



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Computer Forensics (ACCD5000)

Analysis



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

Lab Activities are based on

TryHackMe, EC Council – CHFI, Digital Forensics Workbook and other Industry Digital Forensic Curriculum

Objectives

In continuation to our lectures, this hands-on Activity helps in providing you an overview of digital forensic analysis process.

ETHICAL STATEMENT

As discussed during our lectures, it is very important to adhere to Personal Ethics, Professional Ethics, Computer Ethics and Business Ethics.

We, the participants and stakeholders in the digital forensics laboratory, recognize the significance of ethical conduct when using digital forensics tools and processes for academic purposes. Our commitment to ethical standards is grounded in the principles of integrity, privacy, and responsible handling of digital data.

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various digital forensic activities. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using these tools for educational purposes on an outside environment, you should contact your lecturer prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Based on Activity 2, you must have a lab setup working.	☒
So far:	
HoA1: Understand Digital Evidences - Importance of Computer Forensics – Basic Investigation	☒
HoA2: Understand the importance of ensuring DATA Integrity – Computer Forensics Virtual Lab Setup	☒
HoA3: Understand Investigation Process, Ensure integrity of the evidence by calculating, comparing Hash Values	☒
HoA4: Understand Investigation Process – Copying Evidences and ensuring integrity	☒
Make sure the above activities are completed before starting this week's activity	
Task 1: Understanding File Systems	
Task 2: Analysing File System - Linux Image	
Task 3: Analysing File System – Windows Image	
Task 4: Recover Permanently Deleted Files	

ICONS Used in this document:

Find out the outcome/ Answers/ Solution and record your reflection



Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.



Recommended Screenshot (with Timestamp) for your Coursework.



Recommended to address this part in your Coursework.

Note: For this activity and other upcoming activities, you shall use any relevant screenshots or discussions to your coursework according to your judgement. I will not be recommending Screenshots/ Recommended part to address in the coursework.

Task 1: Analysing GUID Partition Table for anomalies

File List			
Name	Size	Type	Date Modified
00000000a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000000b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000000c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000000d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000000e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000000f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000130	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000140	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000150	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000001a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000001b0	00 00 00 00 00 00 00 00 00 00 77 F6 9F 21 00 00 00 00	----	
00000001c0	02 00 EE FE 7F 99 01 00 00 00 FF FF FF FF 00 00 00 00	----	--ip
00000001d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000001e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000001f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA	----	
0000000200	45 46 49 20 50 41 52 54 00 00 01 00 5C 00 00 00	----	EFI
0000000210	80 E5 81 AB 00 00 00 00 00 00 00 00 00 00 00 00 00	----	-A-
0000000220	AF 32 CF 1D 00 00 00 00 00 00 00 00 00 00 00 00 00	----	-2I-
0000000230	8E 32 CF 1D 00 00 00 00 00 00 00 00 00 00 00 00 00	----	-2I-
0000000240	A1 EF B1 FA C8 C8 F2 F5 02 00 00 00 00 00 00 00 00	----	1ad
0000000250	80 00 00 00 80 00 00 00 00 00 CB 93 1B 23 00 00 00	----	
0000000260	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000270	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000280	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000290	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000002a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000002b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000002c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000002d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000002e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
00000002f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000300	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000310	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000320	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000330	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000340	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000350	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000360	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000370	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	
0000000380	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----	

Resources: Available in Shared Resource Folder – GPT Analysis File

Sector 0	Protective MBR		
Sector 1	Primary GPT Header (Totally here, it uses 92 bytes)	45 46 49 20 50 41 52 54	Signature (8 Bytes)
		00 00 01 00	Revision Number (4)
		5C 00 00 00	GPT Header Size in bytes (4)
			(92 bytes)
		80 E5 81 AB	Header checksum (CRC32) (4)
		00 00 00 00	Reserved (4)
		01 00 00 00 00 00 00 00	LBA of GPT Header (sec 1) (8)
		AF 32 CF 1D 00 00 00 00	LBA of GPT Header (last sector of disk) (8)
		22 00 00 00 00 00 00 00	Starting LBA for partitions (8)
			(defined in partition table)
		8E 32 CF 1D 00 00 00 00	Ending LBA for partitions (8)
		6F 35 4E C1 A9 64 5F 49 A1 EF B1	Globally unique
		FA C8 C8 F2 F5	identifier(GUID) (16) for entire
			disk
		02 00 00 00 00 00 00 00	

