COMP6845 Report 1

Antheo Raviel Santosa

Term 2, 2024

Contents

1 Introduction

1.1 Background

1.1.1 Jim's Forensics (JF) have been engaged by Penelope Legal (PL) in relation to proceedings with Caelus Engineering (CE).

1.1.2 On the 14^{th} of September, 2021, PL instructed JF by letter containing a series of instructions on which we were to proceed.

1.2 My instructions

1.2.1 As a result of the above engagement, on the 14^{th} of September, 2021, PL advised me to prepare a report addressing the following issues:

(a) **Question 1** - Does the data on the laptop provide any indications regarding the reason for its destruction and disposal? If so, what?

(b) **Question 2** - Is there any indication of an attempt to "cover tracks", such as deleting or obscuring data?

(c) **Question 3** - Is there any indication of hidden data, *i.e.*, encryption? If so, are you able to make the data usable?

(d) Any other matters that are relevant to the use or misuse of the laptop?

(e) Has the additional information changed opinions on the events which occurred?

(f) Your recommendation regarding any further enquiries and examinations that needed to be conducted.

1.3 Provided materials

1.3.1 We are provided the following materials from which we are to base our investigations on:

(a) a raw image of the hard disk of Alyx Hamilton's laptop,

(b) a photo of the collection site, and

(c) profiles of the staff at Caelus Engineering.

1.4 Qualifications

1.4.1 I am a second year computer science student at the University of New South Wales, currently enrolled in the COMP6845 course, otherwise known as *Extended Digital Forensics*.

1.5 Information relied upon

1.5.1 I have relied upon the following information in the preparation of my report:

(a) a letter containing instructions addressed to JF dated 14^{th} of September, 2021,

(b) a second letter containing further instructions addressed to JF,

(c) an image of the storage of the laptop used by Alyx Hamilton,

(d) a dump of the memory of the laptop used by Alyx Hamilton,

(e) copies of the logs of the email correspondence of Alyx Hamilton and Michael Harris,

(f) a copy of the network traffic capture data from Alyx Hamilton's laptop, as well as a log of the TLS keys necessary to decrypt the data,

(g) a screenshot of the CCTV overlooking the entry gates at Caelus Engineering,

(h) a copy of the logs of the entry and exit of personnel from the gates at Caelus Engineering,

(i) a photo of the collection site, and

(j) profiles of the staff at Caelus Engineering.

1.6 Disclaimer

1.6.1 I have made all inquiries which I believe are desirable and appropriate for the purposes of this report. There are no matters of significance which I regard as relevant to my opinions which have been withheld.

1.6.2 This report has been prepared solely for the use of PL. In accordance with the usual practice of JF, I expressly disclaim all responsibility to any other person or entity (other than the Court) for any reliance on the content of this report. This report should not be copied or distributed to any other person or entity, other than in connection with the above matter.

1.7 Assumptions

1.7.1 In preparing this report, I have made the following assumptions:

(a) the information described in the background section above is accurate, and

(b) the computers identified by CE, and subsequently imaged, were used by Alyx Hamilton.

Table 1: Google Drive URLs accessed

Date accessed	Title	URL
2020-09-04 14:31:21 AEST	PROJECTS 19:20 - Google Drive	https://drive.google.com/drive/folders/1S7ETsR
2020-09-04 14:27:57 AEST	Shared Drive - Google Drive	https://drive.google.com/drive/folders/1sinCWR
2020-09-04 14:27:55 AEST	Shared with me - Google Drive	https://drive.google.com/drive/shared-with-me

1.8 Structure of this report

1.8.1 The remaining sections of this report addresses the following:

(a) In Section 2, I set out information with respect to Question 1 above;

(b) In Section 3, I set out information with respect to Question 2 above;

(c) In Section 4, I set out information with respect to Question 3 above;

(d) In Section 5, I set out information with respect to Question 4 above;

(e) In Section 6, I set out information with respect to Question 5 above;

(f) In Section 7, I set out information with respect to Question 6 above;

1.8.2 For convenience, I note that I have organised my findings in the same order as the questions outlined in my letter of instruction. I have also included questions, in some instances paraphrased, from the letter of instruction before presenting my corresponding findings. Additionally, I have referred to the appropriate section number as contained in the letter of instruction in my responses.

