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 :

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

run.sh ~/Desktop/DF_Project1

```
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.
echo "-------------------------------------------------------------------------------"
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"
echo "-------------------------------------------------------------------------------"
echo "Enter the username :"
read username
echo "-------------------------------------------------------------------------------"
echo your username is : "$username"
echo press "Enter key" to continue :
sleep 3
echo "-------------------------------------------------------------------------------"
sudo python3 --version
echo ""
echo python 3 main.py --image_file_name.img

echo This analysis / extraction of image file was done by $username

```

Main.py (driver function)

main.py ~/Desktop/DF_Project1

```
from platform import *
import extract_windows
import extract_linux

from sys import *

os = system()

print("\nIMAGE FILE EXTRACTION STARTED...\n\n")

if(os=="Windows"):
    print("Your detected OS : Windows OS\nStarting extraction on windows...\n\n")
    extract_windows.extract(argv[1],argv[2])
else:
    print("Your detected OS : Linux OS\nStarting extraction on Linux...\n\n")
    extract_linux.extract(argv[1])
```

Linux File Extractor

Applications Places gedit Apr 28 2:50 AM 89 %

Open extract_linux.py ~/Desktop/DF_Project1 Save

```python
import subprocess as sp
import os
from sys import argv

def extract(src):
    print("\ninitiating the extraction of "+src+" on Linux OS...\n")
    # Required functions
    def create_directory():
        print("\nCreating the directory(s) to mount "+src)
        os.system("mkdir /mnt")
        os.system("mkdir /mnt/sdb")
        os.system("mkdir /mnt/windows_mount")
        print("Done")



    # Get the present working directory
    cmd = "pwd"
    pwd = sp.getoutput(cmd)



    # Create mount directory
    if(os.path.exists("/mnt/sdb") == True):
        try:
            os.system("umount /mnt/sdb")
        finally:
            os.system("rm -r /mnt")
        create_directory()
    else:
        create_directory()



    # Start mounting
    os.system("mount -o loop "+src+" /mnt/sdb")


```

Python 2 Tab Width: 8 Ln 63, Col 67 INS

Applications Places gedit Apr 28 2:51 AM 89 %

Open extract_linux.py ~/Desktop/DF_Project1 Save

```python
            os.system("umount /mnt/sdb")
        finally:
            os.system("rm -r /mnt")
        create_directory()
    else:
        create_directory()



    # Start mounting
    os.system("mount -o loop "+src+" /mnt/sdb")



    # Get the contents
    cmd = "ls -r /mnt/sdb"
    ls = sp.getoutput(cmd)
    if(ls == "/mnt/sdb:"):
        print("A fatal error occurred while mounting the disk image. Exiting the program...")
        exit(1)
    else:
        print("\nContents in the root directory of "+src+" are:")
        print(ls)



    # Copy the contents
    if(os.path.exists("/"+pwd+"/sdb") == True):
        os.system("rm -r /"+pwd+"/sdb")
    os.system("cp -r /mnt/sdb "+pwd)
    print("\nSaved the contents to "+pwd+"/sdb")



    # Unmount
    os.system("umount /mnt/sdb")
    os.system("rm -r /mnt")
    print("\nUnmounted the image file and removed the directory.")
```

Python 2 Tab Width: 8 Ln 63, Col 67 INS

Windows File Extractor

Applications Places gedit Apr 28 2:51 AM 89 %

Open extract_windows.py ~/Desktop/DF_Project1 Save

```python
import subprocess as sp
import os
from sys import argv

def start(src, dst, dir_7zip, slash_last):
    print("\nInitiating the extraction of "+slash_last+" on Windows OS.")
    os.chdir(dir_7zip)
    if(os.path.exists(src)):
        os.system("7z x \"{}\" -y -o\"{}\"".format(src,dst))
        print("\nThe contents in the root directory of your input file are:")
        for i in os.listdir(dst):
            print(i)
    else:
        print("Fatal error: File is inexistent.")

def extract(src, dst):
    slash_last = src.split('\\')[::-1]
    cwd = os.getcwd()
    dir_7zip = input("Enter the path to 7-Zip directory: ")
    if (len(slash_last)==1):
        slash_last = src
        start(cwd+'\\'+src, cwd+'\\'+dst, dir_7zip, slash_last)
    else:
        slash_last = slash_last[-1]
        start(src, dst, dir_7zip, slash_last)
```

