

# PES UNIVERSITY

UE19CS336

## Digital Forensics Project

Extracting of ext3, NTFS, FAT32  
Image Files

Teammates :

|    |                  |               |           |
|----|------------------|---------------|-----------|
| 1. | Suhan B Revankar | PES2UG19CS412 | G Section |
| 2. | Nishanth M       | PES2UG19CS264 | D Section |
| 3. | Mohammed Nabeel  | PES2UG19CS237 | D Section |

## Table of Contents :

1. Extraction of image files in linux
2. Extraction of image files in windows

### File used here :

Image files .img extension having NTFS , ext3 , FAT32 File systems

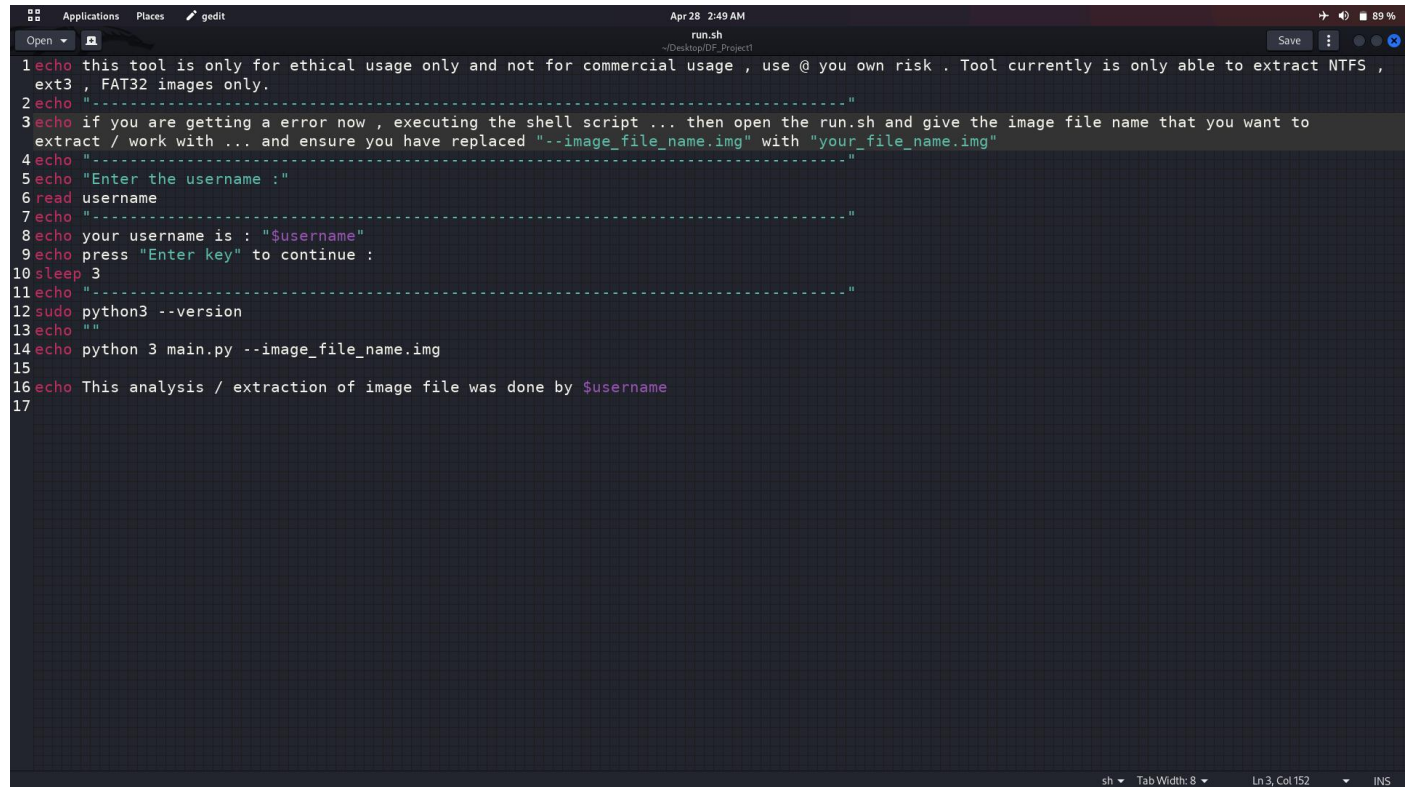
### Tool used :

