Case Study Analysis

Student Name:Laraib Rashid

Contents

[Case study questions 3](#_Toc204552162)

[Question 3](#_Toc204552163)

[Question 3](#_Toc204552164)

[Question 4](#_Toc204552165)

[Question 7](#_Toc204552166)

[Question 7](#_Toc204552167)

[Question 8](#_Toc204552168)

[Question 9](#_Toc204552169)

[Question 9](#_Toc204552170)

[Question: 10](#_Toc204552171)

[Question 11](#_Toc204552172)

[Report 11](#_Toc204552173)

[Tools Used 11](#_Toc204552174)

[Data Acquisition: 12](#_Toc204552175)

[Vlidation and Analysis: 12](#_Toc204552176)

[Limitations Encountered 12](#_Toc204552177)

[References 12](#_Toc204552178)

## Case study questions

Question

What is the image hash? If you are informed that the verification hash is AFF4ECD9301D03C3D054623CD261959A, what would the hash comparison imply?

#### Answer:

The image hash refers to a unique digital fingerprint of a file, which is generated by using the cryptographic hash functions. These functions can be either MD5 , SHA-1 , or SHA-256. Hashes play a vital roleto ensure data integrity and is commonly used in digital forensics and cybersecurity investigations t verify the file and has not been altered.

[1] [2]

Question

What is the current installed operating system? When and how was the earliest operating system installed?

#### Answer:

After examining the image file in Autopsy , discovered the Operating System information was not parsed correctly. All the necessary ingestion modules were checked however the registry keyw as never populated.

Further inspection of “WINDOWS/system32/config32” reveal the “Setup.TXT” which is a standard forensic artifact. Reviewing the metadata for this files reveals current Operating system is Microsoft Windows XP and it was creted on “2004-08-20 at 03:02:22 AEST”

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

### Question

List all active account names (skip the system accounts: Administrator, Guest, sys- temprofile, LocalService, NetworkService), login count, date of creation, system privilege level, and password settings.

#### Answer:

Investigated SAM , SECURITY and SYSTEM hive as initial ingestion did not reveal the account names.However, reingestion with different ingestion module provided the below information

Secondly, exported the SAM hive and uploaded to Registry edit to review the Extracted password policy which is from the “F value”

[3] [4] [5]

**User Accounts**

|  |  |  |
| --- | --- | --- |
| Name | Login Name | Creation Time |
| S-1-5-21-2000478354-688789844-1708537768-1003 | Mr.evil | 2004-08-20 09:03:54 AEST |

Password Policy

|  |  |  |
| --- | --- | --- |
| **Policy Setting** | **Value** | **Interpretation** |
| **Minimum Password Length** | 12 (hex) → **18 (decimal)** | Users must set passwords with at least **18 characters**. |
| **Maximum Password Age** | 30 99 3E E1 0D 86 C4 01 | **42 days** (converted from 64-bit FILETIME format) |
| **Password History Length** | 80 CC 1D CF FB FF FF FF | **1 day** (converted from FILETIME format) |
| **Lockout Threshold** | 00 (hex) → **0** | No password history is enforced. |

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

### Question

What applications were installed by the suspect within 48 hours after installing the latest operating system?

#### Answer:

Based on the contents of the csv file exported from the Autopsy , the following applications appear to have been installed or modified within the 48 hour window.

**Microsoft Internet Explorer**

* /Program Files/Internet Explorer/IE4.DLL
* /Program Files/Internet Explorer/IEDETECT.DLL
* /Program Files/Internet Explorer/Connection Wizard/ICWOOBE.EXE

**Microsoft Data Access Components (MDAC)**

* /Program Files/Common Files/SYSTEM/ADO/ADOAPT15.REG
* /Program Files/Common Files/SYSTEM/ADO/ADOFRE15.REG
* /Program Files/Common Files/SYSTEM/MSADC/...

**Microsoft System Information Tools**

* /Program Files/Common Files/Microsoft Shared/MSINFO/MSIAV.OCX
* /Program Files/Common Files/Microsoft Shared/MSINFO/MSIPRINT.OCX
* /Program Files/Common Files/Microsoft Shared/MSINFO/TXTVIEW.OCX

**Microsoft Web Folders and FrontPage Extensions**

* /Program Files/Common Files/Microsoft Shared/Web Folders/RAGENT.DLL
* /Program Files/Common Files/Microsoft Shared/Web Server Extensions/40/BIN/FP4ANWI.DLL

**MSN Online Services**

* /Program Files/Online Services/MSN50/MSNBOOT.EXE
* /Program Files/Online Services/MSN50/MSN50.CAB

**Microsoft Plus! System Agent**

* /Program Files/PLUS!/SYSAGENT.EXE

A screenshot of a video

AI-generated content may be incorrect.

### Question

In which directories or file paths do web browser history related files reside? From the web browsers, list every keyword searched and URLs with their Timestamp.

#### Answer:



A screenshot of a computer

AI-generated content may be incorrect.

### Question

Which Domains were accessed by the suspect between 09:00 and 18:00? (Provide Domain and Domain first access timestamp.)

