

# **INTRODUCTION TO** **CYBER SECURITY**



**SEMESTER FINAL PROJECT**  
**( GROUP 10 )**

**SUBMITTED BY:**

Muhammad Haseeb	242292
Ahmed Saleem	242348
Muhammad Umair	242300
Faizan Satti	243328

**SUBMITTED TO:**

Mr. Syed Jalal Shah

# **INTRODUCTION TO PROJECT**

Autopsy is a powerful digital forensic tool with a simple user interface to simplify investigations and analysis of digital evidence. Being an open source, it is applied by forensic analysts, cybersecurity professionals, and law enforcement agencies on tasks such as recovery of deleted files, disk images analysis, and data breaches investigation. The Sleuth Kit is a foundation over which Autopsy has built its intuitive graphical interface making it accessible even for those having minimal forensic experience.

Developed initially by Brian Carrier, it is now an advanced forensic tool widely adopted by a huge population, one that continues to undergo improvements until this date. This tool provides support for numerous file systems like NTFS, FAT, and EXT, apart from working perfectly with diverse operating systems: Windows, Linux, or macOS. Key features such as timeline analysis, keyword search, file carving, and auto reporting made this the most precious piece in forensic investigations now.

In this paper, we will discuss its history, features, and practical applications. We'll discuss its advantages, disadvantages, and relevance in daily forensic tasks, such as corporate investigations and personal data recovery. We will also have a comprehensive guide on downloading and using Autopsy by providing step-by-step instructions on how to analyze a USB image. This analysis is practical and demonstrates that Autopsy can identify and recover digital artifacts, which may be important in real-world forensic scenarios.

By the end of this report, readers will have a very good idea of what Autopsy can do and just how fundamental it is in the field of digital forensics.

# AUTOPSY

## INTRODUCTION

Autopsy is a free open-source digital forensic tool which is developed in order to assist investigators analyze and retrieve data from devices. This provides an intuitive graphical user interface based on The Sleuth Kit that is used by users for effectively examining their hard drives, memory dumps, and disk images.

The primary use of Autopsy is in forensic investigations; it recovers deleted files, analyzes file systems, extracts metadata, and provides evidence about cybercrimes. It is a major part of event reconstruction, finding traces of illegal activities, and producing comprehensive reports that will be useful in legal actions. It is used across the world by law enforcement, corporate security, and personal data recovery.

## HISTORY

Autopsy is the graphical interface for The Sleuth Kit (TSK) and was created by Brian Carrier, one of the most prominent digital forensic experts. It simplifies the analysis of the digital evidence, and it has become a go-to source for open-source solutions within digital forensics.

It was first designed for the early 2000s and targeted to make forensic investigations accessible both to experts and novices. It is combined with The Sleuth Kit allowed it to tap into tremendous power in forensic capabilities such as analyzing file systems (NTFS, FAT, EXT) recovery of deleted files as well as extraction of metadata.

With significant updates in the long run, the functionality, user experience of Autopsy have undergone some very important landmarks as:

1. **Timeline Analysis:** The feature helped the investigators visualize events in chronological order, which would make it easier to reconstruct incidents.
2. **Keyword Search Capabilities:** Advanced mechanisms of searching were introduced to locate specific terms or patterns within large datasets.
3. **Integration with Modules:** Features like photo recognition, email parsing, and EXIF data analysis were added via modular plugins.
4. **Cross-Platform Support:** Initially designed for Unix-like systems, Autopsy had evolved to support Windows, Linux, and macOS in order to broaden usability.

Today, Autopsy remains actively maintained and widely utilized in law enforcement, corporate investigations, and cybersecurity contexts, continuing to evolve with contributions from the global digital forensics community.

## **PROPERTIES**

Autopsy is a robust and feature-rich digital forensic tool that caters to the needs of investigators in examining digital evidence. Its primary properties include:

### **Key Features:**

#### **1. Open-Source and User-Friendly Interface**

- Autopsy is free and open-source; users are able to alter and extend the functionality.
- Graphical user interface has proven to be intuitive so is available to both newcomers and professionals alike.

