TEAM: DIGITAL FORENSICS AND INCIDENT RESPONSE

SIFT

WORKSTATION

SIFT (Scale-Invariant Feature Transform) workstation is a software package that provides a suite of tools for computer vision researchers and practitioners. The SIFT algorithm is a popular technique for extracting distinctive and invariant features from digital images, and the SIFT workstation provides a user-friendly interface for implementing the algorithm and analysing its output.

INSTALLATION SUPPORT:

We Can Install It in all types of operating systems such a macOS, Linux, Microsoft Windows using Windows Subsystem for Linux and also in oracle VirtualBox as SIFT Workstation VM Appliance.

I have installed it in VirtualBox just click the downloaded ova image it will do all the setting by himself just import it on our VirtualBox.

Once we have booted the virtual machine, use the credentials below to gain access.

- Login = **sansforensics**
- Password = **forensics**
- $ **sudo su -**
    - Use to elevate privileges to root while mounting disk images.

Key new SIFT Workstation features include:

- Ubuntu LTS 20.04 Base
- 64-bit base system
- Better memory utilization
- Auto-DFIR package update and customizations
- Latest forensic tools and techniques
- VM Appliance ready to tackle forensics
- Cross compatibility between Linux and Windows
- Option to install/upgrade stand-alone system via SIFT-CLI installer
- Expanded Filesystem Support

AUTOPSY

A graphical interface for the Sleuth Kit that enables digital forensic examiners to conduct a thorough analysis of various types of data. Here are some of the key workings of Autopsy:

1. Disk Imaging: Autopsy provides a user-friendly interface for creating forensic images of digital media, such as hard drives, USB drives, and memory cards. This process involves creating a bit-by-bit copy of the original media, which can be analysed without altering the original data.

2. File Recovery: Autopsy includes tools for recovering deleted files and folders from disk images. This process involves searching for and recovering files that have been marked as deleted but still exist on the disk.

3. Keyword Search: Autopsy allows users to search for specific keywords or phrases within a disk image. This feature is useful for quickly identifying relevant data within a large volume of data.

4. Timeline Analysis: Autopsy includes tools for timeline analysis, which allows forensic analysts to identify and visualize the sequence of events that occurred on a computer system. This feature can be used to identify suspicious activity, such as the creation or modification of files or the execution of certain programs.

5. Reporting: Autopsy provides a range of reporting options, allowing users to create detailed reports of their forensic analysis. These reports can be used to document findings and present evidence in legal proceedings.

6. Module Support: Autopsy is designed to be extensible, and additional modules can be added to the software to extend its functionality. For example, there are modules available for analysing email, internet history, and social media artifacts.

we can extract data from a hard drive using the data ingestion feature. Here are the steps to extract data from a hard drive in Autopsy:

1. Open Autopsy and create a new case by clicking on "File" and selecting "New Case."
2. In the "New Case" window, enter the case details, such as case name, description, and examiner name.
3. Click on "Next" and select the data source as "Disk Image File" or "Physical Disk" based on the type of hard drive we want to extract data from.
4. Click on "Next" and select the hard drive image file or physical disk that we want to ingest in Autopsy.
5. Click on "Next" and select the file system of the hard drive, such as NTFS or FAT.
6. Click on "Next" and select the ingest modules that we want to use for data extraction. Ingest modules are used to extract specific types of data from the hard drive, such as email messages, images, videos, or documents.
7. Click on "Finish" to start the data ingestion process. The time taken to ingest the data depends on the size of the hard drive and the modules selected.
8. Once the data ingestion is complete, we can start analyzing the data using various tools and techniques in Autopsy, such as keyword search, timeline analysis, and file carving.
9. To extract specific files or data, we can use the file carving feature in Autopsy. File carving is the process of recovering deleted files or data from the hard drive's unallocated space. To use the file carving feature, right-click on the hard drive image in Autopsy and select "Carve File."
10. In the "Carve File" window, select the file type and file extension that we want to recover and click on "Start." Autopsy will search the hard drive for the specified file type and recover any files that match the search criteria.

WIRESHARK

Wireshark is a network protocol analyzer that allows us to capture and analyze network traffic in real-time or from saved capture files. It is a powerful tool for network troubleshooting, analysis, and security test

Workings of Wireshark :

1. Launch Wireshark and select the interface we want to capture traffic from. Click on the "Capture" menu and select "Interfaces". Choose the appropriate interface and click on "Start" to begin capturing network traffic.

2. Analyse the captured packets in real-time or from saved capture files. Wireshark provides various filters, search options, and statistics to analyse the captured data. We can use the display filter to focus on specific packets and protocols, or use the search function to find specific data within the packets.

3. Use the statistics menu to view various statistics related to the captured packets, including protocol hierarchy, endpoints, conversations, and more.

4. Save the captured packets in a file for future analysis. Click on "File" and select "Save" to save the captured packets as a Wireshark capture file.

5. We can also export the captured data in various formats, including CSV, TXT, HTML, and more. Click on "File" and select "Export Packet Dissections" to export the packet data.

These are some features of Wireshark we can use for our analysis :

1. Packet capturing and analysis: Wireshark can capture and analyze network traffic from various sources, including Ethernet, Wi-Fi, and Bluetooth. It can capture packets

in real-time or from saved capture files, and provides various options for filtering, sorting, and searching packets.

2. Protocol decoding: Wireshark can decode a wide range of network protocols, including TCP, UDP, HTTP, DNS, FTP, SSH, and more. It can display packet details and decode data in various formats, such as ASCII, hexadecimal, and binary.

3. Traffic statistics: Wireshark provides various statistics and graphs to analyze network traffic, such as the number of packets, bytes, and packets per second, as well as protocol distribution, packet size distribution, and more.