No. of		80 00 00 00 80 00 00 00 CB 93 1B 23	Starting LBA of partition table (8) Number of partition entries (4) 128 Size of each entry (4) – 128 CRC Checksum of the Partition Table
--------	--	---	---

Files given to analyse: 1

1. Work on the above image and analyse the GPT Partition Table details. Do you see any anomalies?
2. Review the difference between MBR Partition and GPT Partition. Imagine, you receive two evidences. One with MBR Partition and other with GPT Partition. Document your analysis procedure. Do a “How, What, Why” approach to write your report and submit in moodle – Tutorial 4 Submission.

Task 2 – Analysing File System – Linux – Using Autopsy

Insights:

To investigate a hard disk, as a forensic investigator you must know the types of file systems and how to analyze them using various tools. Performing file system analysis allows an investigator to determine the following information:

File system type

Metadata information

Content information

1. Use Windows Server Machine.
2. For this lab, we are using Autopsy. Download and Install Autopsy.
3. Once the installation is complete, click Finish to exit the setup wizard.
4. Double-click the Autopsy 4.14.0 shortcut icon on the Desktop.
5. Autopsy Welcome window will appear along with Autopsy main window in the background. In the Welcome window, click New Case.
6. A New Case Information window opens asking you to input the Case Name and the Base Directory. The base directory is the location where the case data will get stored. The case name may be entered according to your identification purpose.
7. In this lab, we are assigning the case name as Linux_Analysis.

8. Before specifying the base directory, we will be creating a folder on the Desktop with the name Image File Analysis and setting the path of the Base directory to this folder.
9. Upon setting the base directory, click Next.
10. The New Case Information window now shows the Optional Information section where you can specify details such as name of the examiner and case number. Enter your name and the date when you are doing the activity as case number.
11. The Add Data Source window now appears displaying the section Select Type of Data Source To Add. Here, you need to select the type of data source to be provided as an input. In this lab, we will be analyzing a disk image; therefore, select the option Disk Image or VM File and click Next.
12. The Add Data Source window now displays the section Select Data Source where you need to select the location of the Image that you are going to examine. Click Browse.
13. An Open window will appear where you need to specify the forensic image. Use Linux_Evidence_001.img from our Resource Folder.
14. Once you set the path of the image file, click Next.
15. The Add Data Source window now displays the Configure Ingest Modules section, which contains lists of options that are checked. Select the options according to your requirement and click Next.
16. The Add Data Source window now displays the Add Data Source section, stating that the data source is added. Click Finish.
17. Autopsy will take some time to completely analyze the evidence file. You can proceed to the next steps of this lab even when the analysis of the evidence file is still in progress.
18. The application now displays the result in the Autopsy main window. Expand the Data Sources node in the left pane and click on the image file i.e., Linux_Evidence_001.img. This will show the contents of the image file.
19. Expand the image file Linux_Evidence_001.img to see its contents. Upon expanding the image, Autopsy displays the filesystem of the Linux:
20. You may examine all the required files stored in the image as a part of filesystem analysis. In this lab, we are going to view the passwd file that is stored in /etc location. Therefore, select the etc folder from the left pane.

21. Upon selecting the folder, all the files and folders present in etc are displayed in the right pane of the window.
22. Scroll down the window and select the passwd file.
23. Click the Text tab.
24. Autopsy displays all the text (user account information) present in the passwd file, under the Strings tab:
25. Similarly, click on the File Metadata, Hex, and Annotations tabs to view other details pertaining to the selected file.
26. This way, you can analyze all the other files and folders of your choice to get detailed information on them.
27. Apart from examining the file system, you can also calculate the hashes of the files that you examine, which helps in validating the integrity of the evidence.
28. In this lab, we will be calculating the MD5 hash of a file named SeatPlan.xls, which is located within /home/roger/Documents.
29. To view the MD5 hash value of this file, expand home --> roger --> Documents in the left pane. The SeatPlan.xls file appears in the right pane of the Autopsy window. Click the file.
30. The File Metadata section displays the selected folder/file's metadata information such as the file's created, modified, and accessed times followed by its MD5 hash value.
31. Click on File Metadata and scroll down the section to find the MD5 value for the SeatPlan.xls file.
32. Go through all the options of Autopsy in detail as required for your investigations.

