



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

Applied Computing

Wales Institute of Science and Art (WISA)

Digital Forensics (ACCA7031)

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.

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 1, 2 and 3, (if you have completed them!!!) you must be clear on the process of identifying digital evidence, and secure them, acquiring data from its original sources ensuring its integrity using various tools and working with acquired images. In Activity 3, you analysed different files to find out more information. Now, lets move forward to further analyse GPT file partitions and analyse more in detail.

Task 1: Analysing GPT File Partitions

Task 2: File System Analysis – Scenario 1 using Autopsy

Task 3: File System Analysis – Scenario 2 using Sleuth Kit

Task 4: File System Analysis – Scenario 3 using WinHex

Task 5: Investigating a Suspicious Email

Task 6: Recovering Deleted Email Messages Using Recover My Email

Task 7: Analyzing Android Forensic Image and Carving Deleted Files

Task 8: Investigating digital evidences – 3

ICONS Used in this document:

Find out the outcome/ Answers/ Solution



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 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	----	Å
0000000220	AF 32 CF 1D 00 00 00 00 00 00 00 22 00 00 00 00 00	----	2I
0000000230	8E 32 CF 1D 00 00 00 00 00 00 00 6F 35 4E C1 A9 64 5F 49	----	2I
0000000240	A1 EF B1 FA C8 C8 F2 F5 02 00 00 00 00 00 00 00	----	i&d
0000000250	80 00 00 00 80 00 00 00 00 CB 93 1B 23 00 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 Virtual Machine (Sample GPT 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 identifier (GUID) (16) for entire disk
		FA C8 C8 F2 F5	
		02 00 00 00 00 00 00 00	Starting LBA of partition table
		80 00 00 00	(8) Number of partition entries
		80 00 00 00	(4) 128

		CB 93 1B 23	Size of each entry (4) – 128 CRC Checksum of the Partition Table
--	--	-------------	--

No. of Files given to analyse: 1

Task:

Work on the above image and analyse the GPT Partition Table details. Do you see any anomalies?

Create your own image and analyse for any anomalies. Document the details in a Report.

From your Activity 3 and 4, 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.

Deliverables:

1. Created image (appropriately named and submitted in the shared folder with appropriate name)
2. Analysis Report
3. Review Presentation (MBR & GPT Partition) – Record a Video and submit the link in Moodle. Make sure the link is available for the lecturer to view and feedback.

Task 2: File System Analysis – Scenario 1 using Autopsy

Doing a File System Analysis will help you to determine the type of the file system, collect metadata information and any content available.

No. of Files given to analyse: 1

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

1. Install Autopsy (Ignore if installed already)
2. Create a new case. (Name appropriately)
3. Add data source. Select FSA_Evidence_01 from the Images folder. Note that it is a Disk Image File. (If you haven't selected the appropriate type of data source, redo it)
4. Configure Ingest Modules. (Select appropriate options)
5. Autopsy will complete the analysis of the evidence.
6. Click on the Data Sources and select FSA_Evidence_01 and explore the details. In this task, you are analysing the image to find vital information and important evidence to help in solving a murder incident.

Hint: In order to start your investigation, you must understand the file system of the evidence.

7. By expanding the image, Autopsy displays the filesystem of the image

Name	S	C	Modified Time	Change Time	Access Time
✓ \$OrphanFiles			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
initrd.img			2016-06-09 02:23:27 PDT	2016-06-09 02:23:27 PDT	2016-06-09 02:23:54
vmlinuz			2016-06-09 02:23:27 PDT	2016-06-09 02:23:27 PDT	2016-06-09 02:23:54
✓ \$Unalloc			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
✓ [current folder]			2016-06-09 03:00:51 PDT	2016-06-09 03:00:51 PDT	2016-06-09 03:33:18
✓ [parent folder]			2016-06-09 03:00:51 PDT	2016-06-09 03:00:51 PDT	2016-06-09 03:33:18
bin			2016-06-09 02:28:49 PDT	2016-06-09 02:28:49 PDT	2016-06-09 03:45:57
boot			2016-06-09 02:29:20 PDT	2016-06-09 02:29:20 PDT	2016-06-09 03:45:57
cdrom			2016-06-09 02:22:10 PDT	2016-06-09 02:22:10 PDT	2016-06-09 03:45:57
dev			2016-04-20 15:15:17 PDT	2016-06-09 02:21:38 PDT	2016-06-09 02:22:47

8. By looking at the file system, what are your assumptions?
9. Try to look into the folder "etc" for a password file. Did you manage to find out the password file?

Hint: It is passwd

10. Look for text, Hex, Metadata, Message, Annotation options.

11. Similarly, analyse the other files and folders to get detailed information.
12. In addition to analysing the file system and files, you can also calculate the hash values of the files that you analyse.
13. Go to Home, Roger and Select Documents. Click on SeatPlan.xls, File Metadata and look for the MD5 Value for the xls file.
14. Similarly, do for other files.

