(A462503) CYBER CRIME INVESTIGATION & DIGITAL FORENSICS LAB

B.Tech : V Semester

L	T	P	C
0	0	2	1

List of Experiments

1. Perform email analysis using the tools like Exchange EDB viewer, MBOX viewer and View user mailboxes and public folders, Filter the mailbox data based on various criteria, Search for items in user mailboxes and public folders
2. Perform Browser history analysis and get the downloaded content, history, saved logins, searches, websites visited etc using Foxton Forensics tool, Dumpzilla .
3. Perform mobile analysis in the form of retrieving call logs, SMS log, all contacts list using the forensics tool like SAFT.
4. Perform Registry analysis and get boot time logging using process monitor tool.
5. Perform Disk imaging and cloning the using the X-way Forensics tools.
6. Perform Data Analysis i.e., History about open file and folder, and view folder actions using Lastview activity tool.
7. Perform Network analysis using the Network Miner tool.
8. Perform information for incident response using the crowd Response tool
9. Perform File type detection using Autopsy tool.
10. Perform Memory capture and analysis using the Live RAM capture or any forensic tool.

TEXTBOOKS:

1. Real Digital Forensics for Handheld Devices, E. P. Dorothy, Auerback Publications, 2013.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.

REFERENCE BOOKS:

1. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010
2. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C. H.Malin, E. Casey and J. M. Aquilina, Syngress, 2012
3. Brett shabers, Eric Zimerman, X-ways forensics practitioners guide

COURSE OUTCOMES

On completion of the course students will be able to

1. Learn the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong doing.
2. To Learn the file system storage mechanisms and retrieve files in hidden format
3. Learn the use of computer forensics tools used in data analysis.

Cybercrime investigation and Digital forensic Lab Manual

Aim

To Perform email analysis using the tools like Exchange EDB viewer, MBOX viewer and View user mailboxes and public folders, Filter the mailbox data based on various criteria, Search for items in user mailboxes and public folders

Step by step Procedure

1. Log in to Your Google Account:

-Open your web browser and go to [Google Takeout](https://takeout.google.com/).

- Log in with your Google credentials: Enter your email and password, then follow any additional security prompts (e.g., two-factor authentication).

2. Download MBOX Viewer:

- Go to GitHub: Visit the GitHub repository or website offering the MBOX Viewer tool. Ensure you choose a reliable and secure option.

- Download the MBOX Viewer: Click on the "Download" button or link to get the installer file for the MBOX Viewer.

- Install the MBOX Viewer: Once downloaded, run the installer and follow the on-screen instructions to install the software on your computer.

3. Export Emails Using Google Takeout:

- Access Google Takeout: After logging in, you'll see a list of data types that can be exported.

- Deselect All: Click on the "Deselect all" button to start with a clean slate.

- Select "Mail": Scroll down and find the "Mail" option. Toggle it on to include emails in your export.

- Customize Export Options: Click on the "All Mail data included" button to select specific labels or mail folders if needed. Otherwise, all emails will be included by default.

- Choose Export Format: You can select the file format (MBOX) and other export settings, such as the size of each export file.

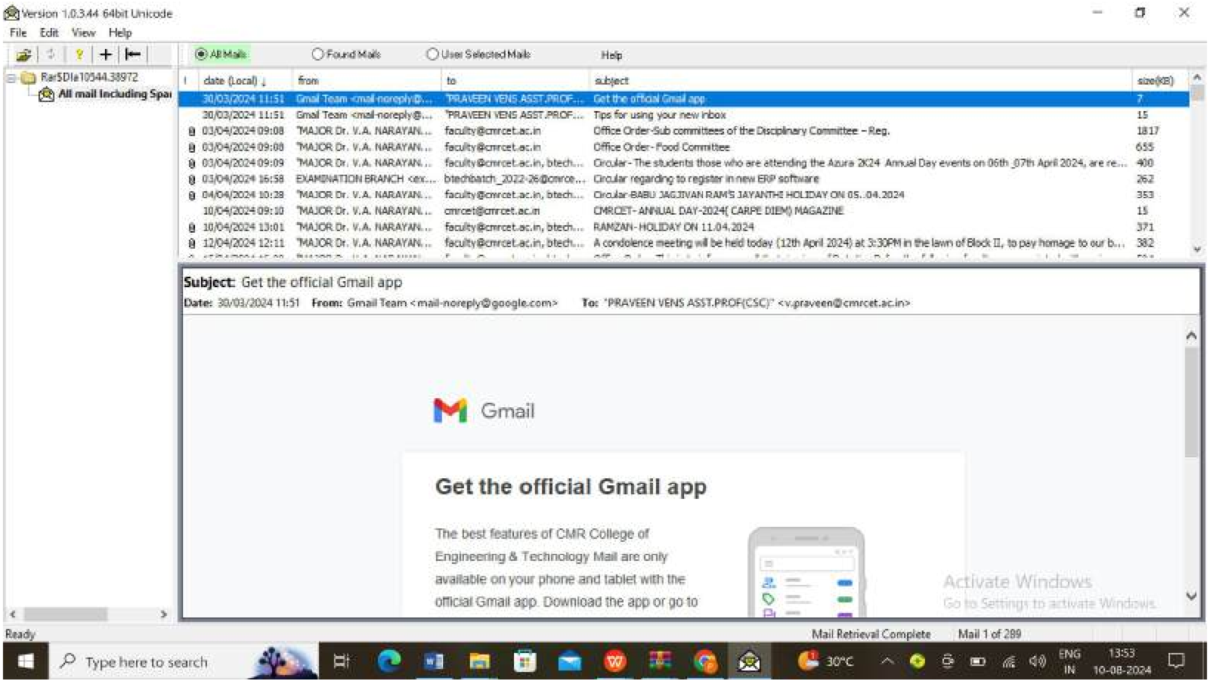
- Create Export: Click on "Next step," then choose your delivery method (e.g., download link via email). Click "Create export" to begin the process.

- Download the Exported Data: Once the export is complete, you'll receive a notification. Download the MBOX file from the provided link.

Result

This Each tool provides a different lens through which to view and analyse email data. Combining these tools and techniques can help in comprehensive email analysis, whether for legal investigations, data migration, or troubleshooting.

