OPEN-SOURCE TECHNOLOGIES (INT301)

Continuous Assessment No. 3

on

Topic: **Use any open-source software to extract data from disk drives and other storage so as to facilitate the forensic analysis of computer systems.**

submitted by

Arpit Ranjan – 11914864

Program Name: B. Tech (Computer Science and Engineering)

Under the guidance of

Faculty: Rajeshwar Sharma

UID: 29484

Department of Computer Science and Engineering
Lovely Professional University, Phagwara

TABLE OF CONTENT

INTRODUCTION

Objective of project

The objective of this project is to conduct a comprehensive digital forensic analysis of electronic devices, including computers, mobile phones, and other digital storage media. The project aims to explore the various tools and techniques used in digital forensics, including data acquisition, preservation, analysis, and presentation. The project will focus on identifying the most effective and efficient methods of digital forensic analysis, including the use of specialized software, hardware, and forensic techniques. The project will also address the legal and ethical considerations associated with digital forensic analysis, including issues related to privacy, confidentiality, and data protection. Ultimately, the project seeks to provide a practical guide for forensic examiners on how to conduct digital forensic analysis, and how to use the results of this analysis to support legal proceedings and investigations.

Description of project

The project aims to investigate and develop effective methods and techniques for extracting data from various types of disk drives and storage devices to facilitate forensic analysis of computer systems.

The project will involve a comprehensive review of existing literature and research on data extraction methods used in digital forensics. This will include studying different types of disk drives, such as hard disk drives (HDDs), solid-state drives (SSDs), optical drives, and other storage media like USB drives, memory cards, and cloud storage.

The project will focus on identifying and evaluating different data extraction techniques, such as imaging, live analysis, forensic duplication, and carving. It will involve researching and testing various software and hardware tools commonly used in digital forensics for data extraction, including open-source and commercial tools.

The project will also explore the challenges and limitations associated with data extraction, including issues related to data preservation, integrity, and privacy.

It will address the impact of different storage technologies, encryption, and other security measures on the data extraction process.

Furthermore, the project will consider legal and ethical considerations associated with digital forensics, including compliance with relevant laws, regulations, and guidelines, as well as issues related to privacy, confidentiality, and data protection.

The project will involve conducting experiments and simulations to evaluate the effectiveness and efficiency of different data extraction methods on various types of disk drives and storage devices. It may also include analyzing real-world case studies to understand practical challenges and solutions in data extraction for forensic analysis.

The project will culminate in the development of a comprehensive report summarizing the findings, recommendations, and best practices for extracting data from disk drives and other storage devices to facilitate forensic analysis of computer systems. The report will aim to provide practical guidance for forensic examiners and investigators in the field of digital forensics, with the goal of advancing the field and contributing to the body of knowledge in this area.

Scope

The scope of the project will include the following:

- *Review of Literature*: A comprehensive review of existing literature and research on data extraction methods used in digital forensics, including academic papers, industry reports, and relevant standards and guidelines.
- *Data Extraction Techniques*: Identification and evaluation of different data extraction techniques, such as imaging, live analysis, forensic duplication, and carving, and their applicability to different types of disk drives and storage devices.
- *Software and Hardware Tools*: Researching and testing various software and hardware tools commonly used in digital forensics for data extraction, including open-source and commercial tools, and evaluating their effectiveness and efficiency in extracting data from disk drives and storage devices.

- *Challenges and Limitations*: Analysis of the challenges and limitations associated with data extraction, including issues related to data preservation, integrity, and privacy, and understanding the impact of different storage technologies, encryption, and other security measures on the data extraction process.
- *Legal and Ethical Considerations*: Consideration of legal and ethical aspects of digital forensics, including compliance with relevant laws, regulations, and guidelines, and addressing issues related to privacy, confidentiality, and data protection in the context of data extraction.
- *Experiments and Simulations*: Conducting experiments and simulations to evaluate the effectiveness and efficiency of different data extraction methods on various types of disk drives and storage devices, and analyzing real-world case studies to understand practical challenges and solutions in data extraction for forensic analysis.
- *Report Development*: Development of a comprehensive report summarizing the findings, recommendations, and best practices for extracting data from disk drives and storage devices to facilitate forensic analysis of computer systems, with practical guidance for forensic examiners and investigators in the field of digital forensics.

