MODULE -3

39. What are the different types of computer forensics tools? Explain

Name	Platform	License	Version	Description
Autopsy	Windows, macOS, Linux	GPL	4.5	A digital forensics platform and GUI to The Sleuth Kit
COFEE	Windows	proprietary	n/a	A suite of tools for Windows developed by Microsoft
Digital Forensics Framework	Unix-like/Windows	GPL	1.3	Framework and user interfaces dedicated to Digital Forensics
EPRB	Windows	proprietary	1435	Set of tools for encrypted systems & data decryption and password recovery
EnCase	Windows	proprietary	8.6	Digital forensics suite created by Guidance Software
FTK	Windows	proprietary	6.0.1	Multi-purpose tool, FTK is a court-cited digital investigations platform built for speed, stability and ease of use.
IsoBuster	Windows	proprietary	4.1	Essential light weight tool to inspect any type data carrier, supporting a wide range of file systems, with advanced export functionality.
Netherlands Forensic Institute / Xiraf[2]	n/a	proprietary	n/a	Computer-forensic online service.

40. What re the tasks performed by computer forensics tools? Explain each task

- 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

41. Explain the command line and GUI computer forensics software tools.

What is a GUI?

A GUI (Graphic User Interface) is a graphical representation in which the users can interact with software or devices through graphical icons.

Eg.Winhex, Autopsy

What is CLI ?

A CLI (Command Line Interface) is a console or text based representation in which the user types the commands to operate the software or devices.

Eg.sleuth kit

GUI vs. CLI:

Ease:

If we talk about ease of use, the new users will pick up a GUI much faster than a CLI. In a CLI, new users have some difficulty operating it because they are not familiar with the commands.

Control:

With a GUI, there's control over files and the operating system – but advanced tasks may still need to use the command line.

With a CLI, users have all the control over file system and operating system, and the tasks become simple. For example, you can copy a file or several with one command.

Speed:

If we talk about speed, in a GUI, using the mouse and the keyboard to control the file system or the operating system is going to be slower than using the command line.

In a CLI, the users only need to utilize the keyboard and may need to execute only few commands to complete the task.

Hacking:

If we talk about hacking, all the vulnerability exploits are done from command line. All the remote access and file manipulation are done from the command line.

Scripting:

One thing I love about command line is that you can create a script that contains few lines of command and it will do the work for you.

Although GUI’s can create shortcuts, tasks or other similar actions, they don’t come close to what command line can do.

42. What is a forensics workstation? What are its different categories? What is a write blocker?

A write blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data. A write blocker, when used properly, can guarantee the protection of the data chain of custody. NIST‘s general write blocking requirements hold that:

- The tool shall not allow a protected drive to be changed.
- The tool shall not prevent obtaining any information from or about any drive.
- The tool shall not prevent any operations to a drive that is not protected.

Software versus hardware write blockers

Software and hardware write blockers do the same job. They prevent writes to storage devices. The main difference between the two types is that software write blockers are installed on a forensic computer workstation, whereas hardware write blockers have write blocking software installed on a controller chip inside a portable physical device.

As determined by NIST’s Software Write Block specifications, a software write block tool operates by monitoring and filtering drive I/O commands sent from an application or OS through a given access interface.

Programs running in the DOS environment can, in addition to direct access via the drive controller, use two other interfaces: DOS service interface (interrupt 0x21) or BIOS service interface (interrupt 0x13).

The primary purpose of a hardware write blocker is to intercept and prevent (or ‘block’) any modifying command operation from ever reaching the storage device. Some of its functions include monitoring and filtering any activity that is transmitted or received between its interface connections to the computer and the storage device.

Hardware write blockers provide built in interfaces to a number of storage devices, and can connect to other types of storage with adapters. Hardware devices that write block also provide visual indication of function through LEDs and switches. This makes them easy to use and makes functionality clear to users.