Deliverables:

1. Record a Presentation Video and submit the link in Moodle. Make sure the link is available for the lecturer to view and feedback.
2. Prepare a simple report to document all your analysis and document the gathered evidences.

Task 3: File System Analysis – Scenario 2 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

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

1. Install and Run The Sleuth Kit (Ignore if installed already)
2. To view partition tables associated with **FSA_Evidence_003.dd**, type **mmls** "**FSA_Evidence_003.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** "**FSA_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** "**FSA_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 "FSA_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 early today (or this week – depends on when you do this task). 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 "FSA_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 "FSA_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 "FSA_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 "FSA_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 "FSA_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 "FSA_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 "FSA_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 "FSA_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

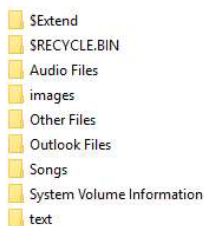
tsk_recover -i raw -e "FSA_Evidence_002.dd"
"C:\Users\Administrator\Desktop\Files_ret" and press **Enter**.

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, as shown in the following screenshot:

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.

Deliverables:

1. Record a Presentation Video and submit the link in Moodle. Make sure the link is available for the lecturer to view and feedback.

2. From Hands-on Activity 3 and 4 (So far), how good are you in using The Sleuth Kit and Autopsy? Did you try to use any other commands not listed in this tutorial? Why and what did you manage to gather?
3. Prepare a simple report to document all your analysis and document the gathered evidences.

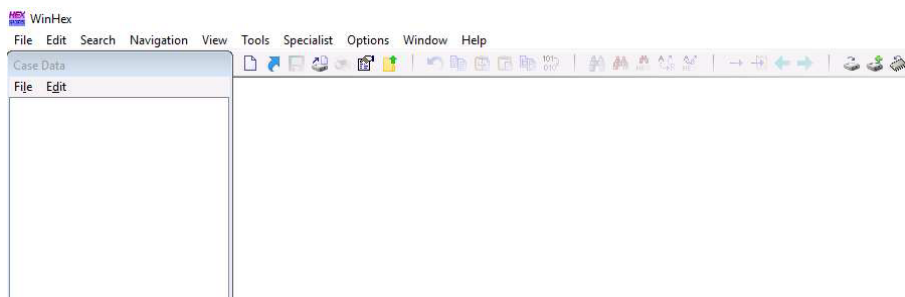
Task 4: File System Analysis – Scenario 3 - Recover permanently deleted files.

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.

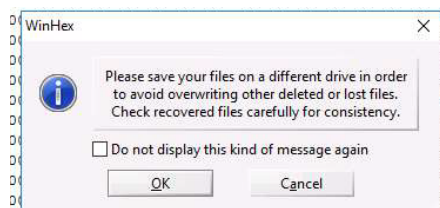
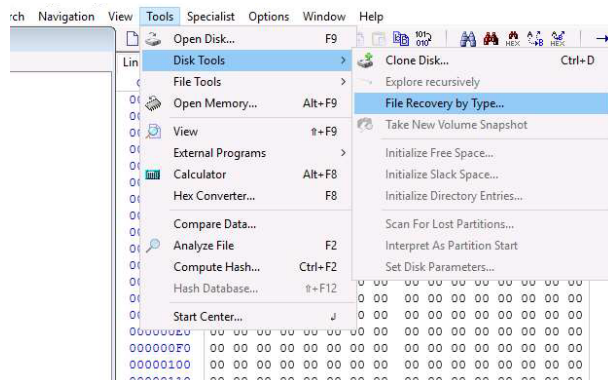


2. Open WinHex and add the evidence file **FSA_Evidence_001.img** and click **Open**.

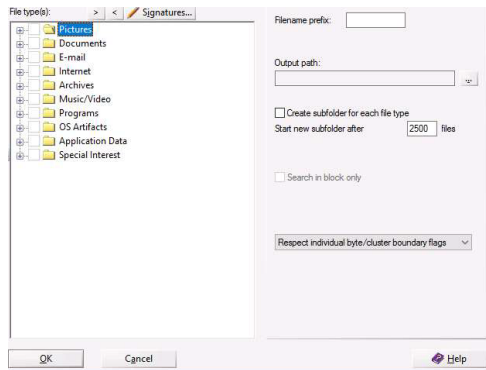
WinHex evaluation pop-up will subsequently appear; click **OK** to close the pop-up.

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 FSA_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 FSA_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**.

Deliverables:

1. Record a Presentation Video and submit the link in Moodle. Make sure the link is available for the lecturer to view and feedback.
2. Prepare a simple report to document all your analysis and document the gathered evidences.