2 Question 1: Reason for destruction

2.1 Procurement and extraction of evidence

2.2 Extraction of evidence

2.2.1 This section describes the method with which the evidence laid out in the rest of this report is procured.

2.2.2 A disk image is a digital replica of the contents of a physical drive, including any unallocated space.

2.2.3 I note that there are no additional cryptographic hashes provided with the disk image, nor is the disk image formatted in a forensically admissible format (such as E01).

2.2.4 I extracted the information presented from this point onwards from the provided disk image using the Autopsy forensics toolkit.

2.3 Email

2.3.1 I note the existence of an email from `alyx.hamilton@caelusengineering.com.au` sent to the address `johndavis5891@gmail.com` at 2020-09-04 16:27:18 AEST with the subject: *"It's done"*. Some notable details include:

(a) The body of the email contains only the following line: *"The files are copying over as we speak. What should I do now? Where do I meet you?"*.

(b) The email is found on the `\\Root - Mailbox\IPM_SUBTREE\[Gmail]\Bin`.

(c) This email is the only correspondence found between Alyx Hamilton and `johndavis5891@gmail.com`.

(d) This email is the last email found on the disk image of Alyx Hamilton's laptop

2.4 Accessing Google Drive

2.4.1 Some of the most web history on the device displays the rapid access of various pages in the Google Suite. These are briefly listed in Table 1

Table 2: List of attached external USB drives

No.	Device make	Device model	Device ID	Date/Time
1	SanDisk Corp.	Cruzer Blade	4C530300831216101192	2020-09-04 10:11:55 AEST
2	SanDisk Corp.	Product: 55A5	4C530000050910115114	2020-09-04 15:50:09 AEST

2.5 Attached USB drives

2.5.1 Table 2 details the make, model, and ID of two external USB drives that are recorded to have been connected to this device, as well as the time they were attached.

2.6 Discussion

The email found on 2.2.1 appears to be suspicious from multiple aspects. The most noticeable among which is its cryptic language. Furthermore, the recipient is not an address within Caelus Engineering, nor is it one which otherwise appears in other emails in Alyx Hamilton's mailbox. Lastly, the email is found in the `Bin` directory, which indicates attempts at hiding it.

The web activity discussed in 2.3.1 were also found to be within temporal proximity of the email discussed above. They directly precede the web history entry belonging to said email. The site accessed, belonging to "Google Drive" and "Google Docs", are benign, but may be used as a method of exfiltrating data.

Likewise, the external USB devices that are noted to have been connected to the device in 2.4.1 are occurences that are otherwise benign, but may be used as a method of exfiltrating data.

3 Question 2: Covering tracks

3.1 Deleted email

3.1.1 The email discussed previously in 2.2.1 was found on the folder `\\Root - Mailbox\IPM_SUBTREE\[Gmail]\Bin`, which indicates an attempt at deleting the email.

3.2 Deleted project archives

3.2.1 ZIP archives containing what appears to be project files appear to have been deleted and are found in the 'Recycle Bin', as can be seen in Figure 4 in the appendix.

4 Question 3: Further evidence

4.0.1 Event log with records of file transfers to external drive with the laptop.

4.0.2 Information on the entity associated with the email address `johndavis5891@gmail.com`.

4.0.3 Information regarding the standard activity at Caelus Engineering, which would assist in identifying 'out of place' observations.