#### **2. Comprehensive File System Analysis**

- Supports multiple file systems, including NTFS, FAT, and EXT, enabling investigators to work with a wide range of storage media.
- Analyze hard drives, disk images, memory dumps, and more.

#### **3. Keyword Search and Image Carving**

- Delivers powerful search tools for finding specific terms, patterns, or file types.
- Image carving is the ability to recover deleted or fragmented files based on their file signatures.

#### **4. Integration with The Sleuth Kit Modules**

- Uses the analytical power of The Sleuth Kit for low-level data analysis.
- Supports plugins for extended functionality, such as photo recognition, email parsing, and registry analysis.

### **Technical Specifications and Supported Platforms**

- **Operating Systems:**  
Works on Windows, Linux, and macOS, making it versatile for investigators using different environments.
- **Requirements:**  
It requires minimal hardware resources, but performance improves with higher RAM and processing power.
- **Extensibility:**  
It has the ability to allow third-party modules and plugins for further enhancement of its capabilities.

Autopsy is the combination of advanced features and flexibility and ease of use, making it a critical tool in modern digital forensic investigations.

## **DAILY LIFE USES**

Autopsy is a multivariant tool used in any real-life scenario in numerous domains. Its simplicity in use and powerful features provide it with the value to its users.

### **1. Digital Forensics by Law Enforcement Agencies**

- Autopsy is widely used for cybercrime investigation, including hacking fraud, online harassment, etc., in law enforcement agencies.
- It facilitates evidence analysis of seized devices such as hard drives and USBs to recover deleted files, analyze timelines, and look for traces of illegal activity.
- It also generates a lot of detail reports which become admissible in courts that would support court proceedings.

### **2. Corporate Investigations for Data Breaches**

- In cybersecurity as well as internal investigations, Autopsy is used for the detection and analysis of data breach, unauthorized access, and insider threats.
- It allows tracing file usage, recovering inadvertently deleted corporate data, identification of suspicious activities such as exfiltration of confidential information.

### **3. Personal Use for Data Recovery or Disk Imaging**

- People use Autopsy in order to recover accidentally removed files, photos, documents from their personal storage disks.
- It can be used to create and analyze images of disks to preserve evidence or troubleshoot problems relating to storage media.

All these require Autopsy to rapidly process and analyze digital data, making it relevant day in and day out within forensic and recovery operations.

## **ADVANTAGES**

Autopsy has numerous advantages which make it a very popular among digital forensic experts and novice users:

### **1. No Cost and Open Source**

- Autopsy is absolutely free to use and therefore would not cost a person or organization or law enforcement agency.
- It is an open source, and so users could customize and extend its functionalities to meet specific investigation needs.

### **2. Exhaustive Forensic Analysis**

- Equipped with powerful features such as file recovery, timeline analysis, and keyword, Autopsy provides an in-depth analysis of digital evidence.
- Integration with The Sleuth Kit adds advanced capabilities for analyzing file systems and recovering fragmented data.

### **3. Wide Compatibility with Multiple Operating Systems**

- Supports major operating systems, including Windows, Linux, and macOS, making it a versatile tool for different environments and setups.
- It supports multiple file systems, such as NTFS, FAT, and EXT, to provide flexibility in working with various storage devices.

### **4. Active Community and Documentation Support**

- Autopsy has an active community of developers and users who contribute plugins, share insights, and provide assistance.
- Comprehensive documentation, tutorials, and forums make it easier for new users to learn and troubleshoot issues.

These benefits make Autopsy a reliable and accessible digital forensic tool that offers incredible capabilities with no high, commercial pricing.

## **DISADVANTAGES**

Despite all that Autopsy offers, a person should know that it does come with some limitations. Consider the following:

### **1. Limited Advanced Features Compared to Premium Forensic Tools**

- Premium forensic tools such as EnCase and FTK offer such features as built-in AI, real-time collaboration and much more comprehensive automation especially for large-scale investigations.
- Autopsy lacks several high-end features that most complex or enterprise-level investigations require.