OUTPUT



!	date (Local) ↓	from	to	subject	size(KB)
	30/03/2024 11:51	Gmail Team <mail-noreply@...	"PRAVEEN VENS ASST.PROF...	Get the official Gmail app	7
	30/03/2024 11:51	Gmail Team <mail-noreply@...	"PRAVEEN VENS ASST.PROF...	Tips for using your new inbox	15
📎	03/04/2024 09:08	"MAJOR Dr. V.A. NARAYAN...	faculty@cmrcet.ac.in	Office Order-Sub committees of the Disciplinary Committee – Reg.	1817
📎	03/04/2024 09:08	"MAJOR Dr. V.A. NARAYAN...	faculty@cmrcet.ac.in	Office Order- Food Committee	655
📎	03/04/2024 09:09	"MAJOR Dr. V.A. NARAYAN...	faculty@cmrcet.ac.in, btech...	Circular - The students those who are attending the Azura 2K24 Annual Day events on 06th _07th April 2024, are re...	400
📎	03/04/2024 16:58	EXAMINATION BRANCH <ex...	btechbatch_2022-26@cmrce...	Circular regarding to register in new ERP software	262
📎	04/04/2024 10:28	"MAJOR Dr. V.A. NARAYAN...	faculty@cmrcet.ac.in, btech...	Circular-BABU JAGJIVAN RAM'S JAYANTHI HOLIDAY ON 05..04.2024	353
	10/04/2024 09:10	"MAJOR Dr. V.A. NARAYAN...	cmrcet@cmrcet.ac.in	CMRCET- ANNUAL DAY-2024(CARPE DIEM) MAGAZINE	15
📎	10/04/2024 13:01	"MAJOR Dr. V.A. NARAYAN...	faculty@cmrcet.ac.in, btech...	RAMZAN- HOLIDAY ON 11.04.2024	371
📎	12/04/2024 12:11	"MAJOR Dr. V.A. NARAYAN...	faculty@cmrcet.ac.in, btech...	A condolence meeting will be held today (12th April 2024) at 3:30PM in the lawn of Block II, to pay homage to our b...	382

Subject: Get the official Gmail app
Date: 30/03/2024 11:51 **From:** Gmail Team <mail-noreply@google.com> **To:** "PRAVEEN VENS ASST.PROF(CSC)" <v.praveen@cmrcet.ac.in>

Gmail

Get the official Gmail app

The best features of CMR College of Engineering & Technology Mail are only available on your phone and tablet with the official Gmail app. Download the app or go to

Experiment-2

Aim: Perform browser history analysis and get the downloaded content,history,saved logins,searches,websites visited etc using Foxton Forensics tool,Dumpzilla.

Step 1: Download Foxton Browser History Examiner

1. Open your preferred web browser.

2. Go to the official website of Foxton Browser History Examiner. If you're looking for a free trial, you can search for "Foxton Browser History Examiner free trial."

3. Click on the download link to get the installer file for your operating system.

Step 2: Install Foxton Browser History Examiner

1. Once the download is complete, navigate to the folder where the installer was downloaded.

2. Double-click on the installer file to begin the installation process.

3. Follow the on-screen prompts to complete the installation.

4. After the installation is complete, you can choose to launch the program immediately or later.

Step 3: Open Foxton Browser History Examiner

1. If the program did not launch automatically after installation, you can open it manually:

- On Windows: Click on the **Start** menu and type "Foxton Browser History Examiner" in the search bar, then press **Enter** to open the program.

- On macOS: Use Spotlight search by pressing `Cmd + Space`, type "Foxton Browser History Examiner," and press **Enter**.

2. The program will open, displaying its main interface.

Step 4: Capture Browser History Files

1. In the main interface, locate the option to **Capture Files** or **Open Browser History** (the exact wording may vary depending on the version).

2. Click on this option, and a new window or prompt will appear asking you to select the browser from which you want to capture the history.

3. The program may automatically detect installed browsers, or you may need to navigate to the browser's history database manually.

Step 5: Select a Folder to Save the Captured Files

1. After capturing the files, you will be prompted to choose a location to save the captured history files.

2. Browse your file system and select an appropriate folder where you want to store the files.

3. Click **OK** or **Save** to confirm the location.

Step 6: Complete the Process

1. Once the files are saved, you can navigate to the folder you selected to view or further analyze the captured browser history.

2. If needed, you can use the features within Foxton Browser History Examiner to analyze or export the data.

Aim : To perform mobile analysis in the form of retrieving call logs,SMS log, all contact list using the forensics tools like SAFT

Step 1: Search for SAFT for Windows**

1. **Open Your Browser:**

- Start by opening your preferred web browser (Chrome, Firefox, etc.).

2. **Search for SAFT:**

- In the search bar, type "SAFT mobile forensic tool for Windows download."

- Look for a reliable source, such as the official website or a trusted repository like GitHub, to download the tool.

****Step 2: Download the SAFT ZIP File****

1. **Download the ZIP File:**

- Once you find the correct website, locate the download link for the SAFT tool compatible with Windows.

- Click the link to download the ZIP file containing the SAFT tool.

2. **Verify the Download:**

- After the download is complete, navigate to your "Downloads" folder to ensure the ZIP file has been downloaded successfully.

****Step 3: Extract the ZIP File****

1. **Extract the Files:**

- Right-click on the downloaded ZIP file and select "Extract All..." from the context menu.

- Choose a destination folder where you want to extract the files, then click "Extract."

2. **Access the Extracted Files**:

- After extraction, navigate to the folder where the files have been extracted.

- You should see the SAFT executable file along with other necessary files.

Step 4: Prepare the Mobile Device

1. **Enable Developer Mode**:

- On your Android device, go to "Settings," then "About Phone."

- Tap "Build Number" seven times to enable Developer Mode.

2. **Enable USB Debugging**:

- In "Developer Options," enable "USB Debugging" to allow communication between the device and your computer.

3. **Connect the Device to the Computer**:

- Use a USB cable to connect your Android device to your computer. Ensure it is detected properly.

Step 5: Run SAFT and Perform Analysis

1. **Open SAFT**:

- Go to the folder where you extracted SAFT and double-click the SAFT executable file (e.g., `saft.exe`).

2. **Retrieve Call Logs**:

- In the SAFT interface, select the option to extract call logs.

- SAFT will retrieve the call logs from the connected device and save them to a designated folder.

3. **Retrieve SMS Logs**:

- Choose the option to extract SMS logs.
- The tool will gather SMS data and store it in a readable format in the specified directory.

4. **Retrieve Contacts List**:

- Select the option to extract the contacts list.
- SAFT will extract the contacts and save them for your review.

Step 6: Review and Document

1. **Review Extracted Data**:

- Open the files containing the extracted call logs, SMS logs, and contacts using a suitable application like Notepad, Excel, or a web browser.

2. **Document Your Findings**:

- Write a report detailing the process, including the steps you followed, the data you retrieved, and any observations.

3. **Backup Data**:

- Ensure that all the extracted data is securely backed up to avoid data loss.

This procedure should align with how you prefer to perform your mobile forensic analysis using SAFT on Windows.

Result :

Forensic tools like SAFT can extract call logs, SMS messages, and contact lists from mobile devices by creating a bit-for-bit copy of the data, analyzing it, and generating detailed reports.

Aim: To Perform Registry Analysis and Get Boot Time Logging Using Process Monitor Tool

Step 1: Download and Install Process Monitor

Download Process Monitor:

Visit the Sysinternals Process Monitor download page.

Click the download link to obtain the zip file.

Extract and Run:

After downloading, extract the zip file to a folder of your choice.

Open the extracted folder and double-click Procmon.exe to launch the application. No installation is required as it is a standalone executable.

