UNCOVERING THE DIGITAL TRIAL

A Project Report

Submitted in the partial fulfillment of the requirements for the award of the degree of

Bachelor of Technology in

Department of Computer Science and Engineering

By

2010030422 – Mani Teja Reddy

2010030436 – DIMPLE

2010030438 – SIRISHA

under the supervision of

Panduraju Pagidimalla

Department of Computer Science and Engineering

K L University Hyderabad,

Aziz Nagar, Moinabad Road, Hyderabad – 500 075, Telangana, India.

March, 2023

Declaration

The Project Report entitled "**UNCOVERING THE DIGITAL TRIAL**" is a record of bonafide work of Mr.ManiTeja Reddy(2010030422), Ms. Dimple(2010030436), Ms. Sirisha(2010030438)., submitted in partial fulfillment for the award of B.Tech in the Department of Computer Science and Engineering to the K L University, Hyderabad. The results embodied in this report have not been copied from any other Departments/University/Institute.

Signature of the Students

MANITEJA REDDY

DIMPLE

SIRISHA

Certificate

This is to certify that the Project Report entitled "**UNCOVERING THE DIGITAL TRIAL**" is being submitted by Mani Teja, Dimple, Sirisha submitted in partial fulfillment for the award of B.Tech in CSE to the K L University, Hyderabad is a record of bonafide work carried out under our guidance and supervision. The results embodied in this report have not been copied from any other departments/ University/Institute.

Signature of the Supervisor

Panduraju Pagidimalla
Assistant professor

Signature of the HOD

Signature of the External Examine

ACKNOWLEDGEMENTS

It is great pleasure for me to express my gratitude to our honorable President **Sri. Koneru Satyanarayana**, for giving the opportunity and platform with facilities in accomplishing the project based laboratory report.

I express the sincere gratitude to our Principal **Dr.A.RamaKrishna** for his administration towards our academic growth.

I express sincere gratitude to our Coordinator **Mr.Panduraju** for his leadership and constant motivation provided in successful completion of our academic semester. I record it as my privilege to deeply thank for providing us the efficient faculty and facilities to make our ideas into reality.

I express my sincere thanks to our project supervisor **Mr.Panduraju** for his/her novel association of ideas, encouragement, appreciation and intellectual zeal which motivated us to venture this project successfully.

Finally, it is pleased to acknowledge the indebtedness to all those who devoted themselves directly or indirectly to make this project report success.

INDEX

PROJECT ABSTRACT

An electronic crime scene has the potential to hold massive amounts of data obtained from media devices. The primary goal of a cyber forensics' investigator is to transform raw evidential data into useful data sets. Depending on the particular illegal activity, it is likely that a media device (i.e., Laptops, digital cameras, phones or hard drives) will vary in the size and amount of evidence. As an example, one criminal case may contain a small fraction of information or devices, another criminal case may contain a substantially larger amount of data and multiple devices.

The main goal of our project is to extract data from the electronic devices, process it and analyzing it.

INTRODUCTION

Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting on data stored electronically.

Electronic evidence is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations.

Electronic evidence can be collected from a wide array of sources, such as computers, smartphones, remote storage, unmanned aerial systems, shipborne equipment, and more.

LITERATURE SURVEY

Role of The Computers In Digital Forensics

- Darshan, University of Mysore 2020.
- skillfully detects cybercriminals at any place or any time in the entire world. Allows to the essence, process, and explains the effective evidence, so this provides the activities of cybercriminal in court.
- Most investigators have no proper technical knowledge in the investigating field. So, they are unable to submit the desired result of any cases.

Digital forensics investigation jurisprudence

- Yeboah-Ofor Journal of Forensic, Legal & Investigative Sciences.
- Digital Forensics investigations jurisprudence is the theory and philosophy of the study of law and the principles upon which a law is based.
- digital evidence to appear at court and be legally admissible, the evidence must be authentic, accurate, complete, and convincing to the jury. Presenting digital forensic evidence at court has proved to be challenging, due to factors such as inadequate chain of custody, not maintaining legal procedures and inadequate evidential integrity.

SYSTEM REQUIREMENTS

SOFTWARE REQUIREMENTS:

Language - Python

Operating system - Windows 10

Tools - Visual Studio Code , OS Forensic tool

HARDWARE REQUIREMENTS:

RAM - 8.00 GB (7.87 GB usable)

Processor - Intel(R) Core (TM) i5-10300H CPU @ 2.50GHz   2.50 GHz

System-type - 64-bit operating system, x64-based processor

Version - 20H2

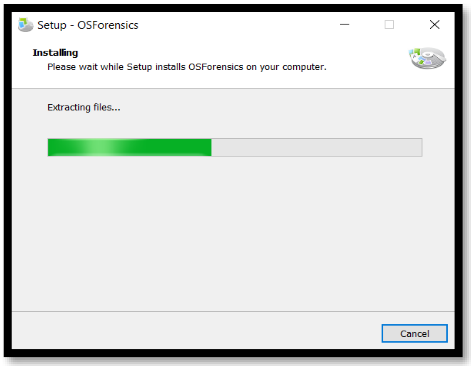
Edition - Windows 10 Home Single Language

METHODS

OS Forensics:

OS Forensics lets you extract forensics evidence fron computers quickly with high performance file searches and indexing, allows you to search for files many times faster than the search functionality in Windows

- Collecting data from computers.
- Manage your investigation
- Extract evidence from computers quickly
- Identify suspicious files and activity
- Group the files and find all the documents/images.

