



Portfolios



# USB Drive Investigate

DIGITAL FORENSIC

2024



Prepared by :

**Arya Widyanto Utomo**

+6285865492276

[www.reallygreatsite.com](http://www.reallygreatsite.com)

[Utomoa448@gmail.com](mailto:Utomoa448@gmail.com)

# DAFTAR ISI

<u>I.</u>	<u>Deskripsi Kasus .....</u>	<u>3</u>
<u>II.</u>	<u>Pembukaan : Sifat Laporan .....</u>	<u>3</u>
<u>III.</u>	<u>Barang Bukti .....</u>	<u>3</u>
<u>IV.</u>	<u>Maksud Pemeriksaan .....</u>	<u>4</u>
<u>V.</u>	<u>Hasil Pemeriksaan .....</u>	<u>4</u>
<u>VI.</u>	<u>Kesimpulan .....</u>	<u>6</u>
<u>VII.</u>	<u>Penutup .....</u>	<u>6</u>

## Deskripsi Kasus

---

Organisasi Narkoba telah menyadap informasi tentang salah satu transaksi narkoba terbesar yang akan terjadi di kota Semarang. Seseorang yang kami yakini terkait dengan transaksi tersebut telah ditangkap. Satu-satunya barang yang mereka miliki adalah sebuah USB thumb drive. Sayangnya, salah satu analis junior kami tidak dapat menemukan sesuatu yang menarik. Sebelum kami melepaskan tersangka ini, kami ingin menemukan sesuatu tentang transaksi tersebut sebelum terjadi. Saya akan mencari tahu di mana dan kapan transaksi tersebut diperkirakan akan terjadi?

## Pembukaan : Sifat Laporan

---


### **Pro Justitia.**

Demi hukum dan undang-undang yang berlaku saya akan memberikan laporan hasil investigasi dan keterangan ahli ini dengan sebenar-benarnya dan seadil-adilnya.

## Barang Bukti

---

bukti tersebut berupa drive usb yang telah disalin bit per bit nya dari media aslinya agar dapat dilakukan forensic digital.

Name	Type	Compressed size	Password p...	Size
 image.dd	DD File	51.072 KB	Yes	

Img 1. Bukti digital

## Maksud Pemeriksaan

---

Maksud pemeriksaan adalah untuk mengetahui :

1. Mencari tahu jam berapa pertemuannya berlangsung?
2. Mencari tahu apa koordinat yang seharusnya untuk transaksi tersebut
3. Mencari tahu lokasi dari koordinat yang didapatkan

## Hasil Pemeriksaan

Adapun berdasarkan Maksud pemeriksaan diatas, maka dilakukan pemeriksaan lebih lanjut dan kemudian menemukan hasil sebagai berikut.

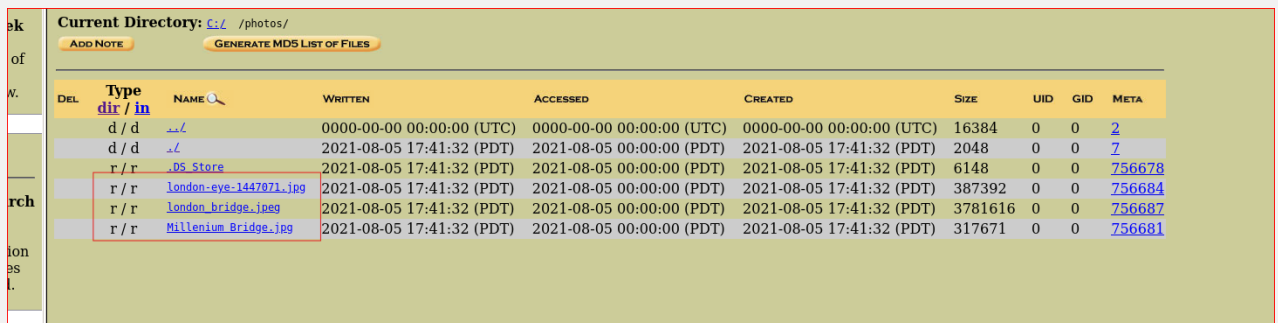
Untuk pemeriksaan pertama,saya coba lakukan analisis terhadap file imagingnya,disini saya lakukan analisis menggunakan tools autopsy.



