

**Enhancing Digital Government and Economy**  
**Cyber Security Course**  
**Classwork-04**



**Submitted by,**  
**Name: Koushiki Devi Agarwalla**  
**Batch: JUR2B11**  
**ID: 2111271**

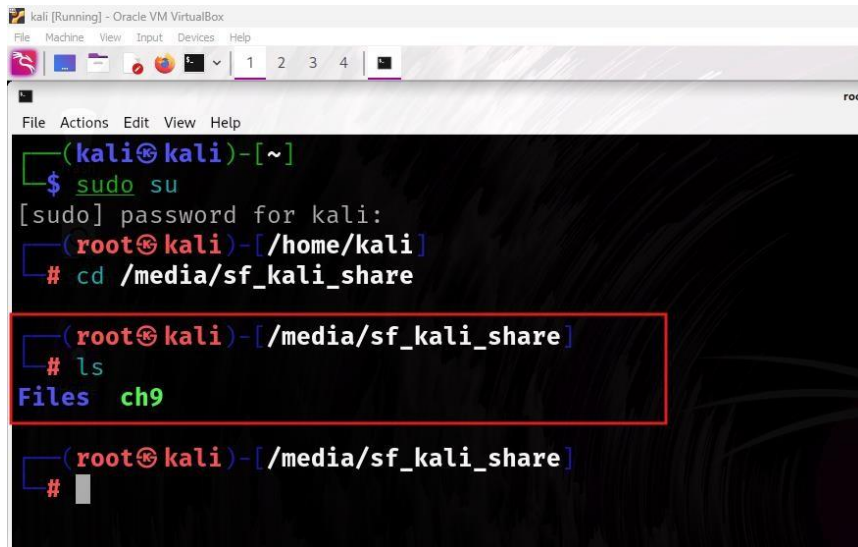
Find the cat location from the disk file.

Step 01: Download disk file name **ch9** from the url  
<https://tinyurl.com/juclassmaterial>

Step 02: Copy this file (ch9) to shared folder. Check from file from kali by using following command

```
# cd /media/sf_kali_share
```

```
# ls
```



```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
# cd /media/sf_kali_share
(kali㉿kali)-[/media/sf_kali_share]
# ls
Files ch9
(kali㉿kali)-[/media/sf_kali_share]
#
```

#testdisk ch9 (testdisk is a free, open-source utility that can help recover lost partitions and repair corrupted file systems)

```
File Actions Edit View Help
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media and choose 'Proceed' using arrow keys:
>Disk ch9 - 134 MB / 128 MiB

>[Proceed ] [ Quit ]
```

Hit enter to Proceed.

```
File Actions Edit View Help
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk ch9 - 134 MB / 128 MiB

Please select the partition table type, press Enter when done.
>[Intel ] Intel/PC partition
[EFI GPT] EFI GPT partition map (Mac i386, some x86_64 ...)
[Humax ] Humax partition table
[Mac ] Apple partition map (legacy)
[None ] Non partitioned media
[Sun ] Sun Solaris partition
[XBox ] Xbox partition
[Return] Return to disk selection
```

Hit select Intel by arrow key and hit enter

```
File Actions Edit View Help
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk ch9 - 134 MB / 128 MiB
CHS 17 255 63 - sector size=512

>[Analyse ] Analyse current partition structure and search for lost partitions
[Advanced ] Filesystem Utils
[Geometry ] Change disk geometry
[Options ] Modify options
[MBR Code ] Write TestDisk MBR code to first sector
[Delete ] Delete all data in the partition table
[Quit ] Return to disk selection
```

## Select Advanced and hit enter

```
File Actions Edit View Help
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk ch9 - 134 MB / 128 MiB - CHS 17 255 63

Partition              Start      End      Size in sectors
> 1 * FAT32             0 32 33   16 81 1   260096

[ Type ] >[ Boot ] [Undelete] [Image Creation] [ Quit ]
                        Boot sector recovery
```

## Select Boot and hit enter

```
File Actions Edit View Help
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk ch9 - 134 MB / 128 MiB - CHS 17 255 63

Partition              Start      End      Size in sectors
1 * FAT32             0 32 33   16 81 1   260096

Boot sector
Warning: number of heads/cylinder mismatches 64 (FAT) ≠ 255 (HD)
Warning: number of sectors per track mismatches 32 (FAT) ≠ 63 (HD)
OK

Backup boot sector
Warning: number of heads/cylinder mismatches 64 (FAT) ≠ 255 (HD)
Warning: number of sectors per track mismatches 32 (FAT) ≠ 63 (HD)
OK

Second sectors (cluster information) are not identical.

A valid FAT Boot sector must be present in order to access
any data; even if the partition is not bootable.

[ Quit ] >[ List ] [Org. BS] [Backup BS] [Rebuild BS] [ Dump ]
                        List directories and files, copy and undelete data from FAT
```