Bracket match found on line: 25 Python 2 Tab Width: 8 Ln 25, Col 46 INS

FAT32.img Extraction

```
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.
echo "-------------------------------------------------------------------------------"
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"
echo "-------------------------------------------------------------------------------"
echo "Enter the username :"
read username
echo "-------------------------------------------------------------------------------"
echo your username is : "$username"
echo press "Enter key" to continue :
sleep 3
echo "-------------------------------------------------------------------------------"
sudo python3 --version
echo ""
sudo python3 main.py FAT32.img

echo This analysis / extraction of image file was done by $username
```

```
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.
-------------------------------------------------------------------------------
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 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
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
asdf@CS412-CS264-CS237:~/DF$
```

NTFS.img Extraction

```
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.
echo "-------------------------------------------------------------------------------"
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"
echo "-------------------------------------------------------------------------------"
echo "Enter the username :"
read username
echo "-------------------------------------------------------------------------------"
echo your username is : "$username"
echo press "Enter key" to continue :
sleep 3
echo "-------------------------------------------------------------------------------"
sudo python3 --version
echo ""
sudo python3 main.py NTFS.img

echo This analysis / extraction of image file was done by $username

```

```
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
asdf@CS412-CS264-CS237:~/DF$
```

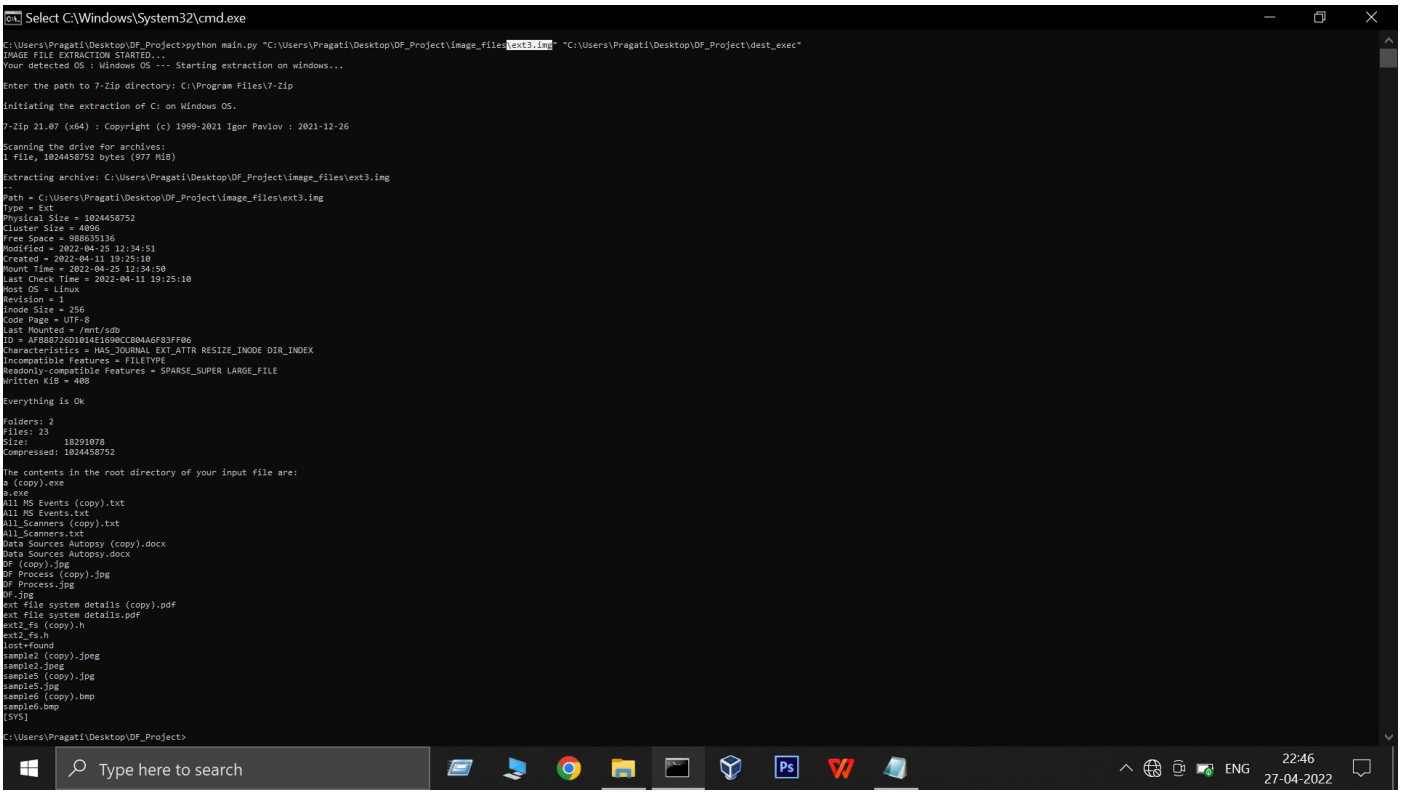
Ext3.img Extraction

```
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.
echo "-----------------------------------------------------------------------------"
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"
echo "-----------------------------------------------------------------------------"
echo "Enter the username :"
read username
echo "-----------------------------------------------------------------------------"
echo your username is : "$username"
echo press "Enter key" to continue :
sleep 3
echo "-----------------------------------------------------------------------------"
sudo python3 --version
echo ""
sudo python3 main.py ext3.img

echo This analysis / extraction of image file was done by $username