7-zip for windows extraction

Ewf tools for linux

# On Linux :

## run.sh

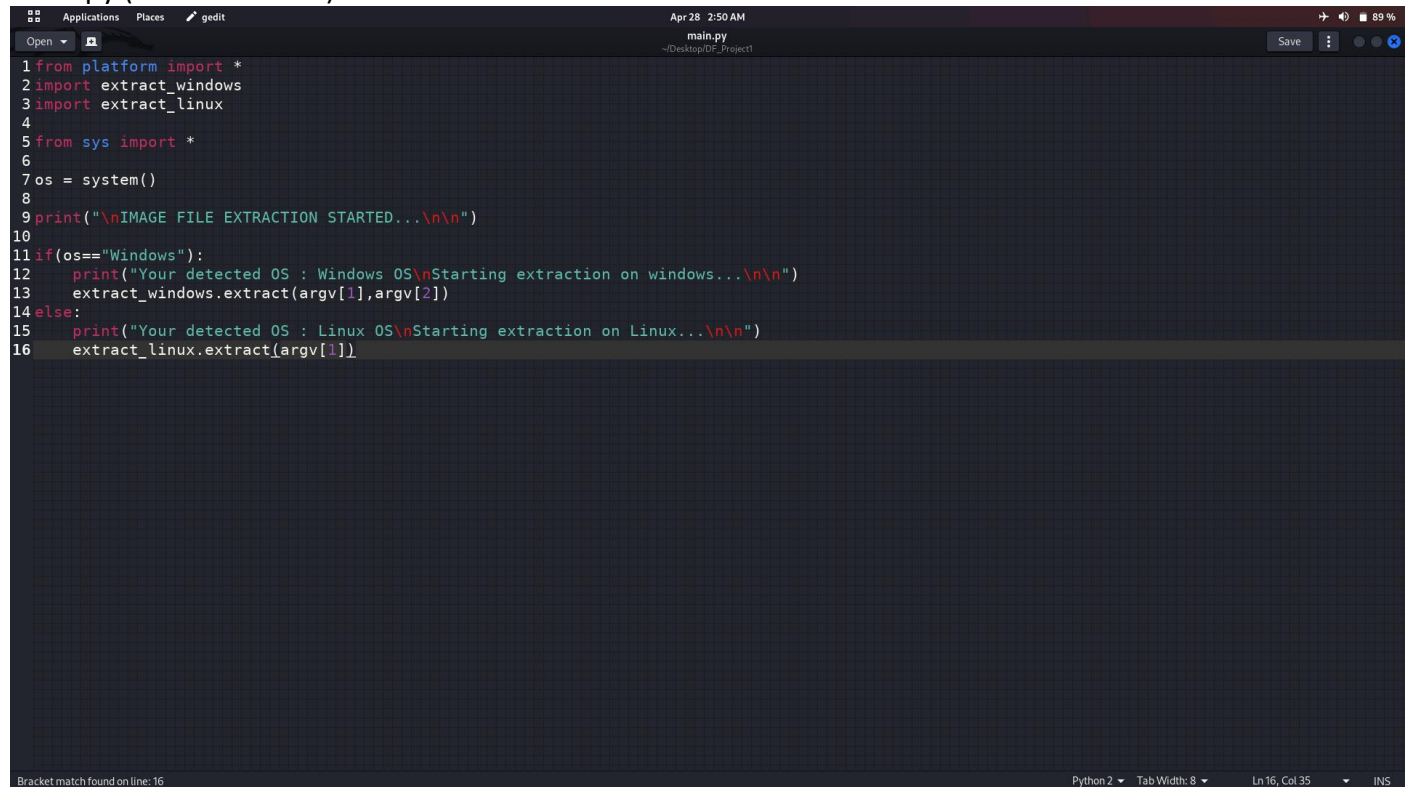


The screenshot shows a terminal window titled 'run.sh' with a dark background and light-colored text. The script contains the following lines:

```
1 echo this tool is only for ethical usage only and not for commercial usage , use @ you own risk . Tool currently is only able to extract NTFS ,
  ext3 , FAT32 images only.
2 echo "-----"
3 echo if you are getting a error now , executing the shell script ... then open the run.sh and give the image file name that you want to
  extract / work with ... and ensure you have replaced "--image_file_name.img" with "your_file_name.img"
4 echo "-----"
5 echo "Enter the username :"
6 read username
7 echo "-----"
8 echo your username is : "$username"
9 echo press "Enter key" to continue :
10 sleep 3
11 echo "-----"
12 sudo python3 --version
13 echo ""
14 echo python 3 main.py --image_file_name.img
15
16 echo This analysis / extraction of image file was done by $username
17
```

The terminal window includes a menu bar with 'Applications', 'Places', and 'gedit'. The status bar at the bottom shows 'sh', 'Tab Width: 8', 'Ln 3, Col 152', and 'INS'.

