



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)

Warmup Activity



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

*Lab Activities are based on **TryHackMe**, **EC Council – CHFI**, and other Industry Digital Forensic Curriculum*

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.

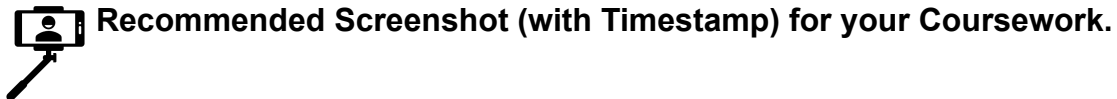
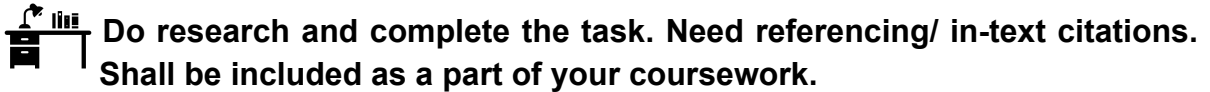
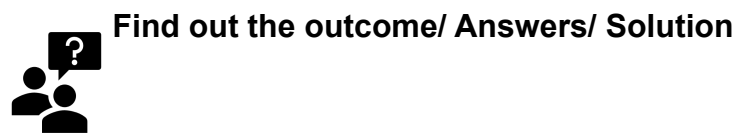
Objectives

In continuation to our lectures, this tutorial helps in providing you an insight on digital forensic investigation process and overview of online resources available.

Task 1: Individual Activity – Analysis of Data from the acquired Image

Task 2: Research and discuss about various online resources available

ICONS Used in this document:

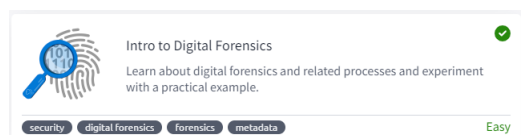


Task 1: Analysis of Data from the acquired Image

(Individual Activity)

Lets assume from the image you acquired as a Team, you found out a folder.
(Access the folder [here](#))

1. Analyse the documents in the folder to find out information to help your investigation.
2. Document the steps you have taken and the details you have identified. Make sure that the authenticity and integrity of the evidence is essential for guaranteeing a forensically sound investigation.
 - a. Document the tools you used
 - b. Procedure followed
 - c. Evidences found
 - d. Ensure the authenticity and integrity of the evidence
3. Did you manage to gather evidence? If YES, Good. If No, Nothing to worry. Continue with Step 4.
4. To get a step-by-step instruction to complete Task 1, signin to tryhackme.com.
 - a. Click Learn Tab and search “Intro to Digital Forensics”
 - b. Complete the Activity and submit the screenshot with tick and timestamp in Moodle. Example below.



Task 2: Research and discuss about various online resources available

(Group Activity)

1. Similar to tryhackme, research other websites, tools that are available to enhance, practice your Digital Forensics Skills.

2. Discuss with your Class about the resources and submit your reflection in Moodle Group Discussion Forum.

Overall Reflection

1. Understanding on the concepts discussed in the lecture and its relation to the activity done.
2. Understanding the need/ requirement of Computer Forensics.
3. Rate yourself: Computer Forensics – Cybercrime, Investigations and Evidences

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

Task 1 resolving :

Image meta data analyse, and step by step reflection and data extract :

Tool used : exiftool on terminal (zsh)

Relevant metadata :

User Comment THM{238956} + Date 2022:02:25 13:37:33

GPS Informations :

Thumbnail Image : (Binary data 4941 bytes, use -b option to extract)

GPS Latitude : 51 deg 30' 51.90" N

GPS Longitude : 0 deg 5' 38.73" W

According to the GPS data, the address found is : **Milk Street, Cheap, London, EC2V 7JB, United Kingdom**

Name found in PDF metadata: Ann Gree Shepard (PDF exiftool data extraction)