```

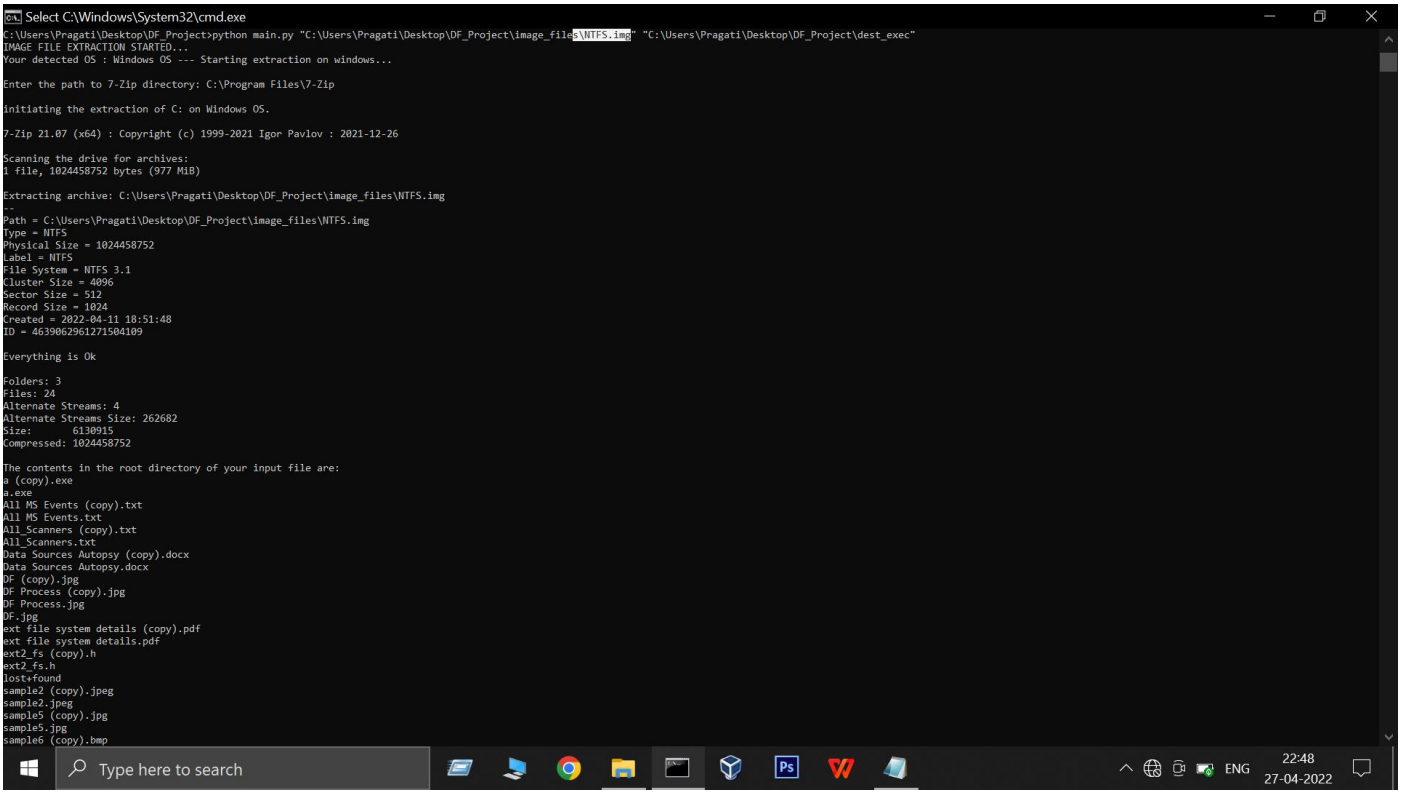
```
asdf@CS412-CS264-CS237:~/DF$ echo Analysis of ext3.img
Analysis of ext3.img
asdf@CS412-CS264-CS237:~/DF$ ./run.sh
this tool is only for ethical usage only and not for commercial usage , use @ you own risk . Tool currently is only able to extract NTFS , ext3 , FAT32 images only.