## Select list and hit enter

```
File Actions Edit View Help
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
1 * FAT32             0 32 33   16 81 1   260096
Directory /

drwxr-xr-x  0  0      0 23-Jul-2013 03:21 Documentations
>drwxr-xr-x  0  0      0 23-Jul-2013 03:21 Files
drwxr-xr-x  0  0      0 23-Jul-2013 03:22 WebSites
```

Select drwxr-xr-x ----- Files and hit enter

```
File Actions Edit View Help
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
1 * FAT32 0 32 33 16 81 1 260096
Directory /Files

drwxr-xr-x 0 0 0 23-Jul-2013 03:20 .
drwxr-xr-x 0 0 0 23-Jul-2013 03:20 ..
> -rwxr-xr-x 0 0 2341273 23-Jul-2013 03:20 revendications.odt
-rwxr-xr-x 0 0 1197056 23-Jul-2013 03:20 421_20080208011.doc
-rwxr-xr-x 0 0 142336 23-Jul-2013 03:20 Coker.doc
-rwxr-xr-x 0 0 63166 23-Jul-2013 03:20 DataSanitizationTutorial.odt
-rwxr-xr-x 0 0 57344 23-Jul-2013 03:20 Creer_votre_association.doc

Next
Use Left arrow to go back, Right to change directory, 'h' to hide deleted files
'q' to quit, ':' to select the current file, 'a' to select all files
'c' to copy the selected files, 'c' to copy the current file
```

Select red color record and press c


```
File Actions Edit View Help
TestDisk 7.2, Data Recovery Utility, February 2024

Please select a destination where /Files/revendications.odt will be copied.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory /media/sf_kali_share
>drwxrwx--- 0 130 0 26-Sep-2024 07:40 .
drwxr-xr-x 0 0 4096 26-Sep-2024 05:59 ..
-rwxrwx--- 0 130 13421728 26-Sep-2024 05:57 ch9
```

Again press c.

```
root@kali: /media/sf_kali_share
File Actions Edit View Help
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
1 * FAT32 0 32 33 16 81 1 260096
Directory /Files/revendications.odt
Copy done! 1 ok, 0 failed
drwxr-xr-x 0 0 0 23-Jul-2013 03:20 .
drwxr-xr-x 0 0 0 23-Jul-2013 03:20 ..
> -rwxr-xr-x 0 0 2341273 23-Jul-2013 03:20 revendications.odt
-rwxr-xr-x 0 0 1197056 23-Jul-2013 03:20 421_20080208011.doc
-rwxr-xr-x 0 0 142336 23-Jul-2013 03:20 Coker.doc
-rwxr-xr-x 0 0 63166 23-Jul-2013 03:20 DataSanitizationTutorial.odt
-rwxr-xr-x 0 0 57344 23-Jul-2013 03:20 Creer_votre_association.doc
```


A successful message will appear.



The screenshot shows a Windows File Explorer window with the address bar displaying the path: This PC > Local Disk (J:) > VMOS > kali\_share >. The left sidebar shows the navigation pane with 'Home' selected. The main area displays a table of files and folders:

Name	Date modified	Type	Size
Files	9/26/2024 5:52 PM	File folder	
ch9	9/26/2024 3:57 PM	File	131,072 KB

The 'Files' folder is highlighted with a red rectangle.



The screenshot shows a Windows File Explorer window. The address bar indicates the path: This PC > Local Disk (J:) > VMOS > kali\_share > Files. The left sidebar shows the navigation pane with 'Home' selected. The main area displays a table of files. The file 'revendications.odt' is highlighted with a red rectangle. The table has columns for Name, Date modified, Type, and Size.

Name	Date modified	Type	Size
revendications.odt	7/23/2013 1:20 PM	OpenDocument T...	2,287 KB

The screenshot shows a Windows File Explorer window with the address bar displaying the path: This PC > Local Disk (J:) > VMOS > kali\_share > Files. The main content area lists the following items:

Name	Date modified	Type	Size
revalidations.zip	7/23/2013 1:20 PM	WinRAR ZIP archive	2,287 KB
revalidations	9/26/2024 5:58 PM	File folder	

The left sidebar shows the following navigation options: Home, Gallery, Desktop, Downloads, and Documents.



Now go to kali machine terminal that previously opened.  
Please q until the following screen appears in terminal.

```
File Actions Edit View Help
(root@kali)-[/media/sf_kali_share]
# testdisk ch09
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Unable to open file or device ch09: No such file or directory

(root@kali)-[/media/sf_kali_share]
# testdisk ch9
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

(root@kali)-[/media/sf_kali_share]
#
```

Go to Pictures folder by following command  
# cd /media/sf\_kali\_share/Files/revendications/Pictures

```
File Actions Edit View Help
(root@kali)-[/media/sf_kali_share]
# testdisk ch09
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Unable to open file or device ch09: No such file or directory

(root@kali)-[/media/sf_kali_share]
# testdisk ch9
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

(root@kali)-[/media/sf_kali_share]
# cd /media/sf_kali_share/Files/revendications/Pictures

(root@kali)-[/media/sf_kali_share/Files/revendications/Pictures]
#
```

