Digital Forensic Analysis with Autopsy

1. Introduction

The purpose of this project was to gain practical exposure to **digital forensic investigation** by using Autopsy, a popular open-source forensic tool. Digital forensics involves the process of identifying, preserving, analyzing, and documenting digital evidence for legal or investigative purposes.

Autopsy provides a GUI for the Sleuth Kit and enables forensic analysts to examine disk images, recover deleted files, extract registry data, analyze browser history, and build case reports efficiently.

2. Lab Setup

- **Tools Used**:
    - **Autopsy** (installed on Kali Linux / Windows)
    - **TryHackMe room:** Disk Analysis & Autopsy
    - Sample forensic disk images provided in the CTF challenge
- **Installation**: Autopsy was installed on Kali Linux using pre-built packages. Java Runtime Environment was configured since it is required by Autopsy.
- **Working Environment**:
  A forensic image file was imported into Autopsy and analyzed through the case management system.

3. Case Analysis

- **Challenge Used**: *TryHackMe – Autopsy Room* (digital forensic CTF)
- **Steps Followed**:
    1. Created a new case in Autopsy and loaded the forensic disk image.
    2. Performed file system analysis to locate user files and hidden directories.
    3. Recovered deleted files and analyzed their content.
    4. Extracted browser history to trace user activity, such as visited websites.
    5. Investigated registry hives and system artifacts for usernames and installed applications.
    6. Answered CTF questions by correlating evidence with case requirements.

- **Recovered Data and Artifacts**:
    - Deleted documents and images
    - User browsing history with suspicious domains
    - Metadata of files revealing creation/modification dates
    - Registry evidence showing installed software and user account names
- **Screenshots**: (to be attached) Evidence views from Autopsy, showing browser history, deleted files, and case timeline.

4. Key Findings

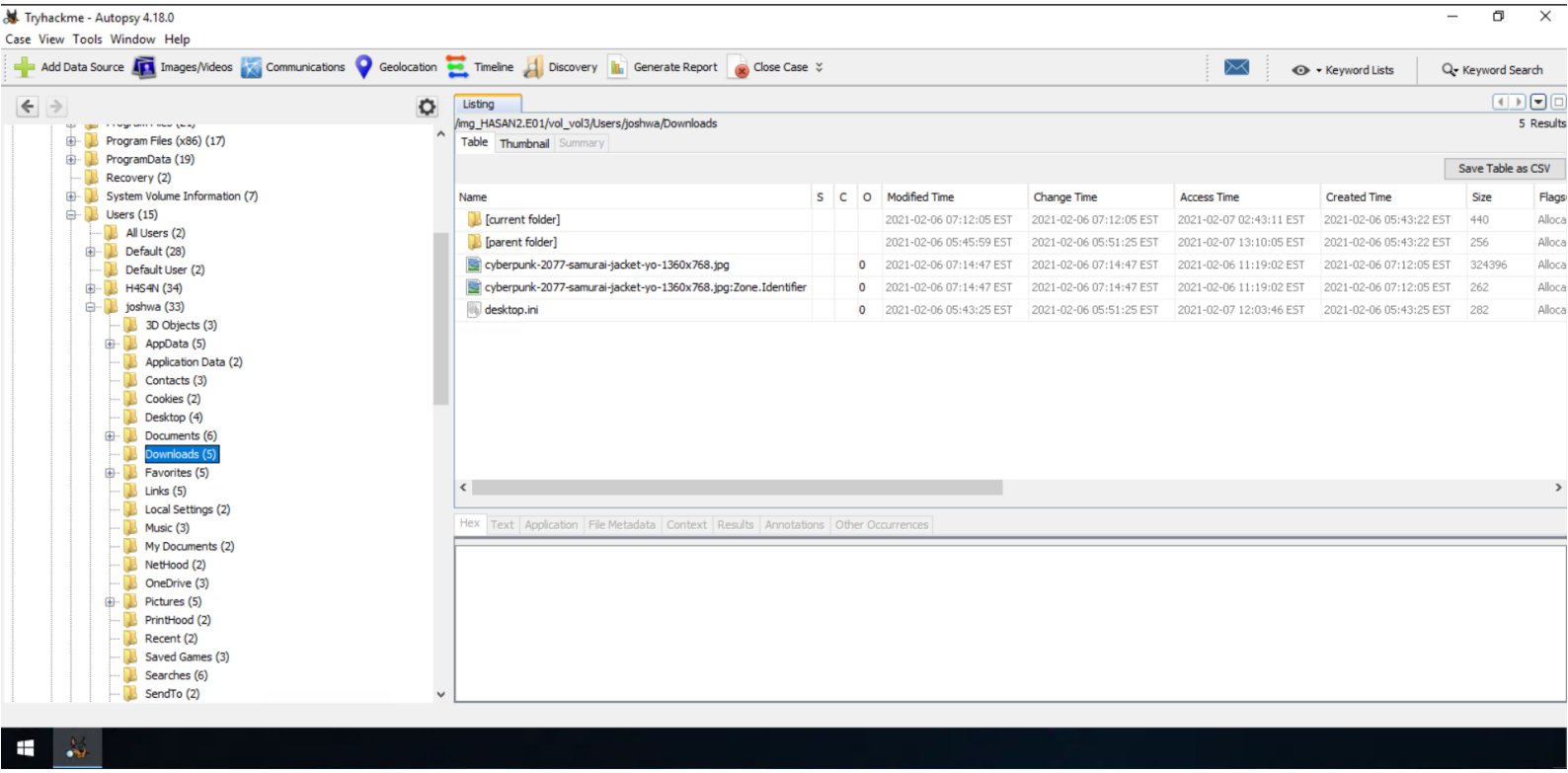
- Autopsy successfully recovered critical forensic evidence such as deleted files and browser activity.
- File metadata provided insights into timestamps and user actions.
- Registry and system logs helped identify user profiles and system configurations.
- The combination of keyword searches, hash filtering, and timeline analysis proved effective in narrowing down artifacts.