Step 2: Configure Process Monitor

Open Process Monitor:

Launch Process Monitor if it's not already open.

Set Up Filters:

Go to the menu bar and click Filter, then select Filter... (or press Ctrl + L).

In the Filter dialog box, set up filters to capture relevant data:

Add Filter for Process Start:

In the filter configuration, set Event Class to Process Start.

Add Filter for File System Events:

Set Event Class to File System.

Click Add to add each filter.

Click OK to apply these filters and close the dialog.

Step 3: Start Logging

Begin Capturing Data:

Click the Capture button (magnifying glass icon) located on the toolbar. This starts the real-time capture of system activities.

Step 4: Reboot the System

Restart Your Computer:

Reboot your system while Process Monitor is actively capturing data. This allows the tool to record all activities occurring during the boot process.

Step 5: Stop Logging After Boot

End Data Capture:

After the system has completely booted up and is fully operational, return to Process Monitor.

Click the Capture button again to stop logging. This halts the data collection process.

Step 6: Save and Analyze Logs

Save the Captured Data:

Go to File > Save to store the captured data.

Choose a location and save the data as a .PML file. This file contains all the logged events.

Review Boot-Time Activities:

Use Process Monitor's search and filtering features to analyze the saved logs.

Focus on boot-time processes and file system activities to identify performance issues, unusual delays, or errors during the system startup.

Result:

Registry Analysis:

Use the Registry Editor to examine boot-related settings and configurations that impact system performance.

Boot Time Logging:

Employ Process Monitor to capture and analyze boot-time activities, providing insights into the processes and file system operations that occur during system startup. This helps in identifying and addressing any performance issues or anomalies.

WinHex is a powerful tool that serves multiple purposes, including data recovery, forensics, and low-level analysis. Let's delve into what it offers:

1. **Hex Editor**: WinHex is an advanced **hexadecimal editor** that allows you to inspect and edit various types of files. Whether you're dealing with hard drives, floppy disks, CD-ROMs, DVDs, or Compact Flash cards, WinHex provides direct access for editing.
2. **Data Recovery**: If you've lost data on a hard drive, WinHex comes to the rescue. It enables you to recover data from almost anywhere on the drive. You can even read areas that contain deleted or damaged data.
3. **Forensics Tool**: WinHex is widely used for **evidence gathering** in forensics. Law enforcement agencies, companies, and organizations rely on it. Some of its features include:

    - Interpreting 20 data types
    - Editing partition tables, boot sectors, and other data structures using templates
    - Analyzing and comparing files
    - Searching and replacing
    - Creating hashes and checksums
    - Wiping drives

WinHex is a versatile tool that can assist you in **data recovery** from various storage media. Let's explore how you can use it:

1. **File Recovery with the Directory Browser**:
    - Open the disk you want to recover data from using the **disk editor** in WinHex.
    - Navigate to a specific directory or explore the root directory recursively.
    - Select the files you wish to recover.
    - Right-click and choose the **Recover/Copy** command from the context menu. This action will copy the selected files to a different location.

2. **Automatic Recovery of Files**:

- This method doesn't require a healthy file system.
- WinHex can automatically recover files of a certain type. Specify the file type you want to recover, and the tool will search for and retrieve those files.

3. **Manual Data Recovery**:

- WinHex is a powerful tool for **manually recovering data**.
- You can restore lost or deleted files that haven't been physically erased or overwritten. These files are typically marked as deleted in the file system (logical deletion).

- Use WinHex to examine the disk’s structure, identify deleted data, and recover it.

Remember that data recovery can be a delicate process, especially when dealing with damaged or corrupted storage media. Always work on a **copy of the original data** to avoid accidental overwrites or further damage.

DISK Image

Creating a disk image using **WinHex** is a valuable skill, especially for data recovery and forensic purposes. Let’s walk through the steps:

1. **Open WinHex**:
   - Launch WinHex on your system.
2. **Select the Physical Disk**:
   - From the **Tools** menu, choose **“Open Disk…”**.
   - In the dialog that appears, select the **physical disk** you want to create an image of.
   - It’s crucial to choose the **Physical Media** option to ensure you capture the entire disk. If you select a **Logical Drive Letter**, you’ll only get an image of a single partition.
3. **Create the Disk Image**:

- Once the disk is open in WinHex, go to the **File** menu.
- Select **“Create Disk Image…”**.
- In the dialog box that appears:
  - Choose **“Raw image (dd)”** as the image file format.
  - Specify a location to save the image by clicking the three-dot button in the **Path and filename** field.
  - Optionally, enter your name in the **Examiner** box.
  - Check the box for **“Compute hash”** (this computes a hash value for integrity verification).
  - Leave other settings at their default values.
  - Click **OK** to proceed.

4. **Select Hash Type**:

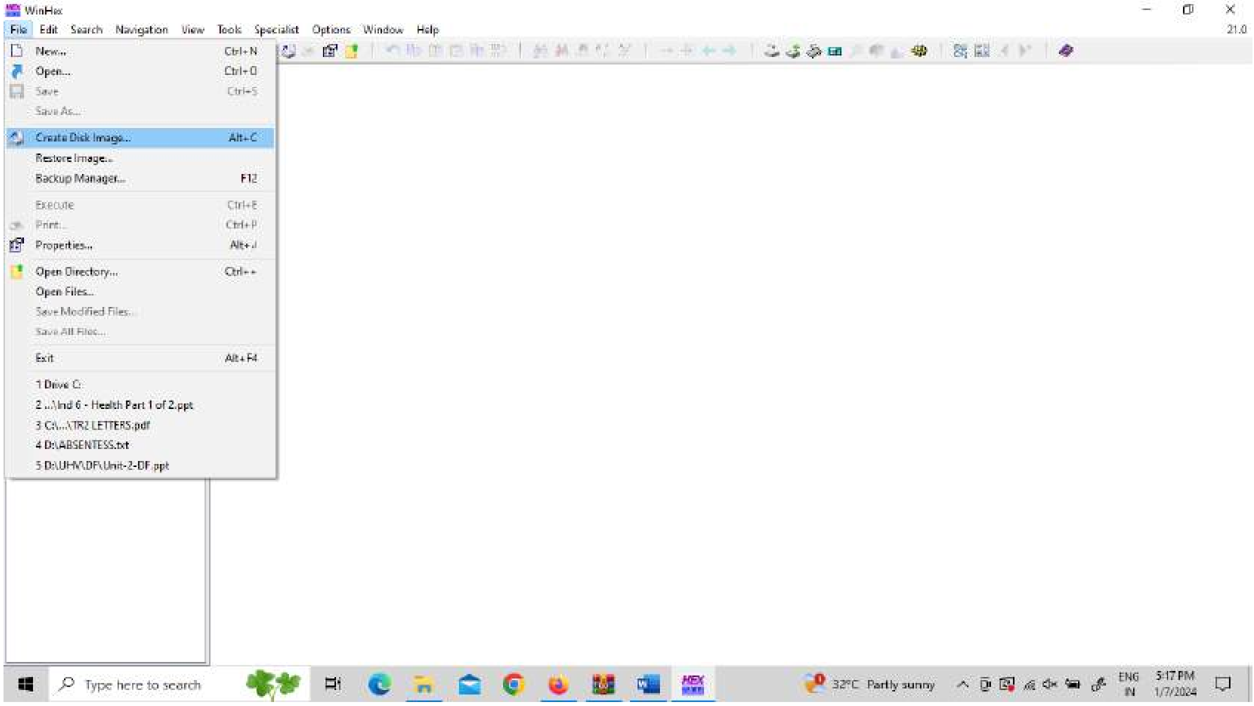
- After clicking OK, choose the type of hash you want to compute (e.g., **MD5**) from the drop-down menu.