Now extract information from the image using following command

#exiftool image\_name [press tab, name comes automatically]

```
File Actions Edit View Help
Compression          : JPEG (old-style)
Thumbnail Offset     : 902
Thumbnail Length     : 8207
Image Width          : 3264
Image Height         : 2448
Encoding Process     : Baseline DCT, Huffman coding
Bits Per Sample      : 8
Color Components      : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Aperture             : 2.4
Image Size           : 3264x2448
Megapixels           : 8.0
Scale Factor To 35 mm Equivalent : 8.2
Shutter Speed        : 1/20
Thumbnail Image       : (Binary data 8207 bytes, use -b option to extract)
GPS Altitude          : 16.7 m Above Sea Level
GPS Latitude          : 47 deg 36' 16.15" N
GPS Longitude         : 7 deg 24' 52.48" E
Circle Of Confusion   : 0.004 mm
Field Of View         : 54.4 deg
Focal Length          : 4.3 mm (35 mm equivalent: 35.0 mm)
GPS Position          : 47 deg 36' 16.15" N, 7 deg 24' 52.48" E
Hyperfocal Distance   : 2.08 m
Light Value           : 6.2

(root@kali) - [ /media/sf_kali_share/Files/revendications/Pictures ]
```

There is much information we need GPS Latitude and GPS Longitude to retrieve image location.

Use <https://www.gps-coordinates.net/> we can find the location.

Address

1 Rue Principale, 68510 Helfrantzkirch, France

Get GPS Coordinates

DD (decimal degrees)\*

Latitude47.6044861

Longitude7.414577777777778

Get Address

Lat,Long

47.6044861,7.414577777777778

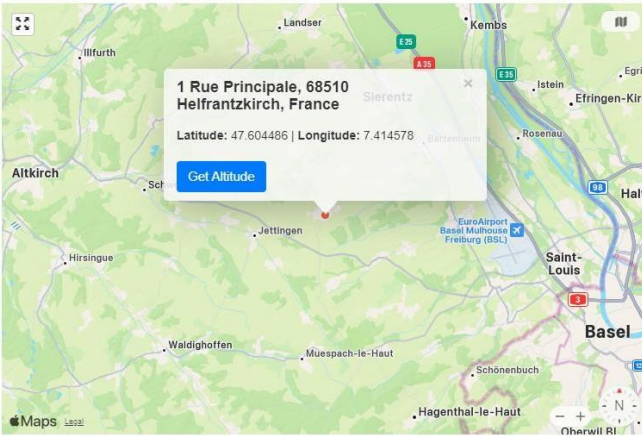
DMS (degrees, minutes, seconds)\*

LatitudeN°47'36"16.15"

LongitudeE°7'24"52.479"

Get Address

\* World Geodetic System 84 (WGS 84)



Result:

The cat location:

1 Rue Principale, 68510 Helfrantzkirch, France



1. MITRE ATT\*ACK Framework
2. Cyber kill chain

<https://exposed.lol/> → Check for, is your email address on international black market?

<https://haveibeenpwned.com/> → someone has been controlled or compromised

# Enhanced Incident Detection with thread intelligent  
#Miter attack

- MITRE Atta\*ck → step by step procedure
- Miter atta\*ck base on: 4 step
  - Adversary : The framework tracks their methods, such as how they gain access, move within networks, and steal data, to help organizations defend against these threats
  - Threat models: gaining access, exploiting vulnerabilities
  - Techniques ,300+ technique
  - Mitigating tactics → age thik kora kon path e agabo →18 technique
- Attacker er perspective e miter attack banano hoy
- Three matrix:
  - Enterpricse attack
  - Pre attack
  - Mobile attack
- One password list and one username list: brute force check user and password
- <https://mitre-attack.github.io/attack-navigator/> -- scanning ip for find vulnerability
- <https://attack.mitre.org/> →matrices →ICS→[View on the ATT&CK® Navigator](#) →
- sudo -i → for root
- nmap → use for find ip details
- nmap - help → find help for specific attribute
- netdiscover -i eth0 → for find all pc which connect with eth0 net
  - nmap -sC -sV -Pn -A target-ipaddress →Scanning IP blocks
- <https://web-check.as93.net/> → to find website vulnerability (best

web site)

- load balancer— 100jn heat korle sobaik 10 second kore dewa,load balancer jei server idle oitak onno serverk dey
- [tinyurl.com/junivgift03](https://tinyurl.com/junivgift03) → gift
- malware is a software or program
- Zero-day Exploit – recently discover vulnerability
- C2 (Command and Control)

#Need to basic for Cyber Security

- Networking
- System
  - Administration
  - Hardware
- Software development

#Job sector

- Vendors
- Banks
- Financial orgs → tk bsi,bank bade onno financial orgs
- Others

#certificates

- <https://www.isc2.org/certifications/cissp> --> most demandable certificate in usa/Europe → odit certificate
- <https://www.comptia.org/>
- <https://www.offsec.com/> → oscp certificate best. best from all course
- <https://mile2.com/>
- <https://www.eccouncil.org/> ceh certification need for beginners