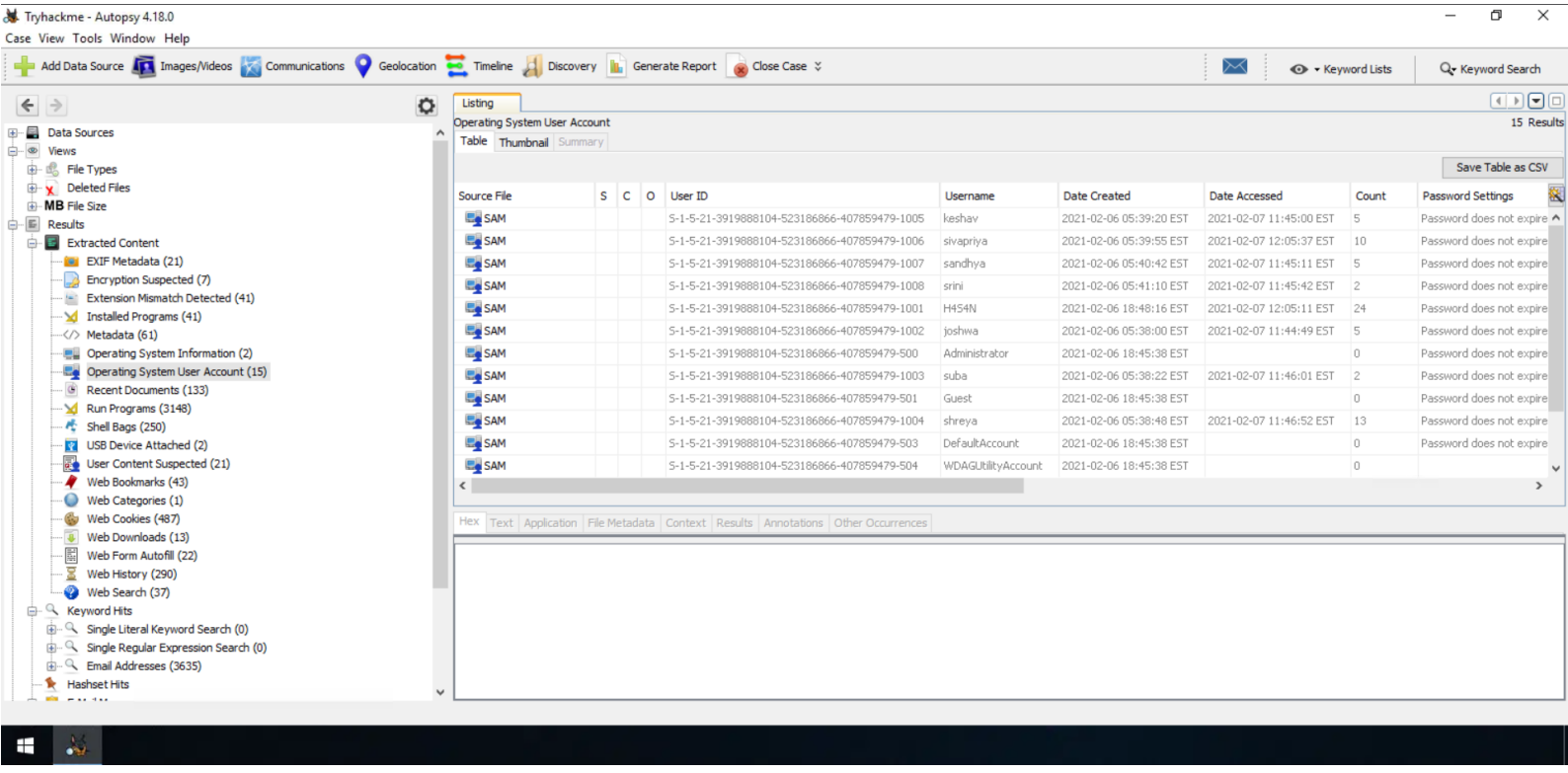
5. Conclusions

- **Lessons Learned**: Practical understanding of Autopsy's modules, case management, and forensic methodologies.
- **Tool Effectiveness**: Autopsy proved to be a powerful tool for disk analysis, supporting multiple artifact extraction techniques.
- **Challenges Faced**: Handling large forensic images required significant system resources; some analysis modules were time-consuming but manageable.

