

# CA – 3 (Project)

Name: Umang Verma Registration no.:11917877

# Roll no.:25 Section:KE026

Submitted to: Rajeshwar Sharma

School of Computer Science

# Introduction

Digital forensics investigations are becoming increasingly important in today's world as more criminal activities are being carried out online. One crucial aspect of digital forensics investigations is the extraction deleted file from disk. By analysing these artifacts, digital forensic investigators can track the suspect's online activities, identify any criminal behavior, and build a solid case against them.

Autopsy forensic tool is an open-source digital forensic tool that can be used to extract or restore images from disk, phone or any other flash drive. It provides various modules and tools that can help investigators search for specific keywords, analyse file metadata, and extract various types of files from disk images. In this task, we will focus on using Autopsy forensic tool to extract deleted image from disk

By leveraging Autopsy's powerful keyword search capabilities, digital forensic investigators can search for specific search terms such as illegal activities, pornography, child exploitation, hacking, and terrorism, among others. By analysing the search results, investigators can identify potentially incriminating evidence and use it to build a solid case against the suspect.

# Objective of the project

Find out the specific search terms on disk and phone using Autopsy forensic tool.

# Description of the project

The above task project involves using forensic tool to extract deleted image from disk The project is intended to provide an introduction to digital forensics investigations and demonstrate how digital forensic investigators can use Autopsy forensic tool to extract deleted image from disk and analyse them for incriminating evidence.

The project involves several steps, including creating a new case in Autopsy, adding disk images or phone images as evidence, creating a keyword list containing specific search terms, configuring the keyword search parameters to include web browser artifacts, running the keyword search job, reviewing the search results, and extracting any relevant

The specific search terms used in the project may vary depending on the investigation, but generally, they include keywords related to illegal activities, pornography, child exploitation, hacking, and terrorism. The project also emphasizes the importance of conducting digital forensics investigations within legal boundaries and with caution when interpreting search results.

Overall, the task project provides a practical demonstration of how Autopsy forensic tool can be used to extract deleted file from disk

activities.

# Scope of the project

The scope of the project is to demonstrate the process of extracting deleted image from disk The project also includes searching for specific search terms on disk images or phone images using Autopsy forensic tool.

The project focuses on using Autopsy forensic tool as the primary digital forensic tool for extracting data from disk.It does not cover other digital forensic tools or techniques that can be used for similar purposes.

The specific search terms used in the project are intended to provide general examples of potentially incriminating evidence that can be found in disk. The project does not cover the investigation of specific criminal cases or provide legal advice.

The project assumes that the disk images or phone images used as evidence are legally obtained and within the boundaries of applicable laws and regulations. It also assumes that the investigation is conducted by trained and authorized digital forensic investigators.

Overall, the scope of the project is to provide an introduction to digital forensics investigations and demonstrate how Autopsy forensic tool can be used to extract deleted images from flash disk and how we can extract important information from website.

# System Description

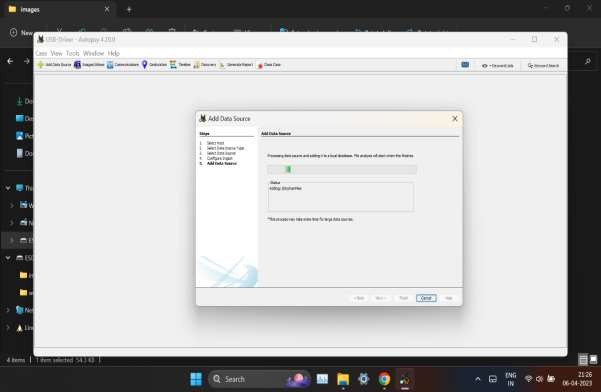
* + The following is a system description for using Autopsy:
    - Operating System: Windows, macOS, or Linux
    - Autopsy Tool: Download the latest version of Autopsy from the official website and install it on your system.
  + The following is a system description for using the Harvester:
    - Operating System: macOS or Linux
    - The Harvester tool: updated with API