Task 3: File System Analysis – Windows - using Sleuth Kit

Doing a File System Analysis will help you to determine the type of the file system, collect metadata information and any content available. Note that for this task, you are investigating a cyber incident.

No. of Files given to analyse: 2

Windows_Evidence_001.dd and Windows_Evidence_002.dd

Use Sleuth Kit for this Task. However, you are free to use other tools as well.

1. Install and Run The Slueth Kit (Ignore if installed already)

Note: To run The Slueth Kit, select the bin folder in the installed location, press shift + Right Click and select open command window here.

2. To view partition tables associated with **Windows_Evidence_001.dd** and **Windows_Evidence_002.dd**, select the image files (type `mmls "path\Windows_Evidence_002.dd"`) and press **Enter** (*Make sure the path of the evidence file is given appropriately*)
3. This displays the partition layout of a volume system (partition tables) associated with the evidence:

```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

   Slot   Start      End          Length      Description
000:  Meta   0000000000    0000000000    0000000001    Primary Table (#0)
001:  ----- 0000000000    0000002047    0000002048    Unallocated
002:  000:000 0000002048    0001026047    0001024000    NTFS / exFAT (0x07)
003:  000:001 0001026048    0052426751    0051400704    NTFS / exFAT (0x07)
004:  ----- 0052426752    0052428799    0000002048    Unallocated
```

4. Similarly, to view the type of file system and the OS, type `fsstat "Windows_Evidence_002.dd"` and then press **Enter**.

```
-----
File System Type: NTFS
Volume Serial Number: 94146F51146F3600
OEM Name: NTFS
Volume Name: Evidence
Version: Windows XP

METADATA INFORMATION
-----
First Cluster of MFT: 262144
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 1280
Root Directory: 5

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 524286
Total Sector Range: 0 - 4194302

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16) Size: 48-72 Flags: Resident
$ATTRIBUTE_LIST (32) Size: No Limit Flags: Non-resident
```

5. From the above commands/ analysis, what is your assumption?
Hint: The file system is **NTFS** and the source OS is **Windows XP**.
6. To view the details of the selected image. Type `img_stat "Windows_Evidence_002.dd"` and press **Enter** to view the details.

```
-----
IMAGE FILE INFORMATION
-----
Image Type: raw

Size in bytes: 2147483648
Sector size: 512
```

7. Use the **istat** tool in **The Sleuth Kit** to view the details of metadata structure.

To display an overview of the MFT file, type

istat -f ntfs "Windows_Evidence_002.dd" 0 and press **Enter**.

```
MFT Entry Header Values:
Entry: 0          Sequence: 1
$LogFile Sequence Number: 2450902
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-18)
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFT
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 16384 Actual Size: 16384
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
```

Refer to our lecture on File System. The **Master File Table (MFT)** has an entry for every file and directory; hence, it is required to find all other files. The layout of the MFT is determined by processing entry **0** in the **MFT**.

8. Type **istat -f ntfs "Windows_Evidence_002.dd" 1** and press **Enter** to display the **MFTMirr** File Overview. MFT entry **1** is for the **MFTMirr** file, which has a non-resident attribute that contains a backup copy of the first MFT entry.
9. To display an overview of the Boot File, type
- istat -f ntfs "Windows_Evidence_002.dd" 7** and press **Enter**.

```
MFT Entry Header Values:
Entry: 7          Sequence: 7
$LogFile Sequence Number: 0
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 0 ( )
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $Boot
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 8192 Actual Size: 8192
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 48
Type: $FILE_NAME (48-2) Name: N/A Resident size: 76
```

The Boot file system metadata file is in MFT entry **7** and contains the boot sector of the file system.