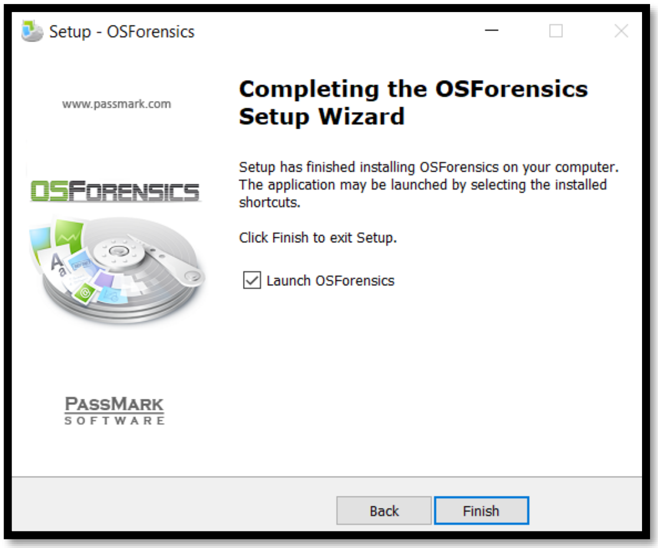


Setup - OSForensics

Installing

Please wait while Setup installs OSForensics on your computer.

Extracting files...



Setup - OSForensics

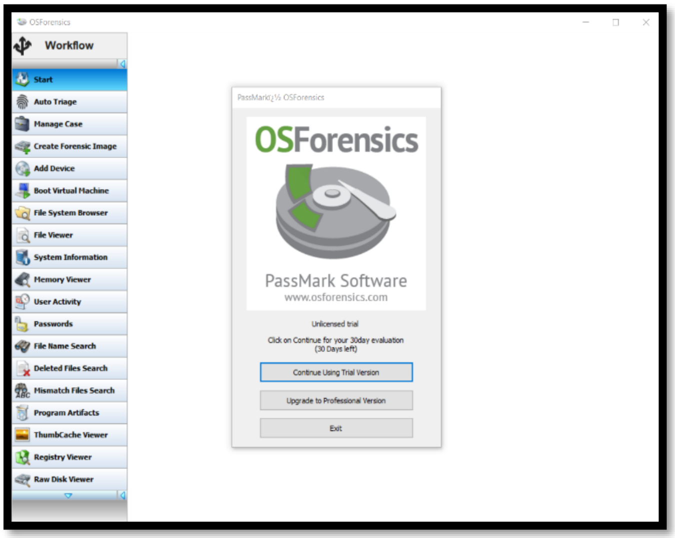
www.passmark.com

Completing the OSForensics Setup Wizard

Setup has finished installing OSForensics on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

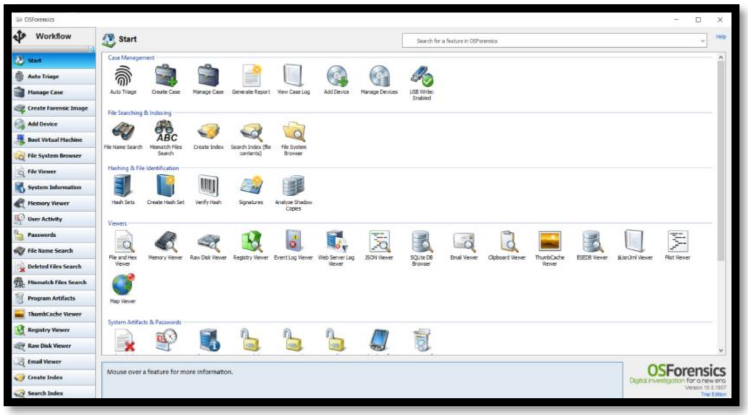
☑ Launch OSForensics



PassMark¿½ OSForensics

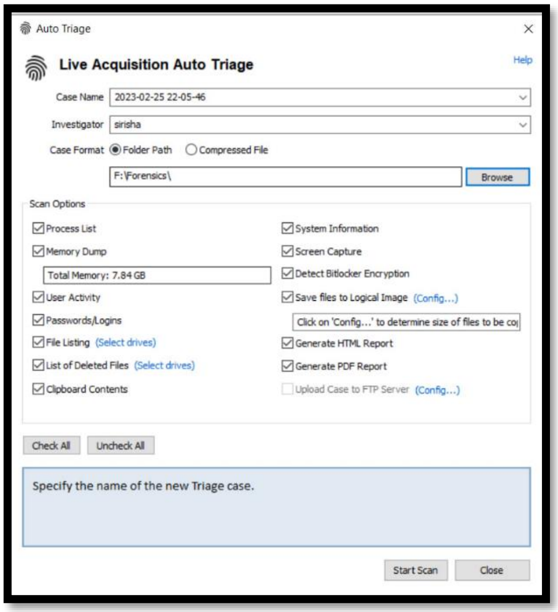
Unlicensed trial

Click on Continue for your 30day evaluation (30 Days left)



Mouse over a feature for more information.