Task 5: Investigating Email Crimes

Lab Scenario

John Dove, a manager at a reputed hotel, received an email in the hotel's official email account that stated that the hotel's Facebook account handle had been compromised and that the password to the account needs to be reset in order to recover the account. The email contained a link and an attachment in the form of a document that supposedly contained the instructions to reset the password for the affected Facebook account. Panicked, John clicked on the link so he could follow the instructions to reset the password for the hotel's Facebook account and recover it.

As he went through the process, John realized that something was fishy about the Facebook page he was interacting with on the screen. However, during this process, he also inadvertently parted with the hotel's confidential information. The hotel's management soon learned that its key confidential information was stolen and was being misused for malicious purposes. John reported his encounter with the fishy email he received that stated itself to be from Facebook. Upon learning of the incident, the hotel's management sought the services of a cyber-forensics agency.

Investigator Johnson now has to analyze the suspicious email and find its origin.

Lab Objectives

Investigating a suspicious e-mail message involves the analysis of its email headers to determine if it is spoofed. It also involves determining the origin of the email message and checking the validity/genuineness of the sender's email address.

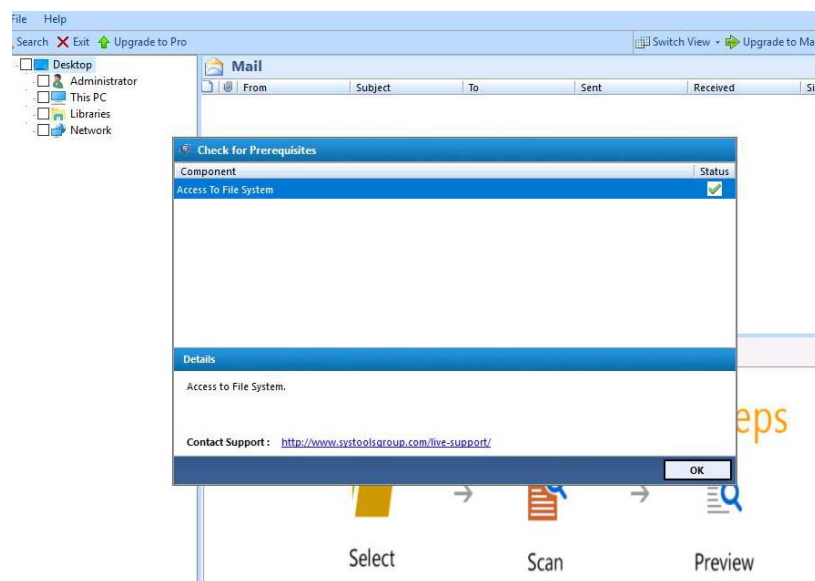
The objective of this lab is to help you understand how to perform forensic investigation on suspicious emails and how to analyze them.

Overview of the Lab

This lab familiarizes you with the process of identifying a suspicious email and examining it in detail to determine if it is spoofed.

1. Login to Windows Server 2019 virtual machine.
2. In this lab exercise, we will be examining and comparing two email files named Suspicious Email Message and Normal Email Message, so that you can differentiate a spoofed email message from a genuine one. Use the EML Files available in the Images, Hands on Activity Images, 4 – Other Files.
3. In a real scenario, as a forensic investigator, you will have to identify and download only the suspicious email message for investigation. The normal-looking email message has been used only for the demonstrative purpose of this lab, wherein we can show you how the details of a normal email message look like by comparing them with those of a suspicious email message.

4. To proceed with our investigation, we need to install the SysTools EML Viewer tool. (You are free to use any of the other tools, if you think is suitable to analyse the EML Files)
5. During the setup, when you see the Select Additional Tasks section, ensure that the Create a desktop icon option is checked so that you also have the convenience of launching the tool from a Desktop shortcut, if needed. Click Next.
6. As you complete the setup, you might see a SysTools web page appearing in the browser window. Close the SysTools web page.
7. In the final step of the setup, ensure that the Launch SysTools EML Viewer option is checked and then click Finish
8. The main window of the SysTools EML Viewer tool will now open along with the Check for Prerequisites window in which you will see that Access To File System is enabled by default. Click OK to proceed further.



9. Next, in the main window of the application, we need to add our evidence file(s). Add the evidence file(s), in the left pane of the application window, navigate to your Evidence Files by expanding the corresponding nodes and then select the folder where your EML files are stored. Upon selecting the folder, the .eml files stored within it will be listed: (Alternately, you shall create your own eml files to work on this lab. Use your knowledge from Ethical Hacking module, where you created an email like for SET tool)
10. The first .eml file is selected by default. Here, the first .eml file corresponds to the Normal Email Message and the second .eml file corresponds to the Suspicious Email Message that we had saved earlier from the suspect Gmail inbox.
11. The contents in the body of an email message can be viewed under the Mail tab in the lower pane of the application window. Select the second .eml file (Suspicious Email Message file) to view its body contents under the Mail tab, as indicated in the screenshot below (drag the margin of the lower pane of the window up using the mouse cursor for a full view of the email's contents):

