Forensic Tools used in Digital Crime Investigation

KEYWORDS: Digital Forensics, Open Source Tools, Proprietary Tools

Mayur Patankar
Student, Institute of Forensic Science, Mumbai-400032

*** Deepika Bhandari**
Assistant Professor (Forensic Science), Institute of Forensic Science, Mumbai-400032
* Corresponding Author

ABSTRACT *Digital Forensics deals with the studies of Computer and memory Forensics, Mobile Forensics, Network Forensics and data recovery. Different Cyber and Digital forensic tools can make the process of investigation easier, accurate and precise. Tools can be software or hardware or a combination of both which can be used in the investigation for information gathering, analysis, report making and giving a direction to the investigation, finally identifying certain aspects that are difficult for a human to conduct. These tools can be either open Source or Proprietary. Some tools come with a hardware as well as software package and some might just be an application. Some of the Forensic Tools may require an active internet connection whereas others can work in offline mode as well. The type of the crime occurred will decide the appropriate tool and these tools used individually or along with other tools can help in a systematic and effective analysis of evidences and lead to an appropriate conclusion. In this research paper we are giving a comprehensive list and explanation of the various Tools that can be useful for Digital Forensic investigation.*

Introduction

Abacus (Computer) forensic is the plea of scientifically proven methods to put, enterprise, to pieces, and to consider digital say-so to furnish a trustworthy in compliance of cybercrime activities.To successfully solve these types of crimes we need Digital Forensic tools. There is a basic, inherent process to computer forensics which can be outlined as Following:-

- Identification: - It is the process of identifying the crimes and the related data as an evidence for the investigation.
- Acquisition: - It is the process of acquiring or gathering information and evidence. Its goal is to preserve the evidence.
- Analysis: - This is the process in which the data obtained is analyzed. Search for relevant data and link that can help in finding the person who has committed it.
- Presentation: - it provides a clear understanding of what occurred to obtain the evidence, and what the evidence represents.

In crime scene investigation we look for evidences, i.e. Corpus Delicti, crime scene and other evidences that may be found. It is important to know that the evidences obtained in the cybercrime will not always be in the physical state as we get in other crimes like that of arson or assault or any other crime. The evidences obtained can be physical in state or can also be digital. Digital evidence is present in the form of patterns of bits and bytes. This pattern can be an evidence itself or can link to a specific evidence that can help in the investigation. The digital evidences are not accessible by just opening the system there are certain digital procedures that has to be followed to access them. Now this crucial evidence can be retrieved with the help of certain tools that will access it, note it, create a report and then will display it to the investigator all by itself. Not only they do this but they also help in maintaining the integrity of the evidences or the acquired data. This is done by cloning the evidence and running different analysis schemes on the cloned data and not on the actual data that may destroy the evidence during the process of analysis.

These forensic tools not just document and preserve the evidences but will also give the relationship of that system with other systems over a network. They give a report of the network status of the system. Also they provide data recovery options in cases where the perpetrator has tried to delete some crucial information so as to hide its presence. They provide other services like image formation, history checking of the browser, login and logoff details, IP address information and much more. The Use of appropriate tools will prompt distinguishing proof, gathering, dissection, acceptance, translation, protection, documentation and presentation of electronic confirmation derived from digital source for the purpose of facilitating or furthering the restoration of actions found to be unlawful. Thus proper tools will help us get accurate evidences and give us crucial information about the crime.

The Digital forensic tools are categorized as follows:-

1) Computer and memory Forensic tools: - Computer forensic tools are used to acquire data from a system or a computer. They are used to acquire registries and other encrypted data from the computer. Whereas memory forensic tools are used to acquire and analyze the computer's Volatile Memory (RAM). They are used to preserve evidence in the memory that is lost when the system is shutdown. They directly examine the Operating system and other running software in the memory. The various platforms wherein these tools works are Windows, UNIX, Linux, DOS, MAC.

a. Windows: - It is a series of Graphical interface Operating Systems, developed and marketed and sold by Microsoft.
b. UNIX: - UNIX is a multitasking, multi-client PC working framework that exists in numerous variants. UNIX was made using C- programming language.
c. Linux: - it is a UNIX-like computer operating system assembled under the model of free and open source software. The users can modify, develop and sell its own version of the OS for his own benefit.
d. DOS: - It is an operating system that provides the abstraction and management of secondary storage devices and the information on them.
e. MAC OS: - It is a series of graphical user interface based operating systems that is developed by the Apple Inc. for their Macintosh line of computers.

