TRY HACK ME: Intro to Digital Forensics Write-Up

Task 1 Introduction To Digital Forensics-

Forensics is the application of science to investigate crimes and establish facts. With the use and spread of digital systems, such as computers and smartphones, a new branch of forensics was born to investigate related crimes: computer forensics, which later evolved into, digital forensics.

Think about the following scenario. The law enforcement agents arrive at a crime scene; however, part of this crime scene includes digital devices and media. Digital devices include desktop computers, laptops, digital cameras, music players, and smartphones, to name a few. Digital media includes CDs, DVDs, USB flash memory drives, and external storage. A few questions arise:

How should the police collect digital evidence, such as smartphones and laptops? What are the procedures to follow if the computer and smartphone are running?

How to transfer the digital evidence? Are there certain best practices to follow when moving computers, for instance?

How to analyze the collected digital evidence? Personal device storage ranges between tens of gigabytes to several terabytes; how can this be analyzed.

Assuming this employee is suspected in the figure above, we can quickly see the digital devices that might be of interest to an investigation. We notice a tablet, a smartphone, a digital camera, and a USB flash memory in addition to a desktop computer. Any of these devices might contain a trove of information that can help with an investigation. Processing these as evidence would require digital forensics.

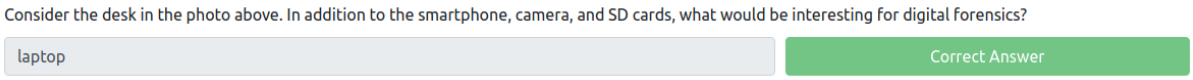
More formally, digital forensics is the application of computer science to investigate digital evidence for a legal purpose. Digital forensics is used in two types of investigations:

Public-sector investigations refer to the investigations carried out by government and law enforcement agencies. They would be part of a crime or civil investigation.

Private-sector investigations refer to the investigations carried out by corporate bodies by assigning a private investigator, whether in-house or outsourced. They are triggered by corporate policy violations.

Whether investigating a crime or a corporate policy violation, part of the evidence is related to digital devices and digital media. This is where digital forensics comes into play and tries to establish what has happened. Without trained digital forensics investigators, it won't be possible to process any digital evidence properly.

Answer to the questions of this section-



Task 2 Digital Forensics Process –

As a digital forensics investigator, you arrive at a scene similar to the one shown in the image above. What should you do as a digital forensics investigator? After getting the proper legal authorization, the basic plan goes as follows:

Acquire the evidence: Collect the digital devices such as laptops, storage devices, and digital cameras. (Note that laptops and computers require special handling if they are turned on; however, this is outside the scope of this room.)

Establish a chain of custody: Fill out the related form appropriately (Sample form). The purpose is to ensure that only the authorized investigators had access to the evidence and no one could have tampered with it.

Place the evidence in a secure container: You want to ensure that the evidence does not get damaged. In the case of smartphones, you want to ensure that they cannot access the network, so they don't get wiped remotely.

Transport the evidence to your digital forensics lab.

At the lab, the process goes as follows:

- Retrieve the digital evidence from the secure container.
- Create a forensic copy of the evidence: The forensic copy requires advanced software to avoid modifying the original data.
- Return the digital evidence to the secure container: You will be working on the copy. If you damage the copy, you can always create a new one.
- Start processing the copy on your forensics workstation.

The above steps have been adapted from Guide to Computer Forensics and Investigations, 6th Edition.

More generally, according to the former director of the Defense Computer Forensics Laboratory, Ken Zatyko, digital forensics includes:

Proper search authority: Investigators cannot commence without the proper legal authority.

Chain of custody: This is necessary to keep track of who was holding the evidence at any time.

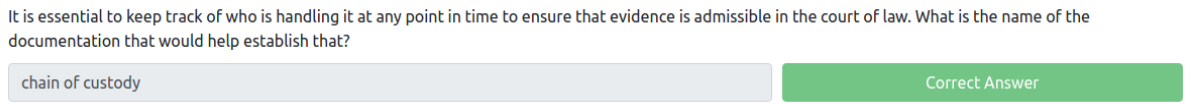
Validation with mathematics: Using a special kind of mathematical function, called a hash function, we can confirm that a file has not been modified.

Use of validated tools: The tools used in digital forensics should be validated to ensure that they work correctly. For example, if you are creating an image of a disk, you want to ensure that the forensic image is identical to the data on the disk.

Repeatability: The findings of digital forensics can be reproduced as long as the proper skills and tools are available.