12. Now we shall examine the body of the suspicious email message in an HTML format to establish whether the email message is genuine or malicious.
13. Therefore, ensure that the second .eml file (Suspicious Email Message file) is selected and then click the HTML tab in the lower pane of the application window. The contents of the email message body will now be displayed in an HTML format:
14. As seen in the screenshot above, in the last line under the HTML tab, we find that the href field displays a private IP address (10.0.0.23) linked to Facebook's URL for its Help Centre page. This means that upon clicking the URL, the user will be redirected to some other page instead of Facebook's Help Centre page. Further, the URL containing the private IP address contains http instead of https, which means that the communication will be unsecure - an indication that the page is unsafe. This strongly indicates email scamming.
15. In HTML, the href attribute shows the URL of a particular web page that will open upon clicking on a link.
16. Having found that the second email message (Suspicious Email Message) is indicative of email scamming, we shall now investigate its email headers and compare them with those of the Normal Email Message. Examining the email header information helps establish whether an email message is genuine or spoofed. When using SysTools EML Viewer, all the email header information pertaining to an email message is under the Message Header tab.
17. We will begin our investigation of email headers by examining the Message ID of Suspicious Email Message and comparing it with that of the Normal Email Message.
18. Therefore, select the second .eml file (Suspicious Email Message file) and click on the Message Header tab. Under this tab, you will find the Message ID of the selected email message. Upon examining the Message ID, you can see that it reflects localhost after the @ symbol instead of reflecting the fully qualified domain name:
19. The presence of localhost after the @ symbol in the Message ID as seen in the screenshot above is a key indicator that the email message is spoofed. If the email message were genuine, the Message ID would have shown the fully qualified domain name (i.e., mail.gmail.com) instead of showing localhost since the sender's email address is a Gmail address (jasoncreek2020@gmail.com).
20. Now select the first .eml file (Normal Email Message file) and click the Message Header tab. Scroll down under this tab to find the Message ID for the selected .eml file. You will find that the Message ID of the normal email message reflects the fully qualified domain name (i.e., mail.gmail.com) after the @ symbol:
21. So, we can infer that the presence of the fully qualified domain name (i.e., mail.gmail.com) after the @ symbol in the Message ID is an indicator of the email being genuine. This is consistent with the sender's email address (cpentuser007@gmail.com).
22. Now we shall examine the Received headers of both email messages.
23. Therefore, first select the second .eml file (Suspicious Email Message file). Under the Message Header tab, you will see that the Received header field

shows localhost in place of the domain name, beside the associated IP address from which the email message originated:

24. The presence of localhost instead of the domain name from which the email originated in the Received header field is another indicator that the email message is spoofed. If it were genuine, then the Received header field would reflect the domain name from which the email message originated instead of reflecting localhost.
25. Now select the first .eml file (Normal Email Message file) and under the Message Header tab, you will see that the Received header field displays the domain name (mail-sor-f41.google.com) and the associated IP address from which the email message originated.
26. We can infer that the presence of the domain name (i.e., mail-sor-f41.google.com) in the Received header field is an indicator that the email is genuine.

We shall now examine the Received-SPF field in both email messages.

27. First select the second .eml file (Suspicious Email Message file) and scroll down under the Message Header tab to find the Received-SPF field. In this field, you will notice the occurrence of a softfail along with a message that reads jasoncreek2020@gmail.com does not designate 93.99.104.21 as permitted sender:
28. For the selected email message above, the occurrence of a softfail along with the message specified above means that IP address 93.99.104.21 is not authorized by the domain (here, gmail.com) to send any emails on its behalf. This is another indication of the email message being spoofed.
29. Now select the first .eml file (Normal Email Message file). Under the Message Header tab, locate the Received-SPF field where you will see the occurrence of a pass along with a message that reads domain of cpentuser007@gmail.com designates 209.85.220.41 as permitted sender:
30. For the selected email message above, the occurrence of a pass along with the message specified above means that the IP address 209.85.220.41 is authorized by the domain (here, gmail.com) to send emails on its behalf. This means that any email message received from cpentuser007@gmail.com is genuine.
31. Now we shall see how to preview the malicious attachment that has been received through the spoofed email message. To preview the attachment, select the Suspicious Email Message (second .eml file listed in the application window) and then click on the Attachments tab. The application will then show a preview of the attachment's contents in the lower right section of the window:
32. In this lab, we are covering only the aspect of how to preview the contents of a malicious attachment within a spoofed email message.
33. Close the tool. Now that we have investigated the critical elements within the spoofed email message, we shall probe its originating IP address on whatismyipaddress.com to determine its geographic origin and the entity that sent it.