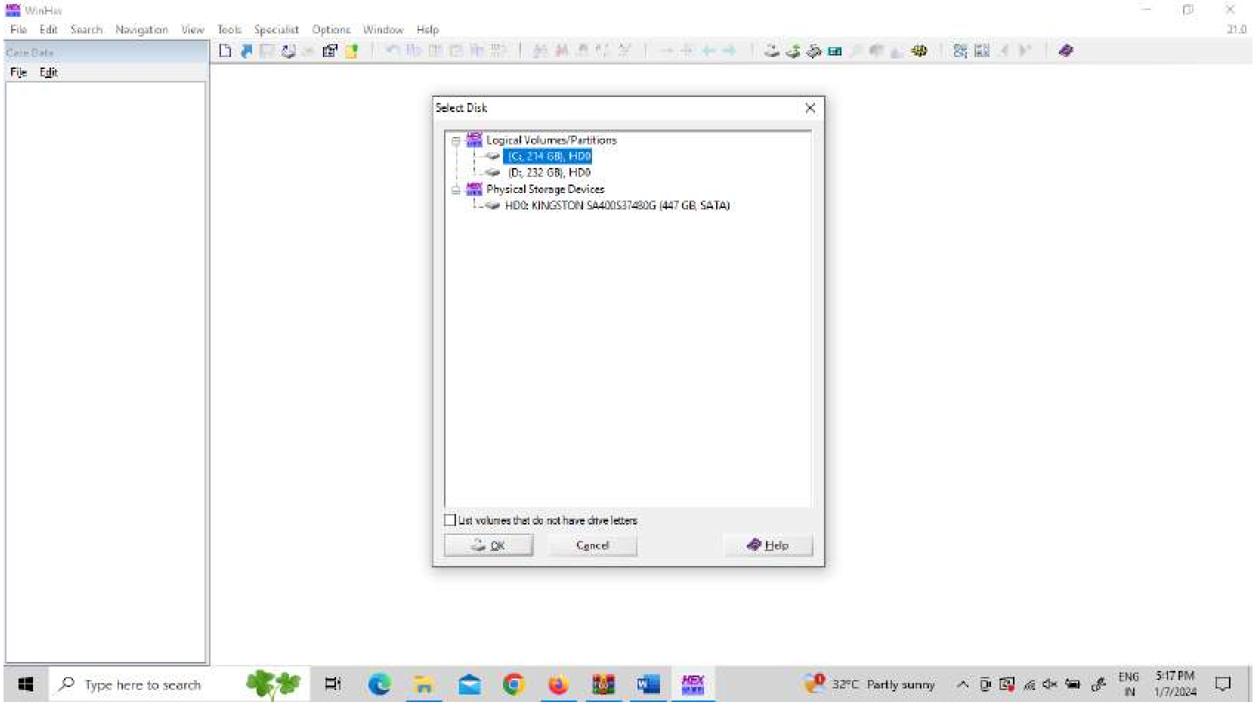
5. **Image Creation Process**:

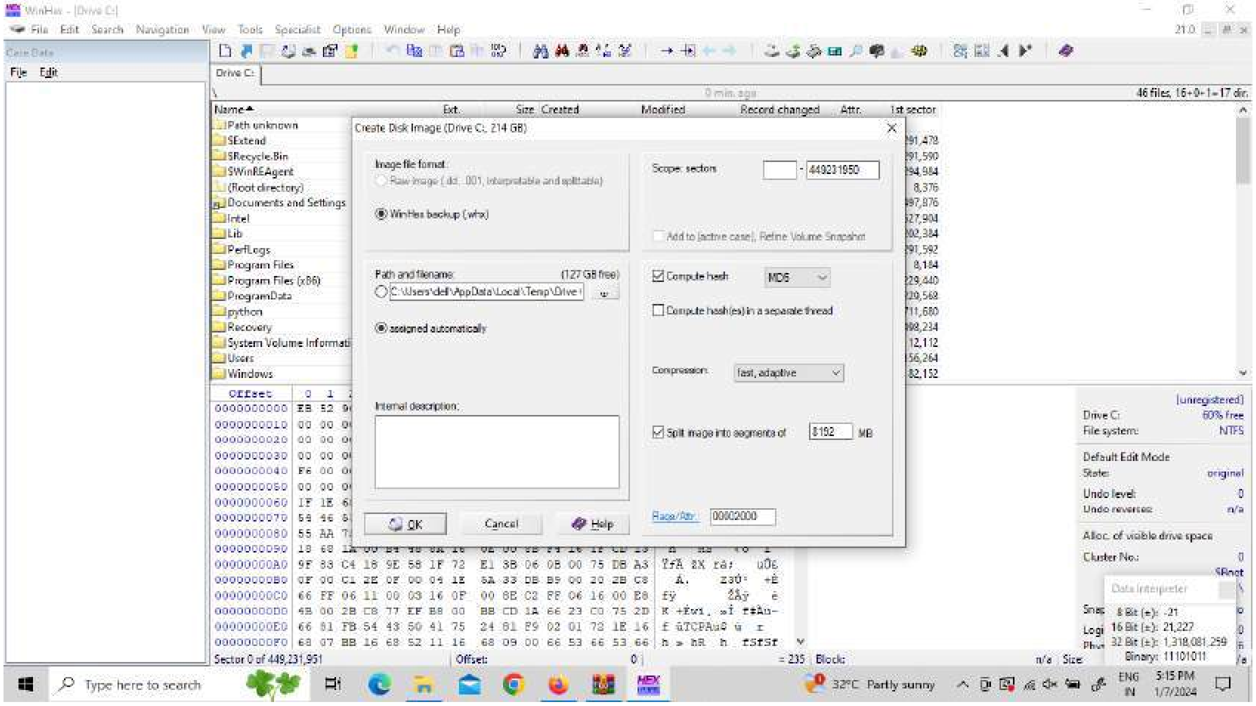
- WinHex will start creating the disk image.
- Once the process is complete, a dialog will display the computed hash value.

- Your image is now complete!

Note: The destination folder will contain the **dd image file** and a **text file** with the computed hash value.




