



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 and 2, (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 this Activity 3, you will be analysing different files to find out more information.

Task 1: Analysing Partitions for anomalies

Task 2: Analysing Meta Data

Task 3: Analysing File Signatures

Task 4: Using The Sleuth Kit to analyse

Task 5: Using Autopsy to analyse raw image

Task 6: Coursework Task – Create and Analyse the image file

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 Partitions for anomalies

(Refer to Anexure 1)

Task 2: Analyse Metadata

The files are available in Shared Folder. (HoA3_Files → Task 2). Refer to the lecture and complete the activities. You need to analyse the metadata of the given files and extract the below requested information.

For each file given, report the type of application, contents, title, author, last modified details, latest revision details, date and time, any previews and other information.

Cover the details of the tool used, the basic principles behind analysing the metadata as a report with adequate screenshots.

No. of Files given to analyse: 3

Deliverables: Report

Task 3: Analysing File Signatures

The files are available in Shared Folder. (HoA3_Files → Task 3). Refer to the lecture and complete the activities. You need to analyse the signatures of the given files and write a report including all the files – its type and information gathered from the file.

No. of Files given to analyse: 9

Deliverables: Report

Task 4: Using The Sleuth Kit to analyse

Filesystem, Metadata and the contents

The files are available in Shared Folder. (HoA3_Files → Task 4).

1. Download The Sleuth Kit
2. Open The Sleuth Kit and open the hoa3_ddimage.dd file

Type

fsstat -f ntfs "hoa3_ddimage.dd"

make sure the path of the image file is given appropriately

```
Administrator: C:\Windows\system32\cmd.exe

E:\CHF109 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>fsstat -f ntfs "E:\Evidence Files\Disk Partitions Raw Image\DiskPartitionsRawImage.dd"
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: A2A4F4DDA4F4B4BF
OEM Name: NTFS
Volume Name: Drive
Version: Windows XP

METADATA INFORMATION
-----
First Cluster of MFT: 87381
First Cluster of MFT Mirror: 131071
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 128
Root Directory: 5

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 262142
Total Sector Range: 0 - 2097150

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16) Size: 48-72 Flags: Resident
$ATTRIBUTE_LIST (32) Size: No Limit Flags: Non-resident
$FILE_NAME (48) Size: 68-578 Flags: Resident, Index
$OBJECT_ID (64) Size: 0-256 Flags: Resident
$SECURITY_DESCRIPTOR (80) Size: No Limit Flags: Non-resident
$VOLUME_NAME (96) Size: 2-256 Flags: Resident
$VOLUME_INFORMATION (112) Size: 12-12 Flags: Resident
$DATA (128) Size: No Limit Flags:
$INDEX_ROOT (144) Size: No Limit Flags: Resident
$INDEX_ALLOCATION (160) Size: No Limit Flags: Non-resident
$BITMAP (176) Size: No Limit Flags: Non-resident
$REPARSE_POINT (192) Size: 0-16384 Flags: Non-resident
$EA_INFORMATION (208) Size: 8-8 Flags: Resident
$EA (224) Size: 0-65536 Flags:
$LOGGED_UTILITY_STREAM (256) Size: 0-65536 Flags: Non-resident

E:\CHF109 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>
```

3. Use the **istat** tool of the sleuth kit to view the details of metadata structure.

type

```
istat -f ntfs "hoa3_ddimage.dd" 0
```

4. Use the following command to view MFTMirr File Overview,

type

```
istat -f ntfs "hoa3_ddimage.dd" 1
```

5. Use the following command to view the Boot File Overview,

type

```
istat -f ntfs "hoa3_ddimage.dd" 7
```

6. Use the following command to view the File volume,

type

```
istat -f ntfs "hoa3_ddimage.dd" 3
```

7. Use the following command to view the AttrDef File Overview,

type

istat -f ntfs "hoa3_ddimage.dd" 4

8. Use the following command to view the Bitmap File Overview,

type

istat -f ntfs "hoa3_ddimage.dd" 6

9. Use the following command to view the BadClus File Overview

type

istat -f ntfs "hoa3_ddimage.dd" 8

10. Use the following command to view the secure File Overview,

type

istat -f ntfs "hoa3_ddimage.dd" 9

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

type

fls -f ntfs "hoa3_ddimage.dd"

12. Use the following command to see only the deleted entries,

type

fls -d "hoa3_ddimage.dd"

13. Use the following command to view the details of the image

type

img_stat "hoa3_ddimage.dd" 6

Report: Document the outcome of the above analysis done. Based on your experience doing Task 1, 2, 3 and 4, so far what is the difference using TSK tool?