5 Appendix

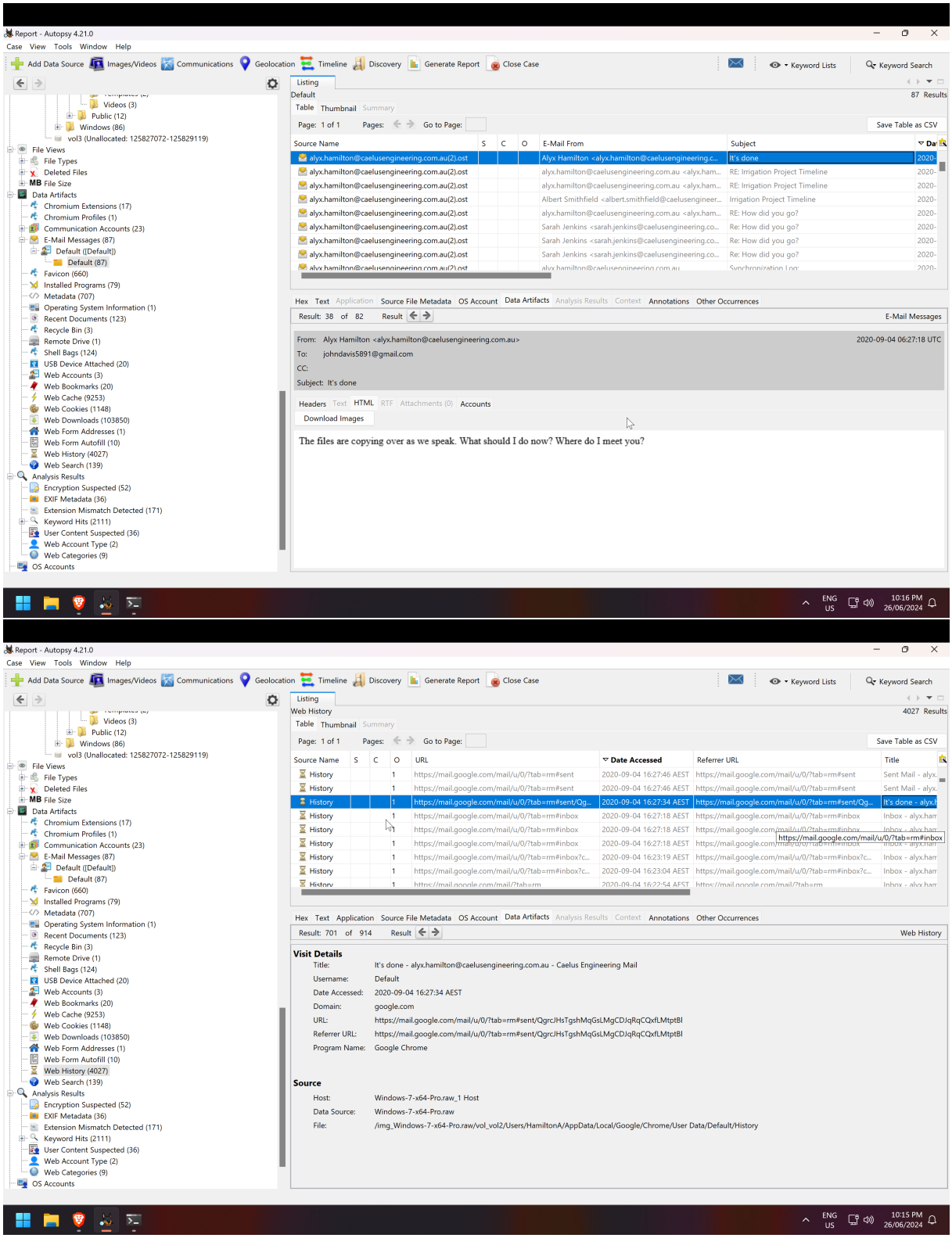