34. Launch a browser, type <https://whatismyipaddress.com/ip-lookup> in the address bar and press Enter. You will land on the whatismyipaddress.com/ip-lookup webpage where you will find the Get IP Details field. Type the IP address 93.99.104.21 in the field and then click on the Get IP Details button:
35. You will now be redirected to the next page where you will see details pertaining to the IP address 93.99.104.21.
36. What is the IP Address is registered with? Where is it geographically located?
37. Now we shall check the suspect email ID's validity using an online tool named Email Dossier.
38. To do so, type <https://centralops.net/co/EmailDossier.aspx> in the browser address bar and press Enter. Email Dossier's homepage appears where you will see the email address field. Type the suspect email ID, i.e., jasoncreek2020@gmail.com in the email address field and then click go:
39. You will now be redirected to the next page, where you will see the validation result pertaining to jasoncreek2020@gmail.com
40. From the above finding, we can infer that the email address jasoncreek2020@gmail.com is valid.

Deliverables:

1. Record a Presentation Video and submit the link in Moodle. Make sure the link is available for the lecturer to view and feedback.
2. Prepare a simple report to document all your analysis and document the gathered evidences.

Task 6: Recovering Deleted Email Messages Using Recover My Email

Lab Scenario

Daniel is a web expert and part of a group that hacks other's accounts for monetary benefits. Daniel was a suspect in a case wherein the attacker has used email attachments to send malware to the victim that could copy the user's passwords and other private details and prompt them to the sender. However, when Robert, the forensic investigator dealing with this case, checked Daniel's system, he did not find any incriminating emails. Robert suspected that Daniel might have deleted those emails already.

Robert now has to use the right forensic tool to retrieve the deleted email messages and examine them, if any.

Lab Objectives

Cybercriminals often delete email messages after committing a crime to avoid being tracked. Investigators can use tools such as Recover My Email, which can retrieve deleted email messages from either Microsoft Outlook PST files or Microsoft Outlook Express DBX files.

The objective of this lab is to help investigators understand how to recover deleted email messages and attachments.

1. Login to Server 2019 virtual machine.
2. In this lab, we will examine Microsoft Outlook database files for deleted emails.
3. Download from appropriate resources, Recover my Email tool. You shall use any other tool if you think so.
4. Now, Follow the wizard-driven instructions to complete its installation.
5. While installing the application, in the Select Additional Tasks section, ensure to check the Create a desktop icon option so that you have the convenience of launching the application using the Desktop shortcut, if needed. Click Next.
6. In the last step of the installation, ensure that the Launch Recover My Email option is checked and then click the Finish button
7. The Recover My Email main window appears along with Tip of the Day pop-up, as shown in the screenshot below. Click the Close button to close the pop-up window.
8. Click the Open Email File button to be able to upload the required evidence file
9. If you see a Microsoft Office Outlook pop-up stating the absence of a default email client, select OK to close it and click the Open Email File button again to proceed.
10. An Open window will appear; create your own .pst file to work with this lab and then click Open.
11. The Recover My Email application will now scan the selected .pst email file and fetch and display the results in the left pane of the window.

12. To see the emails that have been recovered, click Recovered Messages under the Folder View tab in the left pane of the application window. The application will now display the list of recovered email messages in the right pane of the window. Here, details such as the Subject of the emails, their Received date and time, etc. will be shown.
13. To be able to view the content(s) within a particular recovered email message, we need to search through the All Mails folder with the concerned email message's recipient address and its subject line that you see in the Recovered Messages folder. To perform this search operation, first click the Search button at the top:
14. A Recover My Email window will appear where you need to select the options that you want to use as filters to search through the email messages and locate the desired email message.
15. In this lab, we are selecting By To: (this field will include a recipient's email ID) and By Subject: (this will include the subject line) options as our filtering criteria.
16. We will provide the input as martinsmith6 in the By To: field and as Hi in the By Subject: field (we have already seen the terms that match our search filters in the screenshots above in the recipient's (To) email address and the Subject columns, respectively). After specifying the input in these fields, click OK.
17. Now click the All Mail folder option in the left pane of the window. The application will display the list of emails matching your search criteria in the right pane. In a real scenario, if you see more than one result, then make your search more specific by including other details such as file size, dates, etc., in the search operation.
18. To see the actual content(s) of the email in the bottom pane of the window, click on it:
19. To see the attachments, if any, click the file name of the attachment listed under the Attachments tab in the left pane of the window. This operation will display the attachment's content(s) in the Data Viewer pane.:
20. To save the recovered emails, select the email(s) you want to save and click the Save Message(s) as PST button at the top.
21. Select the format in which you want to save the email from the subsequent drop-down list that would appear upon clicking the Save Message(s) button.
22. The trial version of the tool does not allow users to save the recovered messages. If you want to save the files, you need to buy the product activation key from the vendor.
23. Close all open windows.