Tools in digital forensics



Live Acquisition Auto Triage

Case Name: 2023-02-25 22-05-46

Investigator: sirisha

Case Format: ● Folder Path ○ Compressed File

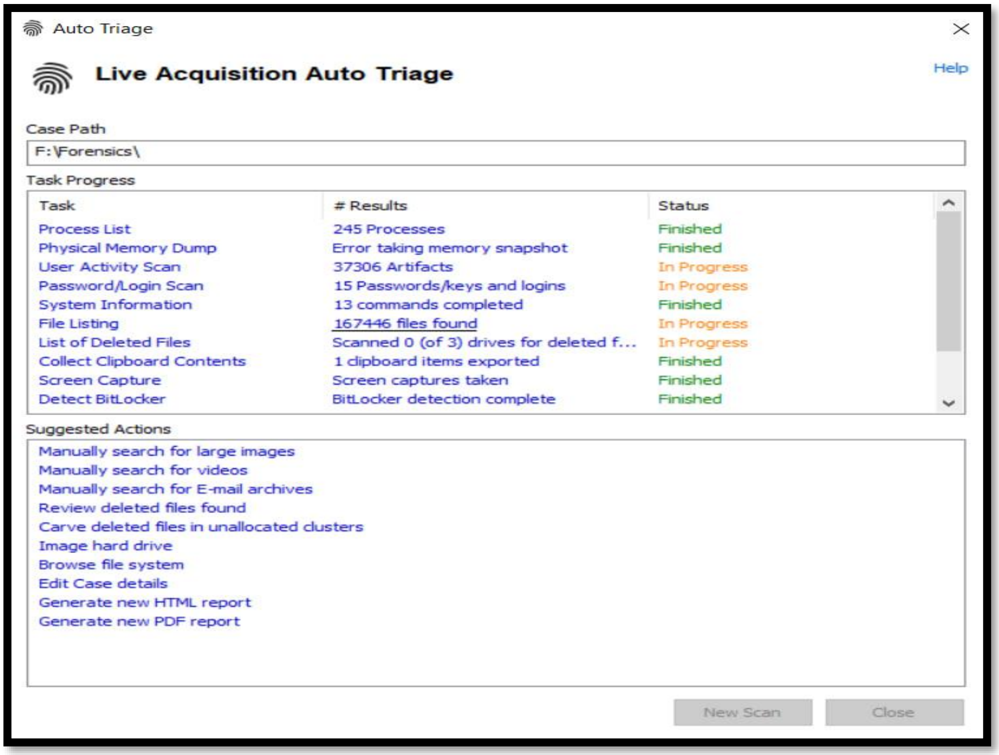
F:\Forensics\

Scan Options

☑ Process List
☑ Memory Dump
Total Memory: 7.84 GB
☑ User Activity
☑ Passwords/Logins
☑ File Listing (Select drives)
☑ List of Deleted Files (Select drives)
☑ Clipboard Contents
☑ System Information
☑ Screen Capture
☑ Detect Bitlocker Encryption
☑ Save files to Logical Image (Config...)
Click on 'Config...' to determine size of files to be co
☑ Generate HTML Report
☑ Generate PDF Report
□ Upload Case to FTP Server (Config...)

Specify the name of the new Triage case.