Current Directory: C:/

ADD NOTE GENERATE MDS LIST OF FILES

DEL	Type	NAME	WRITTEN	ACCESSED
	dir / in			
Error Parsing File (Invalid Characters?):				
V/V 1634534: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0				
	v / v	\$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
	v / v	\$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
	v / v	\$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
	r / r	noise_samples.zip	2021-08-05 17:41:32 (PDT)	2021-08-05 00:00:00 (PDT)
	d / d	photos/	2021-08-05 17:41:32 (PDT)	2021-08-05 00:00:00 (PDT)

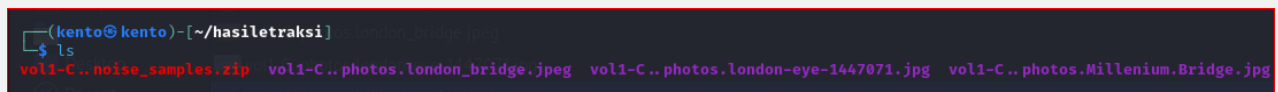


Current Directory: C:/ /photos/

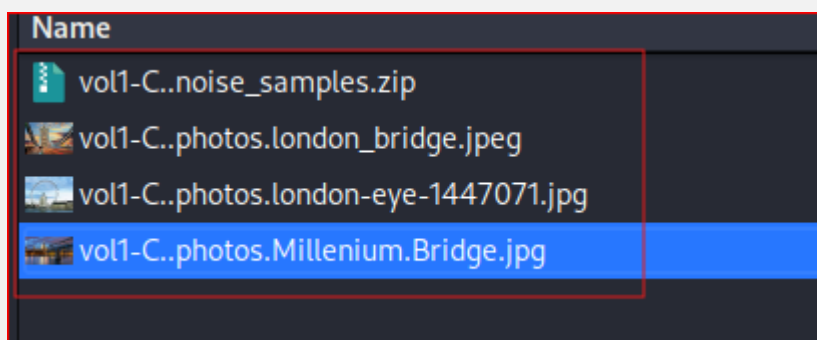
ADD NOTE GENERATE MDS LIST OF FILES

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	dir / in								
	d / d	.	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	16384	0	0	2
	d / d	..	2021-08-05 17:41:32 (PDT)	2021-08-05 00:00:00 (PDT)	2021-08-05 17:41:32 (PDT)	2048	0	0	2
	r / r	DS_Store	2021-08-05 17:41:32 (PDT)	2021-08-05 00:00:00 (PDT)	2021-08-05 17:41:32 (PDT)	6148	0	0	756678
	r / r	london-eye-1447071.jpg	2021-08-05 17:41:32 (PDT)	2021-08-05 00:00:00 (PDT)	2021-08-05 17:41:32 (PDT)	387392	0	0	756684
	r / r	london_bridge.jpeg	2021-08-05 17:41:32 (PDT)	2021-08-05 00:00:00 (PDT)	2021-08-05 17:41:32 (PDT)	3781616	0	0	756687
	r / r	Millenium Bridge.jpg	2021-08-05 17:41:32 (PDT)	2021-08-05 00:00:00 (PDT)	2021-08-05 17:41:32 (PDT)	317671	0	0	756681

Dan hasil analisis tersebut menunjukkan bahwa saya mendapatkan beberapa file,yaitu berupa file zip dan directory berisi 3 foto. Selanjutnya mari kita export data-data tersebut.



```
(kento@kento) - [~/hasiletraksi]
$ ls
vol1-C..noise_samples.zip  vol1-C..photos.london_bridge.jpeg  vol1-C..photos.london-eye-1447071.jpg  vol1-C..photos.Millenium.Bridge.jpg
```



Setelah melakukan ekstrak, saya mendapatkan beberapa data zip dan gambar-gambar, jadi saya akan mulai menganalisis metadata dari gambar-gambar tersebut terlebih dahulu, mungkin ada informasi menarik yang bisa didapatkan. saya akan menggunakan exiftool untuk menganalisis metadata pada gambar.

```
(kento@kento)-[~/hasiletraksi]
$ exiftool vol1-C..photos.london_bridge.jpeg
ExifTool Version Number      : 12.76
File Name                    : vol1-C..photos.london_bridge.jpeg
Directory                    : .
File Size                     : 3.8 MB
File Modification Date/Time   : 2024:07:06 08:01:46-07:00
File Access Date/Time         : 2024:07:06 08:04:11-07:00
File Inode Change Date/Time   : 2024:07:06 08:04:11-07:00
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                    : 5614x3743
Megapixels                    : 21.0
```