Task 7: Analyzing Android Forensic Image and Carving Deleted Files

Lab Scenario

The cybercrime police arrested Joe Smith, who was involved in nefarious activities, and seized his mobile device. To charge the accused with crime, the police have to submit evidence to proceed with the case. Therefore, they appointed a digital forensic investigator to examine the mobile device for evidence. In this case, recovering deleted data is crucial as it might contain evidence required for the case. To carve deleted contents from the mobile device, the forensic investigator acquires dd image of the device contents and examines the image file for required evidence.

Being a mobile forensics expert, you need to have thorough knowledge of carving data from hex codes and various file types.

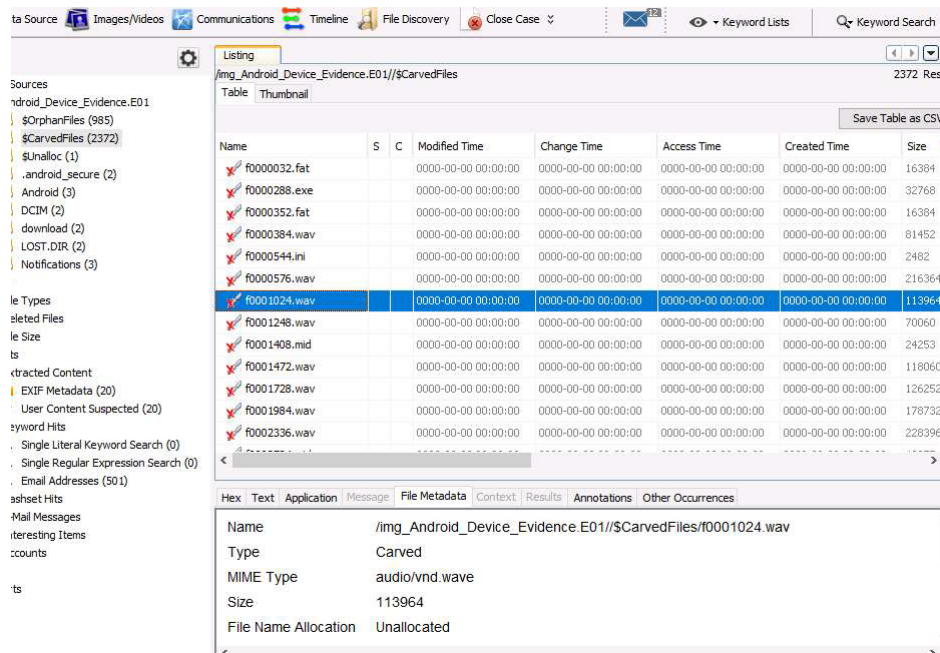
Lab Objectives

File carving is the process of obtaining deleted information from a hard disk or an image in the absence of the filesystem that originally created the file.

In this lab, you will learn how to examine an image file obtained from a mobile device and retrieve deleted data from it.

1. Login to Windows Server 2019 virtual machine.
2. In this lab, we will use Autopsy to examine evidence file obtained from an Android device. (You shall use any other tool – and any image of your own)
3. Install Autopsy. Once the installation is complete, double-click the Autopsy and open the tool.
4. Autopsy main window will appear along its Welcome window; click New Case to create a new case.
5. New Case Information window will appear; enter a case name in the Case Name text field and provide a path for 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. In this lab, we are assigning the case name as Android Device Evidence.
6. Optional Information section will appear; provide the Case Number and Examiner details (here, we have provided Case Number as 102). Enter the details of the Examiner and click the Finish button.
7. Once you click the Finish button, the application will take some time to load the data after which the Add Data Source window will appear. In this window, you will first see the Select Type of Data Source To Add section. Ensure that the Disk Image or VM File option is selected and click the Next button.
8. The Select Data Source section will appear. Click Browse.
9. An Open window will appear. Navigate to the location of your AFI.E01 file, and click the Open button.

10. In the Select Data Source section, the directory of the selected evidence file will now be displayed. Click the Next button.
11. The Configure Ingest Modules section will now appear where you will see a list of modules that are checked in the Run Ingest Modules on: column. Leave these modules as checked by default and click the Next button.
12. When you select a module, it displays options specific to the selected module in the right pane. Here, you can configure settings for each module. In this lab, we set the options to default.
13. The Add Data Source section will appear displaying a message that reads Data source has been added to the local database. Files are being analyzed. Click the Finish button.
14. Autopsy takes time to analyze the image file. View the analysis status at the lower right corner of the Autopsy window. Once the Analysis is complete, the status disappears.
15. After analyzing all the files, Autopsy displays the retrieved information:
16. If you are using the E01 file from the Lecturer resources, you will find the below. Else, you follow the instruction below but the search criteria and outcome may vary depending on your evidence. In the left pane, expand the nodes for Keyword Hits, Email Addresses, $(\{?\}[a-zA-Z0-9\%+_ \-]+(\.[a-zA-Z0\d\ \-]+))$, and select any email address (here, we have selected the email address +info@simephoto.com). The contents/files associated with the selected email address are displayed in the right pane of the window under the Table tab.
17. Select any file (here, we will select AU-wp2.jpg) from the Source File section to view various data associated with it under the Hex data, File Metadata, Text, Annotations, Application, etc., tabs. You can analyze this data to find sensitive information (if any) hidden in the file.
18. Expand the nodes for Data Sources of E01, and then select \$CarvedFiles in the left pane. You can see the carved data related to the image file in the right pane of the window under the Table tab.
19. Select any carved file and then click the File Metadata, Hex, Text, Annotations, etc., tabs to view various data associated with the selected file in the bottom-right pane of the window, as indicated the below screenshot:



20. For demonstrative purposes, we are viewing only the data under the File Metadata tab for the selected carved file as seen in the above screenshot. The data under File Metadata tab contains details such as file name, size, MIME type, and file type description as Carved.
21. Expand the nodes for Views, Deleted Files, and then select All in the left pane. Autopsy displays all the deleted files that have been recovered in the right pane. These files are indicated by a red-colored cross mark.
22. Select a deleted file in the right pane to view the various data associated with it under the Application, File Metadata, Hex, Text, Annotations, etc. tabs. Here, we will select a deleted file named CA-WP6.JPG and are viewing the file's associated data under the Application tab, which displays the image contained in the file.
23. In the same way, you may also view the data pertaining to other files of different formats. For example, here, we are expanding the nodes for File Types and By Extension under Views and then selecting the option Audio in the left pane of the window. This will display all the audio files contained within the evidence file in the right pane of the window. From the listed files, we are selecting an audio file named Windows Pop-up Blocked.wav and are viewing the hex data associated with it by clicking on the Hex tab.
24. Autopsy classifies files of various sizes in three sections: between 50-200 MB, 200-1 GB, and 1 GB+. For instance, we are viewing the File Metadata pertaining to a carved file named f0208576.flv, which amounts to a size of 50-200 MB. To view these files, you need to expand the MB File Size option under Views and then select one of the size categories
25. Expand Data Sources --> .E01 --> Android --> data --> com.cooliris.media --> cache. This displays all the files stored in the cache memory of the Android device in the left pane of the window. Select the cache folder if you want to view its contents in the right pane:

26. Autopsy also lists a directory named OrphanFiles under .E01. It contains broken files (i.e., incompletely carved files). You may also examine these files as part of the forensic investigation.
27. Select the OrphanFiles folder to view its files/contents in the right pane of the window. Then select any one of the files listed in the right pane to view its data in the lower-right pane of the window. Here, we select the file named DMR_48.jpg and then view its data under the Application tab:
28. Autopsy also allows you to view the databases of WhatsApp, Viber, and other applications (if installed on the Android Device), which contain information such as text and voice messages, pictures, etc.
29. The Timeline feature of Autopsy helps you retrieve information on various events that occurred on the device during a selected time period. To view the timeline, select Tools in the menu bar and select Timeline.
30. A timeline window will appear, displaying a logarithmic graph that contains information on various events that occurred during a given time interval.
31. In this window, you can specify a particular time interval to retrieve information on the events or activities that occurred within that specified time interval.
32. The red colored bars in the above graph represent file system activity while the green colored bars represent miscellaneous event types.
33. Set a time interval by specifying the Start and End times in their respective fields and select a bar from the graph. Autopsy displays all the file system events (since we have selected a red colored bar) that occurred during the time interval corresponding to the selected bar in the lower-left pane of the window.
34. Select any file from the resulting data (from the lower-left pane) to view the data associated with it in the lower-right pane (here, we are viewing the File Metadata of the selected file).
35. This way, you can analyze an image and examine the file system of the target device during the process of forensic investigation.

Task 8: Investigating digital evidences – 3 (M57)

One of the employees in M57 is stealing proprietary research from the company and passing it on to an outside entity. This employee has taken some measures to cover their tracks, but probably did not count on the company machines being imaged in the ongoing investigation of other criminal activity.

Electronic identities

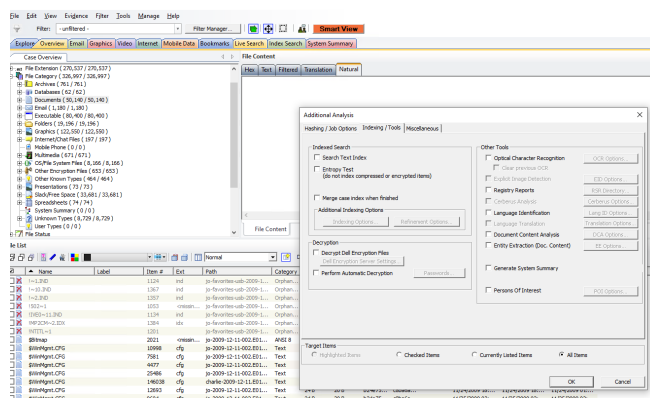
- Pat McGoo (President): pat@m57.biz (email password: mcgoo01)
- Terry Johnson (IT Administrator): terry@m57.biz (email password: johnson01)
- Jo Smith (Patent Researcher): jo@m57.biz (email password: smith01)
- Charlie Brown (Patent Researcher): charlie@m57.biz (email password: brown01)
- Corpus and Supporting Documents