Auto Triage Tool



Live Acquisition Auto Triage

Case Path

F:\Forensics\

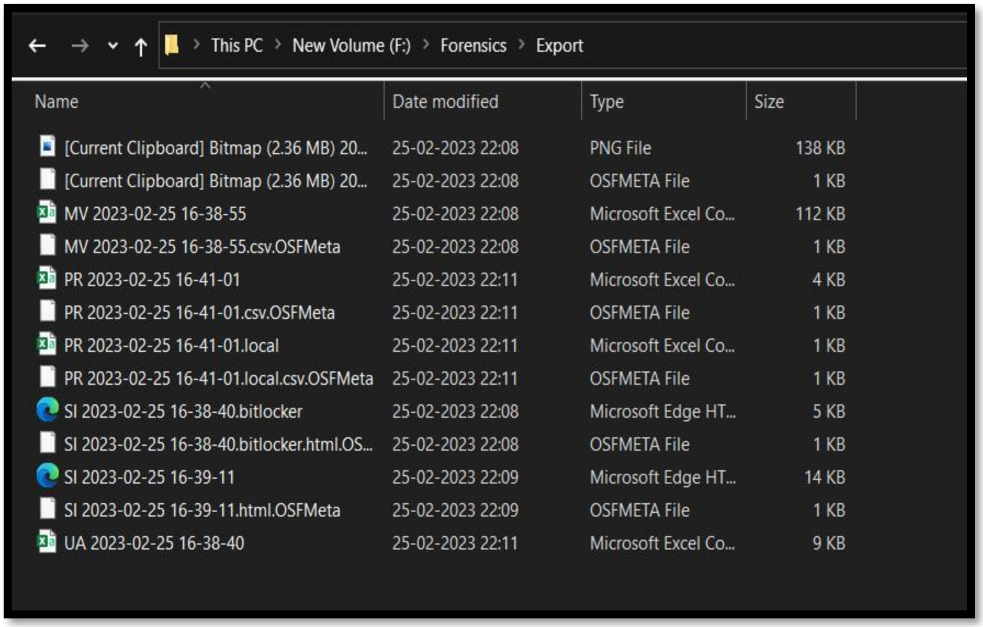
Task Progress

Task	# Results	Status
Process List	245 Processes	Finished
Physical Memory Dump	Error taking memory snapshot	Finished
User Activity Scan	37306 Artifacts	In Progress
Password/Login Scan	15 Passwords/keys and logins	In Progress
System Information	13 commands completed	Finished
File Listing	167446 files found	In Progress
List of Deleted Files	Scanned 0 (of 3) drives for deleted f...	In Progress
Collect Clipboard Contents	1 clipboard items exported	Finished
Screen Capture	Screen captures taken	Finished
Detect BitLocker	BitLocker detection complete	Finished

Suggested Actions

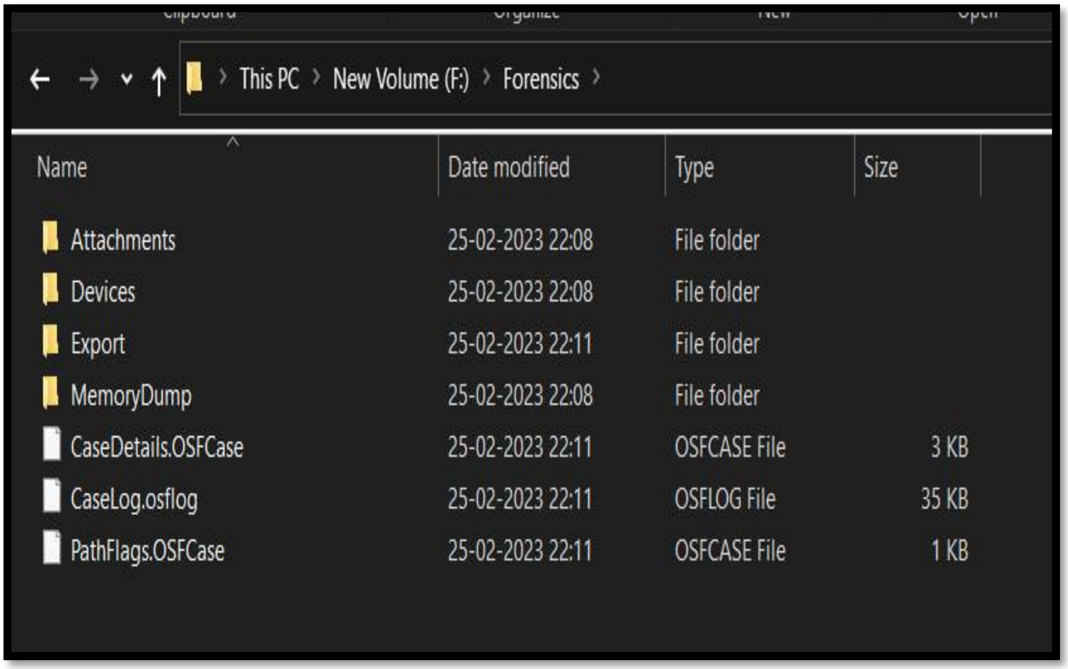
Manually search for large images
Manually search for videos
Manually search for E-mail archives
Review deleted files found
Carve deleted files in unallocated clusters
Image hard drive
Browse file system
Edit Case details
Generate new HTML report
Generate new PDF report

Data Form OS



This PC › New Volume (F:) › Forensics › Export

Name	Date modified	Type	Size
[Current Clipboard] Bitmap (2.36 MB) 20...	25-02-2023 22:08	PNG File	138 KB
[Current Clipboard] Bitmap (2.36 MB) 20...	25-02-2023 22:08	OSFMETA File	1 KB
MV 2023-02-25 16-38-55	25-02-2023 22:08	Microsoft Excel Co...	112 KB
MV 2023-02-25 16-38-55.csv.OSFMeta	25-02-2023 22:08	OSFMETA File	1 KB
PR 2023-02-25 16-41-01	25-02-2023 22:11	Microsoft Excel Co...	4 KB
PR 2023-02-25 16-41-01.csv.OSFMeta	25-02-2023 22:11	OSFMETA File	1 KB
PR 2023-02-25 16-41-01.local	25-02-2023 22:11	Microsoft Excel Co...	1 KB
PR 2023-02-25 16-41-01.local.csv.OSFMeta	25-02-2023 22:11	OSFMETA File	1 KB
SI 2023-02-25 16-38-40.bitlocker	25-02-2023 22:08	Microsoft Edge HT...	5 KB
SI 2023-02-25 16-38-40.bitlocker.html.OS...	25-02-2023 22:08	OSFMETA File	1 KB
SI 2023-02-25 16-39-11	25-02-2023 22:09	Microsoft Edge HT...	14 KB
SI 2023-02-25 16-39-11.html.OSFMeta	25-02-2023 22:09	OSFMETA File	1 KB
UA 2023-02-25 16-38-40	25-02-2023 22:11	Microsoft Excel Co...	9 KB