Metadata1

```
(kento@kento)-[~/hasiletraksi]
$ exiftool vol1-C..photos.london-eye-1447071.jpg
ExifTool Version Number      : 12.76
File Name                    : vol1-C..photos.london-eye-1447071.jpg
Directory                    : .
File Size                    : 387 kB
File Modification Date/Time   : 2024:07:06 08:01:36-07:00
File Access Date/Time        : 2024:07:06 08:04:23-07:00
File Inode Change Date/Time   : 2024:07:06 08:04:23-07:00
File Permissions              : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Exif Byte Order               : Little-endian (Intel, II)
Image Description             : OLYMPUS DIGITAL CAMERA
Make                        : OLYMPUS CORPORATION
Camera Model Name            : C750UZ
Orientation                  : Horizontal (normal)
X Resolution                  : 72
Y Resolution                  : 72
Resolution Unit              : inches
Software                     : Adobe Photoshop CS2 Windows
Modify Date                  : 2006:09:13 01:55:53
Y Cb Cr Positioning          : Co-sited
PrintIM Version              : 0250
Exposure Time                 : 1/320
F Number                     : 4.0
Exposure Program              : Creative (Slow speed)
ISO                           : 50
Exif Version                 : 0220
Date/Time Original           : 0000:00:00 00:00:00
Create Date                  : 0000:00:00 00:00:00
Components Configuration     : Y, Cb, Cr, -
Compressed Bits Per Pixel    : 2
Exposure Compensation        : 0
Max Aperture Value           : 2.8
Metering Mode                 : Multi-segment
Light Source                  : Unknown
Flash                        : Off, Did not fire
Focal Length                  : 6.3 mm
User Comment                  :
Flashpix Version              : 0100
Color Space                   : sRGB
Exif Image Width              : 1500
Exif Image Height            : 1122
Interoperability Index       : R98 - DCF basic file (sRGB)
Interoperability Version     : 0100
File Source                   : Digital Camera
Scene Type                    : Directly photographed
Custom Rendered               : Normal
Exposure Mode                 : Auto
White Balance                 : Auto
Digital Zoom Ratio            : 0
Scene Capture Type            : Standard
Gain Control                  : None
Contrast                      : Normal
Saturation                    : Normal
Sharpness                     : Normal
```

```

(kento@kento)-[~/hasiletraksi]
$ exiftool vol1-C..photos.Millennium.Bridge.jpg
ExifTool Version Number      : 12.76
File Name                    : vol1-C..photos.Millennium.Bridge.jpg
Directory                    : .
File Size                    : 318 kB
File Modification Date/Time   : 2024:07:06 08:01:55-07:00
File Access Date/Time        : 2024:07:06 08:04:39-07:00
File Inode Change Date/Time   : 2024:07:06 08:04:39-07:00
File Permissions              : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
X Resolution                 : 96
Y Resolution                 : 96
Exif Byte Order              : Little-endian (Intel, II)
Copyright                   : desktopsky.com
Padding                     : (Binary data 4122 bytes, use -b option to extract)
XMP Toolkit                  : Image::ExifTool 11.88
Location                    : name of the challenge
Image Width                  : 1920
Image Height                 : 1080
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                   : 1920x1080
Megapixels                   : 2.1

```

### Metadata3

Pada metadata1,saya menemukan informasi menarik,informasi tersebut menunjukan password untuk steghide,yaitu cheese on toast.

Resolution Unit	none
Artist	steghide password: cheese on toast

Jadi saya coba untuk mencoba mengekstrak informasi dari gambar tersebut menggunakan steghide.

```

(kento@kento)-[~/hasiletraksi]
$ steghide extract -sf vol1-C..photos.london_bridge.jpeg
Enter passphrase:
steghide: could not extract any data with that passphrase!

(kento@kento)-[~/hasiletraksi]
$ steghide extract -sf vol1-C..photos.london-eye-1447071.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!

(kento@kento)-[~/hasiletraksi]
$ steghide extract -sf vol1-C..photos.Millennium.Bridge.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!