#### Answer:

|  |  |
| --- | --- |
| **Domain** | **Date Accessed** |
| ethereal.com | 2004-08-27 15:11:13 AEST |
| ethereal.com | 2004-08-27 15:11:33 AEST |
| depaul.edu | 2004-08-27 15:17:15 AEST |
| maktoob.com | 2004-08-27 15:43:19 AEST |
| netstumbler.com | 2004-08-27 15:09:54 AEST |
| msn.com | 2004-08-27 15:42:54 AEST |
| ethereal.com | 2004-08-27 15:10:50 AEST |
| ethereal.com | 2004-08-27 15:10:50 AEST |
| wardriving.com | 2004-08-27 15:09:23 AEST |
| wardriving.com | 2004-08-27 15:09:30 AEST |
| msn.com | 2004-08-27 15:09:12 AEST |
| wardriving.com | 2004-08-27 15:09:23 AEST |
| maktoob.com | 2004-08-27 15:43:19 AEST |
| netstumbler.com | 2004-08-27 15:09:54 AEST |
| ethereal.com | 2004-08-27 15:11:13 AEST |
| netstumbler.com | 2004-08-27 15:10:00 AEST |
| netstumbler.com | 2004-08-27 15:11:07 AEST |
| wardriving.com | 2004-08-27 15:09:27 AEST |

### Question

Where are Volume Shadow Copies stored? When were they created?

#### Answer:

A typical path for Volume Shadow Copies location is C:\System Volume Information

[6]

### Question

What was the e-mail account and account ID used by the suspect? What evidence can you provide to directly link this account to the suspect?

#### Answer:



A screenshot of a computer

AI-generated content may be incorrect.

### Question:

What kinds of data are stored in the Windows Search database?

#### Answer:

Windows typically stores its database as Windows.edb file. However, the encase image could not parse that information and used different Eric Zimmerman’s tool to bypass that but no artifacts were foud, See screenshot as proof.

A screenshot of a computer

AI-generated content may be incorrect.

### Question

List external storage devices attached to the notebook. How might you determine if files were copied from the notebook to the USB drive?

#### Answer:

Investifate registrey key which stores information related to usb devices attached to the device.

|  |  |  |
| --- | --- | --- |
| Name | Type | Value |
| Capabilities | REG\_DWORD | 0x00000080 (128) |
| UINumber | REG\_DWORD | 0x00000000 (0) |
| HardwareID | REG\_MULTI\_SZ | USB\ROOT\_HUB&VID8086&PID7112&REV0001, USB\ROO.. |
| Service | REG\_SZ | 0x00000400 (1024) |
| ConfigFlags | REG\_DWORD | 0x00000400 (1024) |

## Report

## Tools Used

Autopsy 4.22.1: Used for initial analysis of disk images and registry hives.

Registry Explorer v2.1.0: Employed for deep inspection of registry keys and binary values.

VSCMount 1.5.0: Utilized to mount and explore Volume Shadow Copies (VSCs) for historical data recovery.

### Data Acquisition:

Disk images and registry hives were extracted from the portal.

Volume Shadow Copies were mounted using VSCMount to access historical snapshots.

## Vlidation and Analysis:

Autopsy parsed standard artifacts such as user accounts, USB history, and file system metadata.

Registry Explorer was used to manually inspect keys like SAM\Domains\Account to extract password policy from the F value.

VSCs provided access to older registry states and deleted data.

## Limitations Encountered

Encrypted Files: Autopsy was unable to analyze certain files due to encryption, resulting in missing artifacts.

Parser Gaps: Many registry-based artifacts were not parsed by Autopsy, requiring manual inspection using Registry Explorer.

Incomplete Shadow Copy Parsing: VSCMount allowed access, but some data required manual correlation due to lack of automated parsing.

# References

|  |  |
| --- | --- |
| [1] | D. Team, “Hash Functions in Digital Forensics: Best Practices,” Daisie, 07 August 2003. [Online]. Available: https://blog.daisie.com/hash-functions-in-digital-forensics-best-practices/. [Accessed 22 July 2025]. |
| [2] | A. Seth, “Importance of using MD5 and SHA1 Hash Algorithms in Digital Forensics,” Stellar, 20 August 2024. [Online]. Available: https://www.stellarinfo.com/blog/hash-values-in-digital-forensics/. [Accessed 21 July 2025]. |
| [3] | O. C. M. E. &. R. L. Heather Barnhart, “FOR500: Windows Forensic Analysis,” SANS, 07 February 2023. [Online]. Available: https://www.sans.org/posters/windows-forensic-analysis. [Accessed 21 July 2025]. |
| [4] | C. D. Alwis, “Windows Registry Analysis 101,” 05 April 2019. [Online]. Available: https://www.forensicfocus.com/articles/windows-registry-analysis-101/. [Accessed 22 July 2025]. |
| [5] | F. Focus, “A guide to RegRipper and the art of timeline building,” Forensic Focus, 25 September 2014 . [Online]. Available: https://www.forensicfocus.com/articles/a-guide-to-regripper-and-the-art-of-timeline-building/. [Accessed 21 July 2025]. |
| [6] | Microsoft, “Volume Shadow Copy Service (VSS),” Microsoft, 07 July 2025. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service. [Accessed 21 July 2025]. |