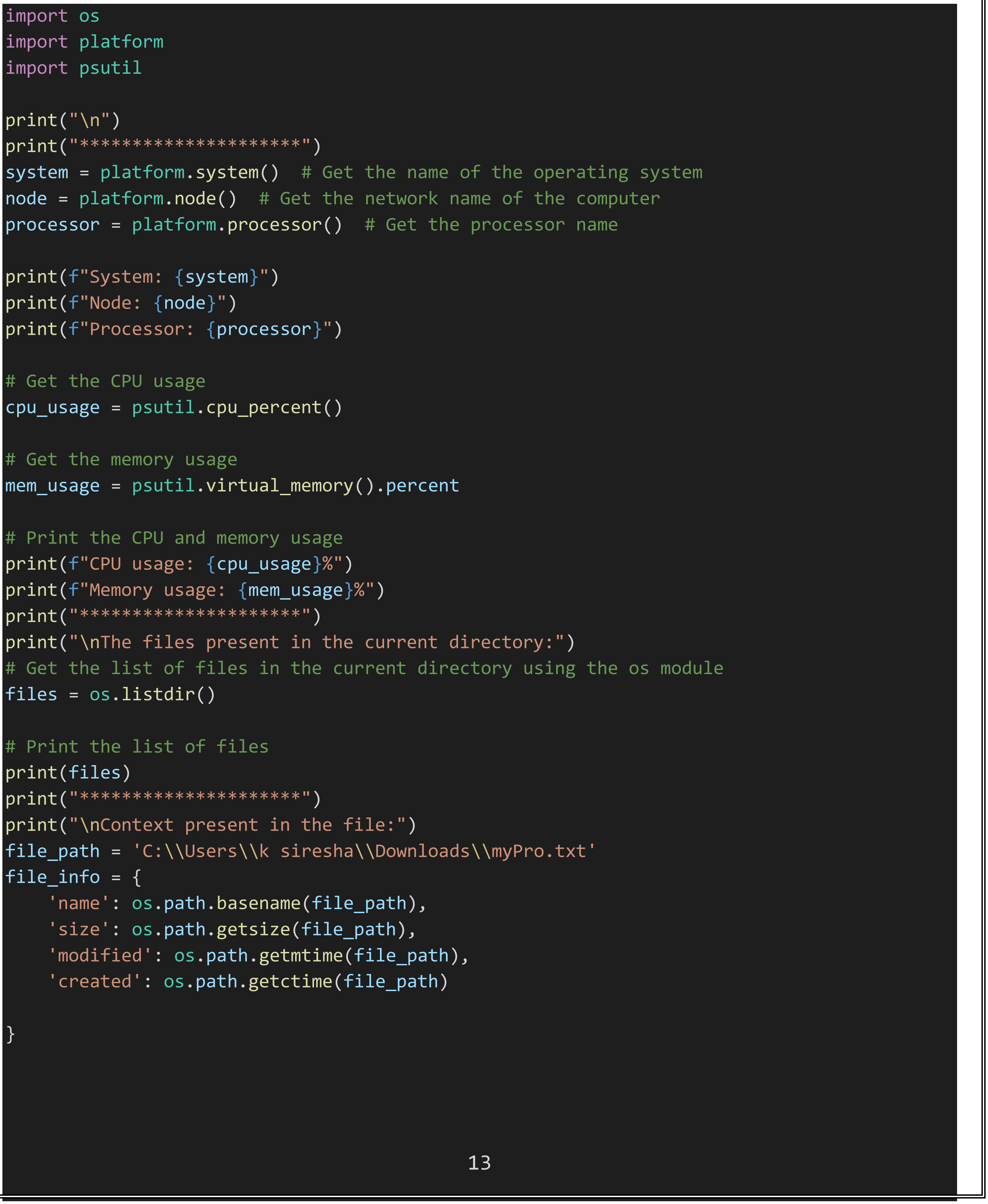
This PC › New Volume (F:) › Forensics ›

Name	Date modified	Type	Size
Attachments	25-02-2023 22:08	File folder	
Devices	25-02-2023 22:08	File folder	
Export	25-02-2023 22:11	File folder	
MemoryDump	25-02-2023 22:08	File folder	
CaseDetails.OSFCase	25-02-2023 22:11	OSFCASE File	3 KB
CaseLog.osflog	25-02-2023 22:11	OSFLOG File	35 KB
PathFlags.OSFCase	25-02-2023 22:11	OSFCASE File	1 KB