Reporting: The digital forensics investigation is concluded with a report that shows the evidence related to the case that was discovered.

Answer to the questions of this section-



Task 3 Practical Example of Digital Forensics-

Everything we do on our digital devices, from smartphones to computers, leaves traces. Let's see how we can use this in the subsequent investigation.

Our cat, Gado, has been kidnapped. The kidnapper has sent us a document with their requests in MS Word Document format. We have converted the document to PDF format and extracted the image from the MS Word file for your convenience.

You can download the attached file to your local machine for inspection; however, for your convenience we have added the files to the AttackBox. To follow along, open the terminal on the AttackBox, then go to the directory **/root/Rooms/introdigitalforensics** as shown below. In the following terminal output, we changed to the directory containing the case files.

Document Metadata

When you create a text file, **TXT,** some metadata gets saved by the Operating System, such as file creation date and last modification date. However, much information gets kept within the file's metadata when you use a more advanced editor, such as MS Word. There are various ways to read the file metadata; you might open them within their official viewer/editor or use a suitable forensic tool. Note that exporting the file to other formats, such as **PDF,** would maintain most of the metadata of the original document, depending on the PDF writer used.

Let's see what we can learn from the PDF file. We can try to read the metadata using the program **pdfinfo**. **Pdfinfo** displays various metadata related to a PDF file, such as title, subject, author, creator, and creation date. (The AttackBox already has **pdfinfo** installed; however, if you are using

Kali Linux and don't have **pdfinfo** installed, you can install it using **sudo apt install poppler-utils**.) Consider the following example of using **pdfinfo DOCUMENT.pdf**.

The PDF metadata clearly shows that it was created using MS Word for Office 365 on October 10, 2018.

ANSWER

Photo EXIF Data

EXIF stands for Exchangeable Image File Format; it is a standard for saving metadata to image files. Whenever you take a photo with your smartphone or with your digital camera, plenty of information gets embedded in the image. The following are examples of metadata that can be found in the original digital images:

Camera model / Smartphone model

Date and time of image capture

Photo settings such as focal length, aperture, shutter speed, and ISO settings

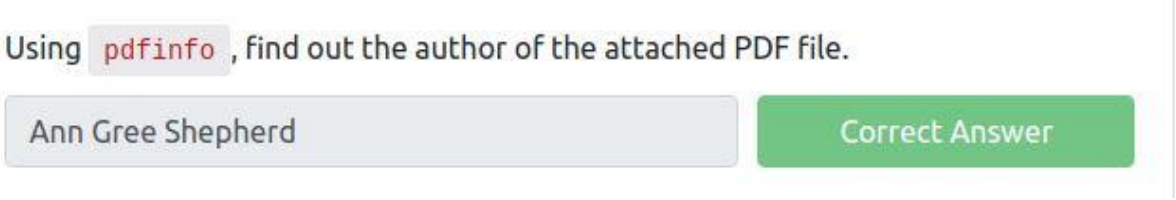
Because smartphones are equipped with a GPS sensor, finding GPS coordinates embedded in the image is highly probable. The GPS coordinates, i.e., latitude and longitude, would generally show the place where the photo was taken.

There are many online and offline tools to read the EXIF data from images. One command-line tool is **exiftool**. ExifTool is used to read and write metadata in various file types, such as JPEG images. (The AttackBox already has **exiftool** installed; however, if you are using Kali Linux and don't have exiftool installed, you can install it **using sudo apt install libimage-exiftool-perl**.) In the following terminal window, we executed **exiftool IMAGE.jpg** to read all the EXIF data embedded in this image.

If you take the above coordinates and search one of the online maps, you will learn more about this location. Searching Microsoft Bing Maps or Google Maps for **51° 31' 4.00" N, 0° 5' 48.30**" W reveals that these coordinates indicate that the image was taken very near to the Museum of London. (We only replaced **deg** with **°** for our search to work.) We noticed that the coordinates were converted to decimal representation on the search page: **51.517776, -0.09675.**

Using **exiftool** or any similar tool, try to find where the kidnappers took the image they attached to their document. What is the name of the street

Answer to the questions of this section-



Using `exiftool` or any similar tool, try to find where the kidnappers took the image they attached to their document. What is the name of the street?

milk street | Correct Answer

What is the model name of the camera used to take this photo?