-----------------------------------------------------------------------------
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:

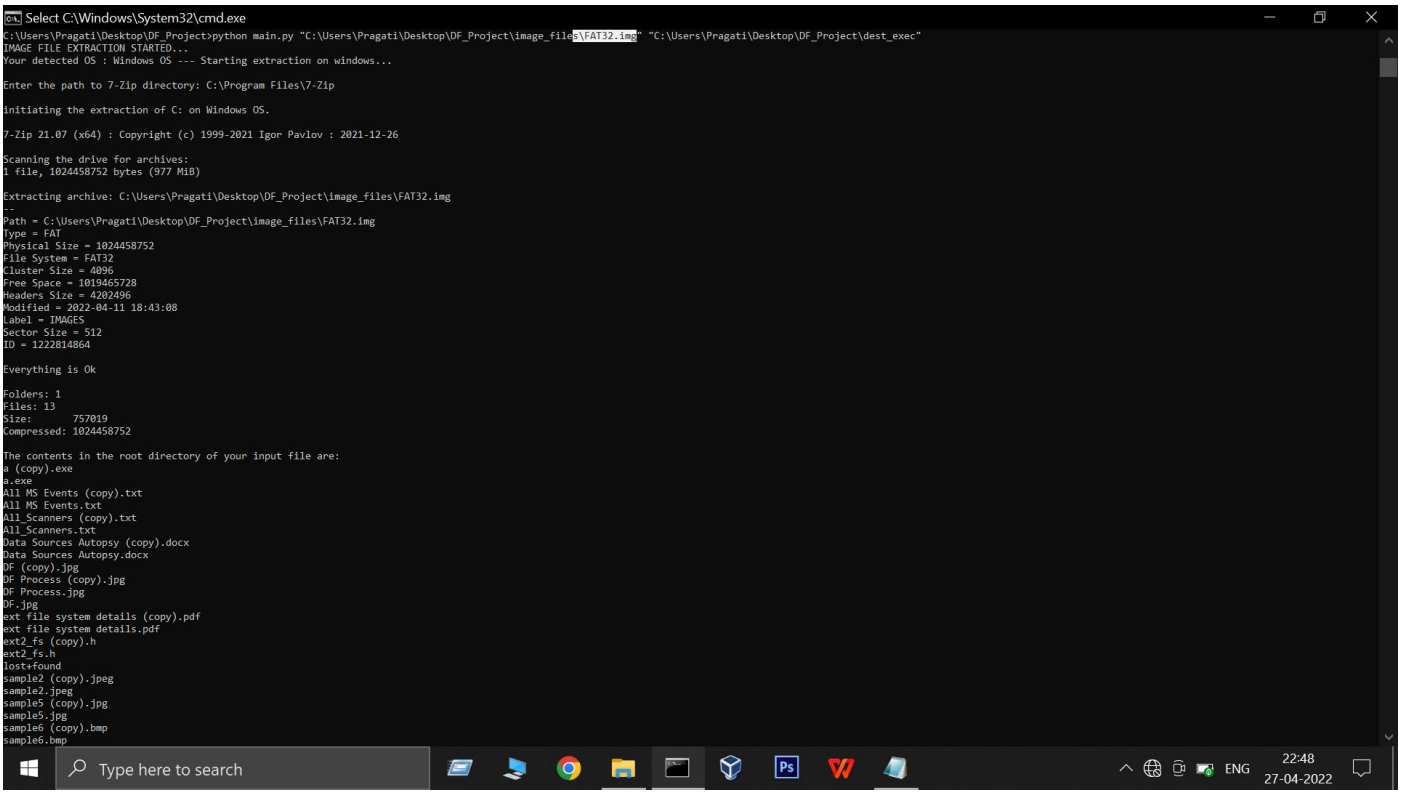
Ext3.img extraction



NTFS.img extraction



FAT32.img Extarction



*****