Figure 1: Cryptic email

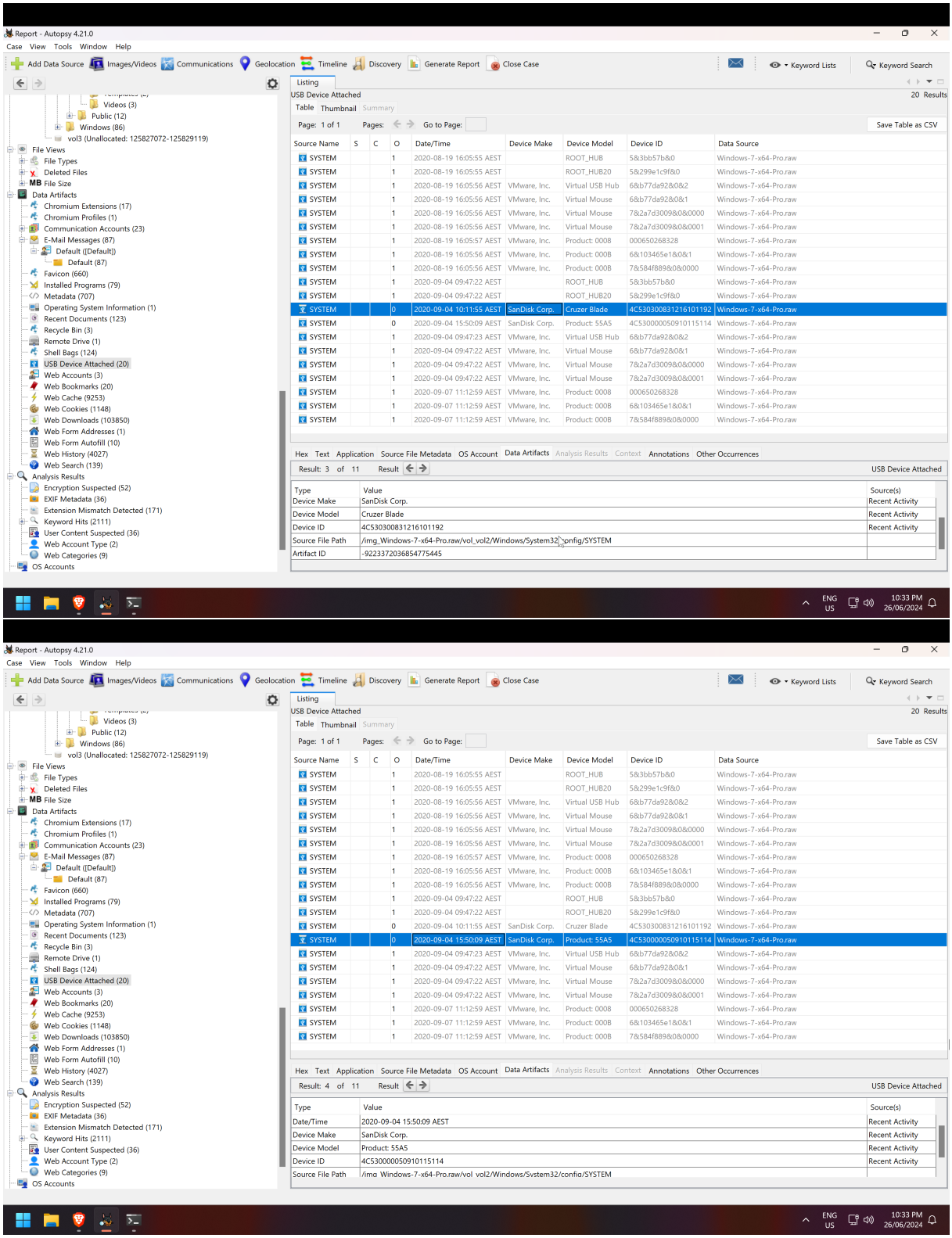
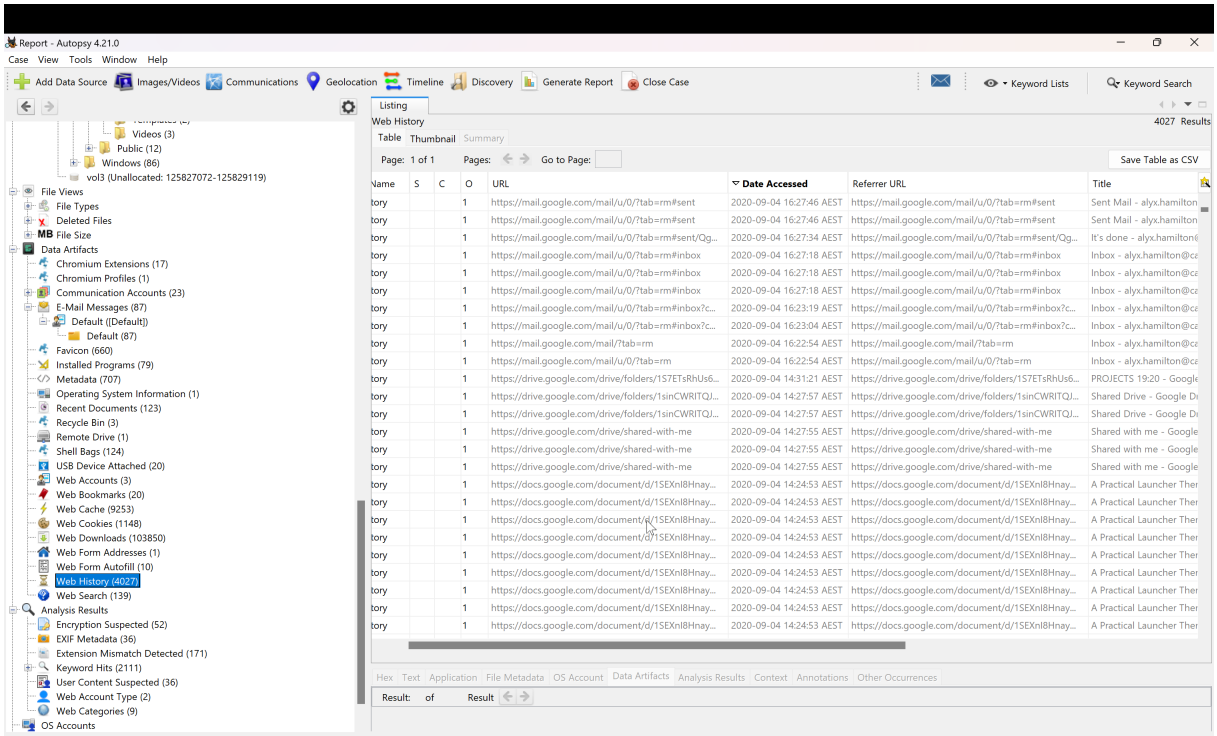
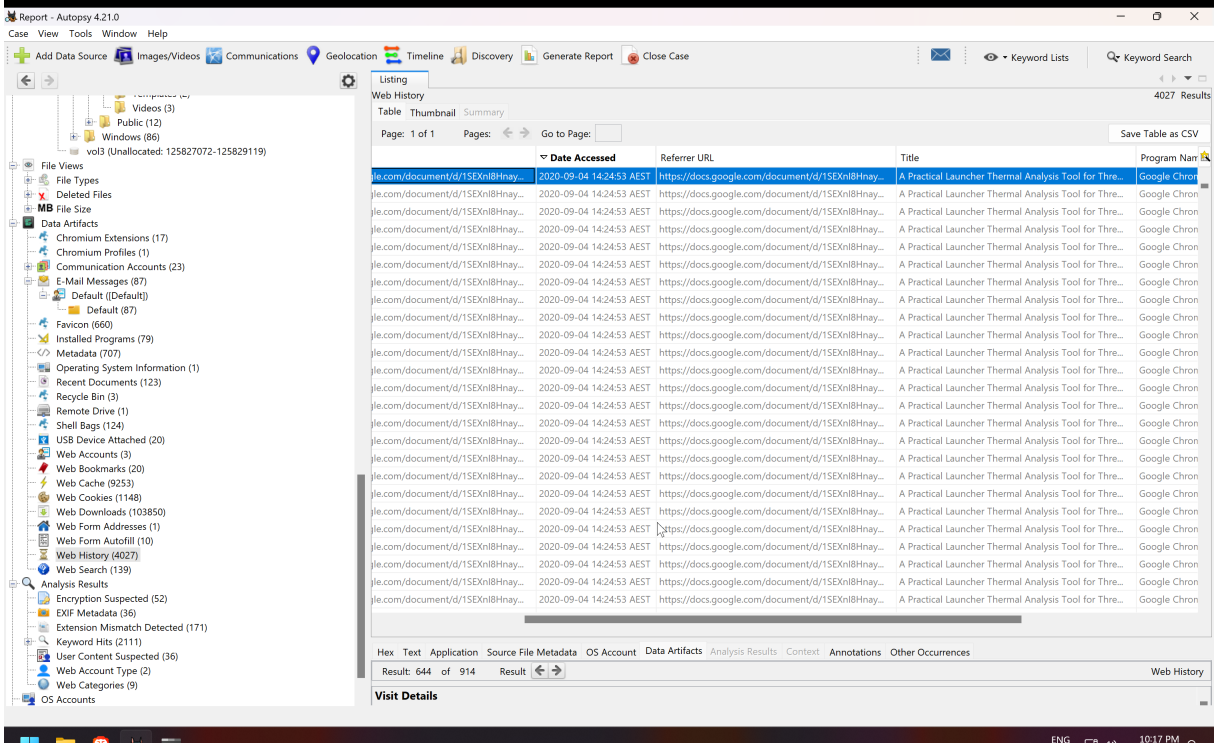
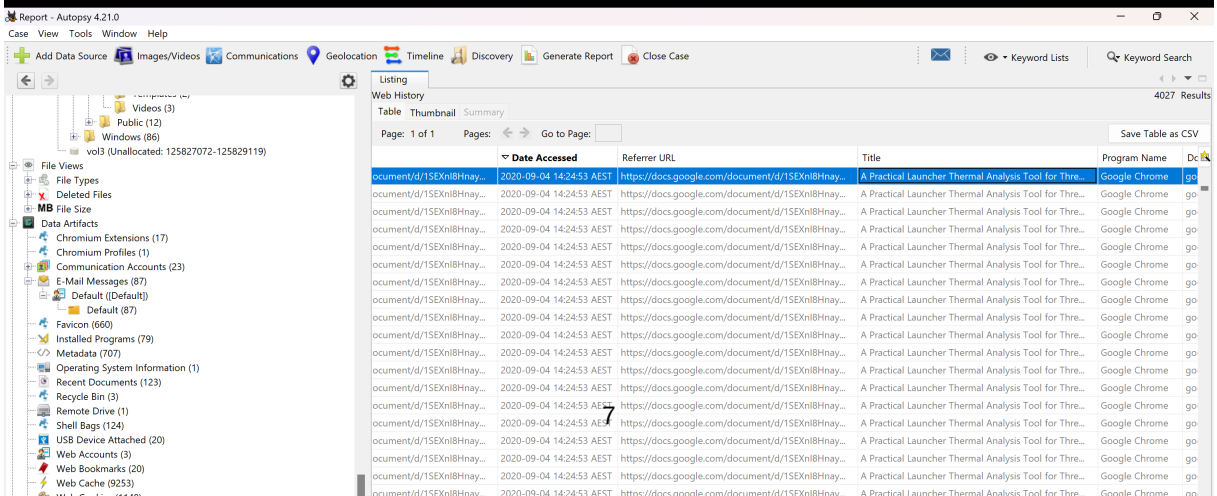


Figure 2: Attached USB drives


Report - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Web History
4027 Results
Table Thumbnail Summary
Page: 1 of 1 Pages: Go to Page:
Save Table as CSV
Name S C O URL Date Accessed Referrer URL Title
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: of Result
ENG US 10:17 PM 26/06/2024


Report - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Web History
4027 Results
Table Thumbnail Summary
Page: 1 of 1 Pages: Go to Page:
Save Table as CSV
Date Accessed Referrer URL Title Program Name
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 644 of 914 Result
Web History
Visit Details
ENG US 10:17 PM 26/06/2024


Report - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Web History
4027 Results
Table Thumbnail Summary
Page: 1 of 1 Pages: Go to Page:
Save Table as CSV
Date Accessed Referrer URL Title Program Name

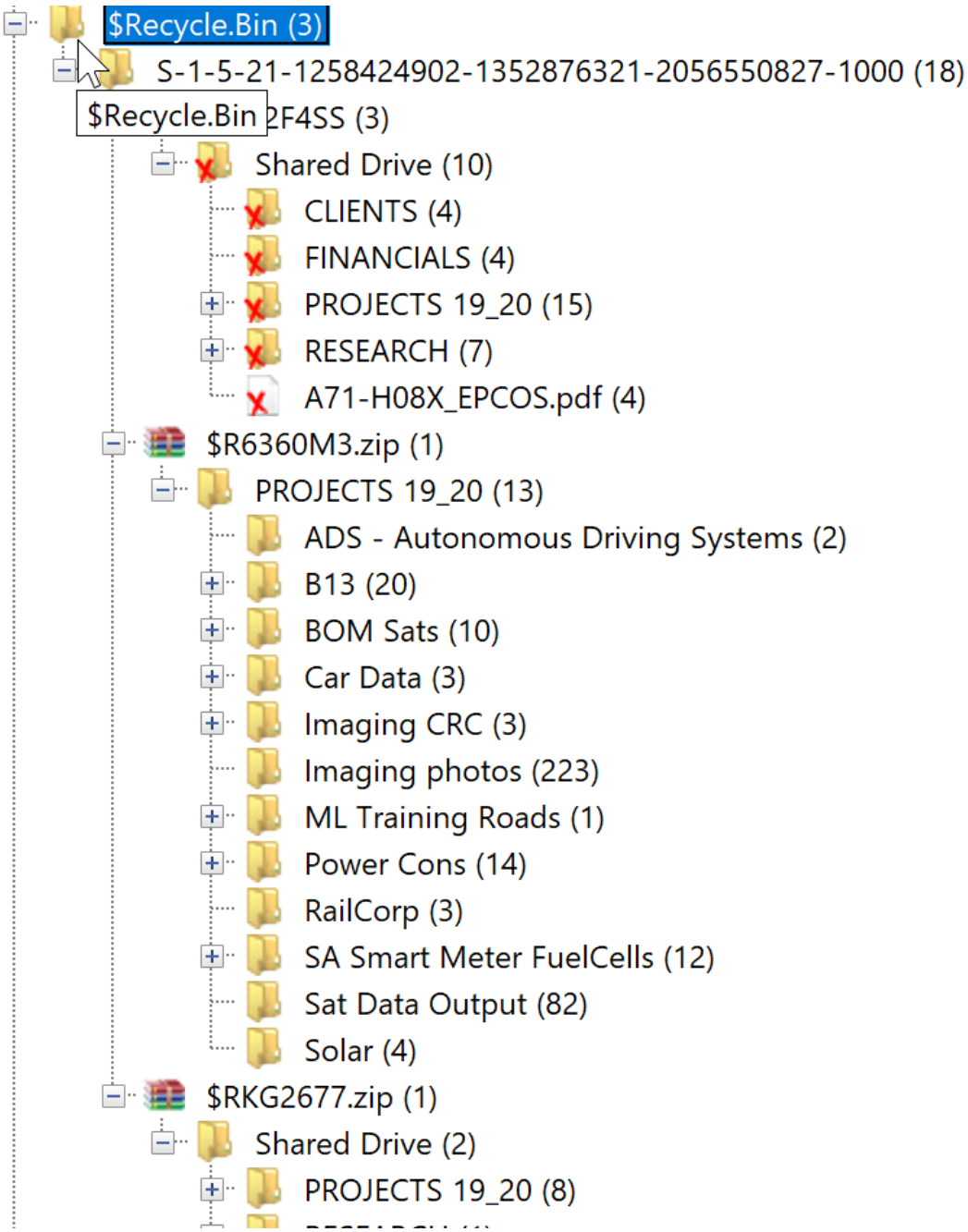


Figure 4: Recycling bin