Data Analysis

IMPLEMENTATION

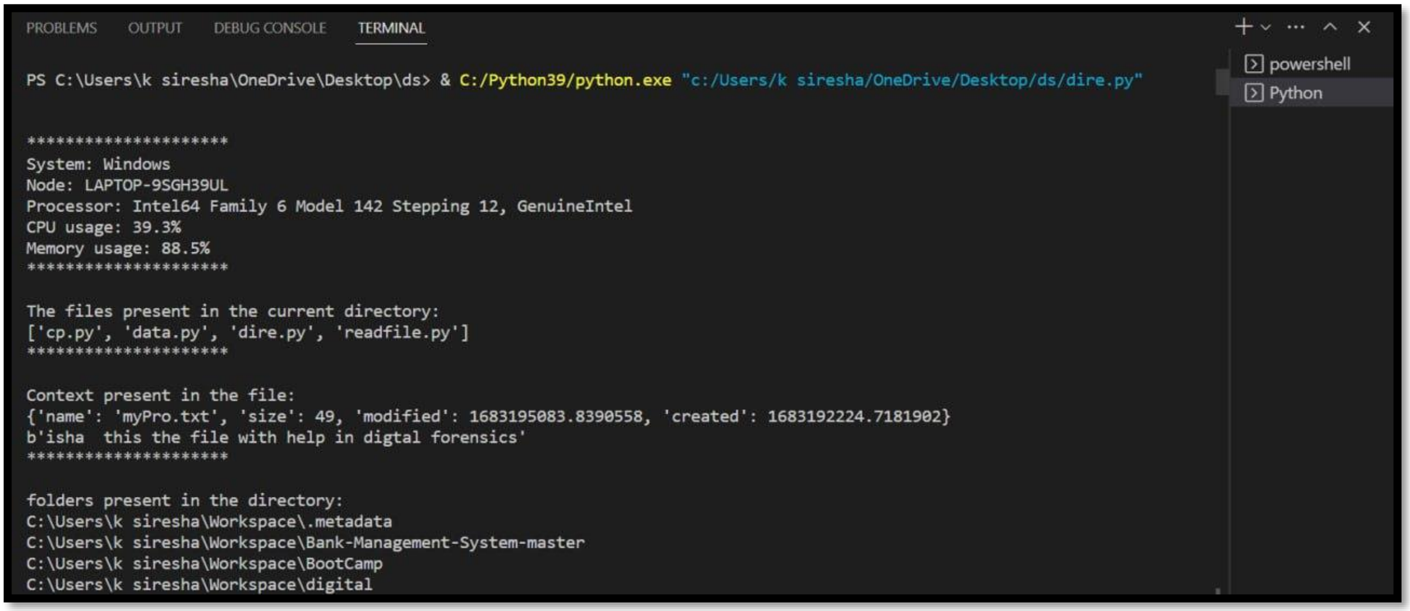
Code:



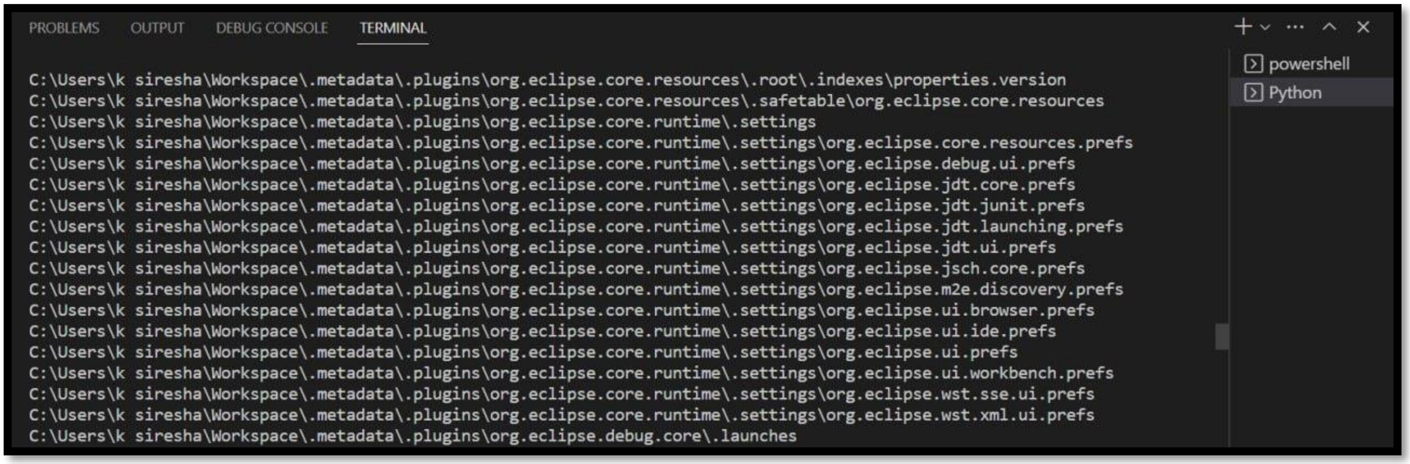
```
import os
import platform
import psutil

print("\n")
print("*********************")
system = platform.system()  # Get the name of the operating system
node = platform.node()  # Get the network name of the computer
processor = platform.processor()  # Get the processor name

print(f"System: {system}")
print(f"Node: {node}")
print(f"Processor: {processor}")

# Get the CPU usage
cpu_usage = psutil.cpu_percent()

# Get the memory usage
mem_usage = psutil.virtual_memory().percent

# Print the CPU and memory usage
print(f"CPU usage: {cpu_usage}%")
print(f"Memory usage: {mem_usage}%")
print("*********************")
print("\nThe files present in the current directory:")
# Get the list of files in the current directory using the os module
files = os.listdir()

# Print the list of files
print(files)
print("*********************")
print("\nContext present in the file:")
file_path = 'C:\\Users\\k siresha\\Downloads\\myPro.txt'
file_info = {
    'name': os.path.basename(file_path),
    'size': os.path.getsize(file_path),
    'modified': os.path.getmtime(file_path),
    'created': os.path.getctime(file_path)

}
```

```python
with open(file_path, "rb") as myPro:
    contents = myPro.read()
# Print the contents of the file
print(file_info)
print(contents)

print("*********************")
print("\nfolders present in the directory:")

# Define the path to the directory you want to scan
directory_path = "C:\\Users\\k siresha\\Workspace\\"

# Loop through all the files and directories in the given directory
for root, directories, files in os.walk(directory_path):
    for filename in files:
        # Print the name of each file
        print(os.path.join(root, filename))
    for directory in directories:
        # Print the name of each subdirectory
        print(os.path.join(root, directory))
```