WinHex
File Edit Search Navigation View Tools Specialist Options Window Help
21.0
Case Data
File Edit
Select Disk
Logical Volumes/Partitions
(C:, 214 GB), HD0
(D:, 232 GB), HD0
Physical Storage Devices
HD0: KINGSTON SA400S37480G (447 GB, SATA)
□ List volumes that do not have drive letters
OK
Cancel
Help
Type here to search
32°C Partly sunny
ENG IN
5:17 PM 1/7/2024



WinHex - [Drive C:]

Create Disk Image (Drive C:, 214 GB)

Image file format:
○ Raw image (.dd, .001, interpretable and splittable)
● WinHex backup (.whx)

Scope: sectors [ ] - [449231950]

□ Add to [active case], Refine Volume Snapshot

Path and filename: (127 GB free)
○ C:\Users\dell\AppData\Local\Temp\Drive
● assigned automatically

☑ Compute hash [MD5]
□ Compute hash(es) in a separate thread

Compression: [fast, adaptive]

Internal description:

☑ Split image into segments of [8192] MB

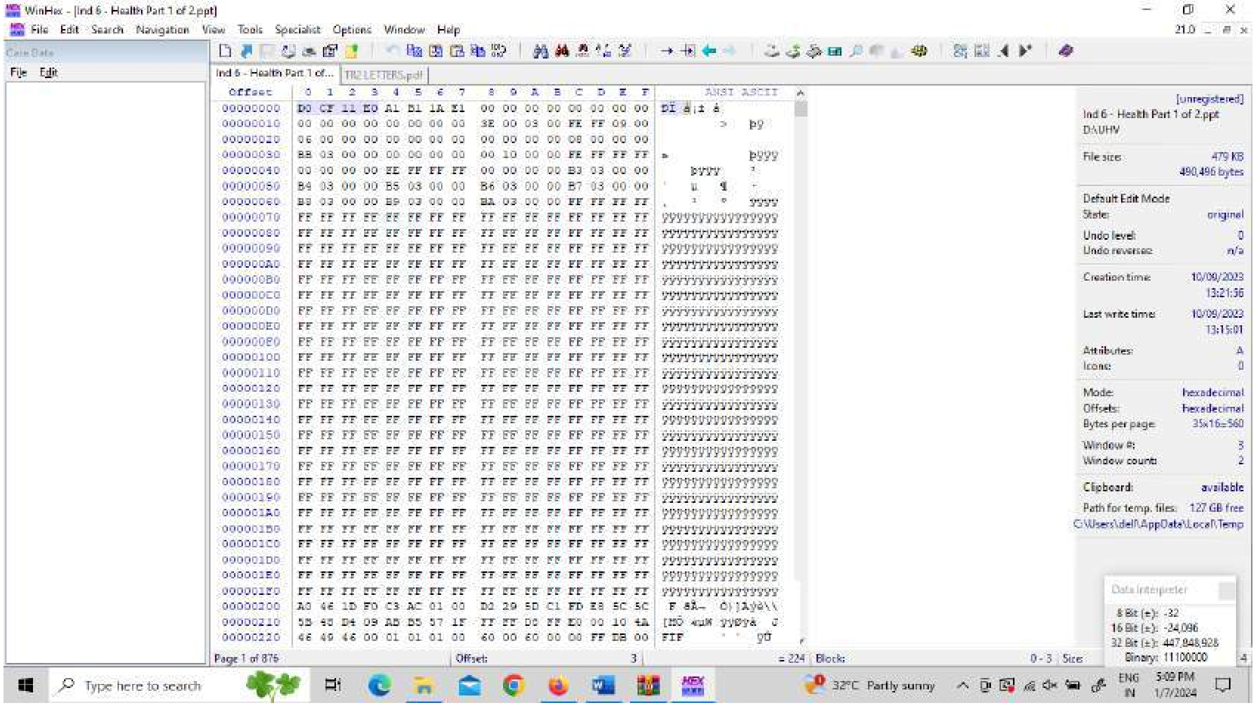
Page/Attr.: [00002000]

Drive C: 60% free
File system: NTFS

Sector 0 of 449,231,951

The highlighted row represents the file type.

PPT file



WinHex - [Ind 6 - Health Part 1 of 2.ppt]

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  D0 CF 11 E0 A1 B1 1A E1  00 00 00 00 00 00 00 00
00000010  00 00 00 00 00 00 00 00  3E 00 03 00 FE FF 09 00
00000020  06 00 00 00 00 00 00 00  00 00 00 00 08 00 00 00
00000030  BB 03 00 00 00 00 00 00  00 10 00 00 FE FF FF FF
00000040  00 00 00 00 BE FF FF FF  00 00 00 00 B3 03 00 00
00000050  B4 03 00 00 B5 03 00 00  B6 03 00 00 B7 03 00 00
00000060  B8 03 00 00 B9 03 00 00  BA 03 00 00 FF FF FF FF
00000070  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000080  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000090  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000000A0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000000B0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000000C0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000000D0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000000E0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000000F0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000100  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000110  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000120  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000130  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000140  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000150  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000160  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000170  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000180  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000190  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000001A0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000001B0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000001C0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000001D0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000001E0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
000001F0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF
00000200  A0 46 1D F0 C3 AC 01 00  D2 29 5D C1 FD E8 5C 5C
00000210  5B 45 D4 09 AB B5 57 1F  FF FF D8 FF E0 00 10 4A
00000220  46 49 46 00 01 01 01 00  60 00 60 00 00 FF DB 00
```

Ind 6 - Health Part 1 of 2.ppt
D:\UHV

File size: 479 KB
490,496 bytes

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 10/09/2023 13:21:36
Last write time: 10/09/2023 13:15:01

Attributes: A
Icons: 0

Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 35x16=560

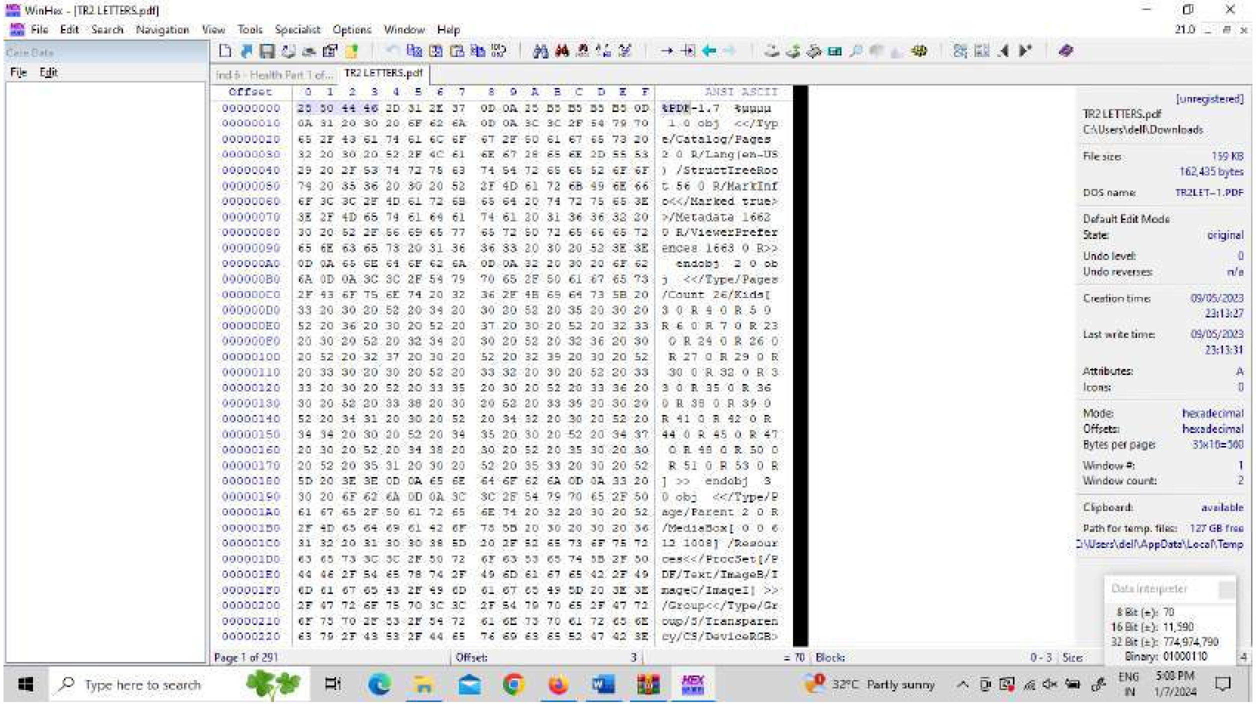
Window #: 3
Window count: 2

Clipboard: available

Path for temp. files: 127 GB free
C:\Users\dell\AppData\Local\Temp

Page 1 of 876

PDF file


WinHex - [TR2 LETTERS.pdf]
File Edit Search Navigation View Tools Specialist Options Window Help
21.0
Case Data
File Edit
Ind 6 - Health Part 1 of...
TR2 LETTERS.pdf