### **2. Slower Processing for Large Data Sets**

- With very large disk images or data volumes, Autopsy is also much slower than commercial products optimized for performance.
- This makes analysis times longer, particularly on underpowered systems.

### **3. Occasional User Interface Complexity for Beginners**

- Though well-designed for ease of use, some features and workflows may be intimidating for users without prior experience in forensics.
- Navigation of complex options or solving error messages may necessitate extra learning and reliance on community support.

These disadvantages make it apparent in which aspects Autopsy is not up to the mark for every user, especially where applications require a faster processing and highly specialized features. Yet, it is most often outweighed by these drawbacks for most applications through access and cost-effectiveness.

# **DOWNLOAD AND INSTALLATION**

Follow these steps to download and install Autopsy on your system:

## **STEP 1: Visit the Autopsy Official Website**

- Go to the official website: <https://www.autopsy.com/>.
- Click on the "**Download**" button prominently displayed on the homepage.

## **STEP 2: Choose the Appropriate Version for Your Operating System**

- Identify your operating system (Windows, Linux, or macOS).
- Download the installer or package that corresponds to your OS.

## **STEP 3: Check Prerequisites**

- Ensure your system meets the minimum requirements:
  - ✓ **RAM:** At least 4 GB (8 GB or more recommended for larger datasets).
  - ✓ **Processor:** Modern multi-core CPU recommended for better performance.
  - ✓ **Java Runtime Environment (JRE):** Autopsy requires JRE to run. If not already installed, download it from [Oracle's official site](#).

## **STEP 4: Install Autopsy**

- **For Windows:**
  - ✓ Run the downloaded **.exe** file.
  - ✓ Follow the on-screen instructions to complete the installation.
  - ✓ Ensure you allow the installer to configure necessary environment variables.
- **For Linux:**
  - ✓ Extract the downloaded **.tar** file or use your package manager (if available).
  - ✓ Install any required dependencies (e.g., **libtsk**).
  - ✓ Use the provided scripts to launch Autopsy.
- **For macOS:**
  - ✓ Install Homebrew or use the **.dmg** file if available.
  - ✓ Install required dependencies and follow installation prompts.

## **STEP 5: Launch Autopsy**

- Open the installed application and verify that it runs without errors.
- If necessary, check for additional modules or plugins to extend functionality.

## **STEP 6: Perform a Test Run**

- Create a test case to confirm the installation works properly and explore the basic interface.



# **HOW TO USE**

We can use the Autopsy tool by following these steps:

## **1. Creating a Case**

- Launch Autopsy and open the main interface.
- Create a new case:
  - ✓ On the main screen, click on "Create New Case".
  - ✓ Enter a case name and description.
  - ✓ Select a location to save the case data.
  - ✓ Choose a case type (e.g., Forensic or Incident Response).
  - ✓ Click "Finish" to create the case.

## **2. Adding a Data Source**

- After creating the case, you'll be prompted to add a data source (e.g., disk image, USB drive).
- Add a data source:
  - ✓ In the "Case" tab, click "Add Data Source".
  - ✓ Choose the type of data source:
    - **Disk Image:** Select a disk image file (e.g., .dd, .iso).
    - **Local Disk:** If analyzing a local disk or partition, select it.
    - **USB Drive:** Plug in a USB drive and select it from the available devices.
  - ✓ Click **Next** and choose any additional configuration options (e.g., hashing for verification).
  - ✓ Click "**Finish**" to load the data source.

## **3. Performing Forensic Analysis**

Autopsy provides several tools for in-depth analysis. Here are some common tasks:


- **Timeline Analysis:**
  - ✓ Click on "**Timeline**" under the "**Analysis**" tab.
  - ✓ Autopsy will generate a chronological view of file activity.
  - ✓ Investigate suspicious events, such as file deletions, modifications, and access times.
- **Keyword Search:**
  - ✓ Click on "**Keyword Search**" under the "**Analysis**" tab.
  - ✓ Enter specific keywords, file names, or patterns to search for.
  - ✓ Review the results and analyze files containing the keywords.
- **Deleted Files Recovery:**
  - ✓ Navigate to the "**File Analysis**" section and click on "**Deleted Files**".
  - ✓ Autopsy will show files marked as deleted but recoverable.
  - ✓ Select files you wish to recover and analyze their contents.