SYSTEM DESCRIPTION

Introduction

The purpose of this project is to develop a system that facilitates the forensic analysis of computer systems by extracting data from disk drives and other storage media. The system will be designed as an open source software tool that can be used by forensic analysts, investigators, and other authorized personnel to collect, preserve, and analyze digital evidence in a forensically sound manner.

System Objectives

The main objectives of the system are as follows:

- Extraction of data from various types of storage media, including hard drives, USB flash drives, SD cards, CDs/DVDs, and other digital storage devices.
- Preservation of the original data through the creation of forensic images using industry-standard imaging techniques, ensuring that the integrity and authenticity of the evidence are maintained.
- Analysis of the extracted data to identify relevant files, folders, and other digital artifacts, such as deleted files, internet history, emails, images, and other forms of digital evidence.
- Recovery of deleted files and folders using specialized tools and techniques to uncover potential evidence that may have been intentionally or unintentionally deleted by users.
- Identification of steganography, which is the practice of hiding information within images or other digital media, using image analysis tools to detect any hidden data.
- Documentation of findings and actions taken during the data extraction and analysis process, including timestamps, metadata, and other relevant information, to support the integrity and admissibility of the evidence in legal proceedings.

System Features

The system will include the following features:

- Support for a wide range of storage media, including hard drives, USB flash drives, SD cards, CDs/DVDs, and other digital storage devices.
- Creation of forensic images using industry-standard imaging techniques, such as "dd" or "dcfldd", to ensure that the original data is preserved in a forensically sound manner.
- Analysis of the forensic images using open source forensic analysis tools, such as "Autopsy", to extract and analyze relevant data.
- User-friendly graphical interface for easy navigation and use of the system, with support for different operating systems, including Windows, macOS, and Linux.
- Detailed reporting and documentation features to record findings, actions taken, and metadata associated with the extracted data, to support the integrity and admissibility of the evidence in legal proceedings.
- Extensibility and customization options to allow for future updates, enhancements, and integration with other forensic tools or systems.

System Workflow

The typical workflow of the system can be summarized as follows:

Step 1: Identification of the storage media to be analyzed, such as a hard drive, USB flash drive, SD card, or CD/DVD.

Step 2: Creation of a forensic image of the storage media using industry-standard imaging techniques, ensuring that the original data is preserved and protected from any modifications.

Step 3: Analysis of the forensic image using open source forensic analysis tools, such as "Autopsy", to extract and analyze relevant data.

Step 4: Recovery of deleted files and folders using specialized tools and techniques to uncover potential evidence that may have been deleted by users.

Step 5: Identification of steganography, if applicable, using image analysis tools to detect any hidden data.

Step 6: Documentation of findings, actions taken, and metadata associated with the extracted data, in a detailed report that can be used in legal proceedings or other investigations.

Conclusion

The system for data extraction from disk drives and other storage is a comprehensive solution for facilitating forensic analysis of computer systems. It provides a range of functionalities for acquiring, preserving, and analyzing data from various storage media, and offers scalability, security, and user management features. This system can be a valuable tool for forensic analysts, investigators, and other stakeholders involved in computer forensic investigations to uncover critical evidence and support legal proceedings.