No. of Files given to analyse: 1

Deliverables: Report and Presentation

Task 5: Using Autopsy to analyse raw image

The files are available in Shared Folder. (HoA3_Files → Task 4).

1. Download Autopsy
2. Open Autopsy and open the hoa3_ddimage.dd file (ignore step 1 if you have autopsy installed already)
3. Create a new case:
 - a. Case Number: 031123
 - b. Description: My Autopsy Analysis before Coursework Task
 - c. Investigator Name: "Your Name"
4. Add the hoa3_ddimage.dd as a new image
5. Choose appropriate partition and import method. Before selecting, do a research on the partition and import methods. Justify your selected option.
6. Analyse the image. Look for General File System Details.

No. of Files given to analyse: 1

Deliverables: Report and Presentation

Do a presentation during the next lecture to briefly describe your understanding on methods used to gather/ analyse the filesystem, metadata information and content information. Cover the key factors about using TSK and Autopsy tools.

Task 6: Coursework Task – Create and Analyse the image file

This is a Team Activity. Simulate a digital forensic investigation by collecting and analysing data from a given hard disk based on a predefined theme or a concept.

- + Team Size: Minimum 6 – Maximum 7
- + Resources required:
 - Hard Disk (one for each Team)¹
 - Theme or Concept
 - Appropriate digital forensic Tools
- + Task
 - Team
 - Form your Team and collect your Hard Disk
 - Selecting Theme
 - Select an appropriate theme from the list below or on your own after discussing with your Team

¹ Note: The hard disk is your teams responsibility. You must keep them safe and handover to your module lecturer in the same physical state as collected without any damage.

- Social Media Investigations (Cyberbullying, Illicit Activities, Harassment etc)
- Corporate Data Theft (Potential Data Theft, unauthorized access, financial records, intellectual property etc)
- Social Engineering Attacks (Pretexting/ Baiting etc)
- Steganography Detection
- Insider Threats
- Malware Analysis
- Financial Crimes
- Etc
- Collecting Data:
 - Draft a scenario based on the selected theme including a clear analysis/ investigation challenge. **Note: Your team will be collecting/ gathering data based on the theme and will challenge the other teams to analyse the newly acquired hard disk to identify the evidence without any prior knowledge of the data.**
 - Collect adequate and relevant data based on the selected theme. Make sure that the data is anonymized and contains various types of files (docs, images, emails, videos, txt messages etc).
 - Create a report (not limited to) including the drafted scenario, collected data, location of evidence, timestamps, total size of data, evidences of team discussions etc.
- Exchanging:
 - Use ChatGPT to anonymously exchange the digital evidence (including the relevant scenario with investigation challenge) with other teams with a condition that reciprocal exchanges not allowed.
- Analysing Data:
 - Analyse the data in the newly acquired hard disk to identify the evidence related to the theme.
 - Document the analysis and findings and present it as a Team clearly specifying the findings of your analysis/ investigation. Your presentation must include the process of Exchanging digital evidence, Analysis Procedure, Findings and Individuals contribution to the Team.

Word Limit: 1000 words or Equivalent

Deliverables: As a part of Final Report

1. Data Collection Report (Task 3 – Report can be common for all members within the team).
2. Digital evidences – (Hard Disk) to be handed over to the Module Lecturer
3. Presentation – Task 3
 - + Present your analysis/ findings as a Team

- + All Team members must contribute to the presentation.
- + Duration: 10 Minutes recording
- + Publish: In a cloud environment (Youtube/ Panapto/ OneDrive etc) and share the link

Deadline: 12th January 2024

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. Rate yourself: Understanding Image Acquisition, Investigation and Analysis

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