## Main.py (driver function)

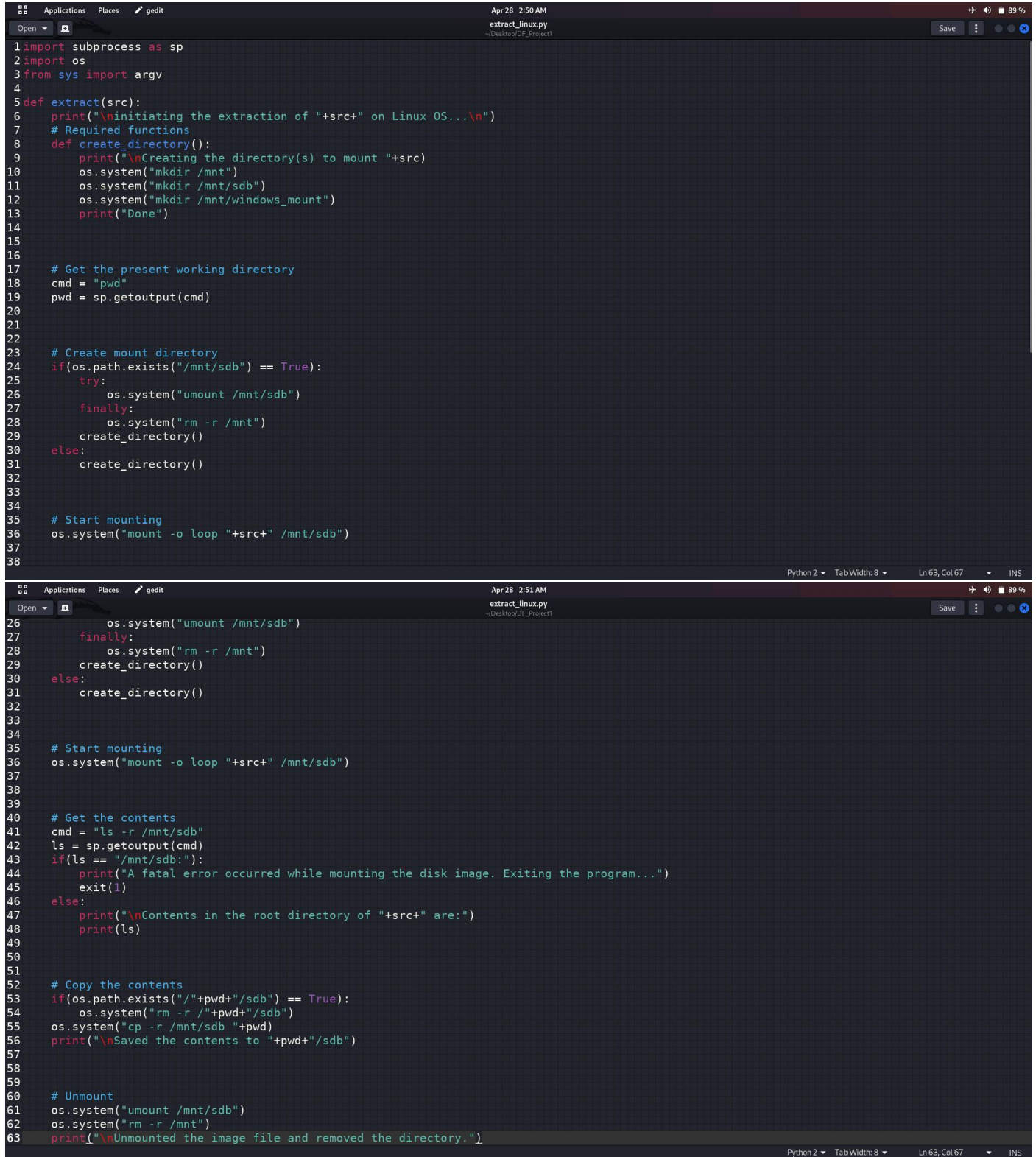


The screenshot shows a terminal window titled 'main.py' with a dark background and light-colored text. The script contains the following lines:

```
1 from platform import *
2 import extract_windows
3 import extract_linux
4
5 from sys import *
6
7 os = system()
8
9 print("\nIMAGE FILE EXTRACTION STARTED...\n\n")
10
11 if(os=="Windows"):
12     print("Your detected OS : Windows OS\nStarting extraction on windows...\n\n")
13     extract_windows.extract(argv[1],argv[2])
14 else:
15     print("Your detected OS : Linux OS\nStarting extraction on Linux...\n\n")
16     extract_linux.extract(argv[1])
```