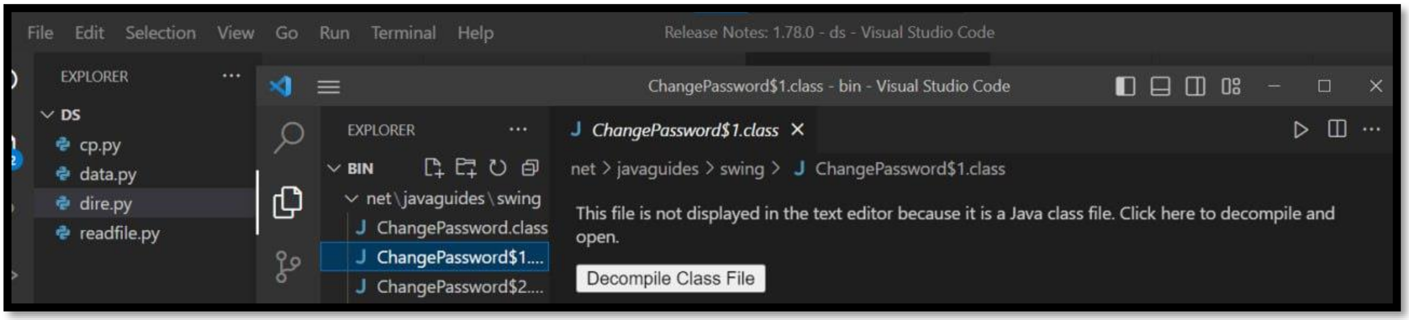
OUTPUT



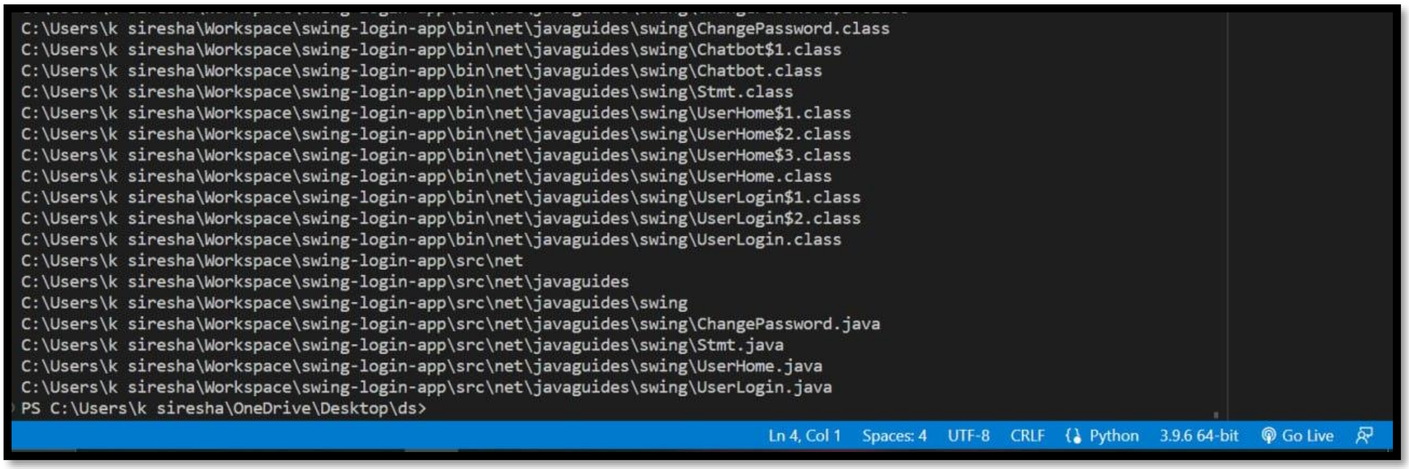
```
PS C:\Users\k siresha\OneDrive\Desktop\ds> & C:/Python39/python.exe "c:/Users/k siresha/OneDrive/Desktop/ds/dire.py"


*********************
System: Windows
Node: LAPTOP-9SGH39UL
Processor: Intel64 Family 6 Model 142 Stepping 12, GenuineIntel
CPU usage: 39.3%
Memory usage: 88.5%
*********************

The files present in the current directory:
['cp.py', 'data.py', 'dire.py', 'readfile.py']
*********************

Context present in the file:
{'name': 'myPro.txt', 'size': 49, 'modified': 1683195083.8390558, 'created': 1683192224.7181902}
b'isha  this the file with help in digtal forensics'
*********************

folders present in the directory:
C:\Users\k siresha\Workspace\.metadata
C:\Users\k siresha\Workspace\Bank-Management-System-master
C:\Users\k siresha\Workspace\BootCamp
C:\Users\k siresha\Workspace\digital
```



```
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.resources\.root\.indexes\properties.version
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.resources\.safetable\org.eclipse.core.resources
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.core.resources.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.debug.ui.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.jdt.core.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.jdt.junit.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.jdt.launching.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.jdt.ui.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.jsch.core.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.m2e.discovery.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.ui.browser.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.ui.ide.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.ui.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.ui.workbench.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.wst.sse.ui.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.core.runtime\.settings\org.eclipse.wst.xml.ui.prefs
C:\Users\k siresha\Workspace\.metadata\.plugins\org.eclipse.debug.core\.launches
```