Through its WiebeTech line of digital investigation products, CRU offers a wide variety of hardware write-blocking solutions.

- The Media WriteBlocker is highly portable, with compact lightweight design. It provides easy, write-blocked access to a variety of flash media, including SD and CF cards.
- The DriveDock family of products provides fast write-blocked access to suspect drives. The LCD and menu system make it convenient to view drive information, error/warning messages, or remove HPA/DCOs.
- The Ditto Forensic FieldStation is ideal for remote data analysis and capture and it

replaces the need for a laptop or other host machine during data acquisition.

43. Describe the methods for validating and testing computer forensics tools

Validating and Testing Forensic Software

Make sure the evidence you recover and analyze can be admitted in court

Test and validate your software to prevent damaging the evidence

Using National Institute of Standards and Technology (NIST) Tools

Computer Forensics Tool Testing (CFTT) program

Manages research on computer forensics tools

NIST has created criteria for testing computer forensics tools based on:

Standard testing methods

ISO 17025 criteria for testing items that have no current standards

ISO 5725

Your lab must meet the following criteria

Establish categories for computer forensics tools

Identify computer forensics category requirements

Develop test assertions

Identify test cases

Establish a test method

Report test results

Also evaluates drive-imaging tools

See link Ch 7g

National Software Reference Library (NSRL) project

Collects all known hash values for commercial software applications and OS files

Uses SHA-1 to generate a known set of digital signatures called the Reference Data Set (RDS)

Helps filtering known information

Can use RDS to locate and identify known bad files

Using Validation Protocols

Always verify your results

Use at least two tools

Retrieving and examination

Verification

Understand how tools work

One way to compare results and verify a new tool is by using a disk editor

Such as Hex Workshop or WinHex

But it won't work with encrypted or compressed files

Disk editors

Do not have a flashy interface

Reliable tools

Can access raw data

Computer Forensics Examination Protocol

Perform the investigation with a GUI tool

Usually FTK or EnCase

Verify your results with a disk editor

If a file is recovered, compare hash values obtained with both tools

Computer Forensics Tool Upgrade Protocol

Test

New releases

OS patches and upgrades

44. Identify and explain the commands used in sleuthkit.

- **blkcalc** - Converts between unallocated disk unit numbers and regular disk unit numbers.
- **blkcat** - Display the contents of file system data unit in a disk image.
- **blkls** - List or output file system data units.
- **blkstat** - Display details of a file system data unit (i.e. block or sector).
- **fcat** - Output the contents of a file based on its name.
- **ffind** - Finds the name of the file or directory using a given inode.
- **fiwalk** - print the filesystem statistics and exit.
- **fls** - List file and directory names in a disk image.
- **fsstat** - Display general details of a file system.
- **hfind** - Lookup a hash value in a hash database.

- **icat** - Output the contents of a file based on its inode number.
- **ifind** - Find the meta-data structure that has allocated a given disk unit or file name.
- **ils** - List inode information.
- **img_cat** - Output contents of an image file.
- **img_stat** - Display details of an image file.
- **istat** - Display details of a meta-data structure (i.e. inode).
- **jcat** - Show the contents of a block in the file system journal.
- **jls** - List the contents of a file system journal.
- **jpeg_extract** - jpeg extractor.
- **mactime** - Create an ASCII time line of file activity.
- **mmcat** - Output the contents of a partition to stdout.
- **mmls** - Display the partition layout of a volume system (partition tables).
- **mmstat** - Display details about the volume system (partition tables).
- **sigfind** - Find a binary signature in a file.
- **sorter** - Sort files in an image into categories based on file type.
- **srch_strings** - Display printable strings in files.
- **tsk_comparedir** - compare the contents of a directory with the contents of an image or local device.
- **tsk_gettimes** - Collect MAC times from a disk image into a body file.
- **tsk_loaddb** - populate a SQLite database with metadata from a disk image.
- **tsk_recover** - Export files from an image into a local directory.