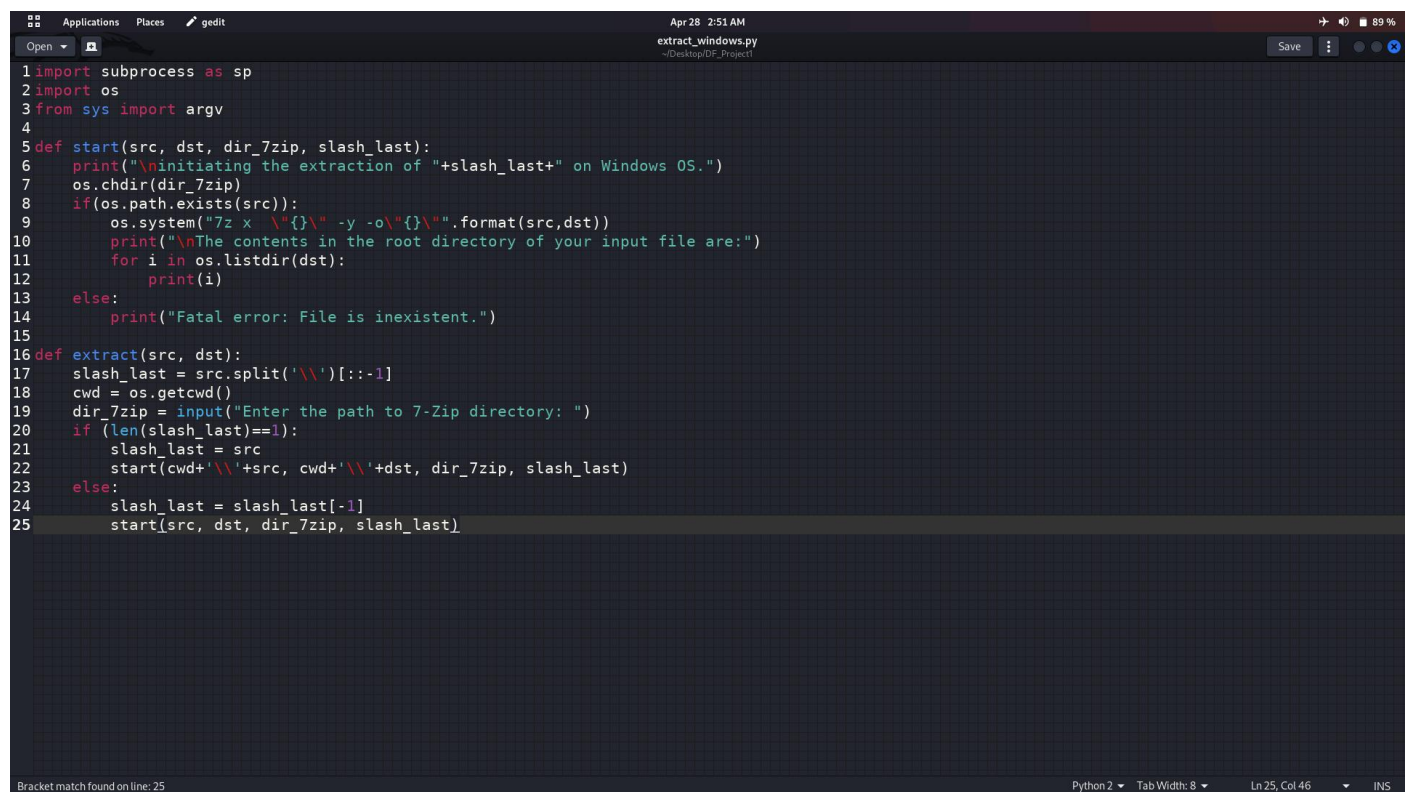
The terminal window includes a menu bar with 'Applications', 'Places', and 'gedit'. The status bar at the bottom shows 'Python 2', 'Tab Width: 8', 'Ln 16, Col 35', and 'INS'. A message 'Bracket match found on line: 16' is visible in the bottom left corner.