- **File Carving:**
  - ✓ Under "**Image Carving**", you can recover deleted or fragmented files based on their file signatures.
  - ✓ This process is useful for identifying images, documents, or other data types that may have been partially overwritten.
- **Other Analysis Tools:**

Use tools like **Web Browser History**, **Email Analysis**, and **Registry Analysis** to examine specific data types related to internet activity or software use.

#### 4. Generating Reports

Once the analysis is complete, you can generate a detailed report:

-  Go to the "**Reports**" tab in the main interface.
- Click on "**Generate Report**".
- Choose the type of report (e.g., **HTML** or **PDF**).
- Select the scope of the report, including:
  - ✓ Case details, timeline analysis, keyword results, file recovery findings, etc.
- Click "**Generate**" to create the report. Autopsy will compile all relevant findings and present them in a structured, easy-to-read format.

#### 5. Reviewing and Exporting Results

- After the report is generated, you can export it for further review or legal submission.
- **Export options:** You can export individual files, hash values, or even full reports depending on your needs.

With these steps, you can efficiently use Autopsy to conduct thorough forensic investigations, recover important evidence, and generate reports suitable for legal proceedings.

# PRACTICAL ANALYSIS OF A USB IMAGE

The USB device, discovered during a police raid in the house of a drug dealer, was initially found in an unreadable form. It was handed over to the Forensic Department for digital analysis. Upon investigation, the USB was found to contain various encrypted files, potentially linked to illicit activities. A detailed examination was carried out to recover and decrypt the data, using specialized forensic tools and techniques. Preliminary findings suggest that the USB might have been used for storing critical evidence or illicit records, with traces of hidden files and potential links to criminal operations. Further analysis is underway to piece together the full extent of the data and its relevance to ongoing investigations.

## Setup

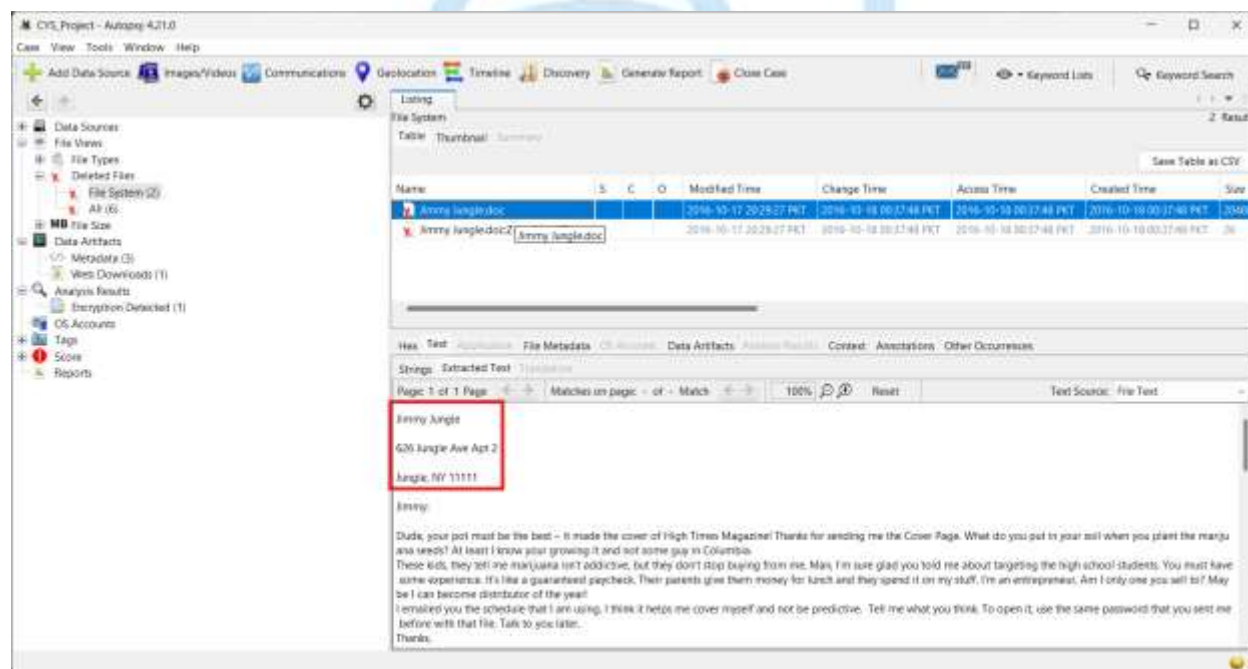
We opened the Autopsy tool created a new case, and added the Disk Image (e.g., **.dd**). Set a hostname, investigator name, and directory to save the extensions.

