA hashing
- Skin colour detection
- Create skeleton, snippet and cleansed images
- Can read and write EnCase images

C. THE SLEUTH KIT (+AUTOPSY)

Is an open-source command-line based application that allow the investigator to analyse disk images and retrieve data from them. It is also used in Autopsy which is a GUI based software which functions in a similar manner. Autopsy provides facilities to find add-on and develop custom modules

Tools integrated with Sleuth Kit includes:
- **ils** : contains metadata
- **blkls** : lists data blocks in a file system
- **fls**: displays allocated and unallocated file names
- **fsstat**: shows statistical information about an image or storage medium.
- **ffind**: finds file names that relate to a specific metadata
- **mactime**: maintains a timeline of files based upon the MAC times.

FEATURES:

Extensible	Multiple Users	Email Analysis
Centralised	Timeline analysis	File type sorting
Ease of Use	Keyword search	Thumbnail Viewer

D. XPLICO

Xplico is a network forensics analysis tool (NFAT), which sniffs network traffic to capture data from various applications such as email, VOIP call etc.

It supports various protocols such as: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv4, IPv6.

FEATURES:
- Port Independent Protocol Identification (PIPI)
- Multithreading
- Output data in SQLite or MySQL database
- Contains an XML file that uniquely identifies the traffic flow
- Maintains a pcap file containing the reassembled data
- No size limit on incoming data
- Modularity

Xplico is installed in: Kali Linux, BackTrack, DEFT, Security Onion, Matriux, BackBox and CERT Linux Forensics Tools Repository

E. UFED (UNIVERSAL FORENSIC EXTRACTION DEVICE)

It is a system which has the ability to extract physical and logical data from mobile devices and recover lost data, decrypt password and other related information.

The UFED has an integrated Subscriber Identity Module (SIM) reader.

It can capture, decode, parse and analyse contacts, multimedi a content, SMS and MMS, call logs, ESN, IMEI and SIM location information from non-volatile memory and volatile storage.

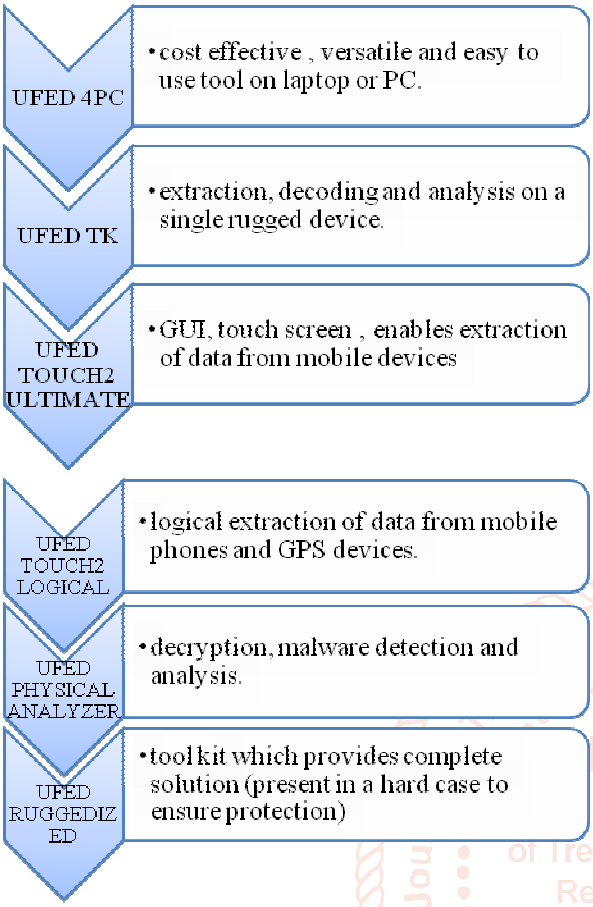
Cellular protocols supported:
- CDMA
- GSM
- IDEN
- TDMA

Operating systems supported:
- iOS
- Android
- BlackBerry
- Symbian
- Windows

It can penetrate the hardest locks to obtain evidence more easily with high accuracy.

FEATURES:
- Break any barrier
- Find hidden evidence
- Solve cases faster
- Unlock devices with ease
- Extract more data

- Convert encrypted data to actionable intelligence
- Unify data for a more comprehensive review
- Translate content with Cellebrite Smart Translator
- Create and share customized reports



3. COMPARISION TABLE:

Function	CAINE	X WAYS FORENSICS	SELUTH KIT (AUTOSPY)	XPLICO	UFED
ACQUISITION					
Physical data copy	√	√	√		√
Logical data copy	√		√	√	√
Data acquisition format	√	√	√	√	√
Command line process			√	√	
GUI process	√	√	√	√	√
Remote acquisition	√	√			
Verification	√	√	√	√	√
VALIDATION AND DISCRIMINATION					
Hashing	√	√	√		√
Filtering	√	√	√	√	√
Analysing file header	√	√	√	√	√
EXTRACTION					
Data viewing	√	√	√		√
Keyword searching	√	√	√	√	√
Decompressing		√			
Carving		√	√		√
Decryption	√	√	√	√	√
Bookmarking	√	√	√	√	√
REPORTING					
Log reports	√	√	√	√	√
Report generation	√	√	√	√	√
AUTOMATION FEATURE					
Scripting language	√				√

4. FUTURE SCOPE

Investigating the cybercrime is not an easy task. It requires the right expertise along with multiple tools and techniques to quickly and productively leap into the digital crime scene. Once this is available, a proper analysis of data and investigate the cause, and discover the attackers behind the cybercrime.

Cyber forensics at the government level will be complicated in the future. To hunt down cyber criminals, governments will need to turn more to their national security organizations. They will also need to discover anti-forensic software and techniques to keep their activities and assets confidential.

Information security standards such as ISO27001 and ITIL will be implemented more in corporate organizations. Only few companies will be able to afford the cost of compliance implementation. Hence, it is important for the companies to have precise incident response methods and related cyber forensic investigation functions.

5. CONCLUSION

In this paper the differences between some forensic tools is listed along with a comparison chart. There are many tools with certain similarities and differences which is available. Selecting the right tool based on the criteria depends on the investigator or the user. The tool which is chosen should ensure the integrity of the acquired information and should be able to generate reports which is useful for further references.

6. REFERENCES

[1] http://www.x-ways.net/winhex/manual.pdf

[2] https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins

[3] https://www.caine-live.net

[4] https://www.teeltech.com/mobile-device-forensic-tools/cellebrite

[5] https://resources.infosecinstitute.com

[6] Copy of Guide to Computer Forensics and Investigations-Bill Nelson (TEXT BOOK)