## Linux File Extractor



```
1 import subprocess as sp
2 import os
3 from sys import argv
4
5 def extract(src):
6     print("\ninitiating the extraction of "+src+" on Linux OS...\n")
7     # Required functions
8     def create_directory():
9         print("\nCreating the directory(s) to mount "+src)
10        os.system("mkdir /mnt")
11        os.system("mkdir /mnt/sdb")
12        os.system("mkdir /mnt/windows_mount")
13        print("Done")
14
15
16
17 # Get the present working directory
18 cmd = "pwd"
19 pwd = sp.getoutput(cmd)
20
21
22
23 # Create mount directory
24 if(os.path.exists("/mnt/sdb") == True):
25     try:
26         os.system("umount /mnt/sdb")
27     finally:
28         os.system("rm -r /mnt")
29     create_directory()
30 else:
31     create_directory()
32
33
34
35 # Start mounting
36 os.system("mount -o loop "+src+" /mnt/sdb")
37
38
39
40 # Get the contents
41 cmd = "ls -r /mnt/sdb"
42 ls = sp.getoutput(cmd)
43 if(ls == "/mnt/sdb:"):
44     print("A fatal error occurred while mounting the disk image. Exiting the program...")
45     exit(1)
46 else:
47     print("\nContents in the root directory of "+src+" are:")
48     print(ls)
49
50
51
52 # Copy the contents
53 if(os.path.exists("/"+pwd+"/sdb") == True):
54     os.system("rm -r /"+pwd+"/sdb")
55     os.system("cp -r /mnt/sdb "+pwd)
56     print("\nSaved the contents to "+pwd+"/sdb")
57
58
59
60 # Unmount
61 os.system("umount /mnt/sdb")
62 os.system("rm -r /mnt")
63 print("\nUnmounted the image file and removed the directory.")
```

## Windows File Extractor



The image shows a code editor window titled "extract\_windows.py" with a dark theme. The script is a Python program designed to extract files from a 7-Zip archive. It includes imports for subprocess, os, and sys.argv. The main logic is contained within two functions: 'start' and 'extract'. The 'start' function handles the initial setup, including path validation and directory creation. The 'extract' function manages the extraction process, including user input for the 7-Zip directory and the extraction command. The script is currently at line 25, column 46.

```
1 import subprocess as sp
2 import os
3 from sys import argv
4
5 def start(src, dst, dir_7zip, slash_last):
6     print("\ninitiating the extraction of "+slash_last+" on Windows OS.")
7     os.chdir(dir_7zip)
8     if os.path.exists(src):
9         os.system("7z x \"%{}\" -y -o\"{}\".format(src,dst))
10        print("\nThe contents in the root directory of your input file are:")
11        for i in os.listdir(dst):
12            print(i)
13    else:
14        print("Fatal error: File is inexistent.")
15
16 def extract(src, dst):
17     slash_last = src.split('\\')[:-1]
18     cwd = os.getcwd()
19     dir_7zip = input("Enter the path to 7-Zip directory: ")
20     if (len(slash_last)==1):
21         slash_last = src
22         start(cwd+'\\'+src, cwd+'\\'+dst, dir_7zip, slash_last)
23     else:
24         slash_last = slash_last[-1]
25     start(src, dst, dir_7zip, slash_last)
```