## Forensic Analysis

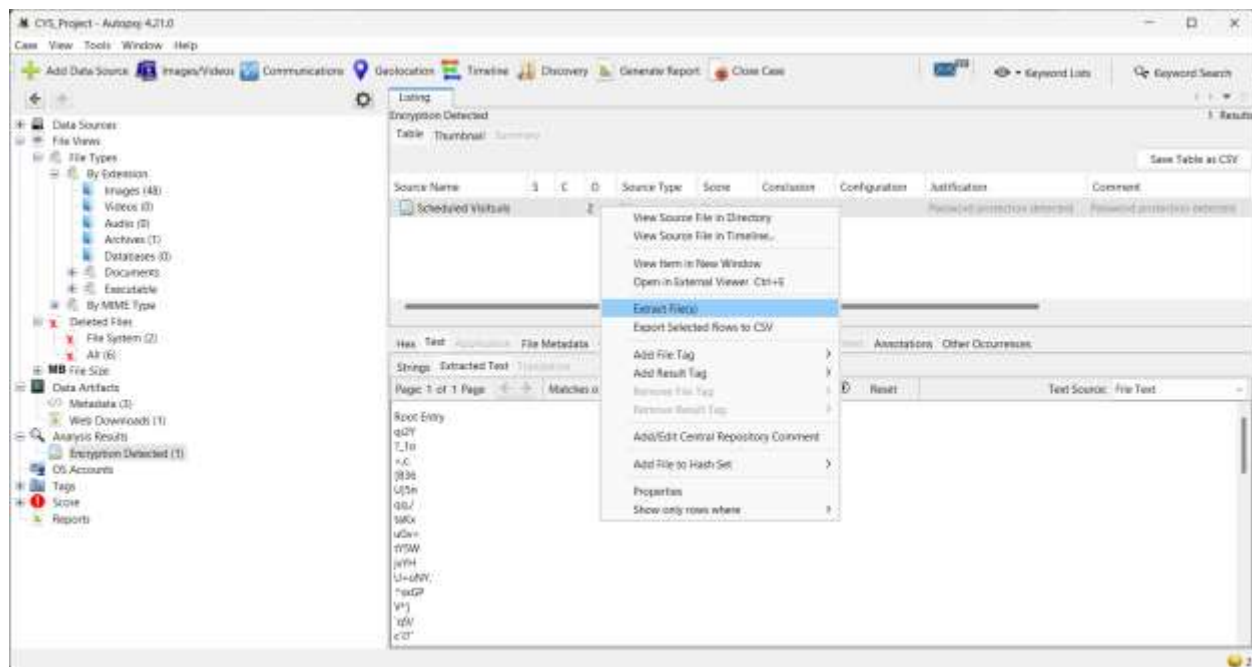
When we examined the image on Autopsy tool, we got a list of files and directories and found some critical evidence.