```

Dan ternyata saya tidak dapat meng extract apapun dari gambar-gambar tersebut.dan yang tersisa tinggal file zip,jadi saya akan mencoba untuk extract isinya dengan melakukan unzip.

```
(kento@kento)-[~/hasiletraksi]
$ unzip vol1-C..noise_samples.zip
Archive:  vol1-C..noise_samples.zip
[vol1-C..noise_samples.zip] brown.wav password: 
```

Dan ternyata zip tersebut juga dilindungi dengan kata sandi, jadi saya tidak dapat dengan mudah meng ekstraksi file tersebut, jadi saya akan menggunakan fcrackzip untuk tujuan ini dan kita akan menggunakan metode brute force dictionary. Secara default, Kali Linux dilengkapi dengan daftar kata yang dikenal sebagai rockyou.txt yang berisi lebih dari 14 juta kata sandi.

```
(kento@kento)-[~/hasiletraksi]
$ fcrackzip -D -p /usr/share/wordlists/rockyou.txt vol1-C..noise_samples.zip
possible pw found: garfield ()
```

Setelah melakukan bruteforce dictionary attack, akhirnya saya mendapatkan kata sandi untuk ekstraksi zip tersebut, jadi saya akan langsung mencoba kata sandi yang didapatkan (garfield).

```
(kento@kento)-[~/hasiletraksi]
$ unzip vol1-C..noise_samples.zip
Archive:  vol1-C..noise_samples.zip
[vol1-C..noise_samples.zip] brown.wav password:
  inflating: brown.wav
  inflating: location.wav
  inflating: wahwah.wav
  inflating: white.wav
```

Dan ternyata berisi beberapa file audio. Dilihat dari clue tadi kita mendapat password steghide, dan sekarang kita mendapatkan beberapa berkas audio. perlu diketahui bahwa steghide ini juga bisa digunakan untuk menyembunyikan data dalam berkas audio. Jadi saya akan mencoba meng ekstrak data dari berkas audio tersebut satu per satu menggunakan steghide.

```
(kento@kento)-[~/hasiletraksi]
$ steghide extract -sf white.wav
Enter passphrase:
wrote extracted data to "stardate.txt".

(kento@kento)-[~/hasiletraksi]
$ steghide extract -sf brown.wav
Enter passphrase:
steghide: could not extract any data with that passphrase!

(kento@kento)-[~/hasiletraksi]
$ steghide extract -sf wahwah.wav
Enter passphrase:
steghide: could not extract any data with that passphrase!

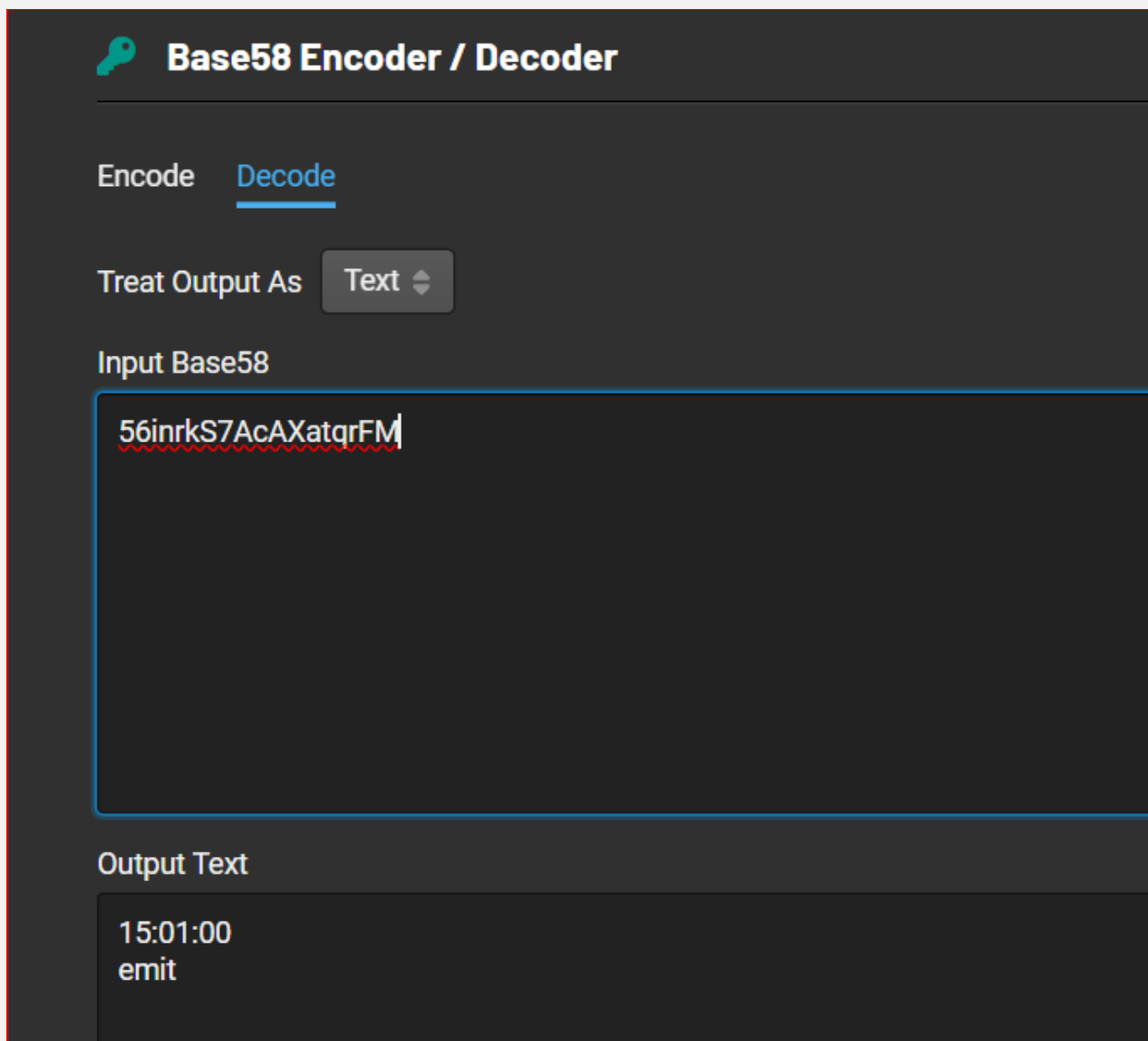
(kento@kento)-[~/hasiletraksi]
$ steghide extract -sf location.wav
Enter passphrase:
steghide: could not extract any data with that passphrase!
```



Dari ekstraksi tersebut, saya mendapatkan file text bernama stardate.txt, jadi langsung saja saya buka isinya.

```
(kento@kento) - [~/hasiletraksi]  
$ cat stardate.txt  
56inrkS7AcAXatqrFM
```

Dan saya menemukan sesuatu. Ada berkas teks yang tersembunyi dalam audio dan berisi string. Jadi saya akan mencoba melakukan decode terhadap string tersebut.



**Base58 Encoder / Decoder**

Encode Decode

Treat Output As

Input Base58

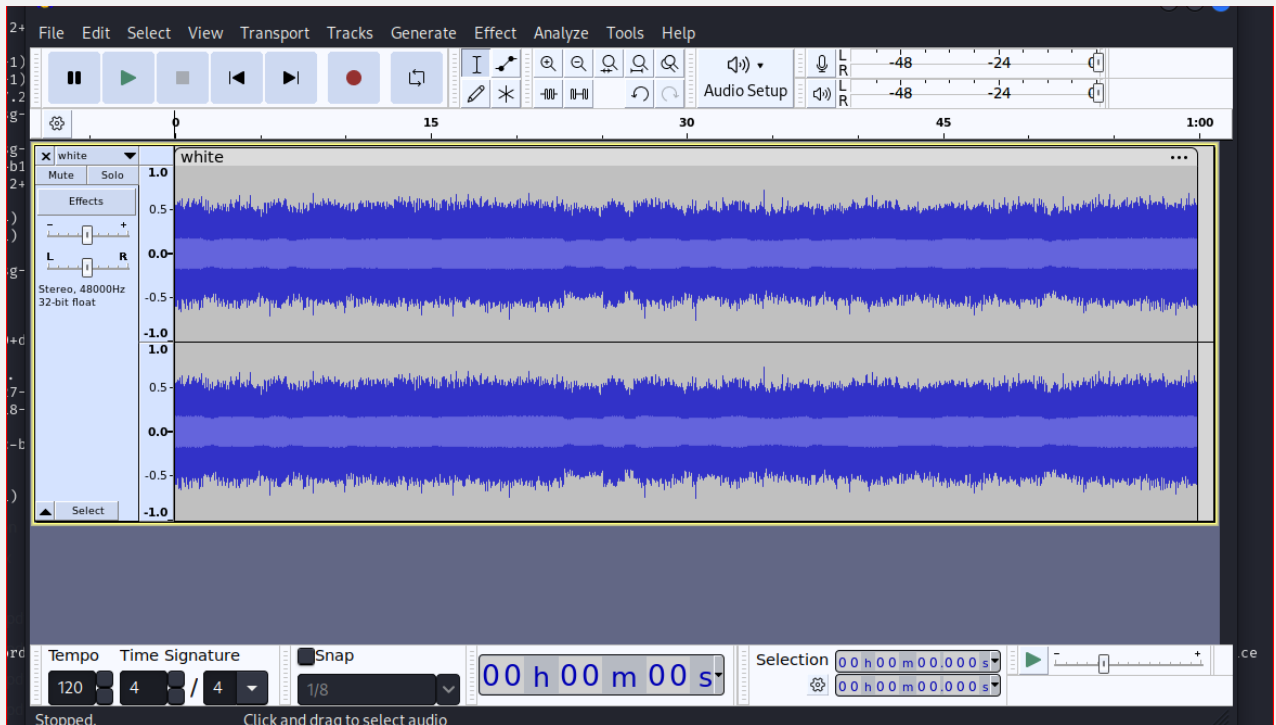
56inrkS7AcAXatqrFM

Output Text

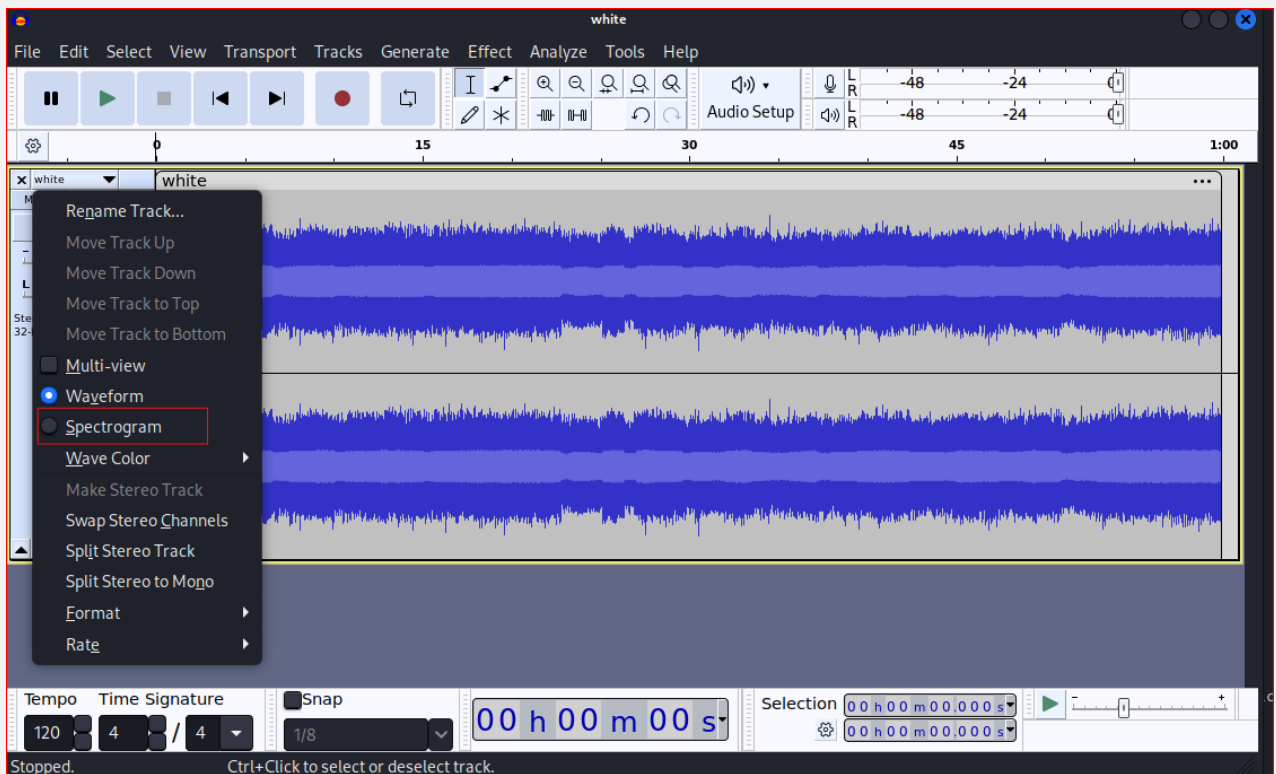
15:01:00  
emit

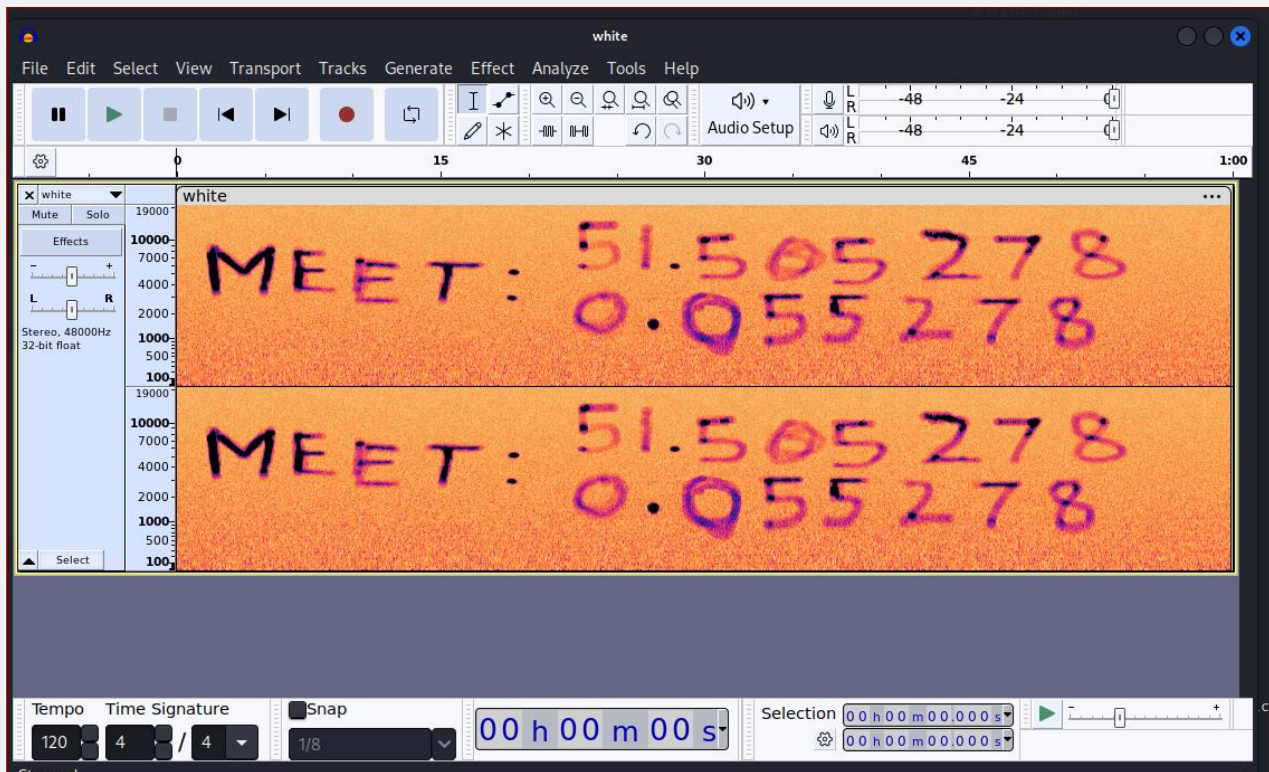
Tampaknya teks asli dikodekan dalam Base58. (Saya menguji string tersebut pada berbagai alat daring dan menemukan bahwa string tersebut dikodekan menggunakan Base58). Dan setelah didecode, saya mendapatkan cap waktu. Tapi apa itu "emit". Mari kita perhatikan baik-baik, bagaimana jika kita membalik "emit", kita dapat "time" jadi jika kita membalik "15:01:00" kita dapat "00:10:51". Di situlah saya menemukan waktu pertemuan.