Bracket match found on line: 25

Python 2 ▾ Tab Width: 8 ▾ Ln 25, Col 46 ▾ IHS



## FAT32.img Extraction

```
Applications Places gedit Apr 28 3:55 AM
Open run.sh ~/Desktop Save
1 echo this tool is only for ethical usage only and not for commercial usage , use @ you own risk . Tool currently is only able to extract NTFS ,
  ext3 , FAT32 images only.
2 echo "-----"
3 echo if you are getting a error now , executing the shell script ... then open the run.sh and give the image file name that you want to
  extract / work with ... and ensure you have replaced "--image_file_name.img" with "your_file_name.img"
4 echo "-----"
5 echo "Enter the username : "
6 read username
7 echo "-----"
8 echo your username is : "$username"
9 echo press "Enter key" to continue :
10 sleep 3
11 echo "-----"
12 sudo python3 --version
13 echo ""
14 sudo python3 main.py FAT32.img
15
16 echo This analysis / extraction of image file was done by $username
17
```

```
Applications Places Terminal Apr 28 3:54 AM
asdf@CS412-CS264-CS237: ~/DF asdf@CS412-CS264-CS237: ~/DF asdf@CS412-CS264-CS237: ~/DF
asdf@CS412-CS264-CS237:~/DF$ echo Analysis of FAT32.img
Analysis of FAT32.img
asdf@CS412-CS264-CS237:~/DF$ ./run.sh
this tool is only for ethical usage only and not for commercial usage , use @ you own risk . Tool currently is only able to extract NTFS , ext3 , FAT32 images only.
-----
Enter the username :
suhan_nishanth_nabeel
-----
your username is : suhan_nishanth_nabeel
press Enter key to continue :
-----
Python 3.9.12
IMAGE FILE EXTRACTION STARTED...
Your detected OS : Linux OS --- Starting extraction on Linux...

initiating the extraction of FAT32.img on Linux OS...

Creating the directory(s) to mount FAT32.img
Done

Contents in the root directory of FAT32.img are:
System Volume Information
sample6.bmp
sample5.jpg
sample2.jpeg
ext file system details.pdf
ext2_fs.h
DF_Process.jpg
Data Sources Autopsy.docx
All Scanners.txt
All MS Events.txt
a.exe

Saved the contents to /home/asdf/DF/sdb

Unmounted the image file and removed the directory.
This analysis / extraction of image file was done by suhan_nishanth_nabeel
asdf@CS412-CS264-CS237:~/DF$
```

## NTFS.img Extraction

```
Applications  Places  gedit
Apr 28 3:55 AM
*run.sh
~/Desktop
Save

1 echo this tool is only for ethical usage only and not for commercial usage , use @ you own risk . Tool currently is only able to extract NTFS ,
2 echo "-----"
3 echo if you are getting a error now , executing the shell script ... then open the run.sh and give the image file name that you want to
4 echo "-----"
5 echo "Enter the username : "
6 read username
7 echo "-----"
8 echo your username is : "$username"
9 echo press "Enter key" to continue :
10 sleep 3
11 echo "-----"
12 sudo python3 --version
13 echo ""
14 sudo python3 main.py NTFS.img
15
16 echo This analysis / extraction of image file was done by $username
17

sh  Tab Width: 8  Ln 17, Col 1  INS
```

```
Applications  Places  Terminal
Apr 28 3:51 AM
asdf@CS412-CS264-CS237: ~/DF
asdf@CS412-CS264-CS237:~/DF$ echo Analysis of NTFS.img
Analysis of NTFS.img
asdf@CS412-CS264-CS237:~/DF$ ./run.sh
this tool is only for ethical usage only and not for commercial usage , use @ you own risk . Tool currently is only able to extract NTFS , ext3 , FAT32 images only.
-----
if you are getting a error now , executing the shell script ... then open the run.sh and give the image file name that you want to extract / work with ... and ensure you hav
e replaced --image_file_name.img with your_file_name.img
-----
Enter the username :
suhan_nishanth_nabeel
-----
your username is : suhan_nishanth_nabeel
press Enter key to continue :
-----
Python 3.9.12

IMAGE FILE EXTRACTION STARTED...
Your detected OS : Linux OS --- Starting extraction on Linux...

initiating the extraction of NTFS.img on Linux OS...

Creating the directory(s) to mount NTFS.img
Done

Contents in the root directory of NTFS.img are:
sample6.bmp
sample5.jpg
sample2.jpeg
ext file system details.pdf
ext2_fs.h
DF Process.jpg
DF.jpg
Data Sources Autopsy.docx
All Scanners.txt
All MS Events.txt
a.exe

Saved the contents to /home/asdf/DF/sdb

Unmounted the image file and removed the directory.
This analysis / extraction of image file was done by suhan_nishanth_nabeel
:~/DF$
```

