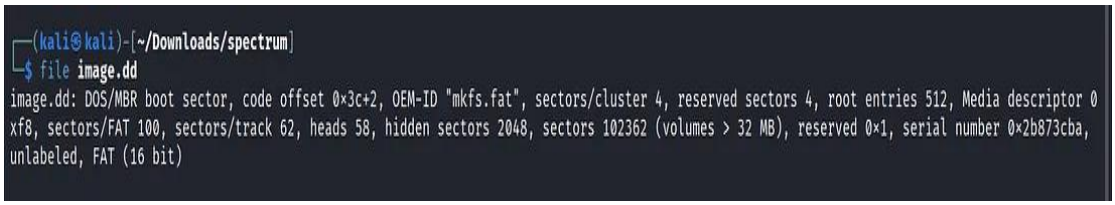
DIGITAL FORENSICS(AUDIO) - SMITH GRACE

AUDIO STEGANOGRAPHY

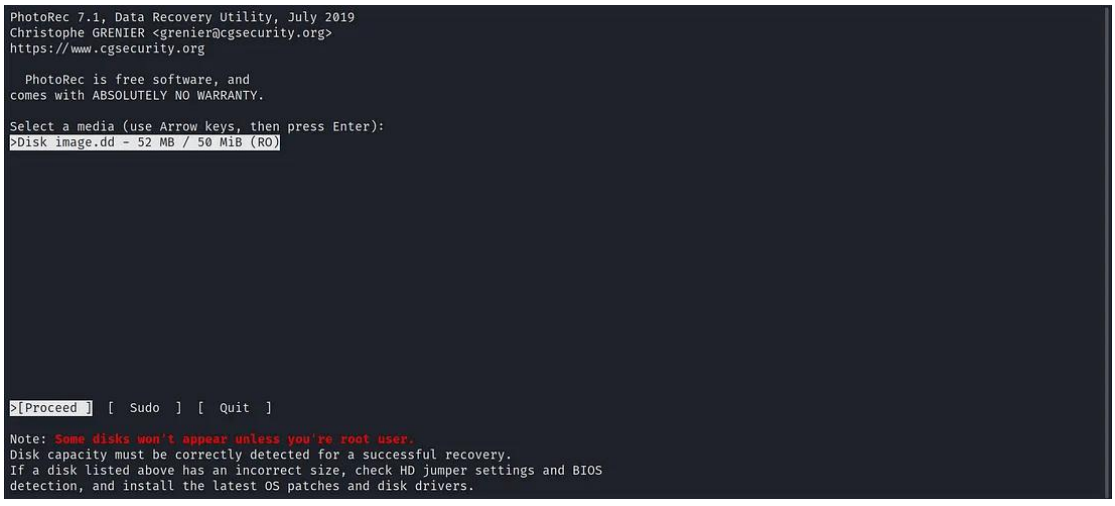
Scenario

Scotland yard have intercepted information about one of the biggest drug deals to go down in the city of London. Someone we believe is linked to the deal was arrested. The only item they had in their possession was a USB thumb drive. Unfortunately, one of our junior analysts was unable to find anything of interest. Before we let this suspect go, we would like one of our DF experts to see if they can find anything about the deal before it goes down. Can you find out where and when the deal is expected to go down?

1. First, I moved the downloaded file into a separate directory to see what the file is. It seemed like a disk image.



2. Then I analyzed what it contains using Photorec and extracted the whole partition from the filesystem.



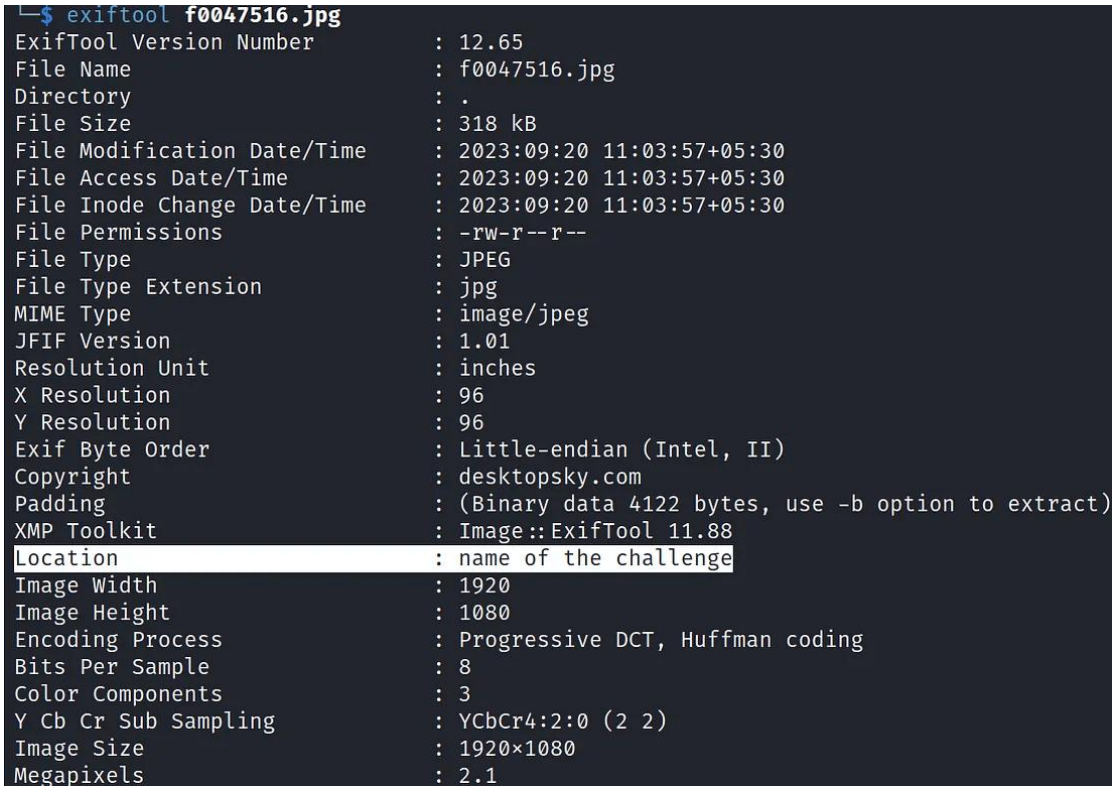
```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk image.dd - 52 MB / 50 MiB (RO)

     Partition                  Start        End    Size in sectors
      Unknown                  0   0  1    28  27 38     102400 [Whole disk]
>   P FAT16                    0   0  1    28  27 38     102400 [NO NAME]

>[ Search ]  [Options ]  [File Opt]  [  Quit  ]
                          Start file recovery
```

```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

   P FAT16                    0   0  1    28  27 38     102400 [NO NAME]

To recover lost files, PhotoRec needs to know the filesystem type where the
file were stored:
>[ ext2/ext3 ] ext2/ext3/ext4 filesystem
 [ Other     ] FAT/NTFS/HFS+/ReiserFS/...
```

```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

   P FAT16                    0   0  1    28  27 38     102400 [NO NAME]


Please choose if all space needs to be analysed:
 [   Free    ] Scan for files from FAT16 unallocated space only
>[   Whole   ] Extract files from whole partition
```

```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk image.dd - 52 MB / 50 MiB (RO)
     Partition                  Start        End    Size in sectors
   P FAT16                    0   0  1    28  27 38     102400 [NO NAME]


5 files saved in /home/kali/Downloads/spectrum/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation

[ Quit ]
```

3. There’s a zip archive and some images so I analyzed the exif data from these images



```
└─$ exiftool f0048900.jpg
ExifTool Version Number         : 12.65
File Name                       : f0048900.jpg
Directory                       : .
File Size                       : 3.8 MB
File Modification Date/Time     : 2023:09:20 11:03:57+05:30
File Access Date/Time           : 2023:09:20 11:03:57+05:30
File Inode Change Date/Time     : 2023:09:20 11:03:57+05:30
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 1
Y Resolution                    : 1
Resolution Unit                 : None
Artist                          : steghide password: cheese on toast
Y Cb Cr Positioning             : Centered
Image Width                     : 5614
Image Height                    : 3743
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 5614×3743
Megapixels                      : 21.0
```

4. I got some clues. The first clue is a bit vague there's no location named as "Spectrum". The second clue is a steghide password when means there could be hidden information in images and audios.There is a zip archive so I unzipped it.

```
┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1]
└─$ ls
f0000240_brown.zip  f0047500.DS_Store  f0047516.jpg  f0048140.jpg  f0048900.jpg  report.xml  t0048140.jpg

┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1]
└─$ unzip -d extractedData f0000240_brown.zip
Archive:  f0000240_brown.zip
[f0000240_brown.zip] brown.wav password:
password incorrect--reenter:
```

5. It was password protected and trying the password from the clue didn't yield any result either. So I tried to brute force the password. I used fcrackzip for this purpose and a dictionary brute forcing using Kali Linux's wordlist known as rockyou.txt which contains over 14 million passwords. I found password "garfield" and used it to extract the zip.

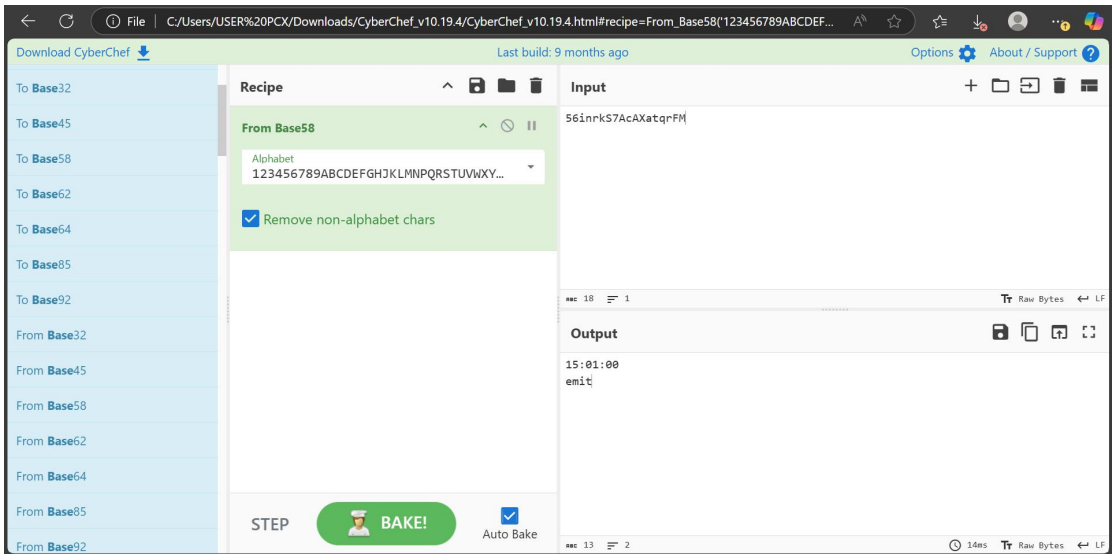
```
┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1]
└─$ cp /usr/share/wordlists/rockyou.txt.gz /home/kali/Downloads/spectrum/recup_dir.1

┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1]
└─$ ls
extractedData  f0000240_brown.zip  f0047500.DS_Store  f0047516.jpg  f0048140.jpg  f0048900.jpg  report.xml  rockyou.txt.gz  t0048140.jpg

┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1]
└─$ gzip -d rockyou.txt.gz

┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1]
└─$ ls
extractedData  f0000240_brown.zip  f0047500.DS_Store  f0047516.jpg  f0048140.jpg  f0048900.jpg  report.xml  rockyou.txt  t0048140.jpg
```

```
┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1]
└─$ fcrackzip -D -p rockyou.txt f0000240_brown.zip
possible pw found: garfield ()

┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1]
└─$
```

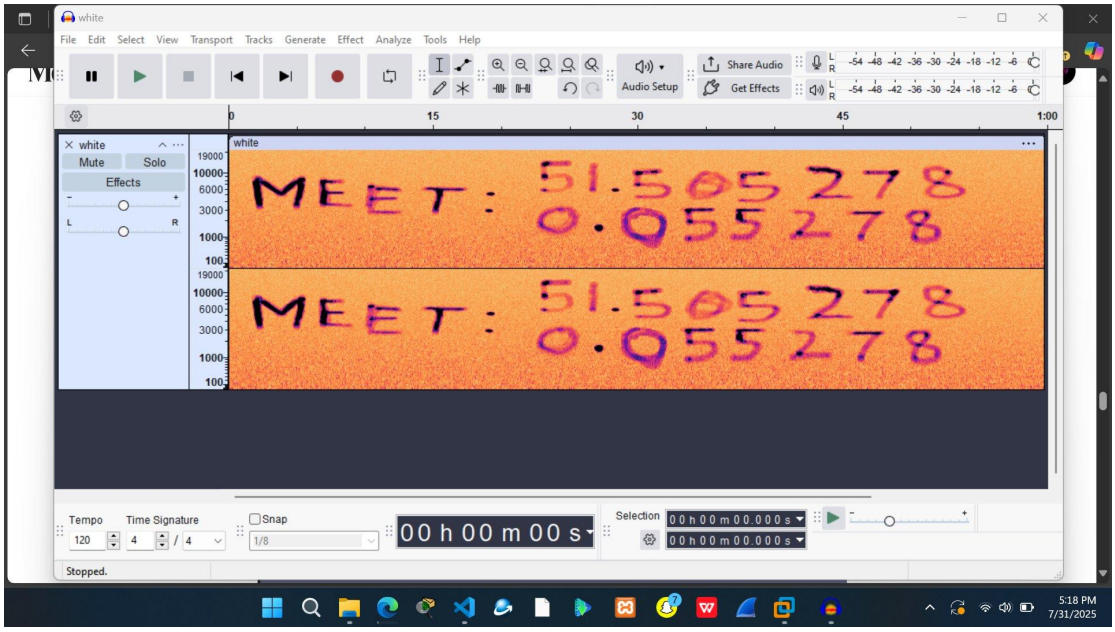
```
┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1]
└─$ unzip -d extractedData f0000240_brown.zip
Archive:  f0000240_brown.zip
[f0000240_brown.zip] brown.wav password:
  inflating: extractedData/brown.wav
  inflating: extractedData/location.wav
  inflating: extractedData/wahwah.wav
  inflating: extractedData/white.wav

┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1]
└─$ ls
extractedData  f0000240_brown.zip  f0047500.DS_Store  f0047516.jpg

┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1]
└─$ ls extractedData
brown.wav  location.wav  wahwah.wav  white.wav
```

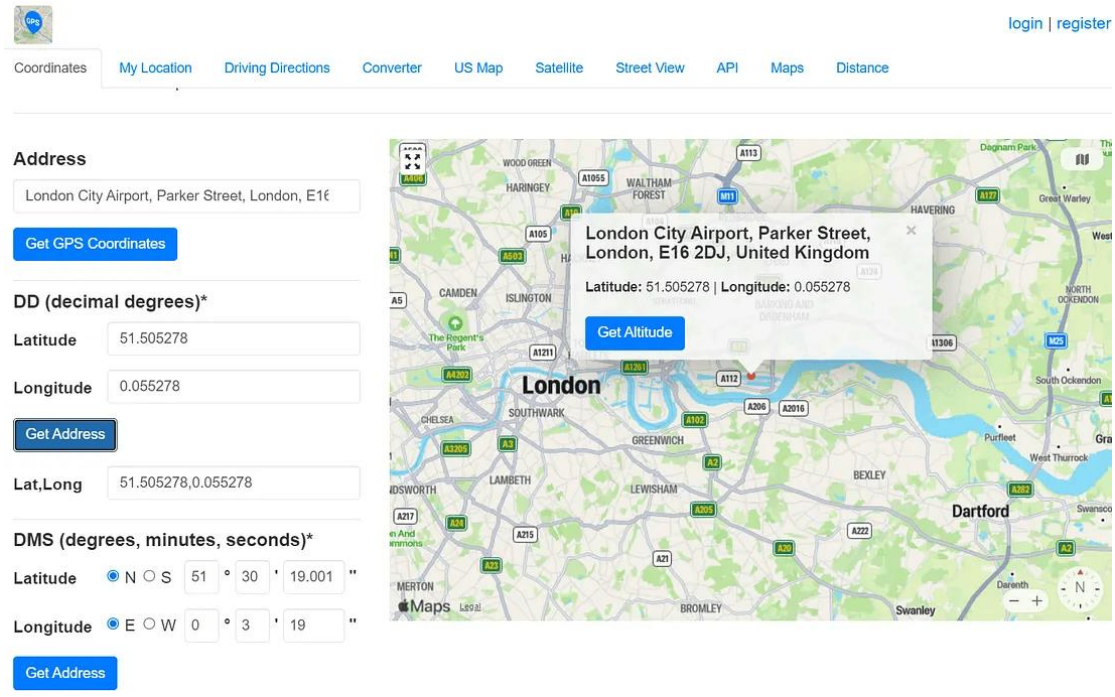
6. There are some audio files so I used steghide to attempt extracting information from it. There was a text file hidden in the audio and it contains a string. It seems the original text was encoded in Base58. (I tested the string on various tools online and found out that it was encoded using Base58). After decoding with CyberChef, I got a timestamp. However, it showed “emit”. After careful observation, I reversed “emit” to get “time” so I also reversed “15:01:00” to get “00:10:51” which is the meeting time.

```
┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1/extractedData]
└─$ steghide extract -sf white.wav -p "cheese on toast"
wrote extracted data to "stardate.txt".

┌──(kali㉿kali)-[~/Downloads/spectrum/recup_dir.1/extractedData]
└─$ cat stardate.txt
56inrkS7AcAXatqrFM
```



7. previously, I loaded it into Audacity for further analysis. I checked the spectogram of the audio file and found GPS coordinates in decimal degrees then proceeded to find the corresponding location.





Key Takeaways

- **Understanding Steganography vs. Cryptography :** The project deepened my understanding of covert data transmission methods and how attackers may exfiltrate information without triggering alarms.
- **Tools and Techniques Used for Detection :** I gained hands-on experience using forensic tools and signal analysis techniques to identify hidden payloads in audio files.
- **Identifying Indicators of Steganography :** I learned how to correlate digital evidence (metadata, hashes, file signatures) with hidden communication methods.

- **Real-World Applications and Threats :** I explored how audio files could be exploited to smuggle data across monitored environments, simulating advanced threat behaviors.
- **Incident Response and Legal Relevance :** I applied digital forensics methodology to audio media, aligning your work with legal and ethical investigation standards.