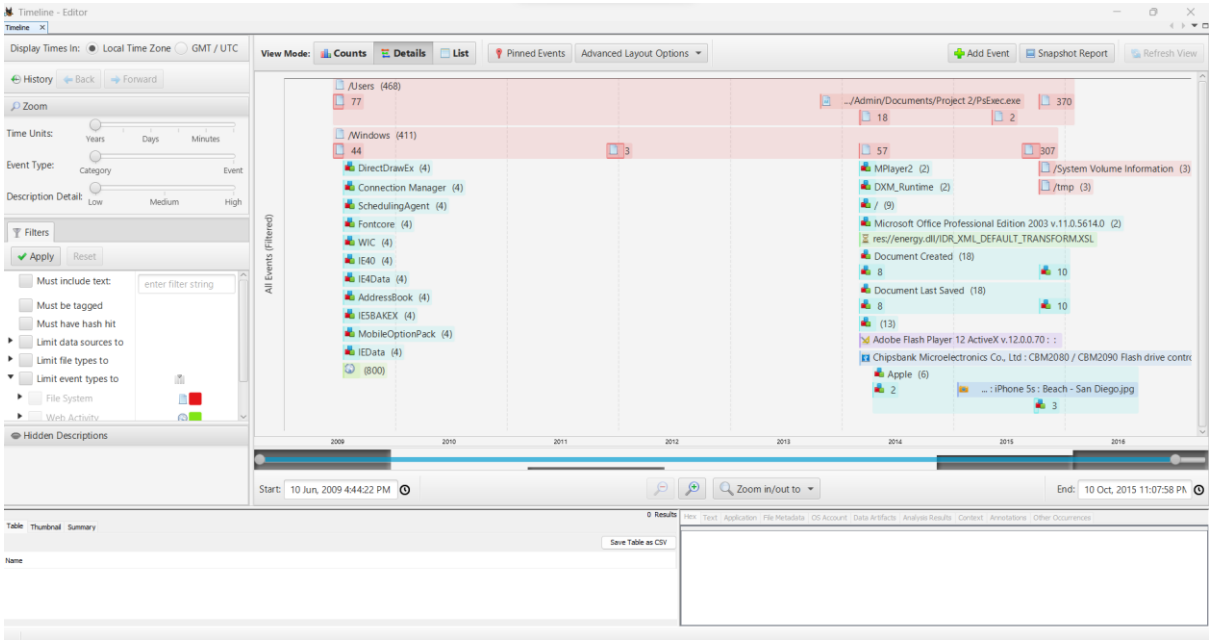
DATASET LINK

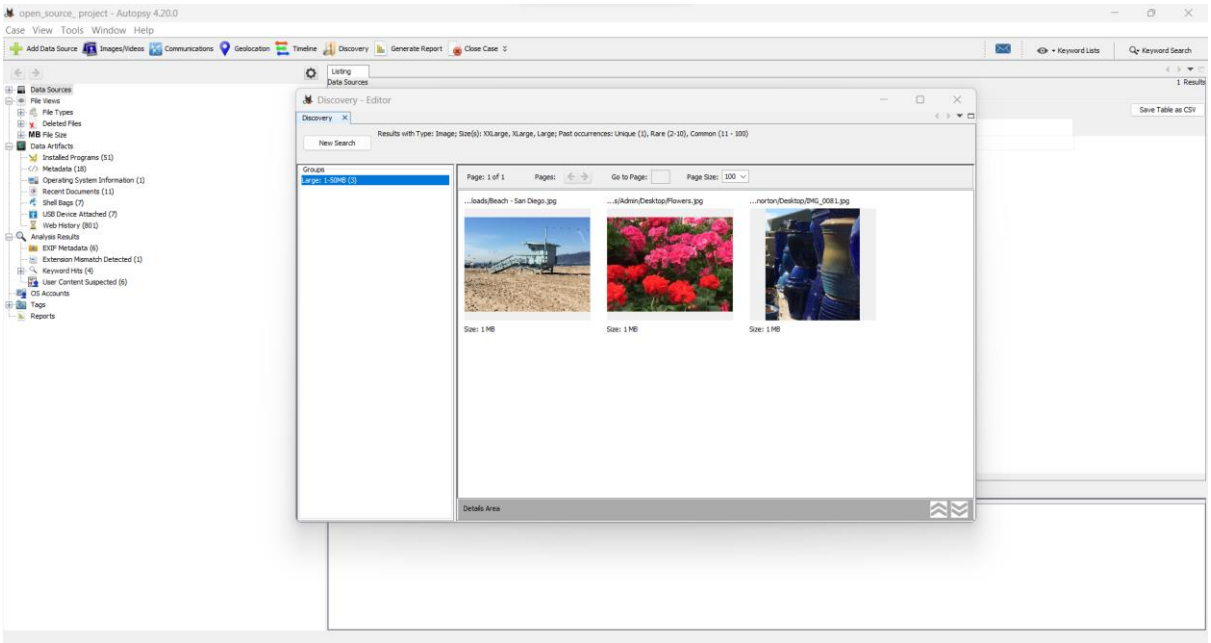
- http://www.digitalforensicsworkbook.com/data-sets