Canon EOS R6 | Correct Answer | Hint

Steps to Investigation the given Task-

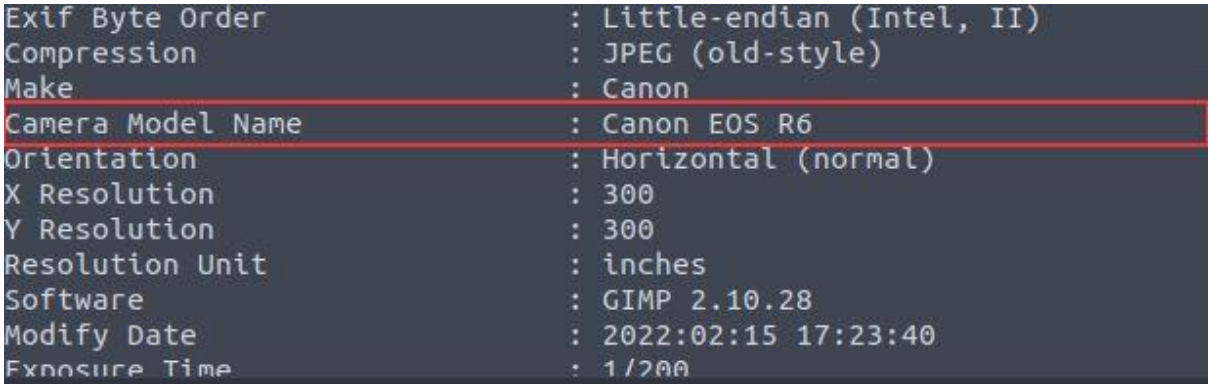
1) Navigate to **/root/Rooms/introdigitalforensics** in the AttackBox

```
root@ip-10-10-252-231:~/Rooms/introdigitalforensics# ls
letter-image.jpg   ransom-letter.pdf
ransom-letter.doc  ransom-lettter-2.zip
```

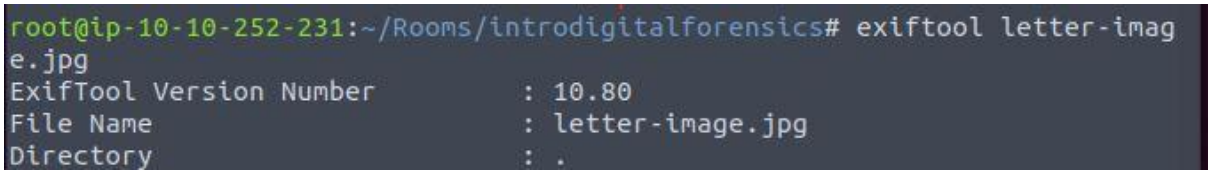
2) Using pdfinfo tool we were able to fetch Author name of the attached PDF

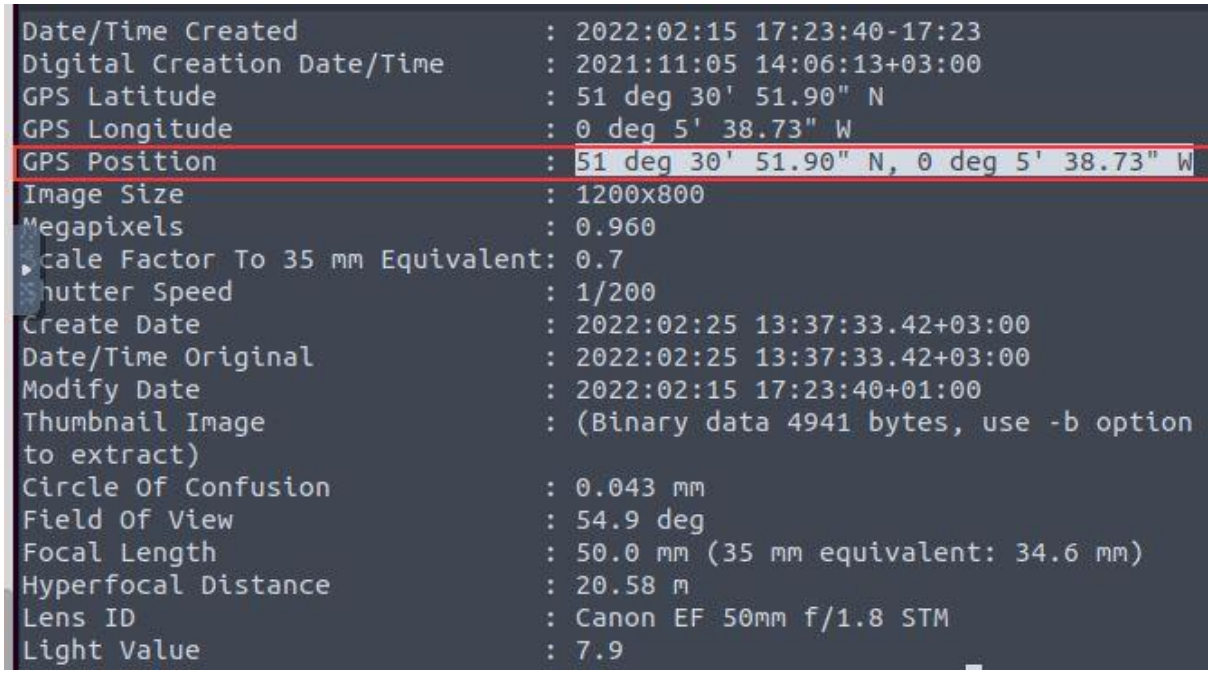
```
root@ip-10-10-252-231:~/Rooms/introdigitalforensics# pdfinfo ransom-lette
r.pdf
Title:          Pay NOW
Subject:        We Have Gato
Author:         Ann Gree Shepherd
Creator:        Microsoft® Word 2016
Producer:       Microsoft® Word 2016
CreationDate:   Wed Feb 23 09:10:36 2022 GMT
ModDate:        Wed Feb 23 09:10:36 2022 GMT
Tagged:         yes
UserProperties: no
Suspects:       no
Form:           none
JavaScript:     no
Pages:          1
Encrypted:      no
Page size:      595.44 x 842.04 pts (A4)
Page rot:       0
File size:      71371 bytes
```