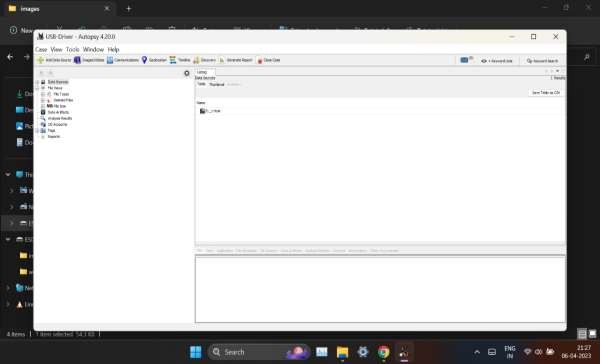
# Target system description

* + - For website I am using lpu.in domain.
    - For Autopsy, I am using a flash drive or pen drive which contains 8GB of storage.

# Analysis Report

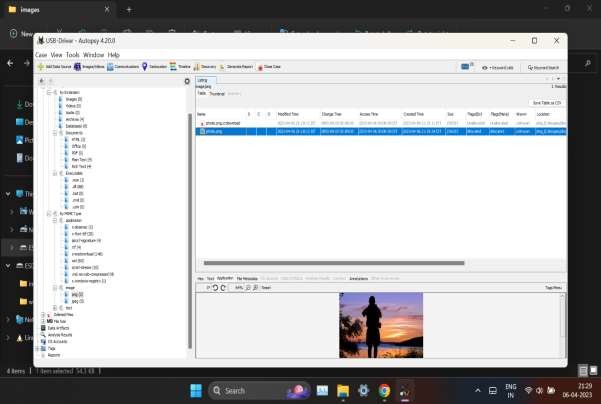
* 1. System snapshots and full analysis report
     + Find out the specific search terms on disk and phone using Autopsy forensic tool.





Graphical user interface

Description automatically generated



Graphical user interface, text, application

Description automatically generated

# 

# 

# 

# 

# 2. For recovery of deleted emails from your email account:

# Firstly create pst file: A PST file (Personal Storage Table) is a file format used by Microsoft Outlook to store email messages, contacts, calendar items, and other data. It is a type of data file used by Microsoft Outlook to store messages and other data on your computer's hard drive. PST files are used to create archives of email messages or to backup email messages from an email account.

# Secondly install Recover My Email tool: This tool can recover deleted or lost emails from your computer's hard drive, external drives, and other storage devices. It supports Microsoft Outlook email client.

# **STEPS TO CREATE A PST FILE:**

**Step 1) Open Microsoft Outlook on your computer’**

# **Step 2) Click on the "File" tab in the top left corner of the screen.**

# 

# Graphical user interface, text, application Description automatically generated

# 

# Graphical user interface, application Description automatically generated

# Graphical user interface, text, application, email Description automatically generated

# Graphical user interface, application, Word Description automatically generated

# Graphical user interface Description automatically generated with medium confidence

# Graphical user interface, application Description automatically generated

# Graphical user interface, text, application Description automatically generated

# Graphical user interface, application Description automatically generated

# Graphical user interface, application Description automatically generated

# Graphical user interface, application, Word Description automatically generated

# 

# Reference/ Bibliography

* + - https://[www.autopsy.com/](http://www.autopsy.com/)
    - https://[www.kali.org/tools/theharvester/#:~:text=The%20package%20con](http://www.kali.org/tools/theharvester/#%3A~%3Atext%3DThe%20package%20con) tains%20a%20tool,Installed%20size%3A%201.72%20MB
    - https://[www.youtube.com/watch?v=S6V66G2tVr8](http://www.youtube.com/watch?v=S6V66G2tVr8)
    - https://[www.youtube.com/watch?v=cDryilcK39c](http://www.youtube.com/watch?v=cDryilcK39c)
    - https://en.wikipedia.org/wiki/Autopsy\_(software)
    - https://[www.oreilly.com/library/view/web-penetration-](http://www.oreilly.com/library/view/web-penetration-) testing/9781788623377/71203ba9-3894-4192-af66-1003405ab8ed.xhtml
    - <https://youtu.be/behDv6HEIrk>
    - https://www.igi-global.com/dictionary/introduction-to-email-web-and-messageforensics/82333