10. To display an overview of the volume filesystem metadata file, type

istat -f ntfs "Windows_Evidence_002.dd" 3 and press Enter.

```

MFT Entry Header Values:
Entry: 3          Sequence: 3
$LogFile Sequence Number: 2119253
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 257 (S-1-5-18)
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $Volume
Parent MFT Entry: 5      Sequence: 5
Allocated Size: 0        Actual Size: 0
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72

```

The volume file system metadata file is in MFT entry **3** and contains the volume label and other version-related information.

11. To display an overview of the AttrDef file, type

istat -f ntfs "Windows_Evidence_002.dd" 4 and press Enter.

```

MFT Entry Header Values:
Entry: 4          Sequence: 4
$LogFile Sequence Number: 2118573
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-18)
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $AttrDef
Parent MFT Entry: 5      Sequence: 5
Allocated Size: 4096     Actual Size: 2400
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72

```

The MFT entry for the AttrDef filesystem metadata file is **4**. It defines the names and type identifiers for each type of attribute.

12. To display an overview of the Bitmap file, type

istat -f ntfs "Windows_Evidence_002.dd" 6 and press Enter.

The MFT entry of the Bitmap file system metadata file, which determines the status of the cluster, is **6**.

13. To display an overview of the BadClus file, type

istat -f ntfs "Windows_Evidence_002.dd" 8 and press Enter.

```

MFT Entry Header Values:
Entry: 8          Sequence: 8
LogFile Sequence Number: 2118643
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-18)
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $BadClus
Parent MFT Entry: 5      Sequence: 5
Allocated Size: 0      Actual Size: 0
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72

```

NTFS keeps track of the damaged clusters by allocating them to a \$DATA attribute of the BadClus file system metadata file. The MFT entry is **8**.

14. To display an overview of the Secure file, type

istat -f ntfs "Windows_Evidence_002.dd" 9 and press **Enter**.

The Secure file metadata file stores the security descriptors that define the access control policy for a file or directory. The MFT entry for it is **9**.

15. Use the fls command-line tool of TSK to list the files and directory names. Type

fls -f ntfs "Windows_Evidence_002.dd" and then press **Enter**.

16. Now, we shall recover these files from the image using the **tsk_recover** module. Before running this module, you need to create a folder named **Files_ret** on the Desktop.

17. Upon creating the folder, switch back to the command prompt, type the command

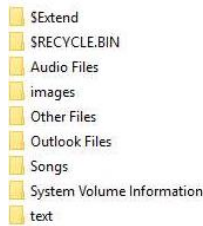
tsk_recover -i raw -e "Windows_Evidence_002.dd" "C:\Users\Administrator\Desktop\Files_ret" and press **Enter**.

The **-i** switch represents the image type. Since we are using a **dd** file, the image type that we specified in the command is **"raw"**. Entering the **-e** switch instructs the tool to recover all the files (allocated and non-allocated).

The tool begins to retrieve the files from the forensic image. Upon completion, it returns a message displaying the number of files recovered:

#Ignore any errors that occur during the recovery process.

18. To view the retrieved files, navigate to the **Desktop** and open the folder. You can view the retrieved files/directories as shown in the following screenshot:



This way, you can use **The Sleuth Kit** to obtain information related to the data contained within an image file and retrieve the files and folders from it.

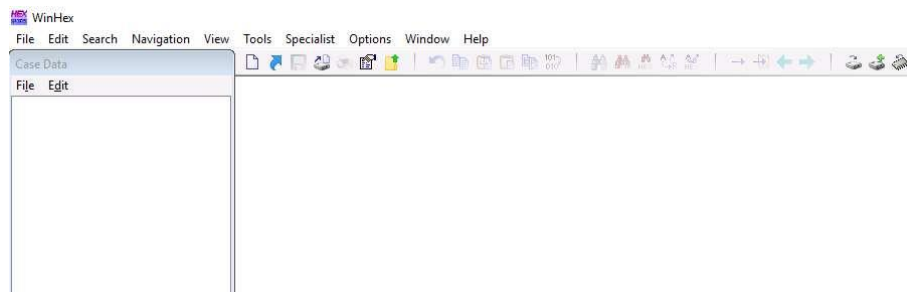
Task 4: File System Analysis – Recover permanently deleted files.

With the earlier tasks (analysing file system), you must be clear and able to visualize the file system and the file types by Analysis the evidences. Now, with this task, let's understand how to recover permanently deleted files.

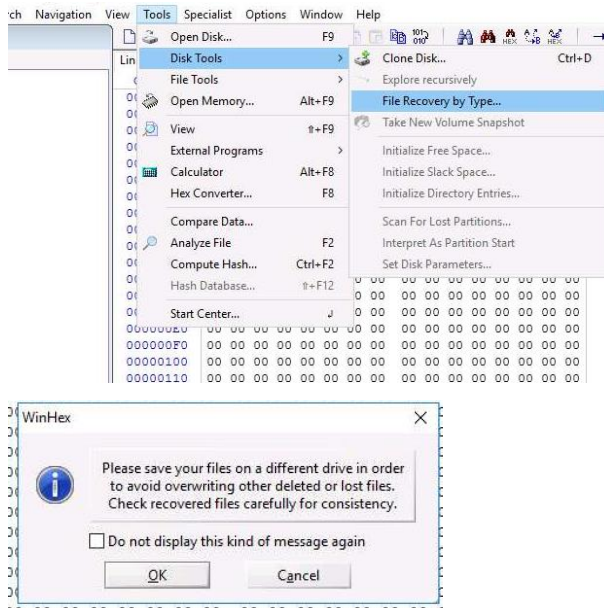
No. of Files given to analyse: 1

Use WinHex for this Task. However, you are free to use other tools as well.

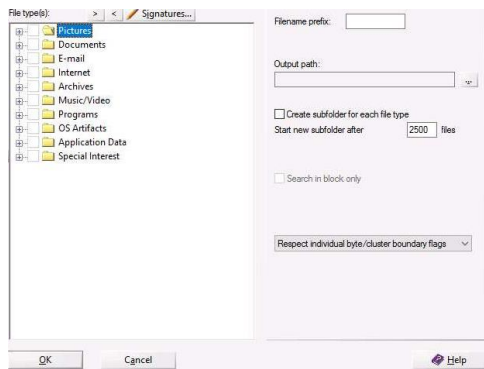
1. Download and install WinHex.



2. Open WinHex and add the evidence file **Windows_Evidence_001.img** and click **Open**. **WinHex** evaluation pop-up will subsequently appear; click **OK** to close the pop-up.
3. **WinHex** will process the image file and display the following window with a **Data Interpreter** pop-up at the lower right corner of the window.
4. Navigate to **Tools**



5. **File Header Search on Windows_Evidence_001.img** window appears displaying file types that you want to extract.



6. Now, let's extract pictures; therefore, click on the + node to expand the **Pictures** folder.
7. Select the image file formats of your choice under the **Pictures** folder and click **OK**.
8. Similarly, you can also choose other file types for the investigation process. The output might vary depending on the file types that you selected.
9. **Select Target Folder** window will appear. Navigate to the location where you want to save the retrieved files (here, **Desktop**), create a folder named **Rec_Files** and then click **Open**.
10. The application now displays the selected folder. Click **OK**.
11. To start the recovery process, click **OK** in the **File Header Search on Windows_Evidence_001.img** window. This action will close the window and start recovering the files (with the specified file types) from the image.

12. After the recovery process is complete, click **OK** in the **File Recovery by Type** pop-up window to close the processing window.
13. To view the recovered files, open the destination folder where you saved them.
14. This way, you can recover files from a forensic image using **WinHex**.



Overall Reflection

Record your reflection via Moodle – Group Discussion.

1. Understanding of the concepts discussed in the lecture and its relation to the activity done.
2. Understanding Analysis Process (Hard Disk and File System).
3. Understanding and implementing an analysis ensuring data integrity.
4. Rate yourself (1 very low – 5 exceptional): Understanding the Investigation Process.

-----**End of Activity**-----