2) Mobile Forensic tools: - Mobile forensic instruments constitute of both hardware and software peripherals. Mobile

phones come with a diverse range of connectors; the hardware devices support a number of different cables and perform the same role as a write blocker in computer devices. Mobile Devices contain important personal data that can be used as evidence. Data acquired from mobile phones continues to be used as evidence in criminal, civil and even high profile cases. The mobile operating systems that are investigated using these tools are Android, IOS, Blackberry OS and Windows Phone etc.

a. Android: - It is from Google Inc. Android is an Open source operating system.
b. Blackberry: - It is a closed source and proprietary OS.
c. iOS: - It is from Apple Inc. It is closed source and proprietary. The apple iPhone, iPod touch and iPad all use iOS.
d. Windows Phone: - It is from Microsoft and is closed source and proprietary. Windows phone devices are made predominantly by Nokia, HTC, Huawei, Samsung and other companies.

3) Network Forensic Tools: - Network forensic tools consists of multiple monitors that can be installed at different points in the network and used for distributed network surveillance. These network monitoring tools integrate data from the different monitors and provide a complete and comprehensive view of the network activity.

Types of Forensic Digital Tools:-
These tools can be open source or proprietary tools.

1) Open Source tools:- Open Source tools is a phrase used to mean a program or a tool that performs an extremely particular assignment, in which the source code is candidly distributed for use and /or modification from its original design, free of charge. They are typically created as a collaborative effort in which programmers improve upon the code and share the changes within the community, and it is usually available at no charge under a license defined by the Open source initiative.
2) Proprietary tools: - Proprietary tools are those tools or programs that are charged by the vendors. These software's have restriction on any blending of the utilization, adjustment, replicating or circulating changed forms of the product. They may also be called as Closed-Source Software.

OPEN SOURCE TOOLS:-
Open Source Forensic tools are those tools that are available free of cost. Many of the software perform various different tasks. The source code of these tools is openly published for use or modification by any of the user or organization.

Table 1:- Open Source Computer and memory forensic tools

Name	Link	Platform	Description
Categorizer 4 pictures	http://www.freedownloadscenter.com/M http://www.ultimedia_and_Graphics/Graphics_Viewers/Categorizer_Download.html	Windows	It makes it possible to quickly and efficiently classify pictures that have been forensically extracted for review. It is a combination of Forensic Enscripts and a standalone Windows application.
Volatility	http://www.code.google.com/p/volatility/ downloads/list	Windows	It is a completely open collection of tools, implemented in python, deals with the extraction of digital artifacts from volatile memory (RAM).
Ftimes	http://www.ftimes.sourceforge.net/FTimes /index.shtml	Windows and Unix	It is a system baseline and evidence collection tool. It gathers and develops topographical information and attributes about specified directories and files in a manner conducive to intrusion and forensic analysis.
Libewf	http://www.sourceforge.net/projects/libewf/	Windows and Unix	It is a library for support of the Expert Witness Compression Format (EWF), it supports both the SMART (EWF-S01) and EnCase (EWF-E01) format. It allows you to read and write EWF files. Recent versions also support the LEV (EWF-L01) format.
Live view	http://www.liveview.sourceforge.net/	Windows	It is a java based graphical forensics tool that creates a VMware virtual machine out of a raw disk image or physical disk.
Psloggedon	http://www.technet.microsoft.com/en-us/ sysinternals/bb897545.aspx	Windows	It is an applet that displays both the locally logged on users and users logged on via resources for either the local computer, or a remote one.
TULP2G	http://www.sourceforge.net/projects/tulp2g/	Windows	It is a forensic software framework developed to make it easy to extract and decode data from the digital devices.
Webjob	http://www.webjob.sourceforge.net/WebJob/index.shtml	Windows	It is useful in incident response and intrusion analysis as it provides a mechanism to run good diagnostic programs on a potentially compromised system .
Pyflag	http://www.pyflag.net/	Windows	It is an acronym for "Forensic and log analysis GUI (Graphical User Interface)", written for analysis of various log file types and network traffic analysis. It is also used for forensic analysis of Disk images.
Test Disk	http://www.cg-security.org/wiki/TestDisk_Download	Windows	This is tool is used to check and undelete partition in the system. Operating system support is comprehensive, with precompiled binaries available for many popular types.
The sleuth kit	http://www.sleuthkit.org/sleuthkit/	Windows	The tools allow for the recovery and analysis of deleted content, hash database lookups, sorting by file type, and timelines of file activity.
Explore2fs	http://www.chrysocome.net/explore2fs	Windows	It allows to view the contents of an Ext2FS partition from Windows.