## Evidence Found

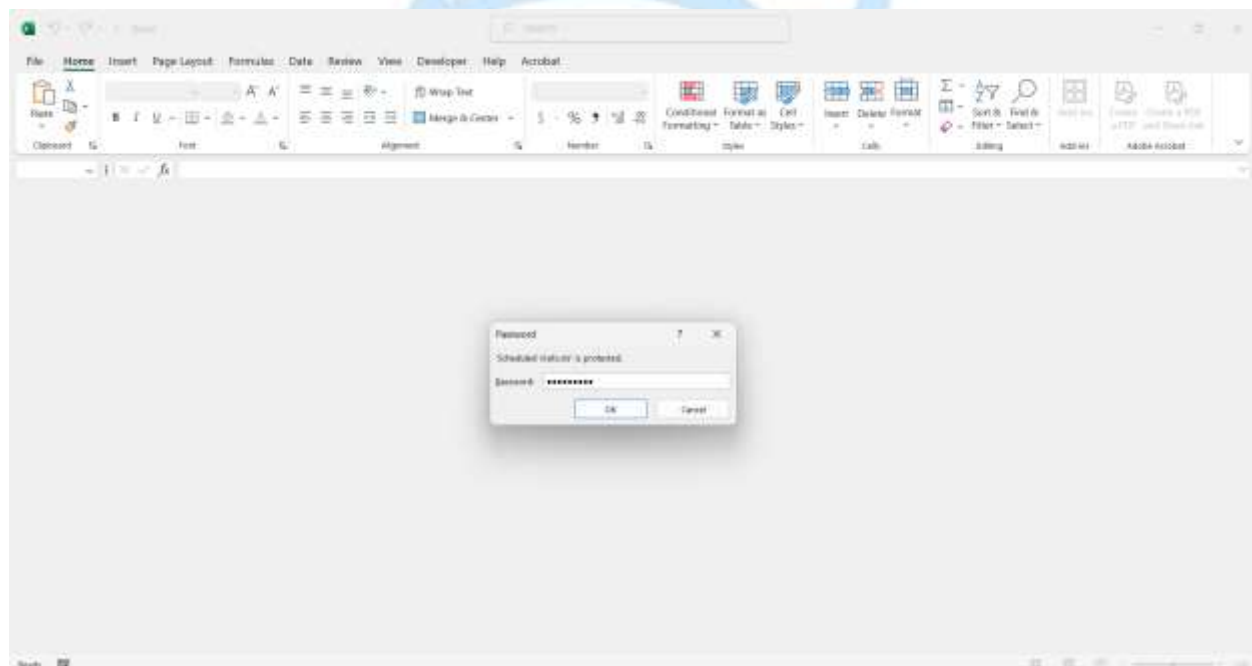
While examining the deleted files, we came across some emails, on opening them we recovered the Full name, address, and Email address of the criminal as shown below.