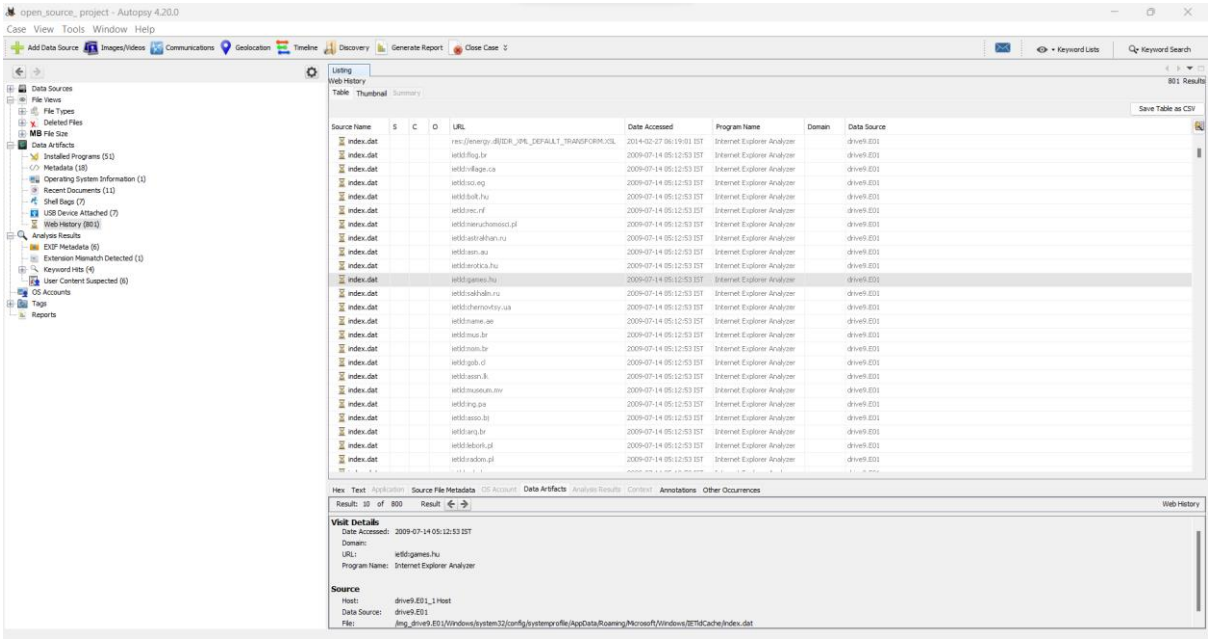
FULL REPORT ANALYSIS

- https://github.com/ranjanarpit27/opensourece-Project/tree/main/Reports/open_source_%20project%20HTML%20Report%2004-12-2023-04-16-09

SCREENSHOT OF PROJECT




open_source_project - Autopsy 4.20.0
Case View Tools Window Help
Discovery - Editor
Results with Type: Image; Size(s): XXLarge, XLarge, Large; Past occurrences: Unique (1), Rare (2-10), Common (11 - 100)
New Search
Groups
Large: 1-50MB (3)
Page: 1 of 1
Pages:
Go to Page:
Page Size: 100
...loads/Beach - San Diego.jpg
...s/Admin/Desktop/Flowers.jpg
...norton/Desktop/IMG_0081.jpg
Size: 1 MB
Size: 1 MB
Size: 1 MB
Details Area


open_source_project - Autopsy 4.20.0
Case View Tools Window Help
Web History
Table
Thumbnail
Summary
Source Name
URL
Date Accessed
Program Name
Domain
Data Source
Visit Details
Date Accessed: 2009-07-14 05:12:53 IST
URL: ie5:d:games.hu
Program Name: Internet Explorer Analyzer
Source
Host: drive9.E01_1 Host
Data Source: drive9.E01
File: /img_drive9.E01/Windows/system32/config/systemprofile/AppData/Roaming/Microsoft/Windows/IE5d\Cache/Index.dat

REFERENCES/ BIBLIOGRAPHY

- “Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.” This book provides in-depth knowledge on file system analysis, including techniques for extracting data from disk drives, understanding file system structures, and analysing file system metadata.
- “Garfinkel, S., & Shelat, A. (2009). Forensic Computing: A Practitioner's Guide. Addison-Wesley Professional.” The comprehensive guide covers various aspects of forensic computing, including data acquisition from disk drives and other storage media, forensic analysis techniques, and best practices for conducting forensic investigations.
- “Autopsy Forensic Browser. (https://www.autopsy.com/)” Autopsy is a popular open-source forensic analysis tool that provides a wide range of features for data extraction from disk drives, file recovery, email analysis, and reporting. It is widely used in the digital forensics’ community.