File Edit Selection View Go Run Terminal Help
Release Notes: 1.78.0 - ds - Visual Studio Code
EXPLORER
DS
cp.py
data.py
dire.py
readfile.py
ChangePassword$1.class - bin - Visual Studio Code
EXPLORER
BIN
net \ javaguides \ swing
ChangePassword.class
ChangePassword$1....
ChangePassword$2....
ChangePassword$1.class
net > javaguides > swing > ChangePassword$1.class

This file is not displayed in the text editor because it is a Java class file. Click here to decompile and open.



```
C:\Users\k siresha\Workspace\swing-login-app\bin\net\javaguides\swing\ChangePassword.class
C:\Users\k siresha\Workspace\swing-login-app\bin\net\javaguides\swing\Chatbot$1.class
C:\Users\k siresha\Workspace\swing-login-app\bin\net\javaguides\swing\Chatbot.class
C:\Users\k siresha\Workspace\swing-login-app\bin\net\javaguides\swing\Stmt.class
C:\Users\k siresha\Workspace\swing-login-app\bin\net\javaguides\swing\UserHome$1.class
C:\Users\k siresha\Workspace\swing-login-app\bin\net\javaguides\swing\UserHome$2.class
C:\Users\k siresha\Workspace\swing-login-app\bin\net\javaguides\swing\UserHome$3.class
C:\Users\k siresha\Workspace\swing-login-app\bin\net\javaguides\swing\UserHome.class
C:\Users\k siresha\Workspace\swing-login-app\bin\net\javaguides\swing\UserLogin$1.class
C:\Users\k siresha\Workspace\swing-login-app\bin\net\javaguides\swing\UserLogin$2.class
C:\Users\k siresha\Workspace\swing-login-app\bin\net\javaguides\swing\UserLogin.class
C:\Users\k siresha\Workspace\swing-login-app\src\net
C:\Users\k siresha\Workspace\swing-login-app\src\net\javaguides
C:\Users\k siresha\Workspace\swing-login-app\src\net\javaguides\swing
C:\Users\k siresha\Workspace\swing-login-app\src\net\javaguides\swing\ChangePassword.java
C:\Users\k siresha\Workspace\swing-login-app\src\net\javaguides\swing\Stmt.java
C:\Users\k siresha\Workspace\swing-login-app\src\net\javaguides\swing\UserHome.java
C:\Users\k siresha\Workspace\swing-login-app\src\net\javaguides\swing\UserLogin.java
PS C:\Users\k siresha\OneDrive\Desktop\ds>
```

REFERENCES

Beebe, & Clark. (2005). A hierarchical, objectives-based framework for the digital investigations process. Retrieved
3/10/2015, from http://www.dfrws.org/2004/day1/Beebe_Obj_Framework_for_DI.pdf

Behr. (2008). Anti-forensics: What it is, what it does and why you need to know. New Jersey Lawyer. Issue No. 255.
Retrieved 3/10/2015, from http://www.njsba.com/images/content/1/0/1002013/Dec2008.pdf#page=4

[BBC+08] Barreno, M. et al.: "Open Problems in the Security of Learning". In: D. Balfanz and J. Staddon,
eds., AISec, ACM, 2008, p.19-26

[KhCY07] Khan, M. and Chatwin, C. and Young, R.: "A framework for post-event timeline reconstruction
using neural networks" Digital Investigation 4, 2007

M. G. Noblett, M. M. Pollitt & L. A. Presley, (2000) "Recovering and Examining Computer
Forensic Evidence", Forensic Science Communications, Vol. 2, No. 4.

M. M. Pollitt, (1995) "Computer Forensics: An Approach to Evidence in Cyberspace", in
Proceeding of the National Information Systems Security Conference, Baltimore, MD, Vol. II, pp. 487-491.

Mark M. Pollitt. "Computer Forensics: An approach to Evidence in Cyberspace".National Information System Security Conference.

CONCLUSION

In conclusion, OS forensics is an essential tool for investigating and analyzing digital data in order to identify and prevent criminal activities. With the increasing use of digital devices and the internet,digital forensic techniques are becoming more important than ever before. Digital forensic investigators use a wide range of methods to extract, preserve, and analyze data from computers, smartphones, and other digital devices. The results of OS forensic investigations can be used to identify evidence in criminal cases, and can also be used to prevent future cyber crimes by improving security measures. Overall, digital forensics plays a critical role in the modern world, and its importance will only continue to grow as technology continues to advance.