2020-11-13

Caelus Engineering Case

Jim's Forensics

Content

1. Preliminary

1.1 I am Yanning Cao whose address is 6845 Forensics Road, Sydney, in the State of New South Wales undertaking the Bachelor of Electrical Engineering (honours) and Bachelor of Science (Computer Science) with a major in Security Engineering.

1.2 I have taken Security Engineering courses including: Extended Security Engineering and Cyber Security (COMP6841), and I'm currently enrolled in Extended Digital Forensics and Incident Response (COMP6845).

1.3 I have taken numerous computer courses such as Operating Systems (COMP3231), Algorithms and Programming Techniques (COMP3121) and Object-Oriented Design & Programming (COMP2511).

2. Case background and instructions

2.1 An Adelaide Company: Caelus engineering which mainly contract to other engineering firms on industrial projects has reported that one of their employee's laptop (Alyx Hamilton) has gone missing.

2.2 The missing laptop was found in bin of a commercial building a few blocks away from Caelus engineering which is located at King William St. It is heavily damaged when the staff member discovered it. Most of the asset tags of the computer had been removed.

2.3 The staff member in question is Alyx Hamilton as she might be the owner of the laptop and has expressed discontent several times.

2.4 The laptop contains sensitivity information on some projects which worth millions of dollars.

2.5 I have been instructed by Penelope Legal to perform analysis on the evidence retrieve from the company and prepare a report addressing the following issues:

a) Question 1 - Was the laptop being used by a Caleus Engineering staff member(s)?

b) Question 2 - Does the data on the laptop provide any indications regarding the reason for its destruction and disposal? If so, what?

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

d) Question 4 - Is there any indication of an attempt to "cover tracks", such as deleting or obscuring data?

e) Question 5 - Any other matters that are relevant to the use or misuse of the laptop?

f) Question 6 - Your recommendation regarding any further enquiries and examinations that need to be conducted.

2.6 A copy of the engagement letter is attached as Appendix A.

3. Assumptions and Limitations

3.1 Assumptions:

a) Assume the permission to access the data has been granted legally.

b) Assume all the data were obtained in the legal and formal procedure.

c) Assume chain of custody of all evidence has been maintained.

d) Assume evidence integrity has been maintained.

3.2 Limitations:

a) Limited funding/tools have been provided otherwise can get more precise information.
b) Can't gain access to physical evidence.
c) Search warrant has not been granted, may contain more information on their personal devices.

4. Disclaimer

4.1 I believe all my Investigation are appropriate for the purpose of this report. There are no matters of significance I considered as relevant to my views which has been withheld.
4.2 I have not conducted an audit of the information or other documents provided to me. I assume all the information provided to me is accurate and reliable unless stated.

5. Summary of POI and evidence

Suspects:

Name	Connection	Role
Michael Harris	John Davis's spy inside Caleus Engineering	Caleus Engineering's Systems Engineer
Alyx Hamilton	Michael's colleague	Caleus Engineering's Senior Business Analyst
John Davis	Cameron's colleague	
Cameron	John's colleague	

Evidence:

Name	Hash(md5)	Description
Windows-7-x64-Pro.raw	402373d94991b7c303b53ba1da62d10b	Missing laptop's image
hamiltona_network_log.pcapng	45330b81a6a3c0b7cc5dfd4428e1e737	Alyx Hamilton's Network activity
Harris.zip	7fb60c6dff0640db3fbee8666b5f7d14	Michael Harris's work email activity
Hamilton.zip	d9b6d861038977145e219354a215b4c1	Alyx Hamilton's work email activity
phone_drops.zip	92d62ae5b2900494079cf2e43c156e56	Spys' phones image
Windows-7-x64-Pro-Snapshot7.vmem	2afc0bd393be75c9492ff32f51a20c77	Memory dump of lost computer

5.1 All the data have been hashed before the investigation and rehashed after the investigation to ensure the data integrity has been maintained.

5.2 All the hash was generated by performing the 'md5sum' command. A hash is a function that converts one value to another. A hash of a file maps all the original data to another value. If the content of the file changes, the hash will change as well. It can be use to validate the integrity of the forensics copy.

5.3 The md5sum commands provide an algorithm to convert a file into a hash without changing the file's original content.

6. Structure of this report

7.1 The remaining sections of this report address the following:

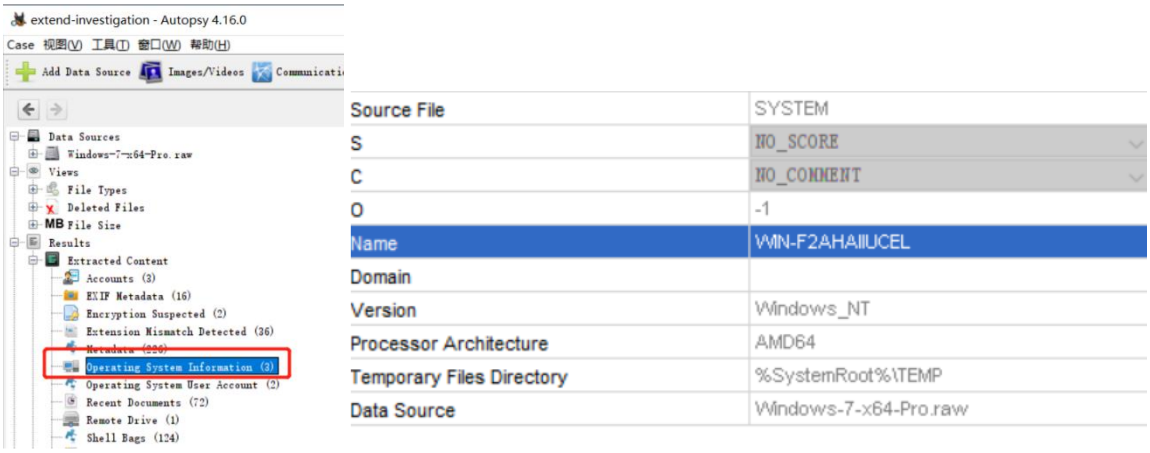
a) In section 8, I set out information regarding Question 1 above.
b) In section 9, I set out information regarding Question 2 above.
c) In section 10, I set out information regarding Question 3 above.
d) In section 11, I set out information regarding Question 4 above.
e) In section 12, I set out information regarding Question 5 above.
f) In section 13, I set out information regarding Question 6 above.
g) In section 14, reliability of time across evidence have been explained and further explain who use the laptop after the laptop went missing.

7. Question 1

8.1 The laptop is used by a Caleus Engineering staff and I think the owner of the laptop is Alyx Hamilton (on the balance of probabilities). I reached this conclusion by analyse the image (an exact replica of the contents of a computer) of the Caleus Engineering's missing computer provided by Penelope Legal and using autopsy (4.16.0) to analysis the image. Autopsy is a free digital forensics platform and graphical interface to forensics tools which helps law enforcement, military, and corporate examiners to investigate what happened on a computer. The detail of the image is provided below.

8.2 The system information is obtained through autopsy, under the Extracted content section, Operating System Information part.

Figure 1 operating system information



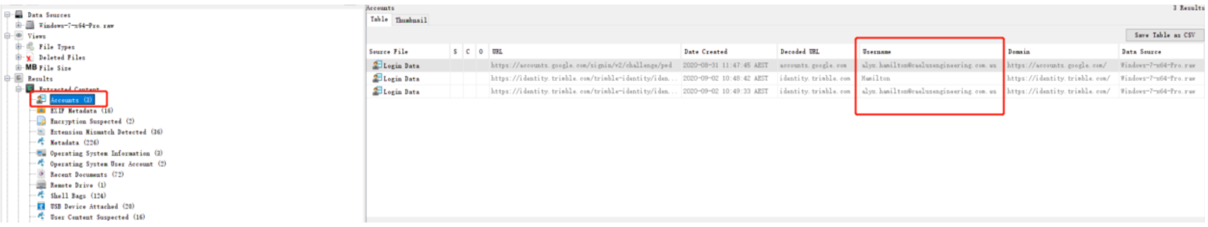
Source File	SYSTEM
S	NO_SCORE
C	NO_COMMENT
O	-1
Name	WIN-F2AHAIIUCEL
Domain	
Version	Windows_NT
Processor Architecture	AMD64
Temporary Files Directory	%SystemRoot%\TEMP
Data Source	Windows-7-x64-Pro.raw

8.3 First, in autopsy, Extracted Content Section, Accounts part have 3 files, which contains login information of 3 websites. The information of the files were present below.

Table 1 Files and hashed

Name	Hash(MD5)
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Local/Google/Chrome/User Data/Default/Login Data	530418eebd294f4ffb6d7390e8e79ca2
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Local/Google/Chrome/User Data/Default/Login Data	530418eebd294f4ffb6d7390e8e79ca2
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Local/Google/Chrome/User Data/Default/Login Data	530418eebd294f4ffb6d7390e8e79ca2

Figure 2 Accounts



Source File	S	C	O	URL	Date Created	Decoded URL	Username	Domain	Data Source
Login Data				https://accounts.google.com/signin/v2/challenge/pwd	2020-08-31 11:47:45 AEST	accounts.google.com	alyx.hamilton@caelusengineering.com.au	https://accounts.google.com/	Windows-7-x64-Pro.raw
Login Data				https://identity.trimble.com/trimble-identity/iden...	2020-09-02 10:48:42 AEST	identity.trimble.com	Hamilton	https://identity.trimble.com/	Windows-7-x64-Pro.raw
Login Data				https://identity.trimble.com/trimble-identity/iden...	2020-09-02 10:49:33 AEST	identity.trimble.com	alyx.hamilton@caelusengineering.com.au	https://identity.trimble.com/	Windows-7-x64-Pro.raw

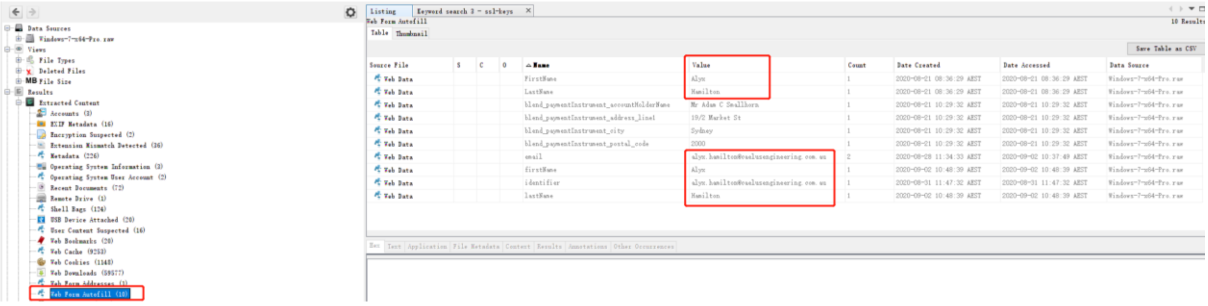
8.4 As the screenshot showed above the owner of this laptop use alyx.hamilton @caelusengineering.com.au to log in to both google.com and trimble.com.

8.5 Second, under the Extracted content, Web Form Autofill section, several files may indicate that the owner is Alyx. A web form is an HTML form on a web page that lets visitors enter their information the autofill function is a build-in function in browser like google chrome which memorize certain information such as name and addresses so that the browser can fill the web form automatically. The details of the files were presented below.

Table 2 Web autofill

Name	Hash(MD5)	Type	Value
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Local/Google/Chrome/User Data/Default/Web Data	3b1308a73a00d10a57ea44483145ff17	FirstName	Alyx
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Local/Google/Chrome/User Data/Default/Web Data	3b1308a73a00d10a57ea44483145ff17	LastName	Hamilton
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Local/Google/Chrome/User Data/Default/Web Data	3b1308a73a00d10a57ea44483145ff17	email	alyx.hamilton@caelusengineering.com.au
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Local/Google/Chrome/User Data/Default/Web Data	3b1308a73a00d10a57ea44483145ff17	identifier	alyx.hamilton@caelusengineering.com.au
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Local/Google/Chrome/User Data/Default/Web Data	3b1308a73a00d10a57ea44483145ff17	firstname	Alyx
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Local/Google/Chrome/User Data/Default/Web Data	3b1308a73a00d10a57ea44483145ff17	Lastname	Hamilton

Figure 3 Web autofill



Web Form Autofill

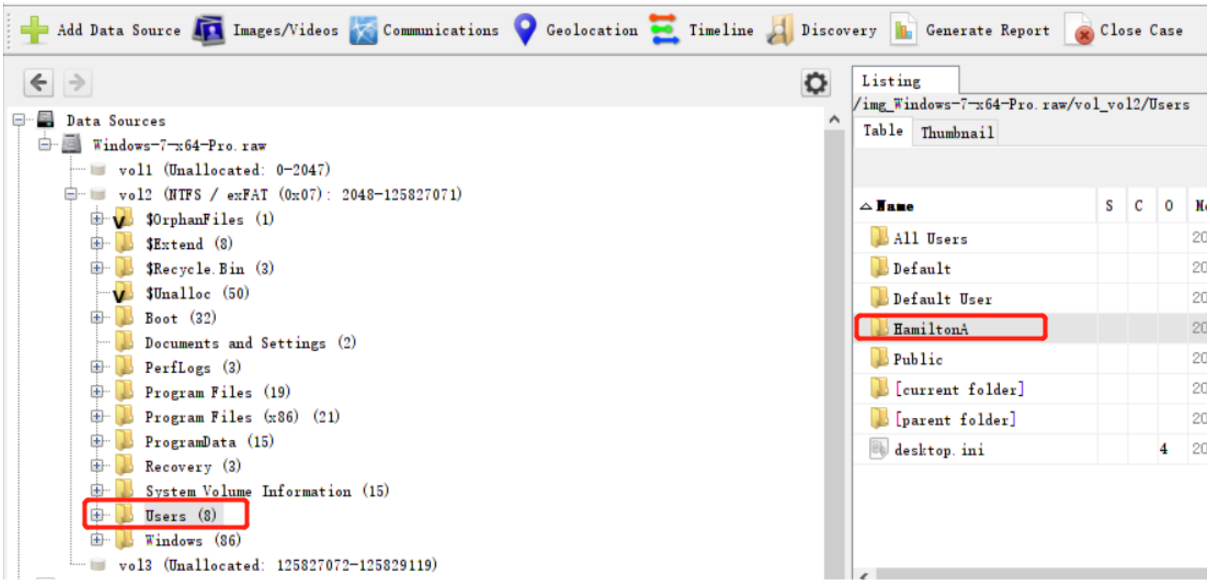
10 Results

Source File	S	C	O	Name	Value	Count	Date Created	Date Accessed	Data Source
Web Data				FirstName	Alyx	1	2020-08-21 08:36:29 AEST	2020-08-21 08:36:29 AEST	Windows-7-x64-Pro.raw
Web Data				LastName	Hamilton	1	2020-08-21 08:36:29 AEST	2020-08-21 08:36:29 AEST	Windows-7-x64-Pro.raw
Web Data				blend_paymentInstrument_accountHolderName	Mr Adam C Smallhorn	1	2020-08-21 10:29:32 AEST	2020-08-21 10:29:32 AEST	Windows-7-x64-Pro.raw
Web Data				blend_paymentInstrument_address_line1	19/2 Market St	1	2020-08-21 10:29:32 AEST	2020-08-21 10:29:32 AEST	Windows-7-x64-Pro.raw
Web Data				blend_paymentInstrument_city	Sydney	1	2020-08-21 10:29:32 AEST	2020-08-21 10:29:32 AEST	Windows-7-x64-Pro.raw
Web Data				blend_paymentInstrument_postal_code	2000	1	2020-08-21 10:29:32 AEST	2020-08-21 10:29:32 AEST	Windows-7-x64-Pro.raw
Web Data				email	alyx.hamilton@caelusengineering.com.au	2	2020-08-28 11:34:33 AEST	2020-09-02 10:37:49 AEST	Windows-7-x64-Pro.raw
Web Data				firstName	Alyx	1	2020-09-02 10:48:39 AEST	2020-09-02 10:48:39 AEST	Windows-7-x64-Pro.raw
Web Data				identifier	alyx.hamilton@caelusengineering.com.au	1	2020-08-31 11:47:32 AEST	2020-08-31 11:47:32 AEST	Windows-7-x64-Pro.raw
Web Data				lastName	Hamilton	1	2020-09-02 10:48:39 AEST	2020-09-02 10:48:39 AEST	Windows-7-x64-Pro.raw

8.6 As the content showed above, most of the web autofill content is related to Alyx Hamilton.

8.7 Third, the user directory use the name: “HamiltonA” Path: /img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA

Figure 4 User directory



```
Data Sources
  Windows-7-x64-Pro.raw
    vol1 (Unallocated: 0-2047)
    vol2 (NTFS / exFAT (0x07): 2048-125827071)
      $OrphanFiles (1)
      $Extend (8)
      $Recycle.Bin (3)
      $Unalloc (50)
      Boot (32)
      Documents and Settings (2)
      PerfLogs (3)
      Program Files (19)
      Program Files (x86) (21)
      ProgramData (15)
      Recovery (3)
      System Volume Information (15)
      Users (8)
      Windows (86)
    vol3 (Unallocated: 125827072-125829119)
```

/img_Windows-7-x64-Pro.raw/vol_vol2/Users

Name	S	C	O	M
All Users				20
Default				20
Default User				20
HamiltonA				20
Public				20
[current folder]				20
[parent folder]				20
desktop.ini			4	20

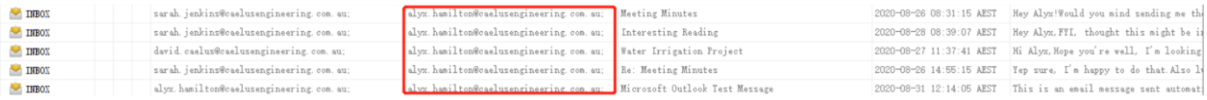
8.8 Which indicates the user of this computer might be Alyx Hamilton.

8.9 Finally, under the autopsy E-mail message section, all the receiver of emails in this machine is Alyx Hamilton.

Table 3 Emails

Name	Hash(MD5)
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Roaming/Thunderbird/Profiles/9233ypdq.default-release/ImapMail/imap.gmail.com/INBOX	8bda598a0d80d1e1ccb3cb132a251c56
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Roaming/Thunderbird/Profiles/9233ypdq.default-release/ImapMail/imap.gmail.com/INBOX	8bda598a0d80d1e1ccb3cb132a251c56
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Roaming/Thunderbird/Profiles/9233ypdq.default-release/ImapMail/imap.gmail.com/INBOX	8bda598a0d80d1e1ccb3cb132a251c56
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Roaming/Thunderbird/Profiles/9233ypdq.default-release/ImapMail/imap.gmail.com/INBOX	8bda598a0d80d1e1ccb3cb132a251c56
/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Roaming/Thunderbird/Profiles/9233ypdq.default-release/ImapMail/imap.gmail.com/INBOX	8bda598a0d80d1e1ccb3cb132a251c56

Table 4 Emails



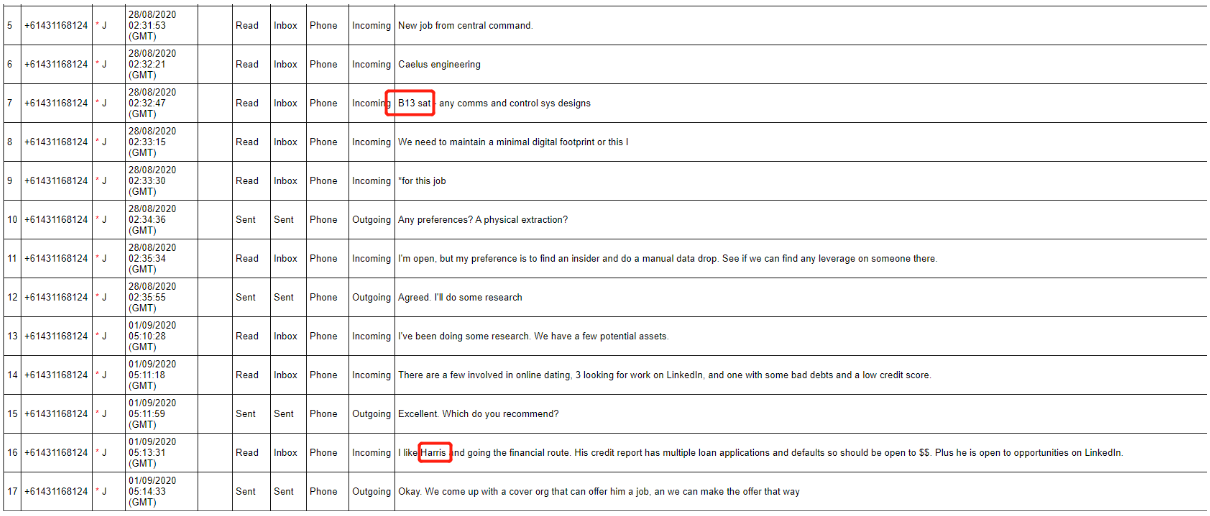
INBOX	sarah.jenkins@caelusengineering.com.au;	alyx.hamilton@caelusengineering.com.au;	Meeting Minutes	2020-08-26 08:31:15 AEST	Hey Alyx!Would you mind sending me th
INBOX	sarah.jenkins@caelusengineering.com.au;	alyx.hamilton@caelusengineering.com.au;	Interesting Reading	2020-08-28 08:39:07 AEST	Hey Alyx,FYI, thought this might be i
INBOX	david.caelus@caelusengineering.com.au;	alyx.hamilton@caelusengineering.com.au;	Water Irrigation Project	2020-08-27 11:37:41 AEST	Hi Alyx,Hope you're well, I'm looking
INBOX	sarah.jenkins@caelusengineering.com.au;	alyx.hamilton@caelusengineering.com.au;	Re: Meeting Minutes	2020-08-26 14:55:15 AEST	Yep sure, I'm happy to do that.Also l
INBOX	alyx.hamilton@caelusengineering.com.au;	alyx.hamilton@caelusengineering.com.au;	Microsoft Outlook Test Message	2020-08-31 12:14:05 AEST	This is an email message sent automat

8.10 In conclusion, this computer belongs to Alyx Hamilton (on balance of probability) as the facts presented above.

8. Question 2

9.1 From the Phone Examination Preview Report Properties on Cameron’s iPhone 4s (A1387) given by Penelope legal. This report is generated by Cellebrite which is a tool to extract information from a mobile device.

Figure 5 Cellebrite report

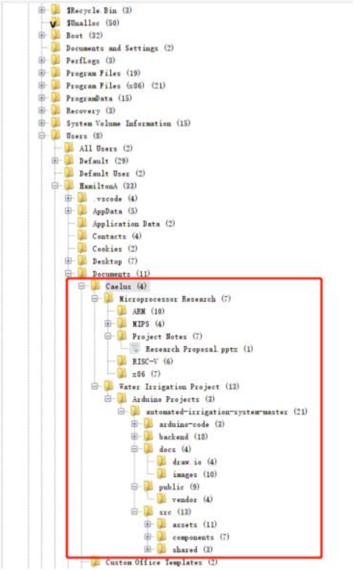


5	+61431168124	* J	28/08/2020 02:31:53 (GMT)		Read	Inbox	Phone	Incoming	New job from central command.
6	+61431168124	* J	28/08/2020 02:32:21 (GMT)		Read	Inbox	Phone	Incoming	Caelus engineering
7	+61431168124	* J	28/08/2020 02:32:47 (GMT)		Read	Inbox	Phone	Incoming	B13 sat - any comms and control sys designs
8	+61431168124	* J	28/08/2020 02:33:15 (GMT)		Read	Inbox	Phone	Incoming	We need to maintain a minimal digital footprint or this I
9	+61431168124	* J	28/08/2020 02:33:30 (GMT)		Read	Inbox	Phone	Incoming	*for this job
10	+61431168124	* J	28/08/2020 02:34:36 (GMT)		Sent	Sent	Phone	Outgoing	Any preferences? A physical extraction?
11	+61431168124	* J	28/08/2020 02:35:34 (GMT)		Read	Inbox	Phone	Incoming	I'm open, but my preference is to find an insider and do a manual data drop. See if we can find any leverage on someone there.
12	+61431168124	* J	28/08/2020 02:35:55 (GMT)		Sent	Sent	Phone	Outgoing	Agreed. I'll do some research
13	+61431168124	* J	01/09/2020 05:10:28 (GMT)		Read	Inbox	Phone	Incoming	I've been doing some research. We have a few potential assets.
14	+61431168124	* J	01/09/2020 05:11:18 (GMT)		Read	Inbox	Phone	Incoming	There are a few involved in online dating, 3 looking for work on LinkedIn, and one with some bad debts and a low credit score.
15	+61431168124	* J	01/09/2020 05:11:59 (GMT)		Sent	Sent	Phone	Outgoing	Excellent. Which do you recommend?
16	+61431168124	* J	01/09/2020 05:13:31 (GMT)		Read	Inbox	Phone	Incoming	I like Harris and going the financial route. His credit report has multiple loan applications and defaults so should be open to $$. Plus he is open to opportunities on LinkedIn.
17	+61431168124	* J	01/09/2020 05:14:33 (GMT)		Sent	Sent	Phone	Outgoing	Okay. We come up with a cover org that can offer him a job, an we can make the offer that way

9.2 According to the information in the report, Cameron and John Davis want a ‘B13 sat cooms and control sys designs’ and they found Michael Harris to help them obtained the information. More specifically, they are probably trying to find a control system design for their project ‘*A Practical Launcher Thermal Analysis Tool for Three-axis Stabilized B13 GEO Communication Satellites - Google Docs*’. This can be found on the laptop image under the Extracted content, Web History section. Path: *‘/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/AppData/Local/Google/Chrome/User Data/Default/History’. Hash: ‘3b77c76b999304a1b4b06b593fa2d351’*

9.3 From the data on the laptop’s image. It contains multiple projects information located in Path: ‘/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/Documents/Caelus’. Some of the projects may meet Michael and Cameron’s requirement.

Figure 6 Project Folder



```
$Recycle.Bin (3)
$Unalloc (50)
Boot (32)
Documents and Settings (2)
PerfLogs (3)
Program Files (19)
Program Files (x86) (21)
ProgramData (15)
Recovery (3)
System Volume Information (15)
Users (8)
  All Users (2)
  Default (29)
  Default User (2)
  HamiltonA (23)
    .vscode (4)
    AppData (5)
    Application Data (2)
    Contacts (4)
    Cookies (2)
    Desktop (7)
    Documents (11)
      Caelus (4)
        Microprocessor Research (7)
          ARM (10)
          MIPS (4)
          Project Notes (7)
            Research Proposal.pptx (1)
          RISC-V (6)
          x86 (7)
        Water Irrigation Project (13)
          Arduino Projects (3)
            automated-irrigation-system-master (21)
              arduino-code (3)
              backend (18)
              docs (4)
                draw.io (4)
                images (10)
              public (9)
                vendor (4)
              src (13)
                assets (11)
                components (7)
                shared (3)
      Custom Office Templates (2)
```

9. Question 3

10.1 There is not much indication of data encryption. I investigate the prefetch folder which is a folder that contains name of the executable files (Path:' /img_Windows-7-x64-Pro.raw/vol_vol2/Windows/Prefetch') and found no evidence of software that is able to perform encryption on the data.

10.2 Through entropy (level of randomness, a higher entropy indicates occurrence of encryption) analysis module in autopsy, no high entropy artefact related to the case has been found.

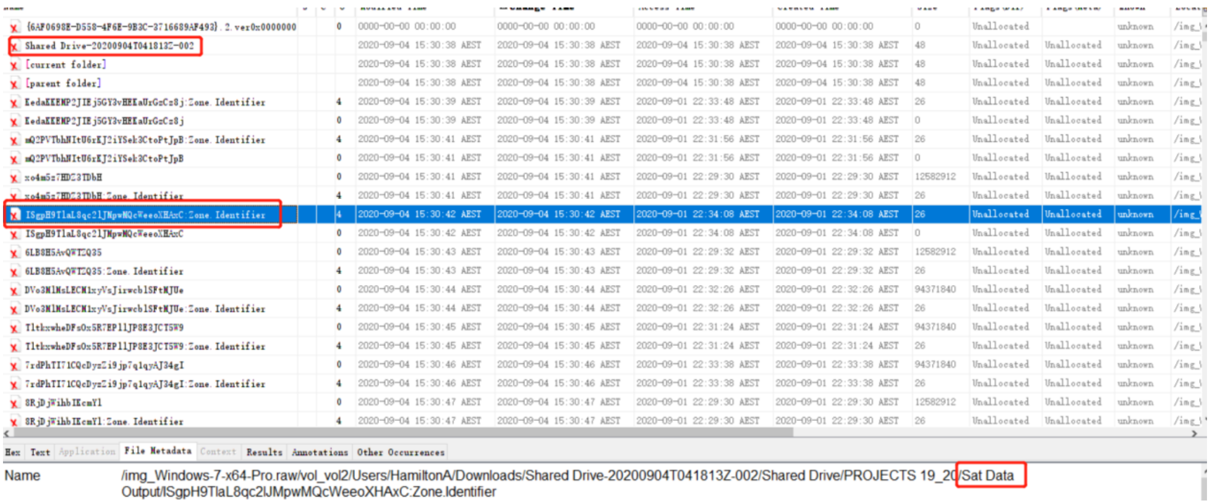
10.3 Analysis regarding on extension mismatched has also been performed on Autopsy. No particular artefact related to this case have been found.

10.4 I only discovered the *ssl-keys.log* in path : '*/img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/Documents/logs/ssl-keys.log*' with hash:" 6ab3c33164a2eeffbb3c1b850e80213d" which can be used to decrypt network traffic on this laptop's network image. Secure Sockets Layer (SSL) is a protocol developed by Netscape for providing a secure connection between two or more devices via the Internet.

10. Question 4

11.1 Yes, especially on 04/09/2020 AEST, lots of files have been downloaded and deleted which can be found in Autopsy under Deleted Files section. Some notable files are presented below:

Figure 7 deleted files 1

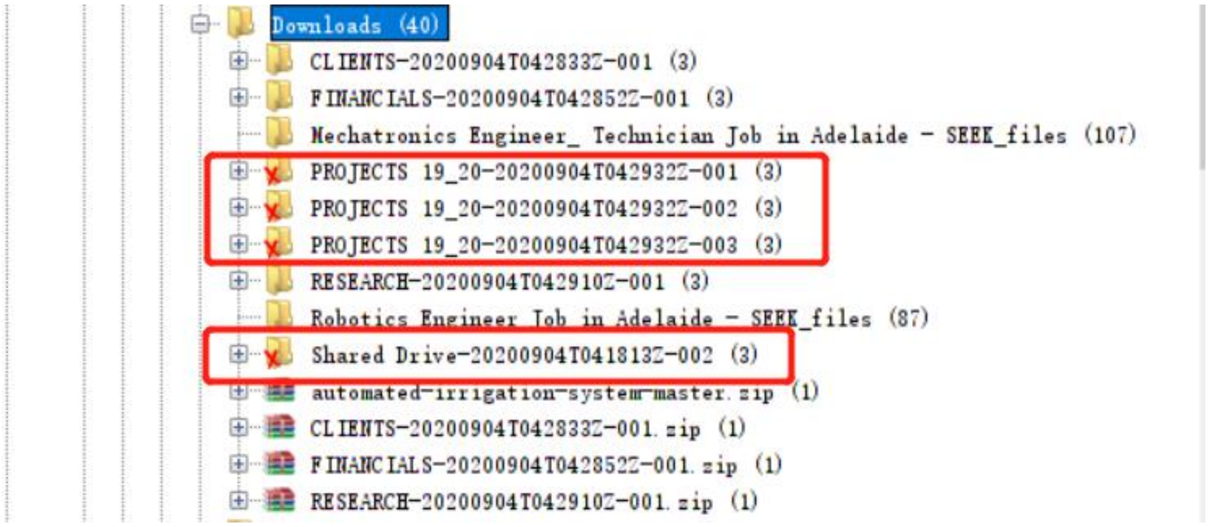


Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags (Dir)	Flags (Meta)	Known	Location
{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x0000000			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/img_\
Shared Drive-20200904T041813Z-002				2020-09-04 15:30:38 AEST	2020-09-04 15:30:38 AEST	2020-09-04 15:30:38 AEST	2020-09-04 15:30:38 AEST	48	Unallocated	Unallocated	unknown	/img_\
[current folder]				2020-09-04 15:30:38 AEST	2020-09-04 15:30:38 AEST	2020-09-04 15:30:38 AEST	2020-09-04 15:30:38 AEST	48	Unallocated	Unallocated	unknown	/img_\
[parent folder]				2020-09-04 15:30:38 AEST	2020-09-04 15:30:38 AEST	2020-09-04 15:30:38 AEST	2020-09-04 15:30:38 AEST	48	Unallocated	Unallocated	unknown	/img_\
KedaKKEMP2JIEj5GY3vHEKaUrGzCz8j:Zone.Identifier			4	2020-09-04 15:30:39 AEST	2020-09-04 15:30:39 AEST	2020-09-01 22:33:48 AEST	2020-09-01 22:33:48 AEST	26	Unallocated	Unallocated	unknown	/img_\
KedaKKEMP2JIEj5GY3vHEKaUrGzCz8j			0	2020-09-04 15:30:39 AEST	2020-09-04 15:30:39 AEST	2020-09-01 22:33:48 AEST	2020-09-01 22:33:48 AEST	0	Unallocated	Unallocated	unknown	/img_\
mQ2PVTbhNItU6rKJ2iYSek3CtoPtJpB:Zone.Identifier			4	2020-09-04 15:30:41 AEST	2020-09-04 15:30:41 AEST	2020-09-01 22:31:56 AEST	2020-09-01 22:31:56 AEST	26	Unallocated	Unallocated	unknown	/img_\
mQ2PVTbhNItU6rKJ2iYSek3CtoPtJpB			0	2020-09-04 15:30:41 AEST	2020-09-04 15:30:41 AEST	2020-09-01 22:31:56 AEST	2020-09-01 22:31:56 AEST	0	Unallocated	Unallocated	unknown	/img_\
xo4m5z7HDZ3TDbH			0	2020-09-04 15:30:41 AEST	2020-09-04 15:30:41 AEST	2020-09-01 22:29:30 AEST	2020-09-01 22:29:30 AEST	12582912	Unallocated	Unallocated	unknown	/img_\
xo4m5z7HDZ3TDbH:Zone.Identifier			4	2020-09-04 15:30:41 AEST	2020-09-04 15:30:41 AEST	2020-09-01 22:29:30 AEST	2020-09-01 22:29:30 AEST	26	Unallocated	Unallocated	unknown	/img_\
ISgpH9TlaL8qc2lJMpwMQcWeeoXHAxC:Zone.Identifier			4	2020-09-04 15:30:42 AEST	2020-09-04 15:30:42 AEST	2020-09-01 22:34:08 AEST	2020-09-01 22:34:08 AEST	26	Unallocated	Unallocated	unknown	/img_\
ISgpH9TlaL8qc2lJMpwMQcWeeoXHAxC			0	2020-09-04 15:30:42 AEST	2020-09-04 15:30:42 AEST	2020-09-01 22:34:08 AEST	2020-09-01 22:34:08 AEST	0	Unallocated	Unallocated	unknown	/img_\
6LB8H5AvQWTZQ35			0	2020-09-04 15:30:43 AEST	2020-09-04 15:30:43 AEST	2020-09-01 22:29:32 AEST	2020-09-01 22:29:32 AEST	12582912	Unallocated	Unallocated	unknown	/img_\
6LB8H5AvQWTZQ35:Zone.Identifier			4	2020-09-04 15:30:43 AEST	2020-09-04 15:30:43 AEST	2020-09-01 22:29:32 AEST	2020-09-01 22:29:32 AEST	26	Unallocated	Unallocated	unknown	/img_\
DVo3MlMsLECM1xyVsJirwcblSFtMJUe			0	2020-09-04 15:30:44 AEST	2020-09-04 15:30:44 AEST	2020-09-01 22:32:26 AEST	2020-09-01 22:32:26 AEST	94371840	Unallocated	Unallocated	unknown	/img_\
DVo3MlMsLECM1xyVsJirwcblSFtMJUe:Zone.Identifier			4	2020-09-04 15:30:44 AEST	2020-09-04 15:30:44 AEST	2020-09-01 22:32:26 AEST	2020-09-01 22:32:26 AEST	26	Unallocated	Unallocated	unknown	/img_\
TltkxwheDFs0x5R7EP1lJP8E3JCT5W9			0	2020-09-04 15:30:45 AEST	2020-09-04 15:30:45 AEST	2020-09-01 22:31:24 AEST	2020-09-01 22:31:24 AEST	94371840	Unallocated	Unallocated	unknown	/img_\
TltkxwheDFs0x5R7EP1lJP8E3JCT5W9:Zone.Identifier			4	2020-09-04 15:30:45 AEST	2020-09-04 15:30:45 AEST	2020-09-01 22:31:24 AEST	2020-09-01 22:31:24 AEST	26	Unallocated	Unallocated	unknown	/img_\
7rdPhTI71CQcDyzZi9jp7qlqyAJ34gI			0	2020-09-04 15:30:46 AEST	2020-09-04 15:30:46 AEST	2020-09-01 22:33:38 AEST	2020-09-01 22:33:38 AEST	94371840	Unallocated	Unallocated	unknown	/img_\
7rdPhTI71CQcDyzZi9jp7qlqyAJ34gI:Zone.Identifier			4	2020-09-04 15:30:46 AEST	2020-09-04 15:30:46 AEST	2020-09-01 22:33:38 AEST	2020-09-01 22:33:38 AEST	26	Unallocated	Unallocated	unknown	/img_\
8RjDjWihbIKcmYl			0	2020-09-04 15:30:47 AEST	2020-09-04 15:30:47 AEST	2020-09-01 22:29:30 AEST	2020-09-01 22:29:30 AEST	12582912	Unallocated	Unallocated	unknown	/img_\
8RjDjWihbIKcmYl:Zone.Identifier			4	2020-09-04 15:30:47 AEST	2020-09-04 15:30:47 AEST	2020-09-01 22:29:30 AEST	2020-09-01 22:29:30 AEST	26	Unallocated	Unallocated	unknown	/img_\

Name /img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/Downloads/Shared Drive-20200904T041813Z-002/Shared Drive/PROJECTS 19_20/Sat Data Output/ISgpH9TlaL8qc2lJMpwMQcWeeoXHAxC:Zone.Identifier

11.2 Also in the path : /img_Windows-7-x64-Pro.raw/vol_vol2/Users/HamiltonA/Downloads

Figure 8 deleted files2



```
Downloads (40)
    CLIENTS-20200904T042833Z-001 (3)
    FINANCIALS-20200904T042852Z-001 (3)
    Mechatronics Engineer_ Technician Job in Adelaide - SEEK_files (107)
    PROJECTS 19_20-20200904T042932Z-001 (3)
    PROJECTS 19_20-20200904T042932Z-002 (3)
    PROJECTS 19_20-20200904T042932Z-003 (3)
    RESEARCH-20200904T042910Z-001 (3)
    Robotics Engineer Job in Adelaide - SEEK_files (87)
    Shared Drive-20200904T041813Z-002 (3)
    automated-irrigation-system-master.zip (1)
    CLIENTS-20200904T042833Z-001.zip (1)
    FINANCIALS-20200904T042852Z-001.zip (1)
    RESEARCH-20200904T042910Z-001.zip (1)
```

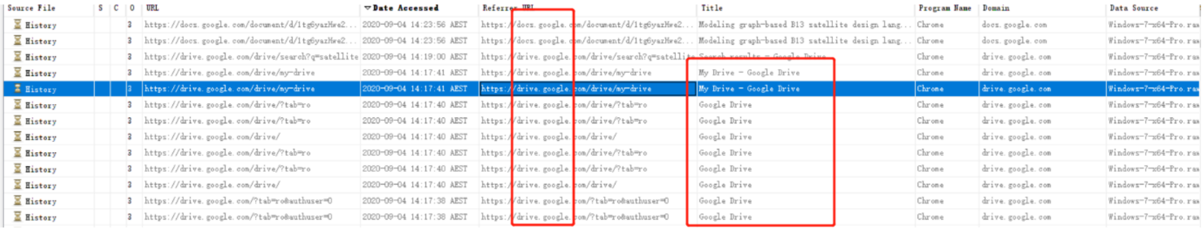
11.3 These folders have been downloaded from the share drive and then deleted to cover tracks.

11.4 Michael, Cameron and John's phone is quite clean, they might have other phone for personal use or they might wipe some of the data from their phone.

11. Question 5

12.1 Indications of Data exfiltration have been found on the missing laptop's image.

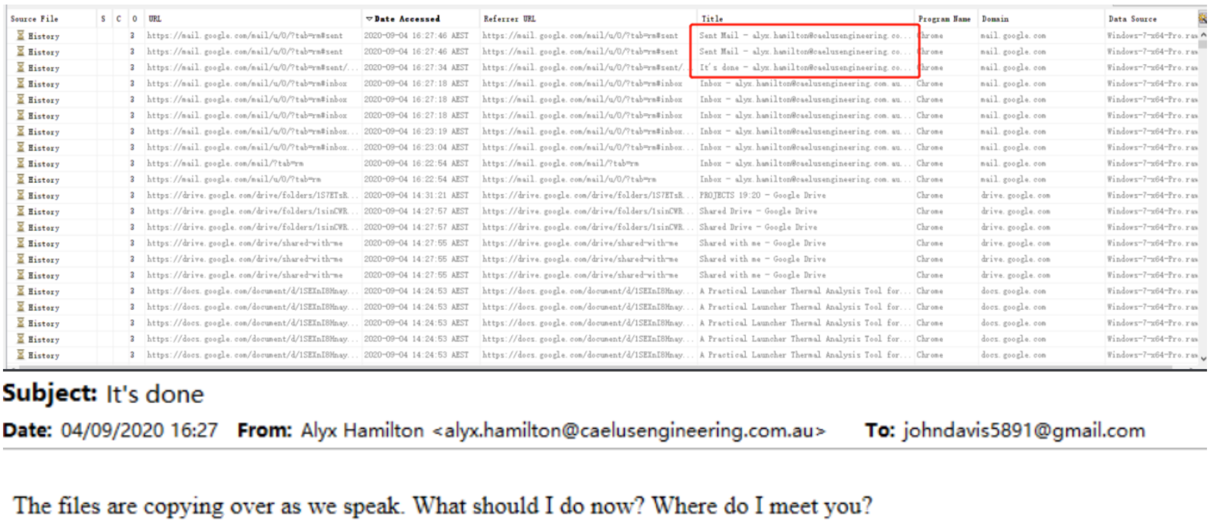
Figure 9 Data exfiltration 1



Source File	S	C	O	URL	▽Date Accessed	Referrer URL	Title	Program Name	Domain	Data Source
History			3	https://docs.google.com/document/d/1tg6yazHwe2...	2020-09-04 14:23:56 AEST	https://docs.google.com/document/d/1tg6yazHwe2...	Modeling graph-based B13 satellite design lang...	Chrome	docs.google.com	Windows-7-x64-Pro.raw
History			3	https://docs.google.com/document/d/1tg6yazHwe2...	2020-09-04 14:23:56 AEST	https://docs.google.com/document/d/1tg6yazHwe2...	Modeling graph-based B13 satellite design lang...	Chrome	docs.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/search?q=satellite	2020-09-04 14:19:00 AEST	https://drive.google.com/drive/search?q=satellite	Search results - Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/my-drive	2020-09-04 14:17:41 AEST	https://drive.google.com/drive/my-drive	My Drive - Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/my-drive	2020-09-04 14:17:41 AEST	https://drive.google.com/drive/my-drive	My Drive - Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/?tab=ro	2020-09-04 14:17:40 AEST	https://drive.google.com/drive/?tab=ro	Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/?tab=ro	2020-09-04 14:17:40 AEST	https://drive.google.com/drive/?tab=ro	Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/	2020-09-04 14:17:40 AEST	https://drive.google.com/drive/	Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/?tab=ro	2020-09-04 14:17:40 AEST	https://drive.google.com/drive/?tab=ro	Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/?tab=ro	2020-09-04 14:17:40 AEST	https://drive.google.com/drive/?tab=ro	Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/	2020-09-04 14:17:40 AEST	https://drive.google.com/drive/	Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/?tab=ro&authuser=0	2020-09-04 14:17:38 AEST	https://drive.google.com/?tab=ro&authuser=0	Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/?tab=ro&authuser=0	2020-09-04 14:17:38 AEST	https://drive.google.com/?tab=ro&authuser=0	Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw

12.2 Since 2020-09-04 AEST, the laptop have been accessing google drive and google doc, until the user of the laptop send an email said “it’s done”.

Figure 10 Data exfiltration 2



Source File	S	C	O	URL	▽Date Accessed	Referrer URL	Title	Program Name	Domain	Data Source
History			3	https://mail.google.com/mail/u/0/?tab=rm#sent	2020-09-04 16:27:46 AEST	https://mail.google.com/mail/u/0/?tab=rm#sent	Sent Mail - alyx.hamilton@caelusengineering.co...	Chrome	mail.google.com	Windows-7-x64-Pro.raw
History			3	https://mail.google.com/mail/u/0/?tab=rm#sent	2020-09-04 16:27:46 AEST	https://mail.google.com/mail/u/0/?tab=rm#sent	Sent Mail - alyx.hamilton@caelusengineering.co...	Chrome	mail.google.com	Windows-7-x64-Pro.raw
History			3	https://mail.google.com/mail/u/0/?tab=rm#sent/...	2020-09-04 16:27:34 AEST	https://mail.google.com/mail/u/0/?tab=rm#sent/...	It's done - alyx.hamilton@caelusengineering.co...	Chrome	mail.google.com	Windows-7-x64-Pro.raw
History			3	https://mail.google.com/mail/u/0/?tab=rm#inbox	2020-09-04 16:27:18 AEST	https://mail.google.com/mail/u/0/?tab=rm#inbox	Inbox - alyx.hamilton@caelusengineering.com.au...	Chrome	mail.google.com	Windows-7-x64-Pro.raw
History			3	https://mail.google.com/mail/u/0/?tab=rm#inbox	2020-09-04 16:27:18 AEST	https://mail.google.com/mail/u/0/?tab=rm#inbox	Inbox - alyx.hamilton@caelusengineering.com.au...	Chrome	mail.google.com	Windows-7-x64-Pro.raw
History			3	https://mail.google.com/mail/u/0/?tab=rm#inbox	2020-09-04 16:27:18 AEST	https://mail.google.com/mail/u/0/?tab=rm#inbox	Inbox - alyx.hamilton@caelusengineering.com.au...	Chrome	mail.google.com	Windows-7-x64-Pro.raw
History			3	https://mail.google.com/mail/u/0/?tab=rm#inbox...	2020-09-04 16:23:19 AEST	https://mail.google.com/mail/u/0/?tab=rm#inbox...	Inbox - alyx.hamilton@caelusengineering.com.au...	Chrome	mail.google.com	Windows-7-x64-Pro.raw
History			3	https://mail.google.com/mail/u/0/?tab=rm#inbox...	2020-09-04 16:23:04 AEST	https://mail.google.com/mail/u/0/?tab=rm#inbox...	Inbox - alyx.hamilton@caelusengineering.com.au...	Chrome	mail.google.com	Windows-7-x64-Pro.raw
History			3	https://mail.google.com/mail/?tab=rm	2020-09-04 16:22:54 AEST	https://mail.google.com/mail/?tab=rm	Inbox - alyx.hamilton@caelusengineering.com.au...	Chrome	mail.google.com	Windows-7-x64-Pro.raw
History			3	https://mail.google.com/mail/u/0/?tab=rm	2020-09-04 16:22:54 AEST	https://mail.google.com/mail/u/0/?tab=rm	Inbox - alyx.hamilton@caelusengineering.com.au...	Chrome	mail.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/folders/1S7ETsR...	2020-09-04 14:31:21 AEST	https://drive.google.com/drive/folders/1S7ETsR...	PROJECTS 19:20 - Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/folders/1sinCWR...	2020-09-04 14:27:57 AEST	https://drive.google.com/drive/folders/1sinCWR...	Shared Drive - Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/folders/1sinCWR...	2020-09-04 14:27:57 AEST	https://drive.google.com/drive/folders/1sinCWR...	Shared Drive - Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/shared-with-me	2020-09-04 14:27:55 AEST	https://drive.google.com/drive/shared-with-me	Shared with me - Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/shared-with-me	2020-09-04 14:27:55 AEST	https://drive.google.com/drive/shared-with-me	Shared with me - Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://drive.google.com/drive/shared-with-me	2020-09-04 14:27:55 AEST	https://drive.google.com/drive/shared-with-me	Shared with me - Google Drive	Chrome	drive.google.com	Windows-7-x64-Pro.raw
History			3	https://docs.google.com/document/d/1SEXnI8Hnay...	2020-09-04 14:24:53 AEST	https://docs.google.com/document/d/1SEXnI8Hnay...	A Practical Launcher Thermal Analysis Tool for...	Chrome	docs.google.com	Windows-7-x64-Pro.raw
History			3	https://docs.google.com/document/d/1SEXnI8Hnay...	2020-09-04 14:24:53 AEST	https://docs.google.com/document/d/1SEXnI8Hnay...	A Practical Launcher Thermal Analysis Tool for...	Chrome	docs.google.com	Windows-7-x64-Pro.raw
History			3	https://docs.google.com/document/d/1SEXnI8Hnay...	2020-09-04 14:24:53 AEST	https://docs.google.com/document/d/1SEXnI8Hnay...	A Practical Launcher Thermal Analysis Tool for...	Chrome	docs.google.com	Windows-7-x64-Pro.raw
History			3	https://docs.google.com/document/d/1SEXnI8Hnay...	2020-09-04 14:24:53 AEST	https://docs.google.com/document/d/1SEXnI8Hnay...	A Practical Launcher Thermal Analysis Tool for...	Chrome	docs.google.com	Windows-7-x64-Pro.raw
History			3	https://docs.google.com/document/d/1SEXnI8Hnay...	2020-09-04 14:24:53 AEST	https://docs.google.com/document/d/1SEXnI8Hnay...	A Practical Launcher Thermal Analysis Tool for...	Chrome	docs.google.com	Windows-7-x64-Pro.raw

Subject: It's done

Date: 04/09/2020 16:27 **From:** Alyx Hamilton <alyx.hamilton@caelusengineering.com.au> **To:** johndavis5891@gmail.com

The files are copying over as we speak. What should I do now? Where do I meet you?

12.3 This email can also be found form ‘Hamilton.zip’

12. Question 6

13.1 Examination should be conducted on the missing laptop’s serial number to check if it match with Alyx’s computer.

13.2 Investigate on Michael, John, Cameron’s personal device to search for direct proof.

13.3 Investigate Alyx’s personal device to check whether she is truly innocent and has no connection with Michael on this matter.

13. Reliability of time across evidence

14.1 Summary of time format the tools provide.

Table 5 List of time used in tools

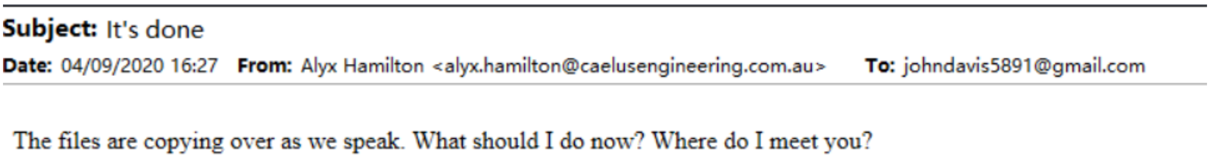
Tool Name	Time Zone

Autopsy (4.16.0)	AEST
Wireshark (3.2.7)	AEST
Cellebrite	GMT

14.2 To prove the reliability of the time, I use multiple tools to inspect the same email sent by Alyx Hamilton.

14.3 First, in ‘Hamilton.zip’:

Table 6 'Hamilton.zip'



Subject: It's done

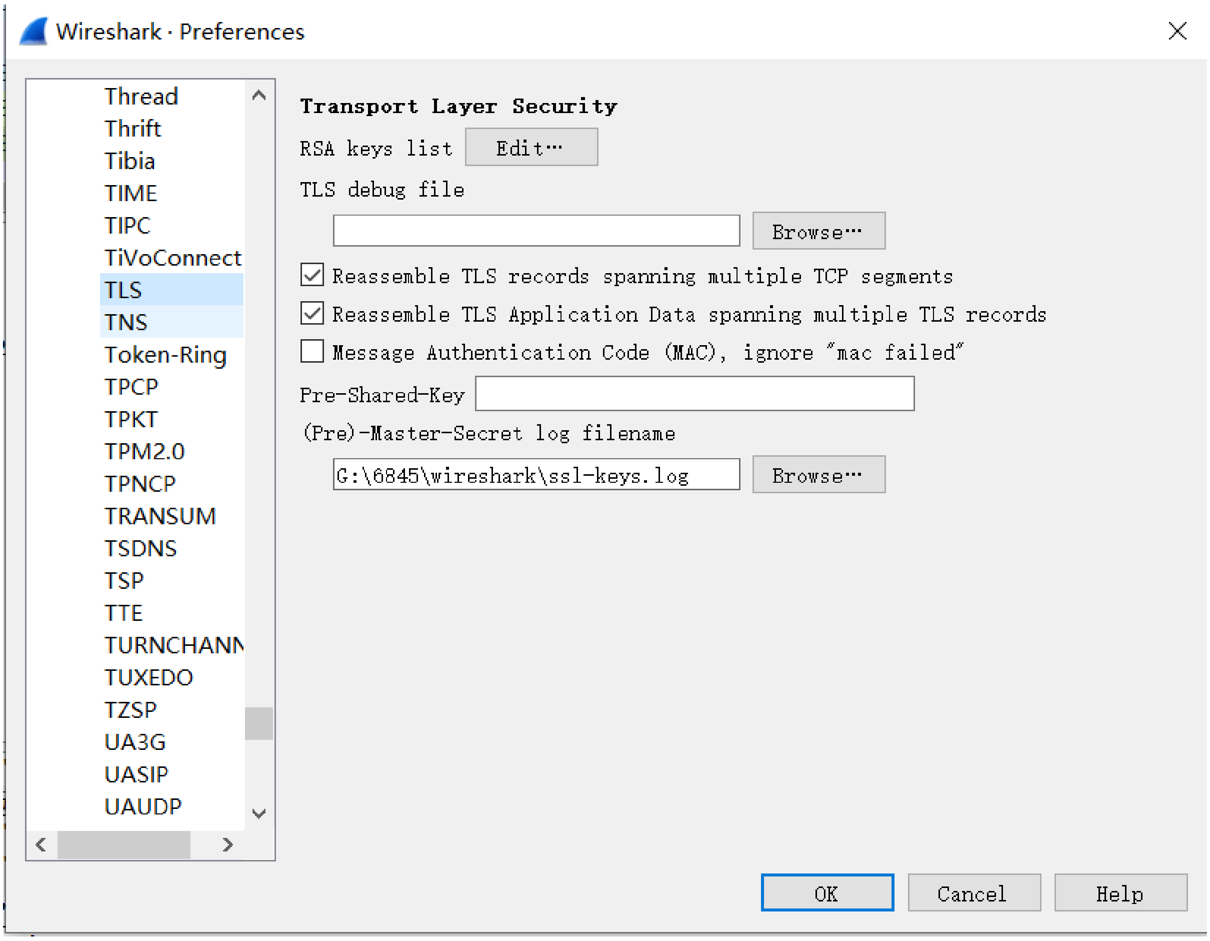
Date: 04/09/2020 16:27 **From:** Alyx Hamilton <alyx.hamilton@caelusengineering.com.au> **To:** johndavis5891@gmail.com

The files are copying over as we speak. What should I do now? Where do I meet you?

14.4 We can extract this message. Which is sent by Alyx Hamilton to `johndavis5891@gmail.com`. The time is 04/09/2020 16:27 AEST.

14.5 Next, in ‘hamiltona_network_log.pcapng’. Using wireshark (3.2.7) an Network Forensic Analysis Tool which can capture and analyse network traffic on the wire as well as in pcapng files. pcapng files contains the information of a network, which is obtained by the sniffer to analyse the packet and import the ssl-keys we found in laptop’s image in order to decode the network traffic.

Figure 11 import ssl-keys.log



Transport Layer Security

RSA keys list

TLS debug file

☑ Reassemble TLS records spanning multiple TCP segments

☑ Reassemble TLS Application Data spanning multiple TLS records

☐ Message Authentication Code (MAC), ignore "mac failed"

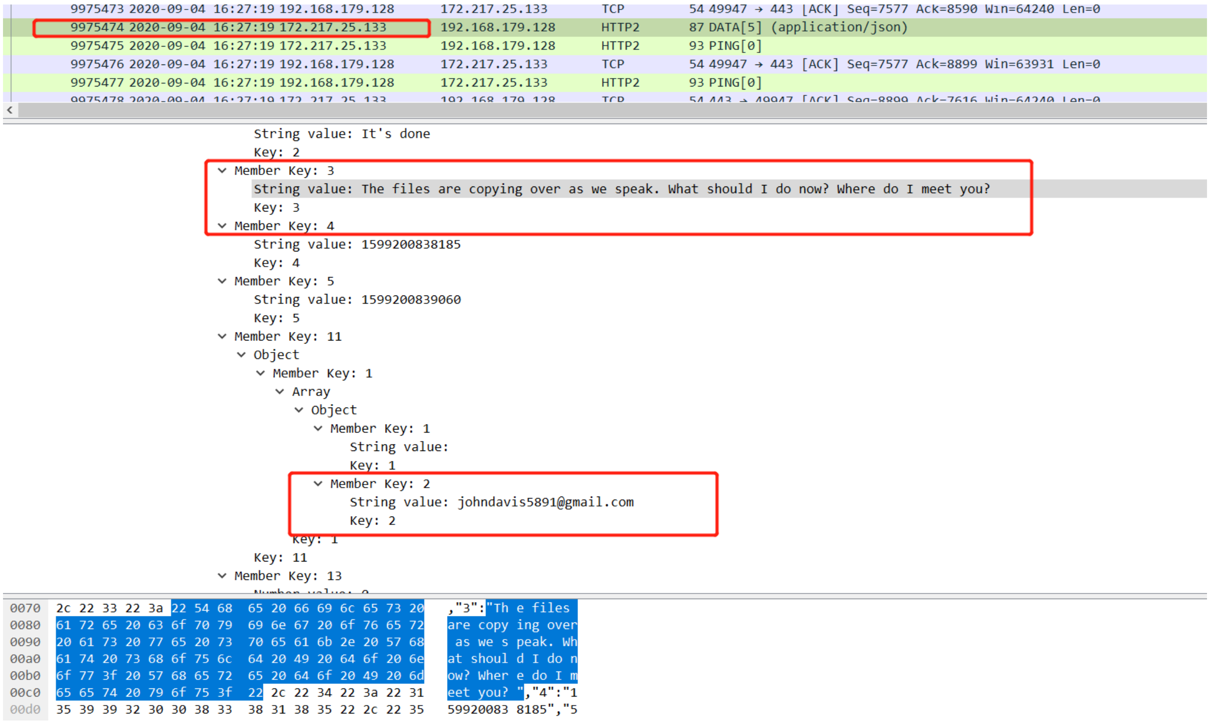
Pre-Shared-Key

(Pre)-Master-Secret log filename

G:\6845\wireshark\ssl-keys.log

14.6 We can see that in packet No:9975096 on 2020-09-04 16:27:19. The email's content is the same as the one we found in 'Hamilton.zip' and the time match.

Figure 12 wireshark pakcet



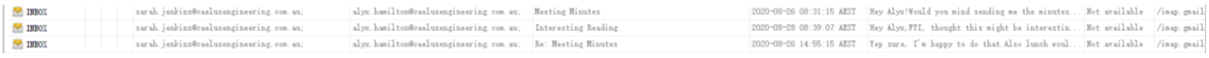
```
9975473 2020-09-04 16:27:19 192.168.179.128    172.217.25.133    TCP      54 49947 → 443 [ACK] Seq=7577 Ack=8590 Win=64240 Len=0
9975474 2020-09-04 16:27:19 172.217.25.133     192.168.179.128   HTTP2    87 DATA[5] (application/json)
9975475 2020-09-04 16:27:19 172.217.25.133     192.168.179.128   HTTP2    93 PING[0]
9975476 2020-09-04 16:27:19 192.168.179.128    172.217.25.133    TCP      54 49947 → 443 [ACK] Seq=7577 Ack=8899 Win=63931 Len=0
9975477 2020-09-04 16:27:19 192.168.179.128    172.217.25.133    HTTP2    93 PING[0]
9975478 2020-09-04 16:27:19 172.217.25.133     192.168.179.128   TCP      54 443 → 49947 [ACK] Seq=8899 Ack=7616 Win=64240 Len=0
```

```
          String value: It's done
          Key: 2
      Member Key: 3
          String value: The files are copying over as we speak. What should I do now? Where do I meet you?
          Key: 3
      Member Key: 4
          String value: 1599200838185
          Key: 4
      Member Key: 5
          String value: 1599200839060
          Key: 5
      Member Key: 11
        Object
          Member Key: 1
            Array
              Object
                Member Key: 1
                    String value:
                    Key: 1
                Member Key: 2
                    String value: johndavis5891@gmail.com
                    Key: 2
              Key: 1
          Key: 11
      Member Key: 13
          Number value: 0
```

```
0070  2c 22 33 22 3a 22 54 68  65 20 66 69 6c 65 73 20   ,"3":"Th e files 
0080  61 72 65 20 63 6f 70 79  69 6e 67 20 6f 76 65 72   are copy ing over
0090  20 61 73 20 77 65 20 73  70 65 61 6b 2e 20 57 68    as we s peak. Wh
00a0  61 74 20 73 68 6f 75 6c  64 20 49 20 64 6f 20 6e   at shoul d I do n
00b0  6f 77 3f 20 57 68 65 72  65 20 64 6f 20 49 20 6d   ow? Wher e do I m
00c0  65 65 74 20 79 6f 75 3f  22 2c 22 34 22 3a 22 31   eet you? ","4":"1
00d0  35 39 39 32 30 30 38 33  38 31 38 35 22 2c 22 35   59920083 8185","5
```

14.7 Next, let’s examine the emails in autopsy. Take these 3 emails as examples.

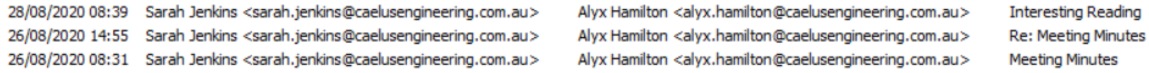
Figure 13 emails in autopsy



```
INBOX    sarah.jenkins@caelusengineering.com.au;   alyx.hamilton@caelusengineering.com.au;   Meeting Minutes       2020-08-26 08:31:15 AEST   Hey Alyx!Would you mind sending me the minutes...   Not available   /imap.gmail
INBOX    sarah.jenkins@caelusengineering.com.au;   alyx.hamilton@caelusengineering.com.au;   Interesting Reading   2020-08-28 08:39:07 AEST   Hey Alyx,FYI, thought this might be interestin...   Not available   /imap.gmail
INBOX    sarah.jenkins@caelusengineering.com.au;   alyx.hamilton@caelusengineering.com.au;   Re: Meeting Minutes   2020-08-26 14:55:15 AEST   Yep sure, I'm happy to do that.Also lunch woul...   Not available   /imap.gmail
```

14.8 The content and the time match the artefact in ‘Hamilton.zip’

Figure 14 emails in 'Hamilton.zip'

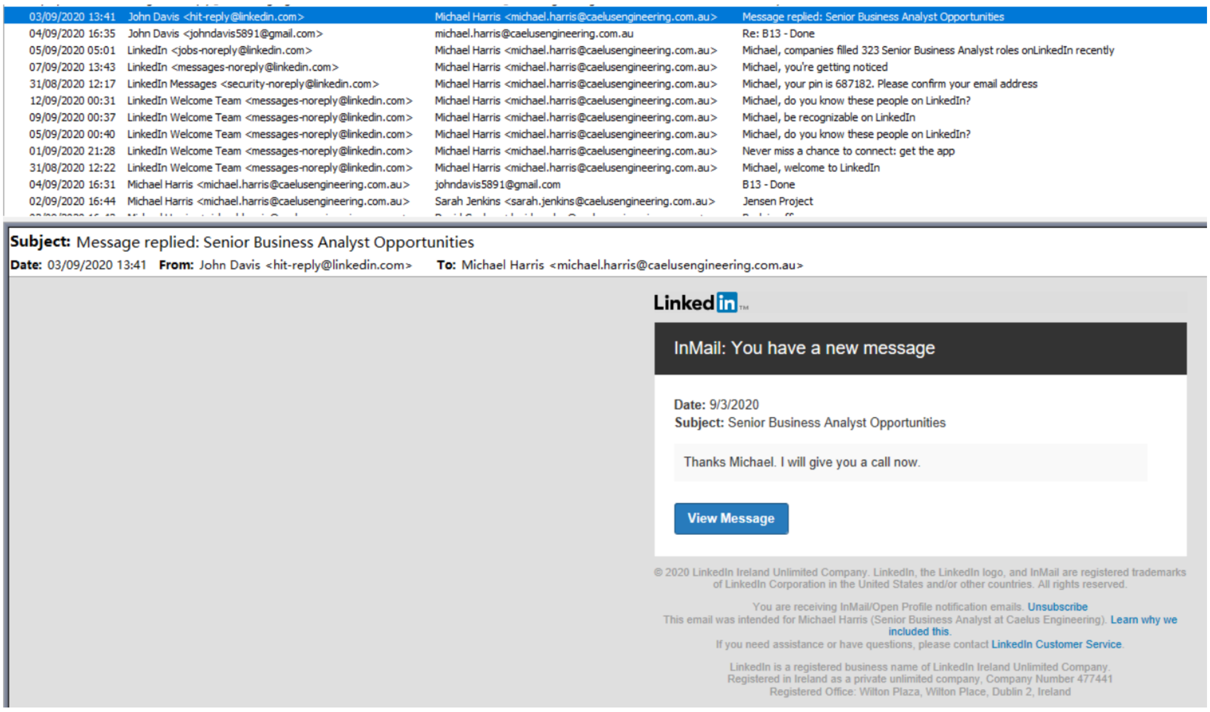


28/08/2020 08:39	Sarah Jenkins <sarah.jenkins@caelusengineering.com.au>	Alyx Hamilton <alyx.hamilton@caelusengineering.com.au>	Interesting Reading
26/08/2020 14:55	Sarah Jenkins <sarah.jenkins@caelusengineering.com.au>	Alyx Hamilton <alyx.hamilton@caelusengineering.com.au>	Re: Meeting Minutes
26/08/2020 08:31	Sarah Jenkins <sarah.jenkins@caelusengineering.com.au>	Alyx Hamilton <alyx.hamilton@caelusengineering.com.au>	Meeting Minutes

14.9 In all, verify the time in these 3 tools, I can conclude that the time in this report is quite reliable.

14.10 To verify whether cellebrite report has reliable time we can compare these 2 artefacts. One is from ‘Harris.zip’:

Figure 15 email from 'Harris.zip'



03/09/2020 13:41	John Davis <hit-reply@linkedin.com>	Michael Harris <michael.harris@caelusengineering.com.au>	Message replied: Senior Business Analyst Opportunities
04/09/2020 16:35	John Davis <johndavis5891@gmail.com>	michael.harris@caelusengineering.com.au	Re: B13 - Done
05/09/2020 05:01	LinkedIn <jobs-noreply@linkedin.com>	Michael Harris <michael.harris@caelusengineering.com.au>	Michael, companies filled 323 Senior Business Analyst roles onLinkedIn recently
07/09/2020 13:43	LinkedIn <messages-noreply@linkedin.com>	Michael Harris <michael.harris@caelusengineering.com.au>	Michael, you're getting noticed
31/08/2020 12:17	LinkedIn Messages <security-noreply@linkedin.com>	Michael Harris <michael.harris@caelusengineering.com.au>	Michael, your pin is 687182. Please confirm your email address
12/09/2020 00:31	LinkedIn Welcome Team <messages-noreply@linkedin.com>	Michael Harris <michael.harris@caelusengineering.com.au>	Michael, do you know these people on LinkedIn?
09/09/2020 00:37	LinkedIn Welcome Team <messages-noreply@linkedin.com>	Michael Harris <michael.harris@caelusengineering.com.au>	Michael, be recognizable on LinkedIn
05/09/2020 00:40	LinkedIn Welcome Team <messages-noreply@linkedin.com>	Michael Harris <michael.harris@caelusengineering.com.au>	Michael, do you know these people on LinkedIn?
01/09/2020 21:28	LinkedIn Welcome Team <messages-noreply@linkedin.com>	Michael Harris <michael.harris@caelusengineering.com.au>	Never miss a chance to connect: get the app
31/08/2020 12:22	LinkedIn Welcome Team <messages-noreply@linkedin.com>	Michael Harris <michael.harris@caelusengineering.com.au>	Michael, welcome to LinkedIn
04/09/2020 16:31	Michael Harris <michael.harris@caelusengineering.com.au>	johndavis5891@gmail.com	B13 - Done
02/09/2020 16:44	Michael Harris <michael.harris@caelusengineering.com.au>	Sarah Jenkins <sarah.jenkins@caelusengineering.com.au>	Jensen Project

Subject: Message replied: Senior Business Analyst Opportunities
Date: 03/09/2020 13:41 **From:** John Davis <hit-reply@linkedin.com> **To:** Michael Harris <michael.harris@caelusengineering.com.au>

InMail: You have a new message

Date: 9/3/2020
Subject: Senior Business Analyst Opportunities

Thanks Michael. I will give you a call now.

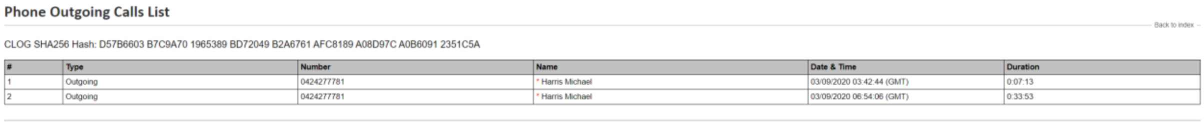
© 2020 LinkedIn Ireland Unlimited Company. LinkedIn, the LinkedIn logo, and InMail are registered trademarks of LinkedIn Corporation in the United States and/or other countries. All rights reserved.

You are receiving InMail/Open Profile notification emails. Unsubscribe
This email was intended for Michael Harris (Senior Business Analyst at Caelus Engineering). Learn why we included this.
If you need assistance or have questions, please contact LinkedIn Customer Service.

LinkedIn is a registered business name of LinkedIn Ireland Unlimited Company.
Registered in Ireland as a private unlimited company, Company Number 477441
Registered Office: Wilton Plaza, Wilton Place, Dublin 2, Ireland

14.11 In this email, John Davis is about to call Michael on (03/09/2020 13:41 AEST). From the cellebrite report on John's phone:

Figure 16 cellebrite report on John's phone



Phone Outgoing Calls List

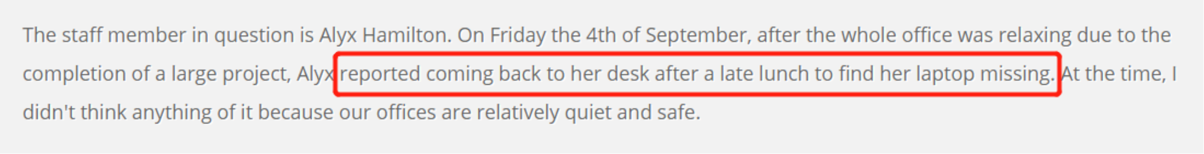
CLOG SHA256 Hash: D57B6603 B7C9A70 1965389 BD72049 B2A6761 AFC8189 A08D97C A0B6091 2351C5A

#	Type	Number	Name	Date & Time	Duration
1	Outgoing	0424277781	* Harris Michael	03/09/2020 03:42:44 (GMT)	0:07:13
2	Outgoing	0424277781	* Harris Michael	03/09/2020 06:54:06 (GMT)	0:33:53

14.12 It shows that on 03/09/2020 03:42 :44 GMT which is 03/09/2020 13:42 :44 AEST, John called Michael which means the time in cellebrite report is quite reliable.

14.13 Time stomping is an Anti-Forensics technique which changed the timestamps of the file. However, such activity is unlikely to happen in these evidence. From Penelope legal's email (full email in appendix B):

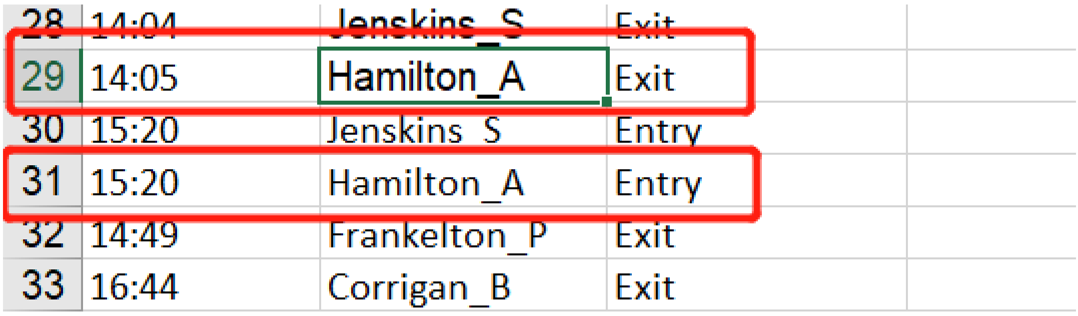
Figure 17 Alyx's statement



The staff member in question is Alyx Hamilton. On Friday the 4th of September, after the whole office was relaxing due to the completion of a large project, Alyx reported coming back to her desk after a late lunch to find her laptop missing. At the time, I didn't think anything of it because our offices are relatively quiet and safe.

14.14 According to Alyx, she reported that her laptop was missing after a late lunch. I look into the entrance record of Caelus Engineering (full record in Appendix C):

Figure 18 entrance record of Caelus Engineering

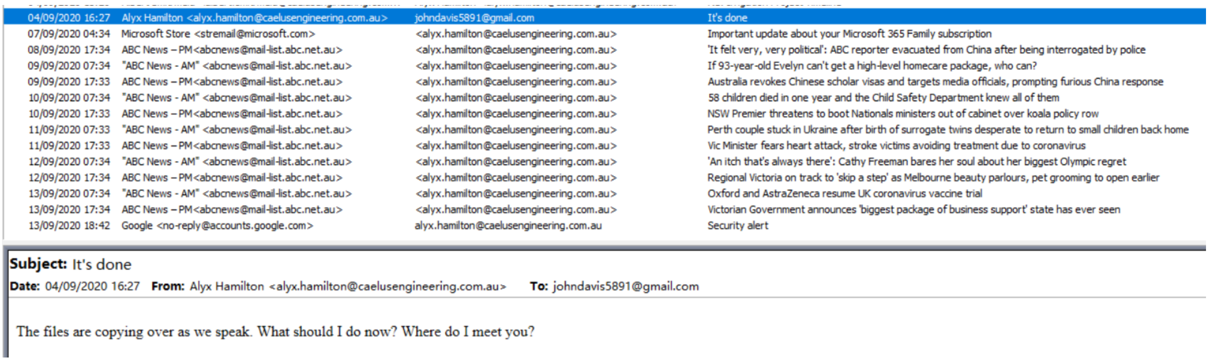


28	14:04	Jenskins_S	Exit
29	14:05	Hamilton_A	Exit
30	15:20	Jenskins_S	Entry
31	15:20	Hamilton_A	Entry
32	14:49	Frankelton_P	Exit
33	16:44	Corrigan_B	Exit

14.15 It shows that Alyx leave the building (probably for late lunch) at 14:05 AEST and come back at 15:20 AEST, the laptop should be missing during this time period.

14.16 In this email found in 'Hamilton.zip':

Figure 19 email from Hamilton.zip



04/09/2020 16:27	Alyx Hamilton <alyx.hamilton@caelusengineering.com.au>	johndavis5891@gmail.com	It's done
07/09/2020 04:34	Microsoft Store <stremail@microsoft.com>	<alyx.hamilton@caelusengineering.com.au>	Important update about your Microsoft 365 Family subscription
08/09/2020 17:34	ABC News – PM<abcnews@mail-list.abc.net.au>	<alyx.hamilton@caelusengineering.com.au>	'It felt very, very political': ABC reporter evacuated from China after being interrogated by police
09/09/2020 07:34	"ABC News - AM" <abcnews@mail-list.abc.net.au>	<alyx.hamilton@caelusengineering.com.au>	If 93-year-old Evelyn can't get a high-level homecare package, who can?
09/09/2020 17:33	ABC News – PM<abcnews@mail-list.abc.net.au>	<alyx.hamilton@caelusengineering.com.au>	Australia revokes Chinese scholar visas and targets media officials, prompting furious China response
10/09/2020 07:34	"ABC News - AM" <abcnews@mail-list.abc.net.au>	<alyx.hamilton@caelusengineering.com.au>	58 children died in one year and the Child Safety Department knew all of them
10/09/2020 17:33	ABC News – PM<abcnews@mail-list.abc.net.au>	<alyx.hamilton@caelusengineering.com.au>	NSW Premier threatens to boot Nationals ministers out of cabinet over koala policy row
11/09/2020 07:33	"ABC News - AM" <abcnews@mail-list.abc.net.au>	<alyx.hamilton@caelusengineering.com.au>	Perth couple stuck in Ukraine after birth of surrogate twins desperate to return to small children back home
11/09/2020 17:33	ABC News – PM<abcnews@mail-list.abc.net.au>	<alyx.hamilton@caelusengineering.com.au>	Vic Minister fears heart attack, stroke victims avoiding treatment due to coronavirus
12/09/2020 07:34	"ABC News - AM" <abcnews@mail-list.abc.net.au>	<alyx.hamilton@caelusengineering.com.au>	'An itch that's always there': Cathy Freeman bares her soul about her biggest Olympic regret
12/09/2020 17:34	ABC News – PM<abcnews@mail-list.abc.net.au>	<alyx.hamilton@caelusengineering.com.au>	Regional Victoria on track to 'skip a step' as Melbourne beauty parlours, pet grooming to open earlier
13/09/2020 07:34	"ABC News - AM" <abcnews@mail-list.abc.net.au>	<alyx.hamilton@caelusengineering.com.au>	Oxford and AstraZeneca resume UK coronavirus vaccine trial
13/09/2020 17:34	ABC News – PM<abcnews@mail-list.abc.net.au>	<alyx.hamilton@caelusengineering.com.au>	Victorian Government announces 'biggest package of business support' state has ever seen
13/09/2020 18:42	Google <no-reply@accounts.google.com>	alyx.hamilton@caelusengineering.com.au	Security alert

Subject: It's done

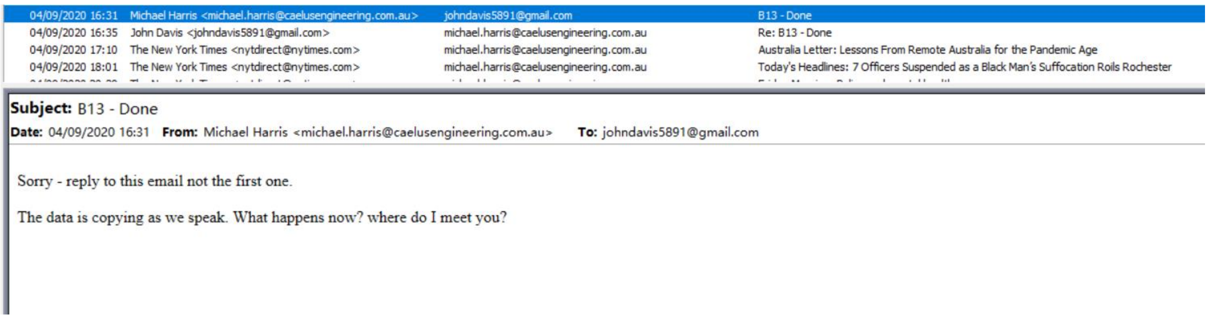
Date: 04/09/2020 16:27 **From:** Alyx Hamilton <alyx.hamilton@caelusengineering.com.au> **To:** johndavis5891@gmail.com

The files are copying over as we speak. What should I do now? Where do I meet you?

14.17 The user of Alyx's laptop sent an email to John Davis on 04/09/2020 16:27 AEST.

14.18 In "Harris.zip":

Figure 20 email from Harris.zip



04/09/2020 16:31	Michael Harris <michael.harris@caelusengineering.com.au>	johndavis5891@gmail.com	B13 - Done
04/09/2020 16:35	John Davis <johndavis5891@gmail.com>	michael.harris@caelusengineering.com.au	Re: B13 - Done
04/09/2020 17:10	The New York Times <nytdirect@nytimes.com>	michael.harris@caelusengineering.com.au	Australia Letter: Lessons From Remote Australia for the Pandemic Age
04/09/2020 18:01	The New York Times <nytdirect@nytimes.com>	michael.harris@caelusengineering.com.au	Today's Headlines: 7 Officers Suspended as a Black Man's Suffocation Roils Rochester

Subject: B13 - Done

Date: 04/09/2020 16:31 **From:** Michael Harris <michael.harris@caelusengineering.com.au> **To:** johndavis5891@gmail.com

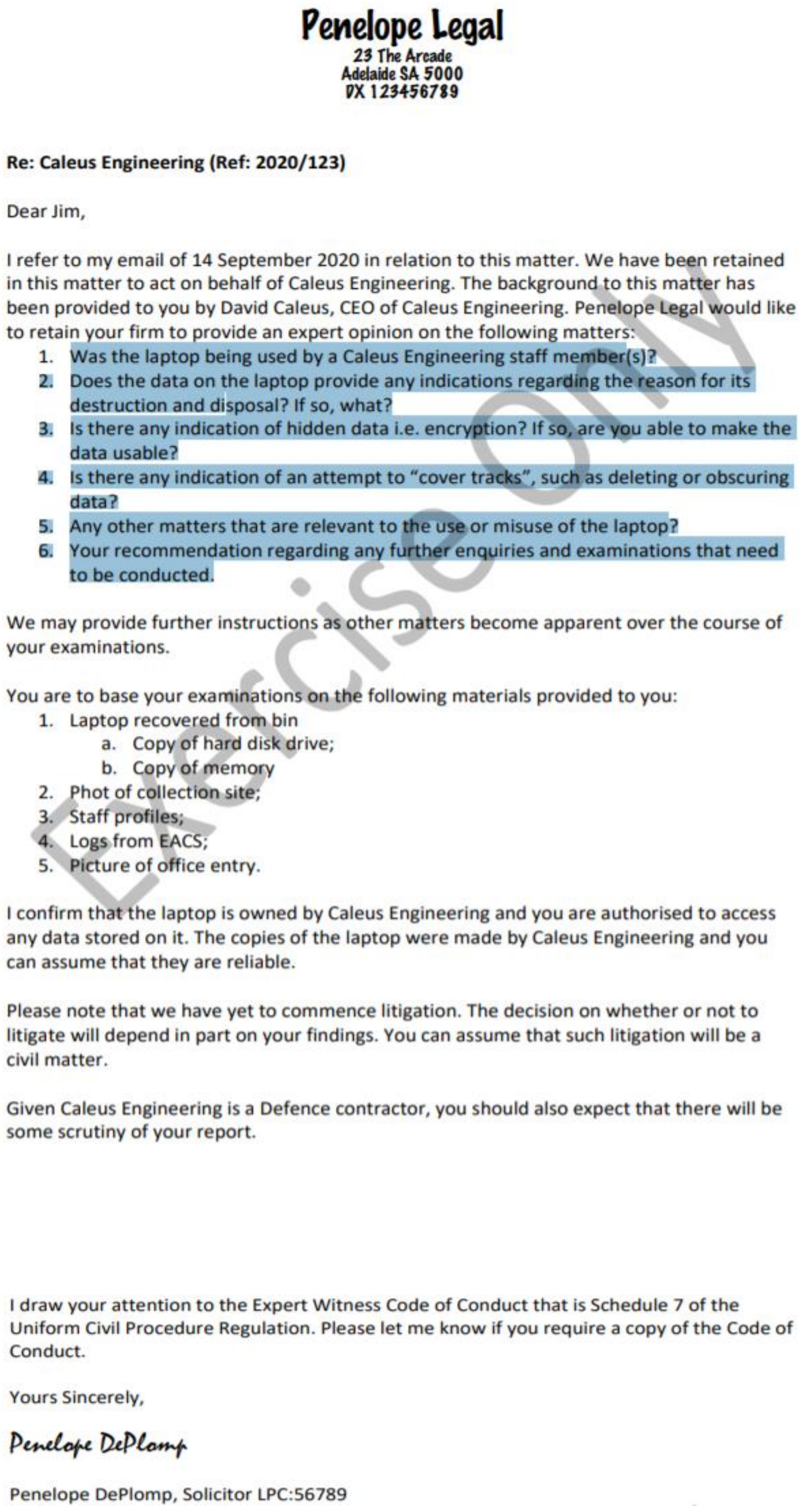
Sorry - reply to this email not the first one.

The data is copying as we speak. What happens now? where do I meet you?

14.19 In this email on 04/09/2020 16:31 AEST, Michael said: 'reply to this email not the first one. 'The first email he mentioned is probably the one sending using Alyx's computer. So the user of Alyx's laptop after should be Michael (on the balance of probability) and the time he sent the email matches the laptop missing time frame which is after 04/09/2020 15:20 AEST.

14.20 Since the time of the artefacts match the critical time frame and no strange time stamps have been found across evidence. Time stomping is unlikely to occur in these evidence.

Appendix A



Penelope Legal
23 The Arcade
Adelaide SA 5000
DX 123456789

Re: Caleus Engineering (Ref: 2020/123)

Dear Jim,

I refer to my email of 14 September 2020 in relation to this matter. We have been retained in this matter to act on behalf of Caleus Engineering. The background to this matter has been provided to you by David Caleus, CEO of Caleus Engineering. Penelope Legal would like to retain your firm to provide an expert opinion on the following matters:

1. Was the laptop being used by a Caleus Engineering staff member(s)?
2. Does the data on the laptop provide any indications regarding the reason for its destruction and disposal? If so, what?
3. Is there any indication of hidden data i.e. encryption? If so, are you able to make the data usable?
4. Is there any indication of an attempt to "cover tracks", such as deleting or obscuring data?
5. Any other matters that are relevant to the use or misuse of the laptop?
6. Your recommendation regarding any further enquiries and examinations that need to be conducted.

We may provide further instructions as other matters become apparent over the course of your examinations.

You are to base your examinations on the following materials provided to you:

1. Laptop recovered from bin
   a. Copy of hard disk drive;
   b. Copy of memory
2. Phot of collection site;
3. Staff profiles;
4. Logs from EACS;
5. Picture of office entry.

I confirm that the laptop is owned by Caleus Engineering and you are authorised to access any data stored on it. The copies of the laptop were made by Caleus Engineering and you can assume that they are reliable.

Please note that we have yet to commence litigation. The decision on whether or not to litigate will depend in part on your findings. You can assume that such litigation will be a civil matter.

Given Caleus Engineering is a Defence contractor, you should also expect that there will be some scrutiny of your report.

I draw your attention to the Expert Witness Code of Conduct that is Schedule 7 of the Uniform Civil Procedure Regulation. Please let me know if you require a copy of the Code of Conduct.

Yours Sincerely,

Penelope DePlomp

Penelope DePlomp, Solicitor LPC:56789

Appendix B

To: info@jimsforensics.net
From: admin@penelopelegal.com.au
Date: 14 September 2020
Subject: FW: Assistance request
Attachment: Letter of instruction.pdf

CONFIDENTIAL - For Jim's eyes only

Hi Jim,

We've had this enquiry come in from Caelus Engineering. Can we ask Jim's Forensics to perform the analysis for this case? I have attached a formal letter of Instruction to this email.

We will direct Caelus engineering to provide you (via open learning) with the data and assets you require. You can assume that all assets obtained via openlearning were collected reliably, though you still need to confirm the reliability of the download evidence packages.

We suspect this will be a civil matter, but high profile and could attract a lot of scrutiny. If so, we will require you to give evidence during the trial.

Regards,
P

On Tuesday 15 September 2020 Penelope forwarded this email from admin@penelopelegal.com.au:

Hi Penelope,

Thank you for taking my call earlier. This matter is quite urgent.

As I mentioned on the phone, I'm writing because of a strange event which occurred a few weeks back. Last week one of my staff reported her laptop stolen, despite it being only a few weeks old.

I am the director of an engineering firm known as Caelus engineering - we're based in Adelaide and mainly contract to other engineering firms on industrial projects.

The staff member in question is Alyx Hamilton. On Friday the 4th of September, after the whole office was relaxing due to the completion of a large project, Alyx reported coming back to her desk after a late lunch to find her laptop missing. At the time, I didn't think anything of it because our offices are relatively quiet and safe.

First thing the next week, I receive a phone call from one of my friends who works in one of the commercial building a few blocks away from our offices in King William St. Apparently, when taking out the garbage on monday morning one of his staff members found a laptop in the bottom of their bin. When they pulled it out, they discovered it had been pretty badly damaged, and most of the asset tags had been removed. Fortunately they didn't remove all of them, so were able to trace it back to us pretty quickly on monday.

I should mention that I have had some suspicions about Alyx Hamilton for several months now - she has expressed discontent a few times, so I fear something suspicious is going on.

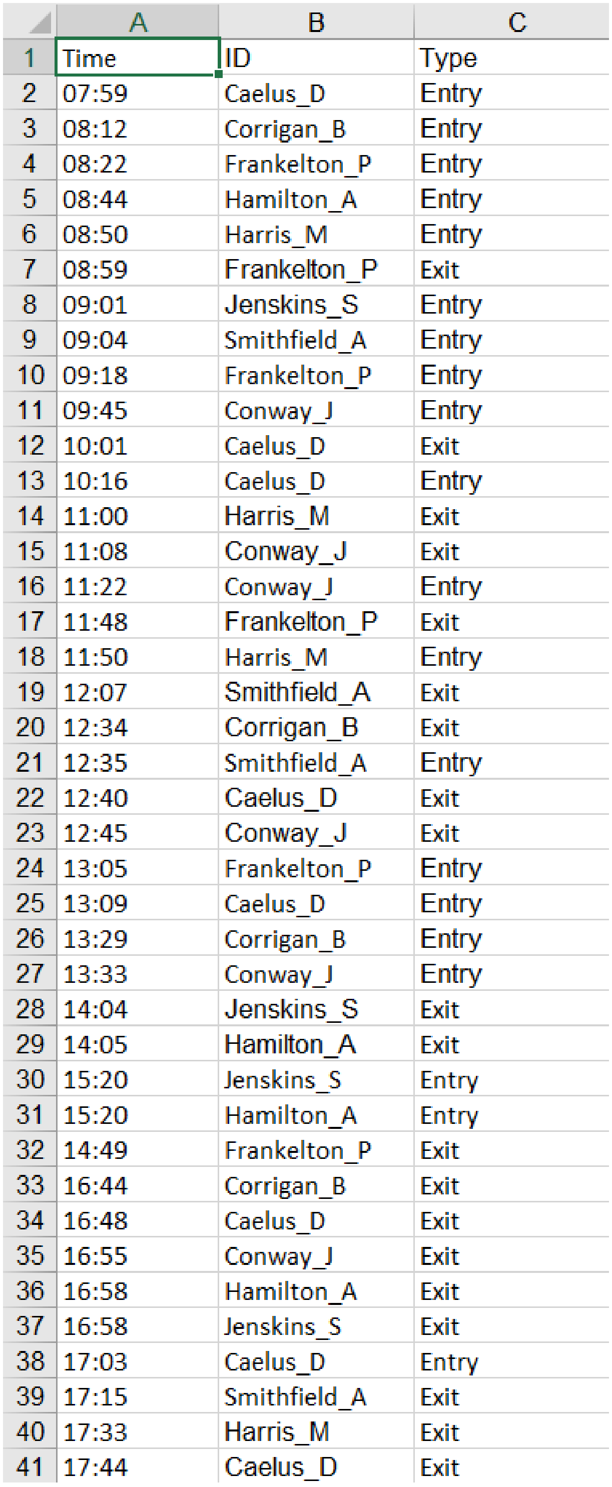
Given the sensitive and commercial nature of our projects which are often multi-year contracts from government and industry worth millions of dollars to us, this would be incredibly damaging.

Can you find out who stole the laptop?

Should you have any questions please contact me via the comment box below.

Yours sincerely,
David Caelus.
Founder, Caelus Engineering

Appendix C



	A	B	C
1	Time	ID	Type
2	07:59	Caelus_D	Entry
3	08:12	Corrigan_B	Entry
4	08:22	Frankelton_P	Entry
5	08:44	Hamilton_A	Entry
6	08:50	Harris_M	Entry
7	08:59	Frankelton_P	Exit
8	09:01	Jenskins_S	Entry
9	09:04	Smithfield_A	Entry
10	09:18	Frankelton_P	Entry
11	09:45	Conway_J	Entry
12	10:01	Caelus_D	Exit
13	10:16	Caelus_D	Entry
14	11:00	Harris_M	Exit
15	11:08	Conway_J	Exit
16	11:22	Conway_J	Entry
17	11:48	Frankelton_P	Exit
18	11:50	Harris_M	Entry
19	12:07	Smithfield_A	Exit
20	12:34	Corrigan_B	Exit
21	12:35	Smithfield_A	Entry
22	12:40	Caelus_D	Exit
23	12:45	Conway_J	Exit
24	13:05	Frankelton_P	Entry
25	13:09	Caelus_D	Entry
26	13:29	Corrigan_B	Entry
27	13:33	Conway_J	Entry
28	14:04	Jenskins_S	Exit
29	14:05	Hamilton_A	Exit
30	15:20	Jenskins_S	Entry
31	15:20	Hamilton_A	Entry
32	14:49	Frankelton_P	Exit
33	16:44	Corrigan_B	Exit
34	16:48	Caelus_D	Exit
35	16:55	Conway_J	Exit
36	16:58	Hamilton_A	Exit
37	16:58	Jenskins_S	Exit
38	17:03	Caelus_D	Entry
39	17:15	Smithfield_A	Exit
40	17:33	Harris_M	Exit
41	17:44	Caelus_D	Exit