```
 Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F    ANSI ASCII
00000000   25 50 44 46 2D 31 2E 37  0D 0A 25 B5 B5 B5 B5 0D   %PDF-1.7  %µµµµ
00000010   0A 31 20 30 20 6F 62 6A  0D 0A 3C 3C 2F 54 79 70    1 0 obj  <</Typ
00000020   65 2F 43 61 74 61 6C 6F  67 2F 50 61 67 65 73 20   e/Catalog/Pages 
00000030   32 20 30 20 52 2F 4C 61  6E 67 28 65 6E 2D 55 53   2 0 R/Lang(en-US
00000040   29 20 2F 53 74 72 75 63  74 54 72 65 65 52 6F 6F   ) /StructTreeRoo
00000050   74 20 35 36 20 30 20 52  2F 4D 61 72 6B 49 6E 66   t 56 0 R/MarkInf
00000060   6F 3C 3C 2F 4D 61 72 6B  65 64 20 74 72 75 65 3E   o<</Marked true>
00000070   3E 2F 4D 65 74 61 64 61  74 61 20 31 36 36 32 20   >/Metadata 1662 
00000080   30 20 52 2F 56 69 65 77  65 72 50 72 65 66 65 72   0 R/ViewerPrefer
00000090   65 6E 63 65 73 20 31 36  36 33 20 30 20 52 3E 3E   ences 1663 0 R>>
000000A0   0D 0A 65 6E 64 6F 62 6A  0D 0A 32 20 30 20 6F 62     endobj  2 0 ob
000000B0   6A 0D 0A 3C 3C 2F 54 79  70 65 2F 50 61 67 65 73   j  <</Type/Pages
000000C0   2F 43 6F 75 6E 74 20 32  36 2F 4B 69 64 73 5B 20   /Count 26/Kids[ 
000000D0   33 20 30 20 52 20 34 20  30 20 52 20 35 20 30 20   3 0 R 4 0 R 5 0 
000000E0   52 20 36 20 30 20 52 20  37 20 30 20 52 20 32 33   R 6 0 R 7 0 R 23
000000F0   20 30 20 52 20 32 34 20  30 20 52 20 32 36 20 30    0 R 24 0 R 26 0
00000100   20 52 20 32 37 20 30 20  52 20 32 39 20 30 20 52    R 27 0 R 29 0 R
00000110   20 33 30 20 30 20 52 20  33 32 20 30 20 52 20 33    30 0 R 32 0 R 3
00000120   33 20 30 20 52 20 33 35  20 30 20 52 20 33 36 20   3 0 R 35 0 R 36 
00000130   30 20 52 20 33 38 20 30  20 52 20 33 39 20 30 20   0 R 38 0 R 39 0 
00000140   52 20 34 31 20 30 20 52  20 34 32 20 30 20 52 20   R 41 0 R 42 0 R 
00000150   34 34 20 30 20 52 20 34  35 20 30 20 52 20 34 37   44 0 R 45 0 R 47
00000160   20 30 20 52 20 34 38 20  30 20 52 20 35 30 20 30    0 R 48 0 R 50 0
00000170   20 52 20 35 31 20 30 20  52 20 35 33 20 30 20 52    R 51 0 R 53 0 R
00000180   5D 20 3E 3E 0D 0A 65 6E  64 6F 62 6A 0D 0A 33 20   ] >>  endobj  3 
00000190   30 20 6F 62 6A 0D 0A 3C  3C 2F 54 79 70 65 2F 50   0 obj  <</Type/P
000001A0   61 67 65 2F 50 61 72 65  6E 74 20 32 20 30 20 52   age/Parent 2 0 R
000001B0   2F 4D 65 64 69 61 42 6F  78 5B 20 30 20 30 20 36   /MediaBox[ 0 0 6
000001C0   31 32 20 31 30 30 38 5D  20 2F 52 65 73 6F 75 72   12 1008] /Resour
000001D0   63 65 73 3C 3C 2F 50 72  6F 63 53 65 74 5B 2F 50   ces<</ProcSet[/P
000001E0   44 46 2F 54 65 78 74 2F  49 6D 61 67 65 42 2F 49   DF/Text/ImageB/I
000001F0   6D 61 67 65 43 2F 49 6D  61 67 65 49 5D 20 3E 3E   mageC/ImageI] >>
00000200   2F 47 72 6F 75 70 3C 3C  2F 54 79 70 65 2F 47 72   /Group<</Type/Gr
00000210   6F 75 70 2F 53 2F 54 72  61 6E 73 70 61 72 65 6E   oup/S/Transparen
00000220   63 79 2F 43 53 2F 44 65  76 69 63 65 52 47 42 3E   cy/CS/DeviceRGB>
```

[unregistered]
TR2 LETTERS.pdf
C:\Users\dell\Downloads

File size: 159 KB
162,435 bytes
DOS name: TR2LET~1.PDF

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 09/05/2023 23:13:27
Last write time: 09/05/2023 23:13:31

Attributes: A
Icons: 0

Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 35x16=560
Window #: 1
Window count: 2

Clipboard: available
Path for temp. files: 127 GB free
C:\Users\dell\AppData\Local\Temp

Data Interpreter
8 Bit (±): 70
16 Bit (±): 11,590
32 Bit (±): 774,974,790
Binary: 01000110

Page 1 of 291 | Offset: 3 | = 70 | Block: 0 - 3 | Size: 4

EXPERIMENT 6 :

perform data analysis on the history of open files and folders using the Last View Activity tool

Step-by-Step Procedure for Data Analysis

Step 1: Prepare Your Environment

1. **Search for Last View Activity Tool**: Open your web browser and search for "Last View Activity tool download."

2. **Download the Tool**: Choose a reliable source and download the free version of the Last View Activity tool.

3. **Extract the Tool**: Locate the downloaded ZIP file, right-click it, and select "Extract All" to unpack its contents.

Step 2: Open the Last View Activity Tool

1. **Launch the Tool**: Navigate to the extracted folder and double-click on the executable file (e.g., `LastView.exe`) to run the tool.

Step 3: Select Data to Analyze

1. **Choose User Profile**: In the tool, select the user profile or directory you wish to analyze for file and folder access history.

2. **Set Filters**: If needed, apply filters for specific time ranges or file types to narrow down your analysis.

Step 4: Run the Analysis

1. **Execute Analysis**: Click the button to start the analysis process and gather information about recently opened files and folders.

Step 5: Review Data Output

1. **Examine Results**: Once the analysis is complete, review the output, which includes:

   - Timestamps of file and folder accesses.

   - User account information.

   - Types of actions performed (e.g., open, modify, delete).

Step 6: Identify Patterns

1. **Analyze Behavior**: Look for patterns in the data, such as frequently accessed files, unusual access times, or specific user activities.

Step 7: Data Organization

1. **Export Data**: If the tool allows, export the analysis results to a CSV or Excel file for easier handling.

2. **Organize Data**: Clean and categorize the data into relevant groups, such as:

   - Date and time of access.

   - Usernames.

   - File or folder paths.

   - Types of actions.

Step 8: Analyze the Data

1. **Perform Statistical Analysis**: Use software like Excel or Python to conduct statistical analysis, such as:

   - Frequency counts of file accesses.

   - Time spent on different folders or files.

   - Access pattern comparisons between users.

Step 9: Visualization

1. **Create Visuals**: Generate graphs or charts to visualize your findings for better insights (e.g., bar charts showing the most accessed files).

Step 10: Draw Conclusions

1. **Summarize Key Findings**: Based on your analysis, summarize the significant findings, such as user behavior patterns or potential security concerns.

2. **Make Recommendations**: Provide recommendations for enhancing data security or optimizing file access if necessary.

Step 11: Document the Experiment

1. **Prepare a Report**: Document the entire process, findings, and conclusions in a comprehensive report format.

2. **Include Visuals**: Add any graphs or charts to the report to support your findings and make them visually appealing.

Experiment-7

AIM:.performing network analysis using network miner tool

PROCEDURE:

Step-by-Step Procedure for Using NetworkMiner

Step 1: Download NetworkMiner

1. Visit the Official Website:

   - Go to the [NetworkMiner download page](https://www.netresec.com/?page=NetworkMiner).

2. Select the Version:

   - Download the latest version of NetworkMiner (either the installer or the portable version).

Step 2: Install NetworkMiner

- For Portable Version:

  1. Extract the ZIP file to a folder of your choice.

  2. No installation is required; you can run the application directly from this folder.

Step 3: Configure Windows Firewall

1. Open Command Prompt:

   - Press `Win + R`, type `cmd`, and press Enter.

2. Open Windows Firewall with Advanced Security:

   - Type the following command and press Enter:

```
wf.msc
```

   - This opens the Windows Firewall with Advanced Security console.

3. Create a New Inbound Rule:

   - In the left pane, click on Inbound Rules.
   - In the right pane, click on New Rule....

4. Select Rule Type:

   - Choose Program and click Next .

5. Browse for NetworkMiner:

   - Click on This program path and browse to the folder where you extracted NetworkMiner. Select NetworkMiner.exe and click Next.

6. Allow the Connection:

   - Select Allow the connection and click Next.

7. Profile Selection:

- Choose the profiles you want the rule to apply to (Domain, Private, Public) and click Next.

8. Name the Rule:

- Give the rule a name (e.g., "NetworkMiner") and click **Finish**.

Step 4: Capture Network Traffic Using Wireshark

1. Install Wireshark(if you haven't already):

- Download from the [Wireshark website](https://www.wireshark.org/download.html) and install it.

2. Open Wireshark:

- Launch Wireshark and select the network interface you want to capture traffic on (e.g., Ethernet or Wi-Fi).

3. Start Capture:

- Click on the interface to start capturing packets.

4. Save the Capture:

- After capturing the traffic for a desired period, stop the capture and save it in **PCAP** format (File > Save As).

Step 5: Analyze Network Traffic with NetworkMiner

1. Open NetworkMiner:

- Navigate to the folder where you extracted NetworkMiner and launch the application (NetworkMiner.exe).

2. Load the Capture File:

- Click on File> Open and select the PCAP file you saved from Wireshark.

3. Start Analyzing:

- NetworkMiner will parse the PCAP file and display information about sessions, files, credentials, and hosts involved in the network traffic.

4. Choose Ethernet Interface:

- If you want to capture traffic live, ensure you select the appropriate Ethernet interface in NetworkMiner.

5. Click on Start:

- Click on the Start button to begin the analysis.

step 6: Export Findings

Export Data:

If you want to save any reports or extracted data, go to File > Export and select the desired format.

Experiment-no: 08

Aim: Perform information for incident response using the CrowdResponse tool

Step-1. Preparation
- Download and install CrowdResponse from the official CrowdStrike website.
- Set up a secure, isolated environment to run the tool.
- Verify the integrity of the CrowdResponse binary to ensure it's legitimate.

Step-2. Initial Configuration
- Unzip the downloaded CrowdResponse package and open the folder.
- Review the *Config.xml* file to understand available modules.
- Customize *Config.xml* to specify the data you want to collect (e.g., processes, services, or files).

Step-3. Run CrowdResponse
- Open a command prompt with administrator privileges.
- Navigate to the folder containing CrowdResponse.
- Run `CrowdResponse.exe` with administrator rights for full access to system data.

Step-4. Data Collection
- Select specific modules in *Config.xml* for collecting artifacts like processes, network connections, and files.
- Run the modules sequentially to avoid overloading the system.
- Save collected data to a specified directory for easy retrieval.

Step-5. Process Analysis
- Review the list of running processes for suspicious or unexpected entries.
- Identify any suspicious process paths, parent-child relationships, and network connections.
- Save the process information for further analysis in a safe location.

Step-6. File Integrity Check
- Use the *FileListing* module to get a list of files with metadata (creation/modification times).
- Identify any recently modified files, especially in critical directories (e.g., System32).
- Save the output for forensic review to confirm if files are altered.

Step-7. Network Analysis
- Run the *NetworkConnections* module to gather information on active connections.
- Look for unusual connections or high volumes of traffic to unknown IPs.
- Note down any anomalies in the report for a detailed investigation.

Step-8. Memory Analysis
- Use *MemoryForensics* to analyze memory dumps for malware or abnormal activity.

- Extract any suspicious processes or injected code for further analysis.
- Save this data for use in a detailed forensic investigation.

Step- 9. Registry Analysis
- Execute *Registry* modules to capture registry settings and changes.
- Focus on startup entries, suspicious persistence mechanisms, or altered configurations.
- Save the registry dump for further examination of malicious persistence tactics.

Step-10. Log Review
- Run the *EventLogs* module to gather system and security event logs.
- Focus on recent logins, access attempts, or other abnormal activities.
- Save event logs for investigation, which can help trace the incident timeline.

Step-11. Artifact Analysis
- Review collected data for anomalies or evidence of compromise.
- Compare suspicious files, processes, or registry changes against known threat indicators.
- Document findings, providing a timeline and summarizing key indicators.

Step-12. Reporting and Escalation
- Summarize findings and provide relevant details on suspicious artifacts.
- Share data with security team members or escalate to higher authorities if needed.
- Compile all findings into a report for an organized summary and follow-up actions.

Step-13. Cleanup
- Clear CrowdResponse tool files and reports from the machine after analysis.
- Re-enable system protections disabled during the response.
- Close out the incident with a post-incident review and lessons learned.

Experiment-09:

Aim: Perform File type detection using Autopsy Tool

Step-1. preparation

- Download and install Autopsy from the official website.
- Launch Autopsy, and create a new case to organize and document the analysis.
- Set up a case name, number, and investigator information as needed.

Step-2. Add Data Source
- Select "Add Data Source" and choose the type of source (disk image, directory, or logical files).