## Ext3.img Extraction

```
Applications  Places  gedit
Apr 28 3:55 AM
*run.sh
~/Desktop
Save
1 echo this tool is only for ethical usage only and not for commercial usage , use @ you own risk . Tool currently is only able to extract NTFS ,
2 echo , FAT32 images only.
3 echo -----"
4 echo if you are getting a error now , executing the shell script ... then open the run.sh and give the image file name that you want to
5 echo extract / work with ... and ensure you have replaced "--image_file_name.img" with "your_file_name.img"
6 echo -----"
7 echo "Enter the username : "
8 read username
9 echo -----"
10 echo your username is : "$username"
11 echo press "Enter key" to continue :
12 sleep 3
13 echo -----"
14 sudo python3 --version
15 echo "
16 sudo python3 main.py ext3.img
17
18 echo This analysis / extraction of image file was done by $username
19
```

```
Applications  Places  Terminal
Apr 28 3:53 AM
asdf@CS412-CS264-CS237: ~/DF
asdf@CS412-CS264-CS237: ~/DF
asdf@CS412-CS264-CS237: ~/DF
asdf@CS412-CS264-CS237: ~/DF
asdf@CS412-CS264-CS237: ~/DF$ echo Analysis of ext3.img
Analysis of ext3.img
asdf@CS412-CS264-CS237:~/DF$ ./run.sh
this tool is only for ethical usage only and not for commercial usage , use @ you own risk . Tool currently is only able to extract NTFS , ext3 , FAT32 images only.
-----"
if you are getting a error now , executing the shell script ... then open the run.sh and give the image file name that you want to extract / work with ... and ensure you have replaced --image_file_name.img with your_file_name.img
-----"
Enter the username :
suhan_nishanth_nabeel
-----"
your username is : suhan_nishanth_nabeel
press Enter key to continue :
Python 3.9.12
IMAGE FILE EXTRACTION STARTED...
Your detected OS : Linux OS --- Starting extraction on Linux...

initiating the extraction of ext3.img on Linux OS...

Creating the directory(s) to mount ext3.img
Done

Contents in the root directory of ext3.img are:
sample6 (copy).bmp
sample6.bmp
sample5.jpg
sample5 (copy).jpg
sample2.jpeg
sample2 (copy).jpeg
lost-found
ext file system details.pdf
ext file system details (copy).pdf
ext2_fs.h
ext2_fs (copy).h
DF Process.jpg
DF Process (copy).jpg
DF.jpg
DF (copy).jpg
Data Sources Autopsy.docx
Data Sources Autopsy (copy).docx
All_Scanners.txt
All_Scanners (copy).txt
All MS Events.txt
All MS Events (copy).txt
a.exe
a (copy).exe

Saved the contents to /home/asdf/DF/sdb

Unmounted the image file and removed the directory.
This analysis / extraction of image file was done by suhan_nishanth_nabeel
asdf@CS412-CS264-CS237:~/DF$
```



## On Windows:

### Ext3.img extraction

```
Select C:\Windows\System32\cmd.exe

C:\Users\Pragati\Desktop\DF_Project>python main.py "C:\Users\Pragati\Desktop\DF_Project\image_files\ext3.img" "C:\Users\Pragati\Desktop\DF_Project\dest_exec"
IMAGE FILE EXTRACTION STARTED...
Your detected OS : Windows OS --- Starting extraction on windows...

Enter the path to 7-Zip directory: C:\Program Files\7-Zip
Initiating the extraction of C: on Windows OS.

7-Zip 21.07 (x64) : Copyright (c) 1999-2021 Igor Pavlov : 2021-12-26

Scanning the drive for archives:
1 file, 1024458752 bytes (977 MiB)

Extracting archive: C:\Users\Pragati\Desktop\DF_Project\image_files\ext3.img
Path = C:\Users\Pragati\Desktop\DF_Project\image_files\ext3.img
Type = Ext
Physical Size = 1024458752
Cluster Size = 4096
Free Space = 808635136
Modified = 2022-04-25 12:34:51
Created = 2022-04-11 19:25:10
Mount Time = 2022-04-25 12:34:50
Last Check Time = 2022-04-11 19:25:10
Host OS = Linux
Revision = 1
Inode Size = 256
Code Page = UTF-8
Last Mounted = /mnt/sdb
ID = AF8887201014E1690C80A6F83FF00
Characteristics = HAS_JOURNAL_EXT_ATTR_RESIZE_INODE_DIR_INDEX
Incompatible features = FILETYPE
Readonly-compatible Features = SPARSE_SUPER_LARGE_FILE
Written KIB = 480

Everything is Ok

Folders: 2
Files: 23
Size: 10291078
Compressed: 1024458752

The contents in the root directory of your input file are:
a (copy).exe
a.exe
All MS Events (copy).txt
All MS Events.txt
All Scanners (copy).txt
All Scanners.txt
Data Sources Autopsy (copy).docx
Data Sources Autopsy.docx
DF (copy).jpg
DF Process (copy).jpg
DF Process.jpg
DF.jpg
ext file system details (copy).pdf
ext file system details.pdf
ext2_fs (copy).h
ext2_fs.h
lost+found
sample2 (copy).jpeg
sample2.jpeg
sample5 (copy).jpg
sample5.jpg
sample6 (copy).bmp
sample6.bmp
[SYS]
```