3) Using exiftool tool on image file we were able to fetch Camera Model Name

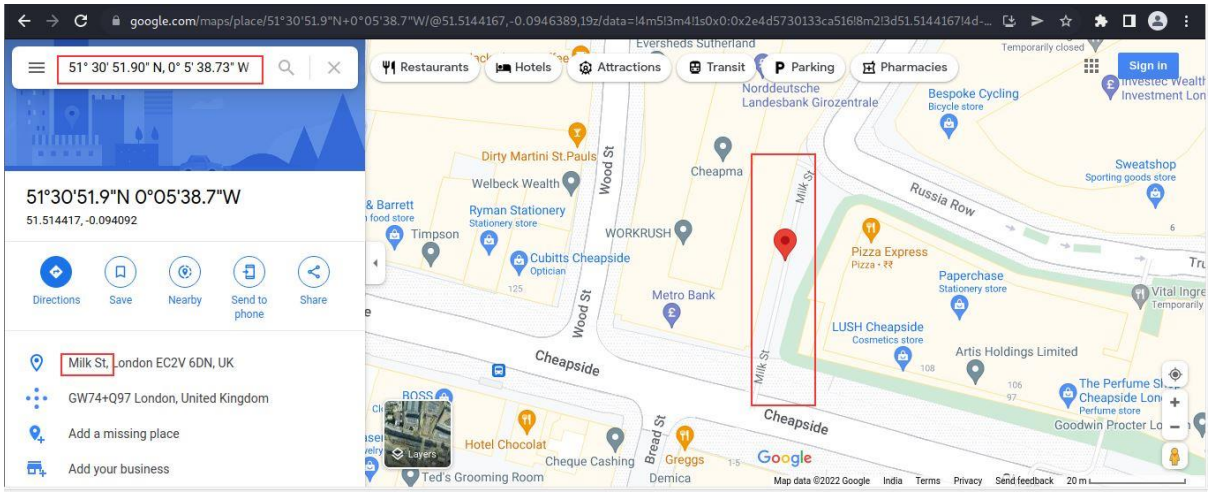


4) Using exiftool tool on image file we were able to fetch GPS Position , Let's check the GPS position on google maps





51° 30' 51.90" N, 0° 5' 38.73" W – results of google map for the mentioned GPS Position is Milk Street.



That is all for this Write-up, hoping this will help you in solving the challenges of intro to Digital Forensics Room. Have Fun and Enjoy Hacking! Do visit other rooms and modules on TryHackMe for more learning.

-by Shefali Kumai

For more cyber security learning follow me here-

https://github.com/ctf-time

https://www.youtube.com/channel/UCf-F-eATCUXYaUVk8Xl7OOQ

https://www.instagram.com/cybersecurity.cyber_seek/

Twitter - https://twitter.com/Shefali37920461