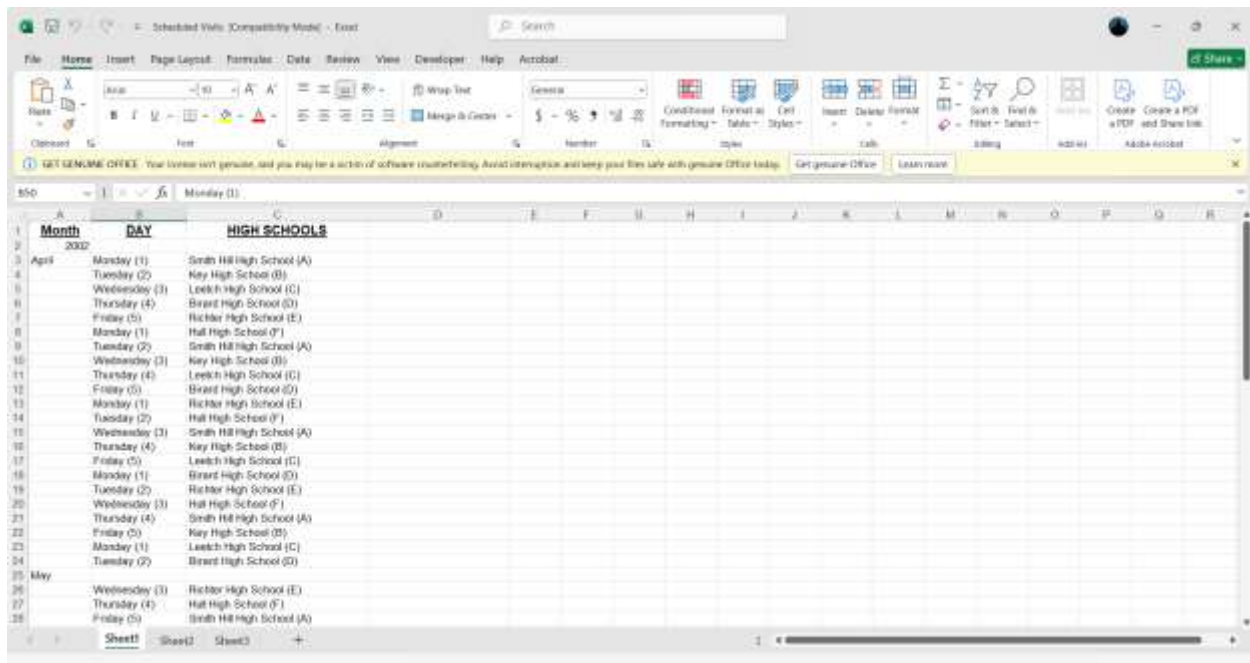
On examining the documents, we came across an Excel file “**Schedule Visits**” that seemed suspicious, so I downloaded it.



On Opening, we discovered that the Excel file was Password protected. So, we started searching for some hidden passwords. On a thorough search, I came across a **.jpg** image. On examining it's text we came across some text **pw: goodtime** that seemed like (pw=password), so we tried it out on the excel file.



It worked and unlocked it, and we got the complete list where the drugs were supplied.



Month	DAY	HIGH SCHOOLS
2022		
April	Monday (1)	Smith Hill High School (A)
	Tuesday (2)	Key High School (B)
	Wednesday (3)	Leitch High School (C)
	Thursday (4)	Brant High School (D)
	Friday (5)	Richter High School (E)
	Monday (1)	Hall High School (F)
	Tuesday (2)	Smith Hill High School (A)
	Wednesday (3)	Key High School (B)
	Thursday (4)	Leitch High School (C)
	Friday (5)	Brant High School (D)
	Monday (1)	Richter High School (E)
	Tuesday (2)	Hall High School (F)
	Wednesday (3)	Smith Hill High School (A)
	Thursday (4)	Key High School (B)
	Friday (5)	Leitch High School (C)
	Monday (1)	Brant High School (D)
	Tuesday (2)	Richter High School (E)
	Wednesday (3)	Hall High School (F)
	Thursday (4)	Smith Hill High School (A)
	Friday (5)	Key High School (B)
	Monday (1)	Leitch High School (C)
	Tuesday (2)	Brant High School (D)
May	Wednesday (3)	Richter High School (E)
	Thursday (4)	Hall High School (F)
	Friday (5)	Smith Hill High School (A)

These evidence were enough to hold him guilty by the investigation team.

## **CONCLUSION**

Autopsy is a powerful tool in the digital forensics field, offering strong features in analyzing and recovering digital evidence. Its open-source nature, user-friendly interface, and compatibility with multiple file systems and operating systems make it a preferred choice for law enforcement, corporate investigators, and individuals.

During the practical experiment, Autopsy proved its ability to analyze a USB image. Key findings included recovery of deleted files, timeline reconstruction of events, and the ability to search for specific keywords within the data. The modular design of the tool and the automated reporting streamlined the investigation process, making it easy to compile and present findings.

In real-world applications, Autopsy stands out for cost-effectiveness and extensibility, especially in scenarios where file recovery, incident analysis, or evidence preparation for legal cases is needed. It may lack some advanced features of commercial tools, but its accessibility and robust functionality make it an invaluable resource for professionals and beginners in digital forensics.