Sekarang saatnya mencari lokasinya.kembali ke berkas audio tersebut dan memuatnya ke dalam perangkat lunak audio menggunakan Audacity untuk tujuan ini.dimulai dengan *white.wav*, yang berisi berkas teks tersembunyi, mungkin ada sesuatu yang lebih tersembunyi di dalamnya.

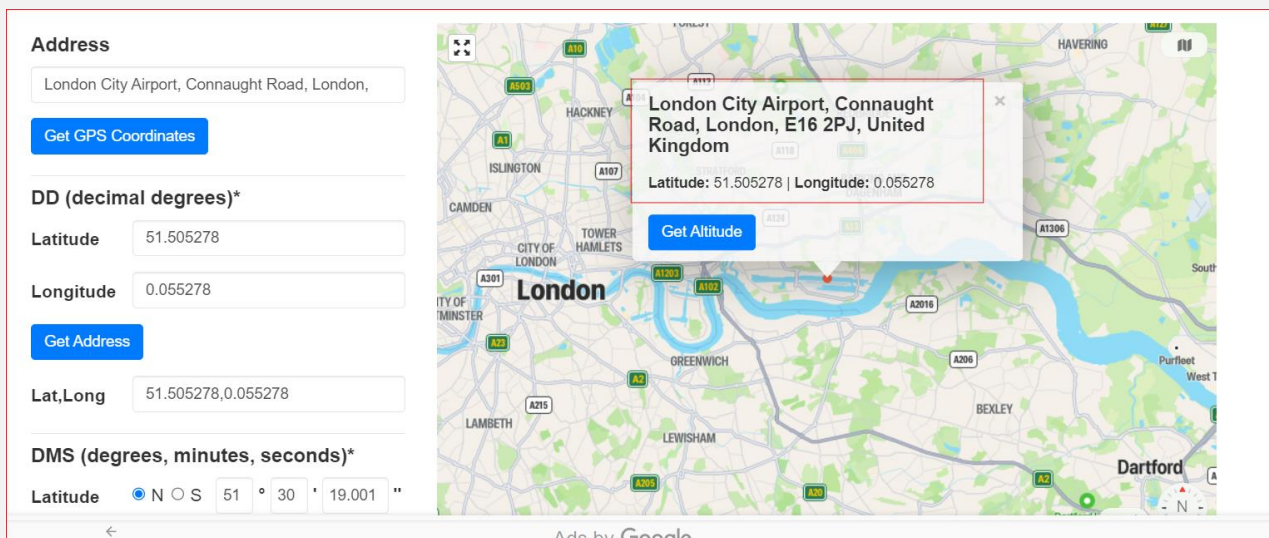


Ternyata tidak ditemukan apa=apa,selanjutnya disini saya coba untuk melihat spektogramnya.





Yah,dan ditemukanlah koordinat lokasi tersebut,yaitu **51.505278** dan **0.055278**.dan saya akan mencoba untuk mencari lokasi koordinat tersebut dengan <https://www.gps-coordinates.net/> untuk melihat lokasinya.



Akhirnya ditemukanlah lokasinya berada **di London City Airport, Connaught Road, London, E16 2PJ, United Kingdom**

## Kesimpulan

---

Telah dilakukan pemeriksaan dan analisis terhadap barang bukti berupa USB. Pemeriksaan dan analisis dilakukan dengan menggunakan sistem operasi kali linux. Hasil analisis berhasil menemukan semua informasi yang diminta.

## Penutup

---

Demikian laporan hasil investigasi dan keterangan ini dibuat dengan sebenarnya dengan menjunjung tinggi nilai keadilan berdasarkan keahlian dan kompetensi yang dimiliki sesuai dengan peraturan dan perundang-undangan yang berlaku.