Use the following set of evidences:

- Hard drive images from all workstations in the office: charlie-2009-12-11.E01, jo-2009-12-11-002.E01, pat-2009-12-11.E01, terry-2009-12-11-002.E01
- (Optional) RAM dumps from the machines taken during the police visit (mdd or windd images): charlie-2009-12-11.mddramimage.zip, jo-2009-12-11.mddramimage.zip, pat-2009-12-11.mddramimage.zip, terry-2009-12-11.mddramimage.zip
- Three company USB drives found on-premises and one personal USB drive seized from Jo: charlie-work-usb-2009-12-11.E01, jo-work-usb-2009-12-11.E01, terry-work-usb-2009-12-11.E01 and jo-favorites-usb-2009-12-11.E01

You can choose between FTK and Autopsy or both

Make sure File Carving, Email Analysis, File Signature File Decryption are all enabled while processing your Evidence. If not, Click on Evidence, Additional Analysis and choose the relevant options.



Digital Investigation

1. In Workstation Images

- Navigate to Overview Tab, Select File Category, Documents and focus on relevant files (Look for Proprietary Files like Patent Drafts, Research Files etc).
- Further use Filter Options based on the given case scenario.
- Use Created, Modified, Accessed Timestamps.
 - Look for files accessed outside normal working hours etc.
 - Look for large data transfers
 - Look for repeated access to sensitive files
 - Look for File access patterns that deviate from an employee's role like IT admin Terry accessing patent files
 - Review Carved Files for proprietary contents like patent, etc
- Navigate to Email Tab.
 - Import email archives from employee's workstation
 - Search for suspicious attachments like ZIP files, PDFs, or encrypted containers
 - Use keywords like "patent", "research", "confidential", "competitors", "domain names" and "external"
 - Analyze email headers for external recipients (non-m57.biz domains)
 - Filter emails by date to identify recent communications.
 - Open emails from external recipients and view the Headers
 - Extract the IP Addresses
 - Emails with large attachments sent to external domains.
 - Export relevant emails to a report (right-click > Export to CSV) for further analysis.
- Navigate to Live Search.

-
- Forensic Toolkit Version: 8.1.0.330 Database: localhost (Pot) Case: MS7 BIZ
- File Edit View Evidence Filter Tools Manage Help
- Filter: - unfiltered - Filter Manager
- Explore Overview Email Graphics Video Internet Mobile Data Bookmarks Live Search Index Search System Summary
- Test Pattern Hex
- Live Search Results
- Live Search (Prefix: - unfiltered -)
- 1 2 3 4 5 6 7 8 9 A B C D E F Add Clear Export Import
- Search Terms Type Code Pages
- Max Hits Per File: 200 Search: - unfiltered - Processing Manager: localhost Search
- Be Content
- Hex Text Filtered Translation Natural

- [illegible]

- Attempt to decrypt the encrypted files. (Note: All decryption might not be successful – so, don't give up – Explore options like Password Recovery Toolkit)
- Use text search and search using IP Addresses from the Email analysis

- Navigate to File List

- Filter and look for Proprietary Files
- Use Keywords like patent, research etc

- Check the file metadata to confirm the date, time of the files copied (Include Created, Modified dates)
- If you have enabled, try to filter using File Signature in Filter Manager (If won't show if you haven't enabled while adding evidences)
- Look for Windows Shortcuts, Registry Artifacts list usbstor to relate with any interaction between workstations
- If possible, try to relate USB Serial number with Workstation Registry Entries.
- Look for large file transfers to USB drives like >10 MB files copied to jo-favorites-usb-2009-12-11.E01.

3. Based on your 1, 2 Steps:

- List out the files based on the images analysed.
- Cross reference the IPs to identify the competitor's organization

Did you check partially overwritten files? – With reference to our earlier lectures, If attempts to cover tracks happened, overwritten files may indicate that. Have a close look. Spend some time on the image. No Hurry here!!!

What is your Outcome?

Did you find any employee exfiltrating data?

Any anomalous activity that you need to highlight?

Can you identify any files that was stolen? Any specific tools or methods you noted for this?

Any outsiders you could identify? What was the communication channel/ PLATFORM used?

Overall Reflection

Present your reflection to the class. (Note that you will have 10 minutes for presentation during the next lecture session. – Before the presentation, you must submit the documentation in Moodle)

1. Understanding on the concepts discussed in the lecture and its relation to the activity done.
2. Understanding about various tools used and various frameworks available for DF analysis.
3. Understanding Image Acquisition, Investigation and Analysis

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