Screen captures :

The first screenshot shows a terminal window with the command `exiftool ransom-letter.pdf` and its output. The output includes file metadata such as File Name, File Size, File Modification Date/Time, File Access Date/Time, File Inode Change Date/Time, File Permissions, File Type, File Type Extension, MIME Type, PDF Version, Linearized, Page Count, Language, Tagged PDF, XMP Toolkit, Producer, Title, Creator, Description, Creator Tool, Create Date, Modify Date, Document ID, Instance ID, Author, and Subject. The GPS coordinates are listed as Latitude: 51.514417 and Longitude: -0.094092.

The second screenshot shows a web browser window with the URL `gps-coordinates.net`. The page displays the address "Milk Street, Cheap, London, EC2V 7JB, United Kingdom" and the corresponding GPS coordinates: Latitude: 51.514417 and Longitude: -0.094092. A map of London is shown with a red pin indicating the location. The map includes labels for various areas such as BARNET, HARINGEY, WALTHAM FOREST, BRENT, REDBRIDGE, BARKING AND DAGENHAM, GREENWICH, LAMBETH, LONDON, HAMMERSMITH AND FULHAM, CHICHESTER, WANDSWORTH, and LEWISHAM.

```

File Type Extension      : jpg
MIME Type               : image/jpeg
JFIF Version            : 1.01
Exif Byte Order         : Little-endian (Intel, II)
Compression             : Jpeg (old-style)
Make                   : Canon
Camera Model Name       : Canon EOS R6
Orientation             : Horizontal (normal)
X Resolution            : 300
Y Resolution            : 300
Resolution Unit         : inches
Software                : GIMP 2.10.28
Modify Date             : 2022:02:15 17:23:40
Exposure Time           : 1/200
F Number                : 2.8
Exposure Program        : Manual
ISO                    : 640
Sensitivity Type        : Recommended Exposure Index
Recommended Exposure Index : 640
Exif Version            : 0231
Date/Time Original      : 2022:02:25 13:37:33
Create Date             : 2022:02:25 13:37:33
Offset Time             : -01:00
Offset Time Original    : +03:00
Offset Time Digitized   : +03:00
Shutter Speed Value     : 1/200
Aperture Value          : 2.8
Exposure Compensation   : 0
Max Aperture Value      : 1.8
Metering Mode           : Multi-segment
Flash                   : No Flash
Focal Length            : 50.0 mm
User Comment            : TIM(238956)
Sub Sec Time Original   : 42
Sub Sec Time Digitized : 42
Color Space             : sRGB
Exif Image Width        : 7900
Exif Image Height       : 5207
Focal Plane X Resolution : 1520
Focal Plane Y Resolution : 1520
Focal Plane Resolution Unit : cm
Custom Rendered         : Normal
Exposure Mode           : Manual
White Balance           : Auto
Scene Capture Type      : Standard
Serial Number           : 083021002010
Lens Info               : 50mm f/2
Lens Model              : EF50mm f/1.8 STM
Lens Serial Number      : 000029720b
GPS Latitude Ref        : North
GPS Longitude Ref       : West
GPS Time Stamp          : 13:37:33
Subfile Type            : Reduced-resolution image
Photometric Interpretation : YCbCr
Samples Per Pixel       : 3
Thumbnail Offset        : 1214
Thumbnail Length        : 4961
XMP Toolkit             : XMP Core 4.4.0-Exiv2
API                    : 2.0
Platform               : Linux
Time Stamp              : 1644938627130718
Approximate Focus Distance : 0.79
Distortion Correction Already Applied: True
Firmware               : 1.2.0

```

To ensure the integrity of the evidence and data, each document has been downloaded in a zip file extracted on an external directory. The original .zip containing the original files has not been modified.

The entire procedure was to analyse all the data present in the file's meta to find potentially helpful informations to find the Gato's location. The data have been analyzed before opening a second copy of the file to read the content.