### NTFS.img extraction

```
Select C:\Windows\System32\cmd.exe

C:\Users\Pragati\Desktop\DF_Project>python main.py "C:\Users\Pragati\Desktop\DF_Project\image_files\NTFS.img" "C:\Users\Pragati\Desktop\DF_Project\dest_exec"
IMAGE FILE EXTRACTION STARTED...
Your detected OS : Windows OS --- Starting extraction on windows...

Enter the path to 7-Zip directory: C:\Program Files\7-Zip
Initiating the extraction of C: on Windows OS.

7-Zip 21.07 (x64) : Copyright (c) 1999-2021 Igor Pavlov : 2021-12-26

Scanning the drive for archives:
1 file, 1024458752 bytes (977 MiB)

Extracting archive: C:\Users\Pragati\Desktop\DF_Project\image_files\NTFS.img
Path = C:\Users\Pragati\Desktop\DF_Project\image_files\NTFS.img
Type = NTFS
Physical Size = 1024458752
Label = NTFS
File System = NTFS 3.1
Cluster Size = 4096
Sector Size = 512
Record Size = 1024
Created = 2022-04-11 18:51:48
ID = 4639062961271504109

Everything is Ok

Folders: 3
Files: 24
Alternate Streams: 4
Alternate Streams Size: 262682
Size: 6130915
Compressed: 1024458752

The contents in the root directory of your input file are:
a (copy).exe
a.exe
All MS Events (copy).txt
All MS Events.txt
All Scanners (copy).txt
All Scanners.txt
Data Sources Autopsy (copy).docx
Data Sources Autopsy.docx
DF (copy).jpg
DF Process (copy).jpg
DF Process.jpg
DF.jpg
ext file system details (copy).pdf
ext file system details.pdf
ext2_fs (copy).h
ext2_fs.h
lost+found
sample2 (copy).jpeg
sample2.jpeg
sample5 (copy).jpg
sample5.jpg
sample6 (copy).bmp
```

# FAT32.img Extarction

```

C:\Users\Pragati\Desktop\System32\cmd.exe
C:\Users\Pragati\Desktop\DF_Project>python main.py "C:\Users\Pragati\Desktop\DF_Project\image_files\FAT32.img" "C:\Users\Pragati\Desktop\DF_Project\dest_exec"
IMAGE FILE EXTRACTION STARTED...
Your detected OS : Windows OS --- Starting extraction on windows...

Enter the path to 7-Zip directory: C:\Program Files\7-Zip

Initiating the extraction of C: on Windows OS.

7-Zip 21.07 (x64) : Copyright (c) 1999-2021 Igor Pavlov : 2021-12-26

Scanning the drive for archives:
1 file, 1024458752 bytes (977 MiB)

Extracting archive: C:\Users\Pragati\Desktop\DF_Project\image_files\FAT32.img
--
Path = C:\Users\Pragati\Desktop\DF_Project\image_files\FAT32.img
Type = FAT
Physical Size = 1024458752
File System = FAT32
Cluster Size = 4096
Free Space = 1019465728
Headers Size = 4202496
Modified = 2022-04-11 18:43:08
Label = IMAGES
Sector Size = 512
ID = 1222814864

Everything is Ok

Folders: 1
Files: 13
Size: 757019
Compressed: 1024458752

The contents in the root directory of your input file are:
a (copy).exe
a.exe
All MS Events (copy).txt
All MS Events.txt
All Scanners (copy).txt
All Scanners.txt
Data Sources Autopsy (copy).docx
Data Sources Autopsy.docx
DF (copy).jpg
DF Process (copy).jpg
DF Process.jpg
DF.jpg
ext file system details (copy).pdf
ext file system details.pdf
ext2_fs (copy).h
ext2_fs.h
lost-found
sample2 (copy).jpeg
sample2.jpeg
sample5 (copy).jpg
sample5.jpg
sample6 (copy).bmp
sample6.bmp

```

\*\*\*\*\*