Volume : 4 | Issue : 5 | May 2014 | ISSN - 2249-555X

Quick hash	http://www.sourceforge.net/projects/quick-hash/	Windows and Linux	It enables the rapid selection and subsequent MD5, SHA, SHA256, SHA512 hashing of files, either individually or throughout a folder structure.
Cuckoo Sandbox	http://www.cuckoosandbox.org/download.html	Windows and Unix	It is a malware analysis system. It is mostly used to analyze Windows executables, DLL files, PDF documents, office documents, PHP scripts and almost anything else.
Galleta	http://wwwfoundstone.com/us/resources/proddesc/galleta.htm	Windows	This tool examines the contents of the cookie file. The output is given in a table format.
Automated image and restore (AIR)	http://www.sourceforge.net/projects/air-imager/	Unix	AIR is a GUI front-end to dd/dcfldd designed for easily creating forensic bit images.
Digital Forensics Framework	http://www.digital-forensic.org/download/	Unix	It is used for reconstructing volumes and file systems with recovery of deleted data and unallocated area. It also extracts metadata.
The coroners toolkit (TCT)	http://www.porcupine.org/forensics/tct.html	Unix	The software assists in digital forensic analysis and analysis of and data recovery.
Autopsy Forensic Browser	http://www.sleuthkit.org/autopsy/	Unix	It allows to view deleted and allocated files, perform keyword searches, and create timelines of file activity.
Disktype	http://www.disktype.sourceforge.net/	Unix	It detects the content format of the disk or disk image. It knows about common file systems, partition tables and boot codes.
Winhex	http://www.x-ways.net/winhex/index-m.html	Windows	It is used to inspect and edit all kinds of files, recovers deleted files and lost data from hard drives with corrupt file system or from digital camera cards.
Chkrootkit	http://www.chkrootkit.org/	Unix	Chkrootkit is a tool to locally check for signs of a rootkit.
DHash	http://www.deftlinux.net/2008/09/08/dhash-11/	Unix	It is a very fast tool to compute and verify MD5, SHA1 and SFV Hash, with a GUI and a useful progress bar.
Unhide	http://www.unhide-forensics.info/	Unix	It is a forensic tool to find hidden processes and TCP/UDP (Transmission control protocol/user datagram protocol) ports by rootkits / LKM's or by another hiding techniques.
Active ports	http://www.majorgeeks.com/files/details/active_ports.html	Windows	This tool shows all open TCP/IP and UDP ports on windows computers and maps them to the parent application.
Advanced email extractor	http://www.emmalabs.com/aee/	Windows	It extracts email addresses from web pages on the internet and from HTML (hypertext markup language) and text files on local disks.
CMOS Recovery tools	http://www.en.kioskea.net/download/download-19507-cmos-password-recovery-tools-5-0	Windows and DOS	It recovers CMOS (complementary metal-oxide semiconductor) passwords. It supports almost all BIOS.
FinalEmail	http://www.finalemail.findmysoft.com/	Windows	It recovers the email database file and locates lost e-mails that do not have data location information associated with them.
SANS SIFT	http://www.digital-forensics.sans.org/community/downloads	Unix	It is an Ubuntu based live CD. It supports analysis of Expert Witness Format, Advanced forensic format and Raw (dd) Forensic format.
ProDiscover Basics	http://www.techpathways.com	Windows	It allows to image, analyze and report on evidence found on the drive. Specific data can be searched using this tool provided it is specified.
FTK Imager	http://www.accessdata.com/support/product-downloads	Windows	It is a data preview and imaging tool that allows to examine files and folders on local hard drives, network drives, CDs/DVDs, and review the content of forensic images or memory dumps. It can also create hash files.
CAINE	http://www.caine-live.net/page5/page5.html	Unix	Its features include a very user-friendly GUI, semi-automated report creation and tools for mobile forensics, Network forensics, data recovery and more.
DEFT	http://www.deftlinux.net/download/	Unix	It aims to help with Incident response, cyber intelligence and computer forensic scenarios. It also contains tools for Mobile Forensics, data recovering and Hashing.

Volume : 4 | Issue : 5 | May 2014 | ISSN - 2249-555X

Table 2:- Open Source Mobile forensics tools

Name	Link	Platform	Description
Oxygen Forensic Suite	http://www.oxygen-forensic.com/en/download/freeware	Windows	It forensically analyzes mobile phones. The software does not change any data on the phone. Oxygen runs on any version of the Windows Operating system.
Iphone analyzer	http://www.ipbackupanalyzer.com/downloads/windows-exe-build/copy-of-windows-exe-build-032013-3	Windows	It is a utility designed to easily browse through the backup folder of an iPhone. Read configuration files, browse archives, lurk into databases and so on.
Whatsapp xtract	http://www.code.google.com/p/hotoloti/downloads/list	Windows	This tool helps to recover the WhatsApp database from the phone. It also helps to read the configuration of the WhatsApp. It is possible to decrypt the encrypted data using this software.
Skype Xtractor	http://www.sourceforge.net/projects/skypextractor/	Windows	This tool takes the folder where the audio files are stored as input, copies the file in a temp folder and adds a header and converts them to another format and saves them to the specified folder, thus creating a backup.
Sim Manager	http://www.sourceforge.net/projects/agsm/	Windows	It recovers phone numbers and short message service (SMS) messages from a range of mobile phones.
OSAF-TK	http://www.sourceforge.net/projects/osaftoolkit/	Windows	This tool helps in android malware analysis and forensics.

Table 3:- Open source Network Forensic tools

Name	Link	Platform	Description
Xplico	http://www.xplico.org/download	Unix	It aids to extract applications data from the internet traffic. Features include support for multitude of protocols, TCP reassembly, and the ability to output data to a MySQL or SQLite database, amongst others.
NetSleuth	http://www.netsleuth.software.informer.com/1.6b/	Windows and Unix	It helps in identifying and fingerprinting the network hosts and devices from the PCAP files captured from Ethernet or Wi-Fi data. It also includes a live mode, silently identifying hosts and devices without needing to send any packets or put the network adapters into promiscuous mode.
Network miner	http://www.sourceforge.net/projects/networkminer/	Windows	It is used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network.
TCP Flow	http://www.sourceforge.net/projects/tcpflow/	Unix	It captures data transmitted as part of TCP connections, and stores the data in a way that is convenient for protocol analysis or debugging.
Webscavator	http://www.webscavator.org/	Windows	It is a visualization suite for analysis of internet history. It accepts CSV (comma separated values) files from Net analysis, Web Historian and many other browser log parsers, and produces images and graphs to display the data. It is web based.
Wireshark	http://www.wireshark.org/	Windows and Unix	It is a network protocol analyzer. It gives deep inspection of hundreds of protocols. It captures live data and provide offline analysis. It can read/write many different capture file formats.

PROPRIETARY TOOLS:-

Proprietary tools are those tools that are charged by the seller or the vendor. The tools may have a validity for which the Software is active. After the validity is completed the user is supposed to renew the license. They are also called as Closed Source Software. Below is the list of some of the tools that are used in Cyber Forensic Investigation.

Table 4:- Proprietary tools for Computer and Memory Forensics

Name	Platform	Description
Registry Recon	Windows	The tool helps in rebuilding Windows registries from anywhere on a hard drive and saves them for deep analysis.

Volume : 4 | Issue : 5 | May 2014 | ISSN - 2249-555X

EnCase Forensic	Windows	It acquires data from a wide variety of devices. It finds the evidence by itself then analyzes it and creates a report by itself. Encase is considered as one of the best cyber forensic tool worldwide.
Elcomsoft Password recovery Bundle	Windows	It helps to unprotect disks and systems and decrypt files and documents protected with popular applications. The tool is easy to use and least expensive among the same category of tools.
FTK	Windows	It is solution for decryption and recovery. It allows for graphical interface filtering function. It is one of the best tool foe email investigation.
Computer online forensic Evidence extractor (COFEE)	Windows	It is developed by Microsoft itself to extract evidence from a Windows Computer. It is installed in a USB flash drive, consists of around 150 tools with GUI to help the user select the appropriate tool for investigation.
Safeback	Windows	Tool designed for Computer Incident Response. Contains options like decryption and password recovery as well. It also helps in taking bit-stream backup of data.
NUIX / Proof finder	Windows and linux	It is used as a Forensic analysis & fraud prevention software. Some of its features are- Full text search, extracts emails, credit card numbers, IP addresses, URLs. Skin tone analysis.
Windows SCOPE	Windows	It allows the user in memory acquisition and access to locked computers. Access live memory and encrypted disks without needing passwords.
I2 Analyst's Notebook	Windows and Linux	It rapidly piece together disparate data into single cohesive intelligence picture. It identifies and highlights relevant data. It also uses multiple methods of information representation.
Prodiscover Incident Response	Windows and MAC	It allows disk preview, imaging and analysis over any TCP/IP network. It has an ability to find hidden data, file metadata information, and hash keeping, as well as gather data on disks across an entire network.

Table 5:- Proprietary tools for Mobile forensics

Name	Platform	Description
Paraben's Cell Seizure	Windows	It supports a wide range of cell phones and also supports GSM (global system for mobile communications) SIM cards with the use of a SIM card reader. It extracts user data such as logs, SMS, contacts, pictures etc. It is also compatible for the investigation of several GPS devices.
Cellebrite Mobile Forensic toolkits (UFED 4PC ULTIMATE)	Windows	It is a Software based Mobile forensic Solution. It provides device extraction via USB and RJ45 (a connector standard for telephone cables), SIM clone and extraction. It is compatible with almost all types of cell phone having different OS and make and model.
ACESO KIOSK	N/A	It helps in blocking the network access. Helps in acquisition of data from SIM, Mobile phone and memory card. It also supports SIM-less acquisition. It gives metadata access and stores all the data in AES encrypted file.
Elcomsoft IOS Forensic toolkit	Windows and MAC	It acquires data bit by bit. It supports physical and logical acquisition. It also decrypts keychain items and then extracts it from the IOS phone. This tool can also obtain passwords using brute force technique.
Elcomsoft Phone password breaker	Windows	It helps to gain access to information stored in password protected iPhone, iPad, iPod touch and blackberry backups. It performs advanced dictionary attacks with highly customizable permutations. It performs online attacks without apple iTunes or Blackberry desktop software installed.
MOBILedit Forensics	Windows	It supports almost all phones. This tool extracts data from an iPhone even when the system is locked using a passcode. Data can be examined even in the absence of the phone. It also allows to gain Gmail, Skype or Facebook contacts without even knowing the accounts password. This tool allows to investigate an android phone without the cable by using Wi-Fi. It also has a powerful SIM analyzer.

Table 6:- Proprietary tools for Network Forensics

Name	Platform	Description
Paraben Netanalysis	Windows	It interrogates the Web browser cache and history data with powerful searching, filtering, and evidence identification.
LogLogic's LX 2000	Windows	It is a log analysis tool. It ingests and processes all log files to secure, monitor and manage the IT environment. It dramatically reduces the time and cost required to uncover the information.
Webtracer	N/A	It determines the Owner of the website, the location of the server, the sender of an email, and other evidence of internet identity.
Spector CNE	Windows and Linux	It records everything the employees do online, Including IM (Instant messengers), chats, sending and receiving e-mails, visiting websites, launching applications, downloading files, and typing keys.
dtSearch	Windows	It searches terabytes of text across a desktop, network, Internet or intranet sites. It consists of special forensic search options. It supports public and secure, static and dynamic web data.

Conclusion: -

In this research paper we have mentioned about the various types of forensic tools that can be used for solving digital crimes. In some cases, the tools are software-based, but at times hardware are also required to acquire evidences. Some of the software's are freely available and some software's are paid. Freely available software's are also known as Open Source tools. A comprehensive list of these tools with their download link, use and the platforms like Windows, UNIX, Linux, DOS, and MAC etc. on which they can function accordingly has been mentioned. The paid tools are also known as closed source tools or Proprietary tools. These tools have more features compared to open source tools and are highly expensive. The list of tools mentioned in this paper is an effort to throw an insight on the existing tools that can be useful in digital forensics. These tools are not the only tools available for the purpose of forensic investigation, there is much more to the list. In this paper we have tried to mention about the tools which can be frequently used in the present scenario of the digital crimes.

REFERENCE 1) Casey, E.(2002) Handbook of Computer Crime Investigation. Great Britain; Academic Press. | 2) Cross, M. 2nd Edition (2008) Scene of the Cyber Crime. USA, Elsevier Syngress Publishing. | 3) Menendez , M. 2nd Edition (2008) Cyber Forensics, Field Manual. USA, Auerbach Publications. | 4) Ravikumar, K.V. and Jain, B. (2006) Cyber Forensics, Concepts and Approaches. Hyderabad, IUP Publications. | 5) Tiwari, R. K., Sastey, P.K. and Ravikumar, K.V. (2002). Computer Crime and Computer Forensics. Delhi; Select Publishers. |