4. Protocol analysis: Wireshark can analyze network protocols in real-time or from saved capture files, and can detect various issues, such as errors, retransmissions, lost packets, and more. It can also detect and analyze network attacks, such as port scans, denial-of-service attacks, and more.

5. VoIP analysis: Wireshark can analyze Voice-over-IP (VoIP) traffic, such as SIP and RTP protocols, and provides various statistics and graphs to analyze call quality, packet loss, jitter, and more.

6. Exporting data: Wireshark allows us to export captured data in various formats, such as CSV, TXT, XML, and more. We can also save the captured packets as a Wireshark capture file, or export the packet dissections as a PDF, PostScript, or HTML file.

7. Command-line interface: Wireshark can be used from the command-line interface (CLI), which allows us to automate capture and analysis tasks, and integrate Wireshark with other tools and scripts.

8. Customization: Wireshark provides various options for customization, such as color schemes, packet details, and protocol dissectors. We can also create our own protocol dissectors using Wireshark's Lua scripting language.

VOLATILITY

Volatility is a powerful and flexible memory forensics tool that can be used to extract and analyze digital artifacts from volatile memory. Here's how Volatility works.

1. Memory acquisition: The first step in using Volatility is to acquire the memory dump from the target system. This can be done using various methods, such as physical memory acquisition, live memory acquisition, or kernel memory dumping. Volatility supports various formats for memory dumps, such as raw memory images, crash dump files, hibernation files, and virtual machine snapshots.

2. Memory analysis: Once you have acquired the memory dump, we can use Volatility to analyze it and extract digital artifacts. Volatility provides various plugins for analyzing different types of data structures and data formats, such as processes, threads, DLLs, network connections, files, registry keys, and more. Each plugin corresponds to a specific data structure or data format and provides a set of commands and options for analyzing and extracting data.

3. Profile selection: Before analyzing the memory dump, we need to select the appropriate memory profile that matches the operating system and service pack version of the target system. Volatility provides a list of pre-built memory profiles for various versions of Windows, Linux, and macOS, and also allows US to create custom profiles if needed.

4. Plugin usage: Once WE have selected the memory profile, WE can use Volatility plugins to analyze the memory dump and extract digital artifacts. Each plugin has a specific syntax and set of options, and can be used to perform various tasks, such as listing processes, identifying malware, extracting registry keys, analyzing network traffic, and more.

5. Output generation: Volatility provides various output formats for the results of analysis, such as plaintext, JSON, CSV, and more. we can also use Volatility's built-in scripting language or other scripting languages, such as Python, to automate analysis tasks and generate custom reports.

CASE OF THE ASHLEY MADISON DATA BREACH IN 2015

Ashley Madison, a Canadian-based online dating service marketed to people who are married or in relationships, was hacked in July 2015. The hackers stole personal and confidential information from the website, including user names, email addresses, and credit card details. The incident was one of the largest data breaches at the time, affecting over 30 million users.Digital forensics experts were brought in to investigate the breach, and they utilized the SIFT Workstation as part of their investigation. The SIFT Workstation is a free, open-source toolkit that provides powerful digital forensic tools and capabilities. The SIFT Workstation was used to analyze forensic images of the affected servers and identify potential sources of the breach.The digital forensics team utilized several tools available in the SIFT Workstation, including Autopsy, to conduct a deep dive into the data and identify suspicious activity. They used memory analysis tools such as Volatility Framework to search for indications of malware and other malicious activity.Through the use of the SIFT Workstation's forensic tools, the digital forensics team was able to identify several suspicious files and folders that had been downloaded onto the Ashley Madison servers. The team also found evidence of data exfiltration, indicating that an unauthorized individual had stolen data from the system.The team also utilized the SIFT Workstation's advanced search capabilities to find keywords, IP addresses, and email addresses that could be linked to the attack. They were able to trace the attack back to a group of hackers known as "The Impact Team".

The use of the SIFT Workstation proved to be an invaluable tool for the digital forensics team investigating the Ashley Madison breach. Its powerful forensic tools allowed the team to conduct a thorough analysis of the affected servers and identify potential sources of the breach. The SIFT Workstation's memory analysis tools provided valuable insights that may have been missed using traditional forensic methods.

In conclusion, the use of the SIFT Workstation in the Ashley Madison investigation highlights the importance of having access to powerful forensic tools in digital forensics investigations. The SIFT Workstation proved to be a powerful and effective tool for digital forensics investigations and incident response, aiding in the recovery of stolen data and the identification of the perpetrators.

Internship Assessment for Tutelr Infinity Internships Week 2

Answer the following questions based on your understanding of SIFT Workstation

1. What is the SIFT Workstation?

Ans -> a) A digital forensic toolkit

c) A malware analysis tool

2. What is the primary use of the SIFT Workstation?

Ans -> a) Data recovery

b) Network monitoring

c) Incident response

3. Which operating system is the SIFT Workstation based on?

Ans -> c) Linux

4. Which tool is included in the SIFT Workstation for file carving?

Ans -> c) Autopsy

d) Scalpel

5. Which file system can the SIFT Workstation analyze?

a) NTFS

b) FAT32

c) EXT4

Ans -> d) All of the above

6. What is the purpose of the SIFT Workstation's log2timeline tool?

Ans -> c) To create a timeline of system events

7. Which tool in the SIFT Workstation is used for memory analysis?

Ans-> a) Volatility

8. Which forensic tool in the SIFT Workstation is used for database analysis?

Ans -> a) SQLite

9. What is the function of the SIFT Workstation's bulk extractor tool?

Ans -> c) To extract metadata from files

10. Which type of investigation is the SIFT Workstation commonly used for?

Ans -> a) Cybersecurity incident response