- Browse to the file, disk image, or folder you want to analyze.
- Click "Next" to load the data into the Autopsy case.

Step-3. Enable File Type Detection
- Under "Ingest Modules," enable the *File Type Identification* module.
- This module uses file signatures and extensions to identify file types.
- Select any additional modules (like Hash Lookup or Keyword Search) for further analysis if needed.

Step-4 Run Ingest Process
- Click "Start" to begin the analysis process, and Autopsy will apply the selected modules.
- The file type detection module will identify files based on their headers and extensions.
- Allow the process to complete, as it may take time depending on the data size.

Step-5. View File Types
- Navigate to the "File Types" section in the left pane of Autopsy.
- Review categorized files by types like documents, images, videos, executables, etc.
- Double-click on any file type to see specific files and metadata within that category.

Step-6. Confirm File Types
- For detailed verification, view the file signature and compare it with the listed extension.
- Check any mismatches between expected and detected file types for anomalies.
- Document any suspicious files for further investigation.

Step-7. Export or Save Report
- Go to "Reports" and select the report format (HTML, CSV, or PDF) to export results.
- Customize the report to include relevant details like file paths, types, and metadata.
- Generate and save the report for documentation or sharing with other investigators.

Step-8. Review Findings
- Analyze the results to identify any potentially hidden or renamed file types.
- Use identified file types to investigate potential anomalies or malicious files.
- Close the case, keeping all findings for future reference or incident reporting.

This process allows you to efficiently detect and verify file types within a given data set using Autopsy.

Experiment-10:

Aim: Perform Memory Capture and Analysis using Live RAM Capture or any forensic tool

Part 1: Memory Capture with Live RAM Capture

Step-1. Preparation

- Download “Live RAM Capture” from the official Belkasoft website.
- Ensure you have administrator rights on the machine where you will perform the memory capture.

Step-2. Launch Live RAM Capture
- Run “Live RAM Capture” as an administrator to access and capture the memory correctly.
- Once opened, it will display a simple interface with a button to start capturing RAM.

Step-3. Configure Output Location
- Click on “Browse”to select a destination directory for the memory dump file (e.g., C:\memory_dump.mem).
- Name the output file, ensuring there is sufficient space on the drive to store the entire memory dump.

Step-4. Start Capture
- Click “Capture Memory” to begin the memory capture process.
- The tool will start creating a `.mem` file containing a full copy of the system’s active memory.

Step-5. Verify Completion
- Once the capture is complete, navigate to the output location to confirm the presence of the memory dump file.
- Check the file size to ensure it matches the size of the system's RAM (e.g., an 8 GB memory capture will result in a file approximately 8 GB in size).

Part 2: Memory Analysis with Volatility

Now that you have the memory dump, you can proceed with analysis using *Volatility*, a free and open-source memory forensics framework.

Step-1. Install Volatility
- Download Volatility from the official repository (works on Windows, Linux, or macOS).
- If you’re using Volatility 2.x, ensure Python 2.7 is installed.

Step-2. Determine the Profile
- Open a command prompt or terminal, and navigate to the folder containing Volatility.
- Run the following command to identify the operating system profile:
  - `volatility -f path_to_memory_dump imageinfo`
  - Replace `path_to_memory_dump` with the path of your `.mem` file (e.g., C:\memory_dump.mem).
- Note the suggested OS profile for use in later commands.

Step-3. Analyze Running Processes

- Run the “pslist” plugin to view all active processes at the time of capture:
  - `volatility -f path_to_memory_dump --profile=PROFILE pslist`
  - Replace `PROFILE` with the OS profile identified in the previous step.
- Review the process list to identify any unusual or suspicious processes.

Step-4. Examine Network Connections
- Use the *netscan* plugin to check open network connections:
  - `volatility -f path_to_memory_dump --profile=PROFILE netscan`
- This will display active and recent network connections, useful for spotting potentially malicious activity.

Step-5. Check DLLs and Suspicious Processes
- Run *dlllist* to list loaded DLLs for each process, which can reveal unusual or injected DLLs:
  - `volatility -f path_to_memory_dump --profile=PROFILE dlllist`
- Use *malfind* to detect potential code injections or malicious processes:
  - `volatility -f path_to_memory_dump --profile=PROFILE malfind`

Step-6. Registry Hive Inspection
- List registry hives using *hivelist* to inspect specific registry keys:
  - `volatility -f path_to_memory_dump --profile=PROFILE hivelist`
  - Use *printkey* for specific registry keys as needed.

Step-7. Strings Extraction
- Run *strings* to extract ASCII and Unicode strings from memory, which can reveal embedded text or indicators:
  - `strings path_to_memory_dump > strings_output.txt`

Step-8. Document Findings
- Summarize any findings, noting suspicious processes, connections, and potential malicious code.
- Save all relevant outputs, including logs and screenshots, for your report.

Step-9. Cleanup
- Store the memory dump and analysis files in a secure location for later reference.
- Exit Volatility, and delete sensitive files from the system if no longer needed to ensure data security.

Using *Live RAM Capture* with *Volatility* allows for a comprehensive memory analysis at no cost, providing insights into potential malware or other suspicious activity.