6. References

- TryHackMe Room: Autopsy
- Autopsy Official Documentation: https://www.sleuthkit.org/autopsy/


Tryhackme - Autopsy 4.18.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Program Files (x86) (17)
ProgramData (19)
Recovery (2)
System Volume Information (7)
Users (15)
All Users (2)
Default (28)
Default User (2)
H4S4N (34)
joshwa (33)
3D Objects (3)
AppData (5)
Application Data (2)
Contacts (3)
Cookies (2)
Desktop (4)
Documents (6)
Downloads (5)
Favorites (5)
Links (5)
Local Settings (2)
Music (3)
My Documents (2)
NetHood (2)
OneDrive (3)
Pictures (5)
PrintHood (2)
Recent (2)
Saved Games (3)
Searches (6)
SendTo (2)
Listing
/img_HASAN2.E01/vol_vol3/Users/joshwa/Downloads
5 Results
Table
Thumbnail
Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags
[current folder] 2021-02-06 07:12:05 EST 2021-02-06 07:12:05 EST 2021-02-07 02:43:11 EST 2021-02-06 05:43:22 EST 440 Alloca
[parent folder] 2021-02-06 05:45:59 EST 2021-02-06 05:51:25 EST 2021-02-07 13:10:05 EST 2021-02-06 05:43:22 EST 256 Alloca
cyberpunk-2077-samurai-jacket-yo-1360x768.jpg 0 2021-02-06 07:14:47 EST 2021-02-06 07:14:47 EST 2021-02-06 11:19:02 EST 2021-02-06 07:12:05 EST 324396 Alloca
cyberpunk-2077-samurai-jacket-yo-1360x768.jpg:Zone.Identifier 0 2021-02-06 07:14:47 EST 2021-02-06 07:14:47 EST 2021-02-06 11:19:02 EST 2021-02-06 07:12:05 EST 262 Alloca
desktop.ini 0 2021-02-06 05:43:25 EST 2021-02-06 05:51:25 EST 2021-02-07 12:03:46 EST 2021-02-06 05:43:25 EST 282 Alloca
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences


Tryhackme - Autopsy 4.18.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
Views
File Types
Deleted Files
MB File Size
Results
Extracted Content
EXIF Metadata (21)
Encryption Suspected (7)
Extension Mismatch Detected (41)
Installed Programs (41)
Metadata (61)
Operating System Information (2)
Operating System User Account (15)
Recent Documents (133)
Run Programs (3148)
Shell Bags (250)
USB Device Attached (2)
User Content Suspected (21)
Web Bookmarks (43)
Web Categories (1)
Web Cookies (487)
Web Downloads (13)
Web Form Autofill (22)
Web History (290)
Web Search (37)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (3635)
Hashset Hits
Listing
Operating System User Account
15 Results
Table
Thumbnail
Summary
Save Table as CSV
Source File S C O User ID Username Date Created Date Accessed Count Password Settings
SAM S-1-5-21-3919888104-523186866-407859479-1005 keshav 2021-02-06 05:39:20 EST 2021-02-07 11:45:00 EST 5 Password does not expire
SAM S-1-5-21-3919888104-523186866-407859479-1006 sivapriya 2021-02-06 05:39:55 EST 2021-02-07 12:05:37 EST 10 Password does not expire
SAM S-1-5-21-3919888104-523186866-407859479-1007 sandhya 2021-02-06 05:40:42 EST 2021-02-07 11:45:11 EST 5 Password does not expire
SAM S-1-5-21-3919888104-523186866-407859479-1008 srini 2021-02-06 05:41:10 EST 2021-02-07 11:45:42 EST 2 Password does not expire
SAM S-1-5-21-3919888104-523186866-407859479-1001 H4S4N 2021-02-06 18:48:16 EST 2021-02-07 12:05:11 EST 24 Password does not expire
SAM S-1-5-21-3919888104-523186866-407859479-1002 joshwa 2021-02-06 05:38:00 EST 2021-02-07 11:44:49 EST 5 Password does not expire
SAM S-1-5-21-3919888104-523186866-407859479-500 Administrator 2021-02-06 18:45:38 EST 0 Password does not expire
SAM S-1-5-21-3919888104-523186866-407859479-1003 suba 2021-02-06 05:38:22 EST 2021-02-07 11:46:01 EST 2 Password does not expire
SAM S-1-5-21-3919888104-523186866-407859479-501 Guest 2021-02-06 18:45:38 EST 0 Password does not expire
SAM S-1-5-21-3919888104-523186866-407859479-1004 shreya 2021-02-06 05:38:48 EST 2021-02-07 11:46:52 EST 13 Password does not expire
SAM S-1-5-21-3919888104-523186866-407859479-503 DefaultAccount 2021-02-06 18:45:38 EST 0 Password does not expire
SAM S-1-5-21-3919888104-523186866-407859479-504 WDAGUtilityAccount 2021-02-06 18:45:38 EST 0
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences