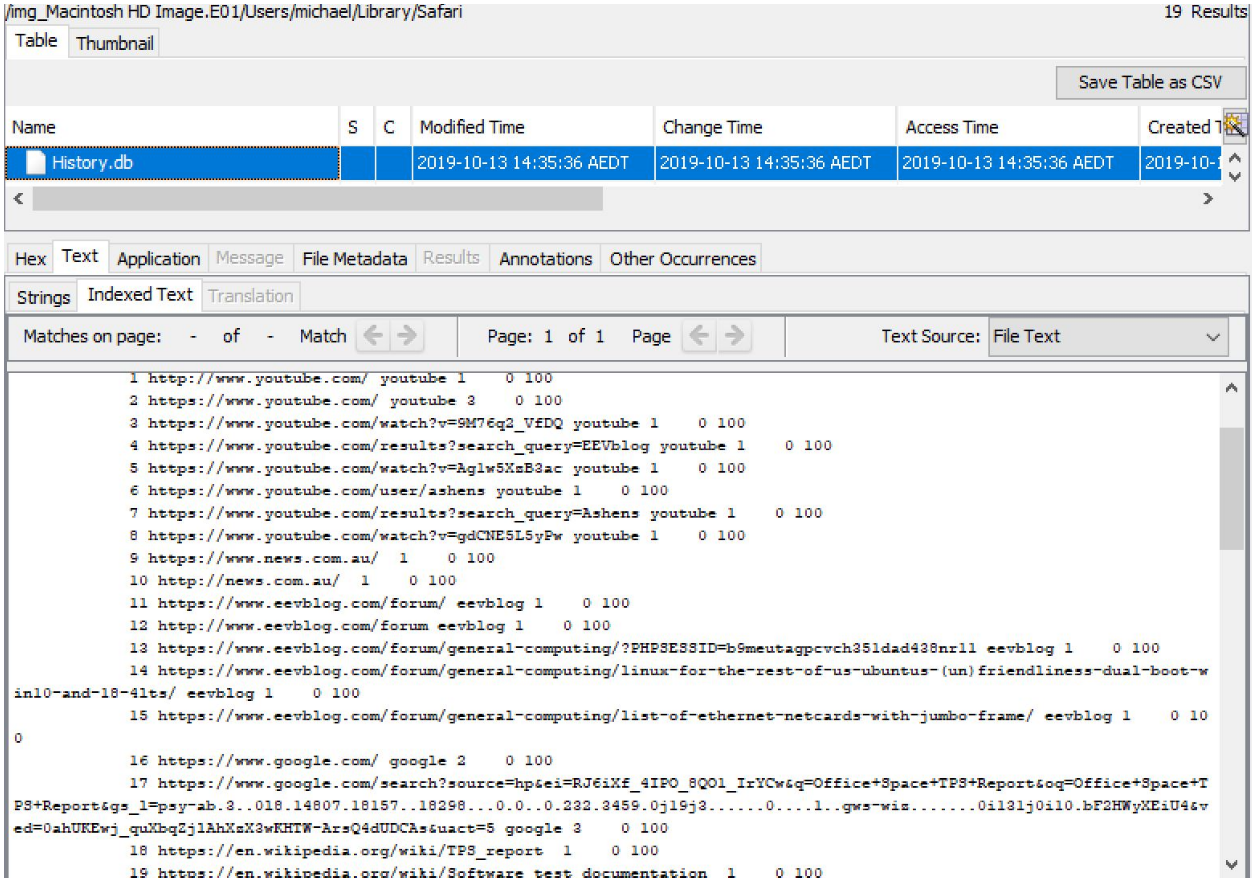
Analysing the images, answer the following questions, providing evidence for each:

1. Web history?

Various items including youtube pages and wikipedia pages. Found in Users/Michael/Library/Safari.



/img_Macintosh HD Image.E01/Users/michael/Library/Safari — 19 Results

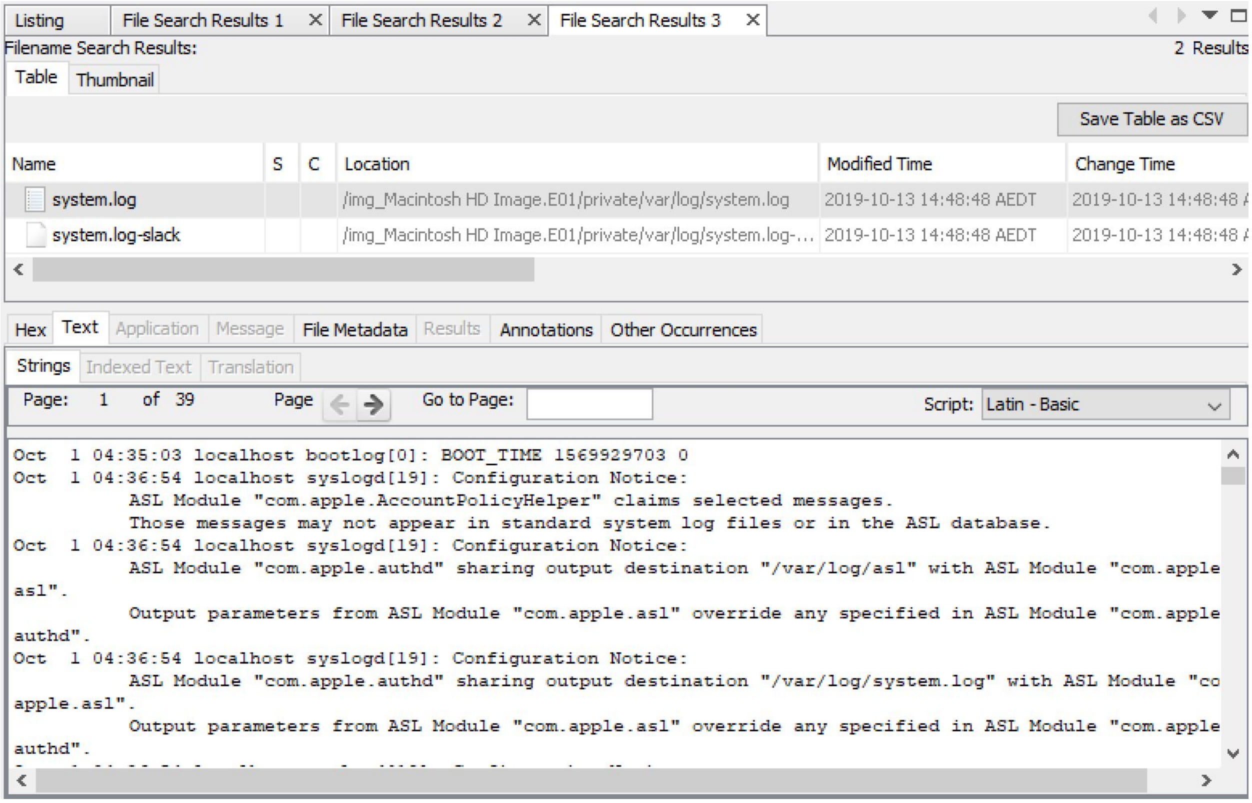
Name	S	C	Modified Time	Change Time	Access Time	Created T
History.db			2019-10-13 14:35:36 AEDT	2019-10-13 14:35:36 AEDT	2019-10-13 14:35:36 AEDT	2019-10-1

```
            1 http://www.youtube.com/ youtube 1     0 100
            2 https://www.youtube.com/ youtube 3     0 100
            3 https://www.youtube.com/watch?v=9M76q2_VfDQ youtube 1     0 100
            4 https://www.youtube.com/results?search_query=EEVblog youtube 1     0 100
            5 https://www.youtube.com/watch?v=Aglw5XsB3ac youtube 1     0 100
            6 https://www.youtube.com/user/ashens youtube 1     0 100
            7 https://www.youtube.com/results?search_query=Ashens youtube 1     0 100
            8 https://www.youtube.com/watch?v=gdCNE5L5yPw youtube 1     0 100
            9 https://www.news.com.au/  1     0 100
            10 http://news.com.au/  1     0 100
            11 https://www.eevblog.com/forum/ eevblog 1     0 100
            12 http://www.eevblog.com/forum eevblog 1     0 100
            13 https://www.eevblog.com/forum/general-computing/?PHPSESSID=b9meutagpcvch351dad438nr11 eevblog 1     0 100
            14 https://www.eevblog.com/forum/general-computing/linux-for-the-rest-of-us-ubuntus-(un)friendliness-dual-boot-w
in10-and-18-4lts/ eevblog 1     0 100
            15 https://www.eevblog.com/forum/general-computing/list-of-ethernet-netcards-with-jumbo-frame/ eevblog 1     0 10
0

            16 https://www.google.com/ google 2     0 100
            17 https://www.google.com/search?source=hp&ei=RJ6iXf_4IPO_8QO1_IrYCw&q=Office+Space+TPS+Report&oq=Office+Space+T
PS+Report&gs_l=psy-ab.3..018.14807.18157..18298...0.0..0.232.3459.0j19j3......0....1..gws-wiz.......0i131j0i10.bF2HWyXEiU4&v
ed=0ahUKEwj_quXbqZj1AhXsX3wKHTW-ArsQ4dUDCAs&uact=5 google 3     0 100
            18 https://en.wikipedia.org/wiki/TPS_report  1     0 100
            19 https://en.wikipedia.org/wiki/Software_test_documentation  1     0 100
```

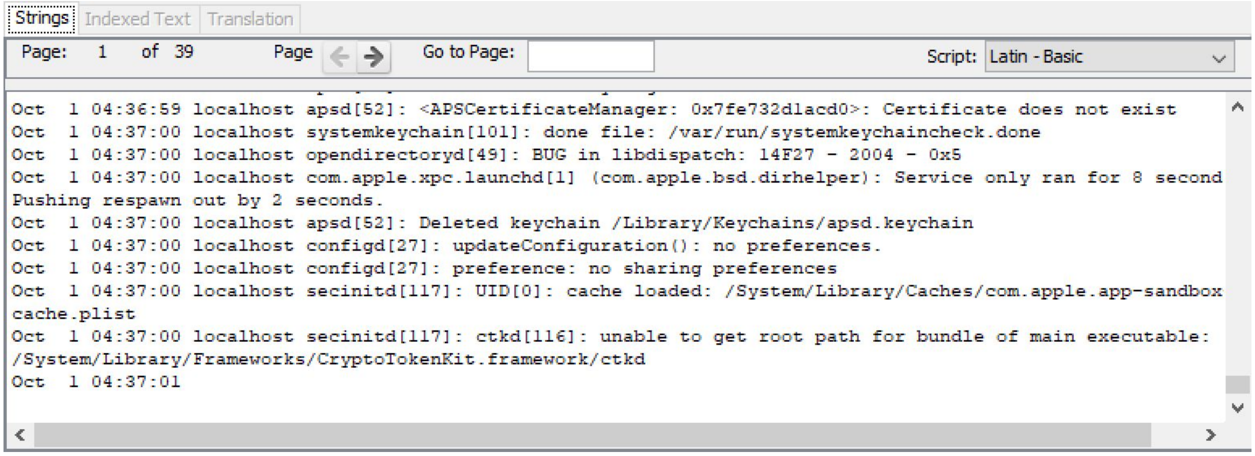
2. When was the computer last used?

The computer can be seen to be booted at 4:35:03 on Oct 1 with the last log occuring at Oct 1 4:37:01.



Name	S	C	Location	Modified Time	Change Time
system.log			/img_Macintosh HD Image.E01/private/var/log/system.log	2019-10-13 14:48:48 AEDT	2019-10-13 14:48:48 A
system.log-slack			/img_Macintosh HD Image.E01/private/var/log/system.log-…	2019-10-13 14:48:48 AEDT	2019-10-13 14:48:48 A

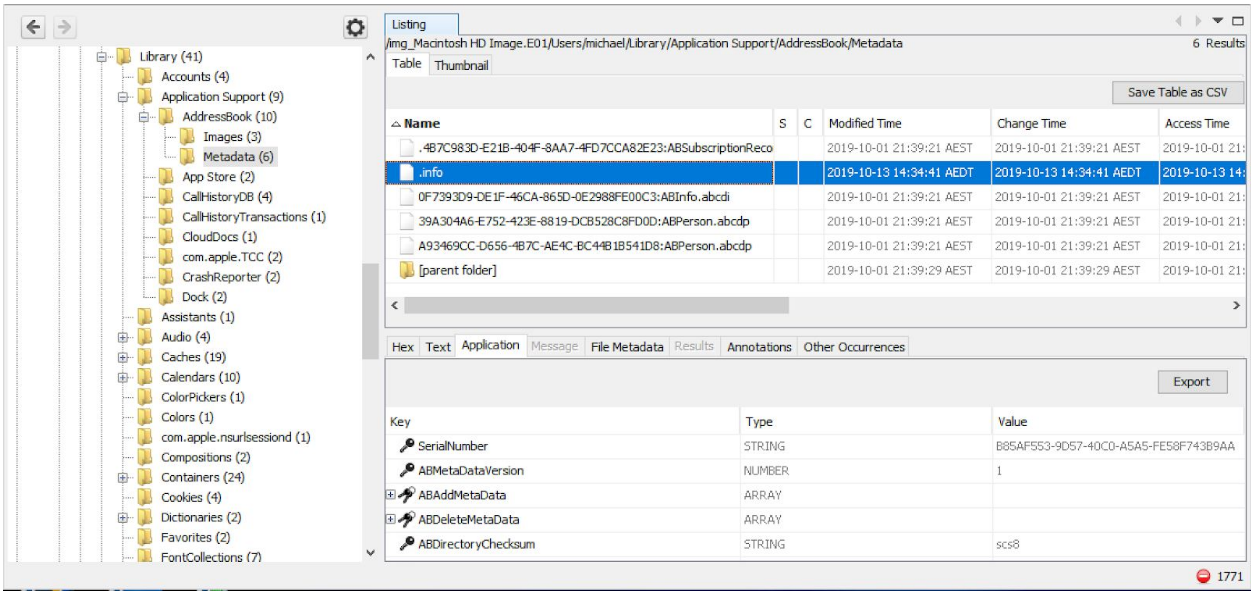
```
Oct  1 04:35:03 localhost bootlog[0]: BOOT_TIME 1569929703 0
Oct  1 04:36:54 localhost syslogd[19]: Configuration Notice:
          ASL Module "com.apple.AccountPolicyHelper" claims selected messages.
          Those messages may not appear in standard system log files or in the ASL database.
Oct  1 04:36:54 localhost syslogd[19]: Configuration Notice:
          ASL Module "com.apple.authd" sharing output destination "/var/log/asl" with ASL Module "com.apple
asl".
          Output parameters from ASL Module "com.apple.asl" override any specified in ASL Module "com.apple
authd".
Oct  1 04:36:54 localhost syslogd[19]: Configuration Notice:
          ASL Module "com.apple.authd" sharing output destination "/var/log/system.log" with ASL Module "co
apple.asl".
          Output parameters from ASL Module "com.apple.asl" override any specified in ASL Module "com.apple
authd".
```



```
Oct  1 04:36:59 localhost apsd[52]: <APSCertificateManager: 0x7fe732d1acd0>: Certificate does not exist
Oct  1 04:37:00 localhost systemkeychain[101]: done file: /var/run/systemkeychaincheck.done
Oct  1 04:37:00 localhost opendirectoryd[49]: BUG in libdispatch: 14F27 - 2004 - 0x5
Oct  1 04:37:00 localhost com.apple.xpc.launchd[1] (com.apple.bsd.dirhelper): Service only ran for 8 second
Pushing respawn out by 2 seconds.
Oct  1 04:37:00 localhost apsd[52]: Deleted keychain /Library/Keychains/apsd.keychain
Oct  1 04:37:00 localhost configd[27]: updateConfiguration(): no preferences.
Oct  1 04:37:00 localhost configd[27]: preference: no sharing preferences
Oct  1 04:37:00 localhost secinitd[117]: UID[0]: cache loaded: /System/Library/Caches/com.apple.app-sandbox
cache.plist
Oct  1 04:37:00 localhost secinitd[117]: ctkd[116]: unable to get root path for bundle of main executable:
/System/Library/Frameworks/CryptoTokenKit.framework/ctkd
Oct  1 04:37:01
```

3. Does this person have any contacts?

The user has a few contacts that can be found at Users/Michael/Library/Application Support/Address Book/Metadata which shows Michael as a contact, 1800-Apple, etc.

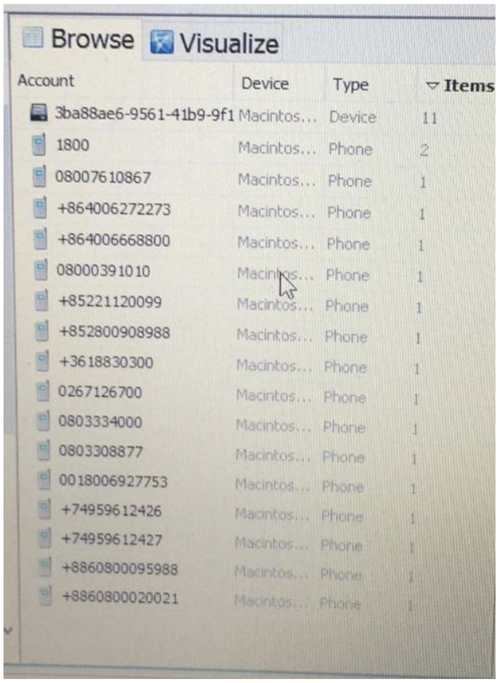


/img_Macintosh HD Image.E01/Users/michael/Library/Application Support/AddressBook/Metadata 6 Results

Name	S	C	Modified Time	Change Time	Access Time
.4B7C983D-E21B-404F-8AA7-4FD7CCA82E23:ABSubscriptionReco			2019-10-01 21:39:21 AEST	2019-10-01 21:39:21 AEST	2019-10-01 21:
.info			2019-10-13 14:34:41 AEDT	2019-10-13 14:34:41 AEDT	2019-10-13 14:
0F7393D9-DE1F-46CA-865D-0E2988FE00C3:ABInfo.abcdi			2019-10-01 21:39:21 AEST	2019-10-01 21:39:21 AEST	2019-10-01 21:
39A304A6-E752-423E-8819-DCB528C8FD0D:ABPerson.abcdp			2019-10-01 21:39:21 AEST	2019-10-01 21:39:21 AEST	2019-10-01 21:
A93469CC-D656-4B7C-AE4C-BC44B1B541D8:ABPerson.abcdp			2019-10-01 21:39:21 AEST	2019-10-01 21:39:21 AEST	2019-10-01 21:
[parent folder]			2019-10-01 21:39:29 AEST	2019-10-01 21:39:29 AEST	2019-10-01 21:

Key	Type	Value
SerialNumber	STRING	B85AF553-9D57-40C0-A5A5-FE58F743B9AA
ABMetaDataVersion	NUMBER	1
⊞ ABAddMetaData	ARRAY	
⊞ ABDeleteMetaData	ARRAY	
ABDirectoryChecksum	STRING	scs8

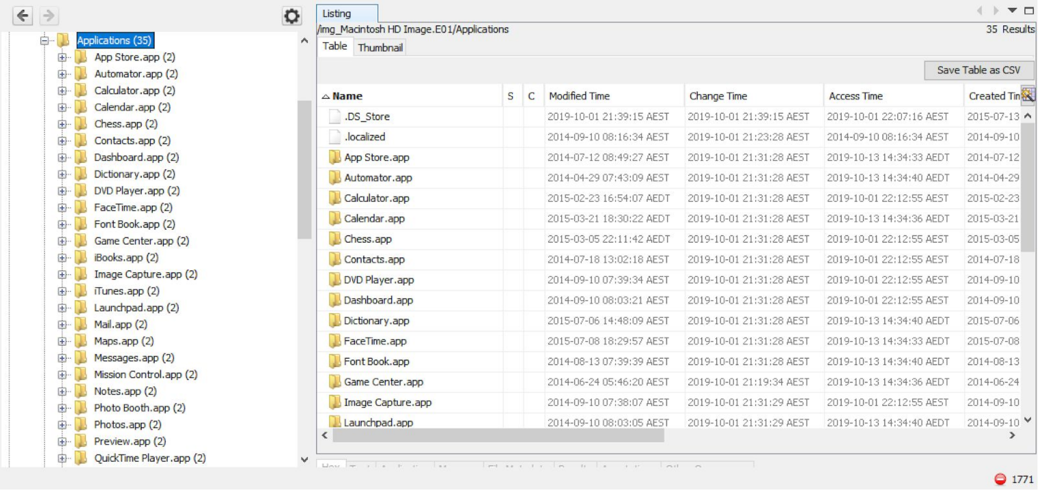
Furthermore, going into the “communications” tabs reveals some more contacts.



Account	Device	Type	Items
3ba88ae6-9561-41b9-9f1	Macintos...	Device	11
1800	Macintos...	Phone	2
08007610867	Macintos...	Phone	1
+864006272273	Macintos...	Phone	1
+864006668800	Macintos...	Phone	1
08000391010	Macintos...	Phone	1
+85221120099	Macintos...	Phone	1
+852800908988	Macintos...	Phone	1
+3618830300	Macintos...	Phone	1
0267126700	Macintos...	Phone	1
0803334000	Macintos...	Phone	1
0803308877	Macintos...	Phone	1
0018006927753	Macintos...	Phone	1
+74959612426	Macintos...	Phone	1
+74959612427	Macintos...	Phone	1
+8860800095988	Macintos...	Phone	1
+8860800020021	Macintos...	Phone	1

4. What programs are installed?

The user Michael has many programs installed (35). The image is just a snapshot of a few.



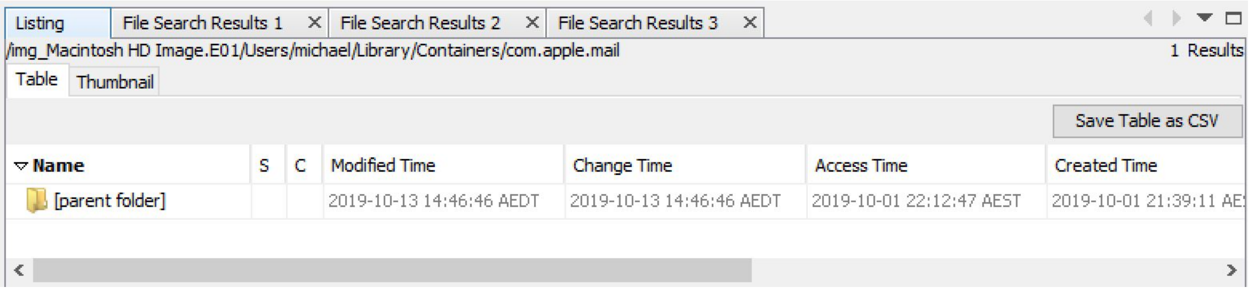
- Applications (35)
  - App Store.app (2)
  - Automator.app (2)
  - Calculator.app (2)
  - Calendar.app (2)
  - Chess.app (2)
  - Contacts.app (2)
  - Dashboard.app (2)
  - Dictionary.app (2)
  - DVD Player.app (2)
  - FaceTime.app (2)
  - Font Book.app (2)
  - Game Center.app (2)
  - iBooks.app (2)
  - Image Capture.app (2)
  - iTunes.app (2)
  - Launchpad.app (2)
  - Mail.app (2)
  - Maps.app (2)
  - Messages.app (2)
  - Mission Control.app (2)
  - Notes.app (2)
  - Photo Booth.app (2)
  - Photos.app (2)
  - Preview.app (2)
  - QuickTime Player.app (2)

/img_Macintosh HD Image.E01/Applications 35 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Tin
.DS_Store			2019-10-01 21:39:15 AEST	2019-10-01 21:39:15 AEST	2019-10-01 22:07:16 AEST	2015-07-13
.localized			2014-09-10 08:16:34 AEST	2019-10-01 21:23:28 AEST	2014-09-10 08:16:34 AEST	2014-09-10
App Store.app			2014-07-12 08:49:27 AEST	2019-10-01 21:31:28 AEST	2019-10-13 14:34:33 AEDT	2014-07-12
Automator.app			2014-04-29 07:43:09 AEST	2019-10-01 21:31:28 AEST	2019-10-13 14:34:40 AEDT	2014-04-29
Calculator.app			2015-02-23 16:54:07 AEDT	2019-10-01 21:31:28 AEST	2019-10-01 22:12:55 AEST	2015-02-23
Calendar.app			2015-03-21 18:30:22 AEDT	2019-10-01 21:31:28 AEST	2019-10-13 14:34:36 AEDT	2015-03-21
Chess.app			2015-03-05 22:11:42 AEDT	2019-10-01 21:31:28 AEST	2019-10-01 22:12:55 AEST	2015-03-05
Contacts.app			2014-07-18 13:02:18 AEST	2019-10-01 21:31:28 AEST	2019-10-01 22:12:55 AEST	2014-07-18
DVD Player.app			2014-09-10 07:39:34 AEST	2019-10-01 21:31:28 AEST	2019-10-01 22:12:55 AEST	2014-09-10
Dashboard.app			2014-09-10 08:03:21 AEST	2019-10-01 21:31:28 AEST	2019-10-01 22:12:55 AEST	2014-09-10
Dictionary.app			2015-07-06 14:48:09 AEST	2019-10-01 21:31:28 AEST	2019-10-13 14:34:40 AEDT	2015-07-06
FaceTime.app			2015-07-08 18:29:57 AEST	2019-10-01 21:31:28 AEST	2019-10-13 14:34:33 AEDT	2015-07-08
Font Book.app			2014-08-13 07:39:39 AEST	2019-10-01 21:31:28 AEST	2019-10-13 14:34:40 AEDT	2014-08-13
Game Center.app			2014-06-24 05:46:20 AEST	2019-10-01 21:19:34 AEST	2019-10-13 14:34:36 AEDT	2014-06-24
Image Capture.app			2014-09-10 07:38:07 AEST	2019-10-01 21:31:29 AEST	2019-10-01 22:12:55 AEST	2014-09-10
Launchpad.app			2014-09-10 08:03:05 AEST	2019-10-01 21:31:29 AEST	2019-10-13 14:34:40 AEDT	2014-09-10

5. Did the owner send/receive any emails?

Since /Users/Michael/Library/Containers/com.apple.mail is empty, no mail was exchanged.

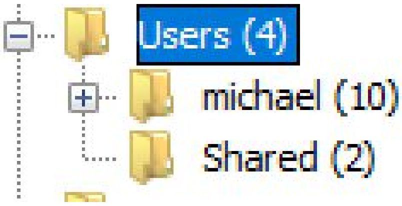


/img_Macintosh HD Image.E01/Users/michael/Library/Containers/com.apple.mail 1 Results

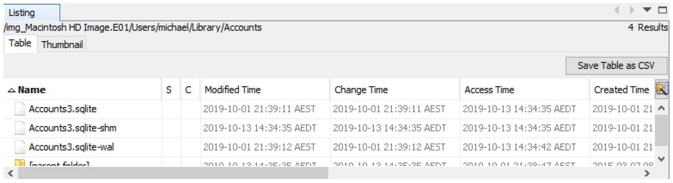
Name	S	C	Modified Time	Change Time	Access Time	Created Time
[parent folder]			2019-10-13 14:46:46 AEDT	2019-10-13 14:46:46 AEDT	2019-10-01 22:12:47 AEST	2019-10-01 21:39:11 AE

6. What accounts does the owner own?

The computer has two accounts, “Michael” and “Shared”. Within Michael, he has some SQL accounts.



- Users (4)
  - michael (10)
  - Shared (2)

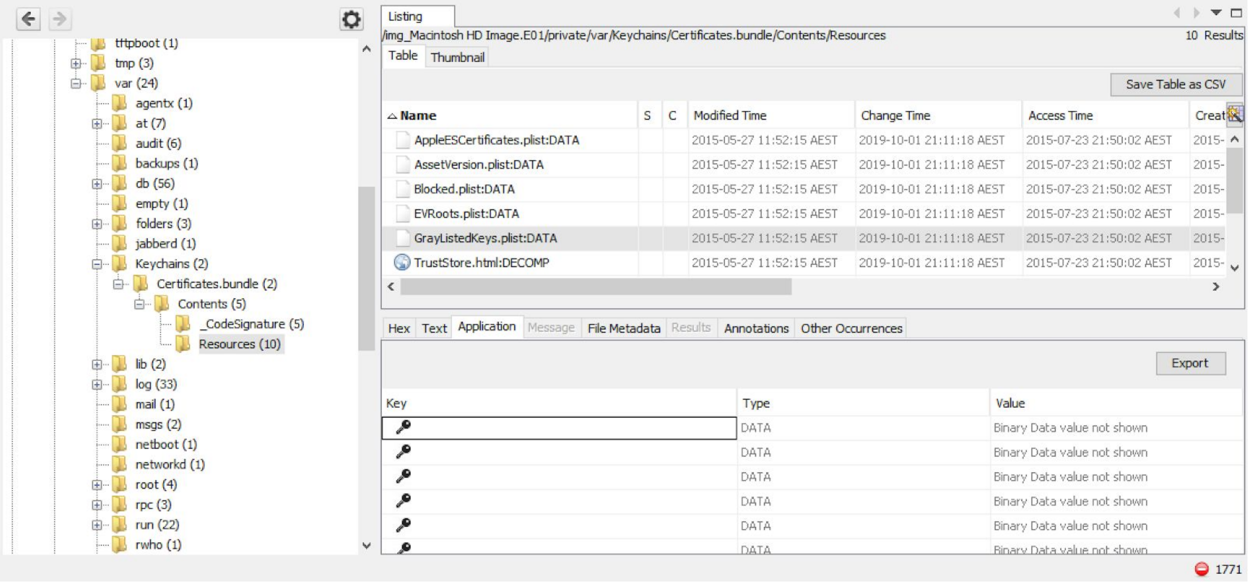


/img_Macintosh HD Image.E01/Users/michael/Library/Accounts 4 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time
Accounts3.sqlite			2019-10-01 21:39:11 AEST	2019-10-01 21:39:11 AEST	2019-10-13 14:34:35 AEDT	2019-10-01 21
Accounts3.sqlite-shm			2019-10-13 14:34:35 AEDT	2019-10-13 14:34:35 AEDT	2019-10-13 14:34:35 AEDT	2019-10-01 21
Accounts3.sqlite-wal			2019-10-01 21:39:12 AEST	2019-10-01 21:39:12 AEST	2019-10-13 14:34:42 AEDT	2019-10-01 21
[parent folder]			2019-10-13 14:35:35 AEDT	2019-10-13 14:35:35 AEDT	2019-10-01 21:38:47 AEST	2015-03-07 08

7. Are there any passwords in the system keychain?

There are a bunch of password stored in the system keychain, however they are encrypted so you would not be able to see them in plaintext. The can be seen in /private/var/keychains.



/img_Macintosh HD Image.E01/private/var/Keychains/Certificates.bundle/Contents/Resources

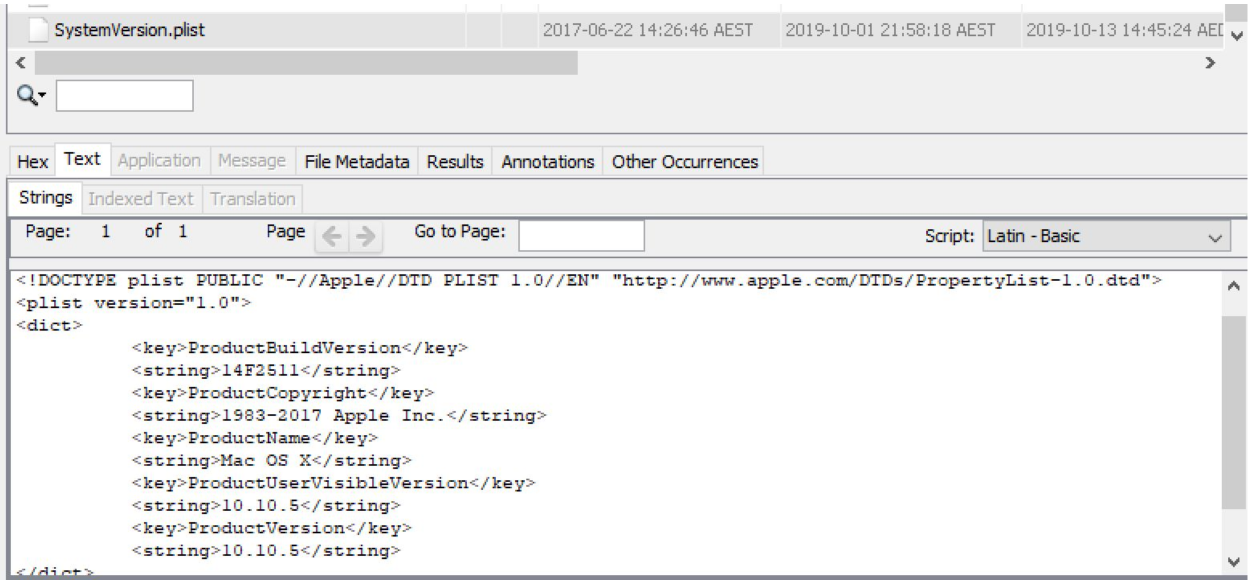
10 Results

Name	S	C	Modified Time	Change Time	Access Time	Creat
AppleESCertificates.plist:DATA			2015-05-27 11:52:15 AEST	2019-10-01 21:11:18 AEST	2015-07-23 21:50:02 AEST	2015-
AssetVersion.plist:DATA			2015-05-27 11:52:15 AEST	2019-10-01 21:11:18 AEST	2015-07-23 21:50:02 AEST	2015-
Blocked.plist:DATA			2015-05-27 11:52:15 AEST	2019-10-01 21:11:18 AEST	2015-07-23 21:50:02 AEST	2015-
EVRoots.plist:DATA			2015-05-27 11:52:15 AEST	2019-10-01 21:11:18 AEST	2015-07-23 21:50:02 AEST	2015-
GrayListedKeys.plist:DATA			2015-05-27 11:52:15 AEST	2019-10-01 21:11:18 AEST	2015-07-23 21:50:02 AEST	2015-
TrustStore.html:DECOMP			2015-05-27 11:52:15 AEST	2019-10-01 21:11:18 AEST	2015-07-23 21:50:02 AEST	2015-

Key	Type	Value
	DATA	Binary Data value not shown
	DATA	Binary Data value not shown
	DATA	Binary Data value not shown
	DATA	Binary Data value not shown
	DATA	Binary Data value not shown
	DATA	Binary Data value not shown

8. What version is the operating system?

The operating system version can be found in System/Library/CoreServices/SystemVersion.plist. It is Mac OS X 10.10.5.



SystemVersion.plist		2017-06-22 14:26:46 AEST	2019-10-01 21:58:18 AEST	2019-10-13 14:45:24 AEI

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
          <key>ProductBuildVersion</key>
          <string>14F2511</string>
          <key>ProductCopyright</key>
          <string>1983-2017 Apple Inc.</string>
          <key>ProductName</key>
          <string>Mac OS X</string>
          <key>ProductUserVisibleVersion</key>
          <string>10.10.5</string>
          <key>ProductVersion</key>
          <string>10.10.5</string>
</dict>
```