EXPERIMENT NO: 2

**Aim:** To study digital forensic tool.

**Theory:**

**Digital forensic:**

Digital forensics is a very important branch of computer science in relation to computer and Internet related crimes. Earlier, computers were only used to produce data but now it has expanded to all devices related to digital data. The goal of digital forensics is to perform crime investigations by using evidence from digital data to find who was the responsible for that particular crime.

For better research and investigation, developers have created many computer forensics tools. Police departments and investigation agencies select the tools based on various factors including budget and available experts on the team.

These computer forensics tools can also be classified into various categories:

* Disk and data capture tools
* File viewers
* File analysis tools
* Registry analysis tools
* Internet analysis tools
* Email analysis tools
* Mobile devices analysis tools
* Mac OS analysis tools
* Network forensics tools
* Database forensics tools

**1. Digital Forensics Framework**

Digital Forensics Framework is another popular platform dedicated to digital forensics. The tool is open source and comes under GPL License. It can be used either by professionals or non-experts without any trouble. It can be used for digital chain of custody, to access the remote or local devices, forensics of Windows or Linux OS, recovery hidden of deleted files, quick search for files’ metadata, and various other things.

**2. Open Computer Forensics Architecture**

Open Computer Forensics Architecture (OCFA) is another popular distributed open-source computer forensics framework. This framework was built on Linux platform and uses postgreSQL database for storing data.

It was built by the Dutch National Police Agency for automating digital forensics process. It is available to download under GPL license.

**3. CAINE**

CAINE (Computer Aided Investigative Environment) is the Linux distro created for digital forensics. It offers an environment to integrate existing software tools as software modules in a user friendly manner. This tool is open source.

**4. X-Ways Forensics**

X-Ways Forensics is an advanced platform for digital forensics examiners. It runs on all available version of Windows. It claims to not be very resource hungry and to work efficiently. If we talk about the features, find the key features in the list below:

* Disk imaging and cloning
* Ability to read file system structures inside various image files
* It supports most of the file systems including FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3®, CDFS/ISO9660/Joliet, UDF
* Automatic detection of deleted or lost hard disk partition
* Various data recovery techniques and powerful file carving
* Bulk hash calculation
* Viewing and editing binary data structures using templates
* Easy detection of and access NTFS ADS
* Well maintained file header
* Automated activity logging
* Data authenticity
* Complete case management
* Memory and RAM analysis
* Gallery view for pictures
* Internal viewer for Windows registry file
* Automated registry report
* Extracts metadata from various file types
* Ability to extract emails from various available email clients.

**5. SANS Investigative Forensics Toolkit – SIFT**

SANS Investigative Forensics Toolkit or SIFT is a multi-purpose forensic operating system which comes with all the necessary tools used in the digital forensic process. It is built on Ubuntu with many tools related to digital forensics. Earlier this year, SIFT 3.0 was released. It comes for free or charge and contains free open-source forensic tools.

In a previous post at resource.infosecinstitute.com, we already covered SIFT in detail. You can read those posts about SIFT to know more about this digital forensics platform.

**6. EnCase**

EnCase is another popular multi-purpose forensic platform with many nice tools for several areas of the digital forensic process. This tool can rapidly gather data from various devices and unearth potential evidence. It also produces a report based on the evidence.

This tool does not come for free. The license costs $995.

**7. Registry Recon**

Registry Recon is a popular registry analysis tool. It extracts the registry information from the evidence and then rebuilds the registry representation. It can rebuild registries from both current and previous Windows installations.

**8. The Sleuth Kit**

The Sleuth Kit is a Unix and Windows based tool which helps in forensic analysis of computers. It comes with various tools which helps in digital forensics. These tools help in analyzing disk images, performing in-depth analysis of file systems, and various other things.

**9. Llib Forensics**

Libforensics is a library for developing digital forensics applications. It was developed in Python and comes with various demo tools to extract information from various types of evidence.

**10. Volatility**

Volatility is the memory forensics framework. It used for incident response and malware analysis. With this tool, you can extract information from running processes, network sockets, network connection, DLLs and registry hives. It also has support for extracting information from Windows crash dump files and hibernation files. This tool is available for free under GPL license.

**11. WindowsSCOPE**

WindowsSCOPE is another memory forensics and reverse engineering tool used for analyzing volatile memory. It is basically used for reverse engineering of malwares. It provides the capability of analyzing the Windows kernel, drivers, DLLs, virtual and physical memory.

**12. The Coroner’s Toolkit**

The Coroner’s Toolkit or TCT is also a good digital forensic analysis tool. It runs under several Unix-related operating systems. It can be used to aid analysis of computer disasters and data recovery.

**13. Oxygen Forensic Suite**

Oxygen Forensic Suite is a nice software to gather evidence from a mobile phone to support your case. This tool helps in gathering device information (including manufacturer, OS, IMEI number, serial number), contacts, messages (emails, SMS, MMS), recover deleted messages, call logs and calendar information. It also lets you access and analyze mobile device data and documents. It generates easy to understand reports for better understanding.

**14. Bulk Extractor**

Bulk Extractor is also an important and popular digital forensics tool. It scans the disk images, file or directory of files to extract useful information. In this process, it ignores the file system structure, so it is faster than other available similar kinds of tools. It is basically used by intelligence and law enforcement agencies in solving cyber crimes.

**15. Xplico**

Xplico is an open source network forensic analysis tool. It is basically used to extract useful data from applications which use Internet and network protocols. It supports most of the popular protocols including HTTP, IMAP, POP, SMTP, SIP, TCP, UDP, TCP and others. Output data of the tool is stored in SQLite database of MySQL database. It also supports IPv4 and IPv6 both.

**16. Mandiant RedLine**

Mandiant RedLine is a popular tool for memory and file analysis. It collects information about running processes on a host, drivers from memory and gathers other data like metadata, registry data, tasks, services, network information and Internet history to build a proper report.

**17. Computer Online Forensic Evidence Extractor (COFEE)**

Computer Online Forensic Evidence Extractor or COFEE is a tool kit developed for computer forensic experts. This tool was developed by Microsoft to gather evidence from Windows systems. It can be installed on a USB pen drive or external hard disk. Just plug in the USB device in the target computer and it starts a live analysis. It comes with 150 different tools with a GUI based interface to command the tools. It is fast and can perform the whole analysis in as few as 20 minutes. To law enforcement agencies, Microsoft provides free technical support for the tool.

**18. P2 eXplorer**

P2 eXplorer is a forensic image mounting tool which aims to help investigating officers with examination of a case. With this image, you can mount forensic images as a read-only local and physical disc and then explore the contents of the image with file explorer. You can easily view deleted data and unallocated space of the image.

It can mount several images at a time. It supports most of the image formats including EnCasem, safeBack, PFR, FTK DD, WinImage, Raw images from Linux DD, and VMWare images. It supports both logical and physical image types.

This tool comes for $199, but you can grab the limited feature version of the tool for free.

**19. PlainSight**

PlainSight is another useful digital forensics tool. It is a CD based Knoppix which is a Linux distribution. Some of its uses include viewing Internet histories, data carving, checking USB device usage, memory dumps extracting password hashes, information gathering, examining Windows firewall configuration, seeing recent documents, and other useful tasks. For using this too, you only need to boot from the CD and the follow the instructions.

This tool is available for free.

**20. XRY**

XRY is the mobile forensics tool developed by Micro Systemation. It is used to analyze and recover crucial information from mobile devices. This tool comes with a hardware device and software. Hardware connects mobile phones to PC and software performs the analysis of the device and extract data. It is designed to recover data for forensic analysis.

The latest version of the tool can recover data from all kind of smartphones including Android, iPhone and BlackBerry. It gathers deleted data like call records, images, SMS and text messages.

**21. HELIX3**

HELIX3 is a live CD-based digital forensic suite created to be used in incident response. It comes with many open source digital forensics tools including hex editors, data carving and password cracking tools.

This tool can collect data from physical memory, network connections, user accounts, executing processes and services, scheduled jobs, Windows Registry, chat logs, screen captures, SAM files, applications, drivers, environment variables and Internet history. Then it analyzes and reviews the data to generate the complied results based on reports.

**22. Cellebrite UFED**

Cellebrite’s UFED solutions present a unified workflow to allow examiners, investigators and first responders to collect, protect and act decisively on mobile data with the speed and accuracy a situation demands – without ever compromising one for the other. The UFED Pro Series is designed for forensic examiners and investigators who require the most comprehensive, up-to-date mobile data extraction and decoding support available to handle the influx of new data sources. Platform agnostic, the UFED Field Series is designed to unify workflows between the field and lab, making it possible to view, access and share mobile data via in-car workstations, laptops, tablets or a secure, self-service kiosk located at a station.

**Conclusion:**

It will help you in better understanding the whole process and tools.With the increasing use of digital data and mobile phones, digital forensics has become more important. Cyber crimes are also increasing day by day. So companies are also trying to launch more powerful version of the tools.