

Lab 2 Forensic

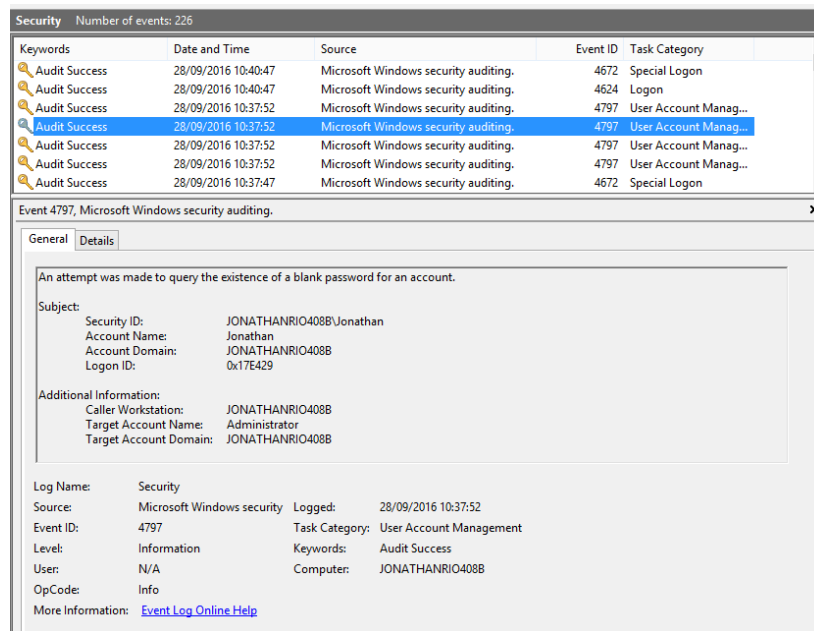
Student ID: C13432152

Student Name: Jonathan Riordan

1. Windows

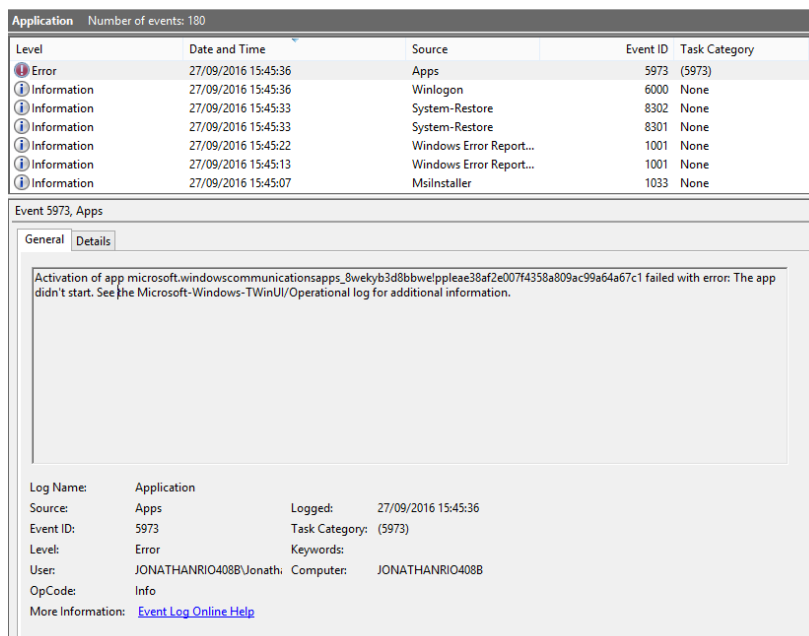
Security Log

The security log in Windows is a log that contains records of login and logout on the system. The data and time can be used by forensic to check when a user was logged in. Information such as the account name can be retrieved from the log when a user logged in. Other information such as failed login attempts onto the system is recorded.



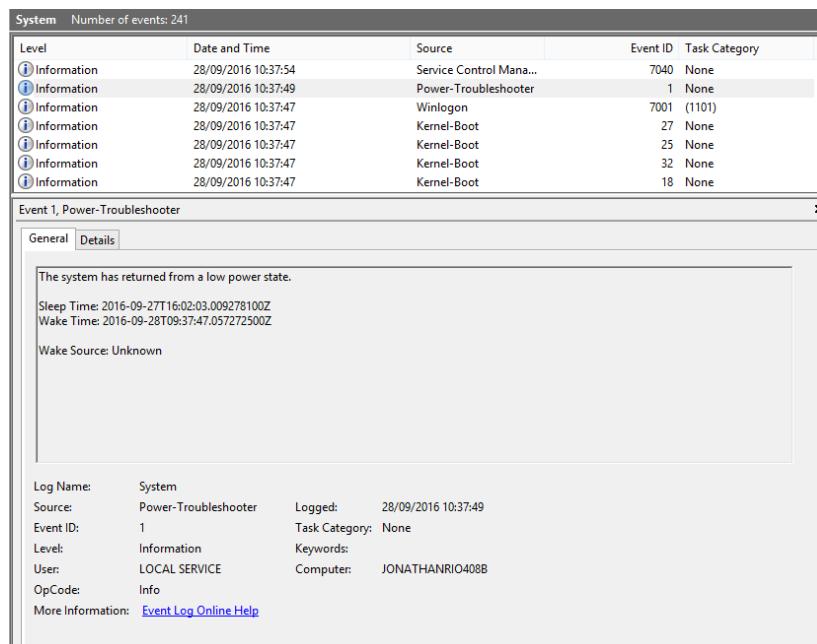
Application log

The application log records details about the applications on the system. This information can be as application crashes. The computer name, the date and time of the log and level is stored in the application log. The following screen shot shows displays a log where the microsoft communication app failed to open. Its events were recorded.



System log

The system log is used to record information in relation the system. Information such as time change of the system to the hard ware clock is recorded. Any event that the system does it recorded. Another type of event could be when the system went to sleep then woke up. As before, information such as the user, date and time of the log and Computer name is recorded. The Systems log records information written by device drivers.



Forwarded Events log

This log records events written by other computers in the same network. One computer is selected as the hub for all these computers, where other computers logs will be sent to. From this log, a user will be able to keep track of event logs from other computer while on one computer.

Application and services log.

These logs record information about a single event of an application. There are different types of subcategory in these logs such as Admin, Analytic, Debug and Operational.

The debug logs store information about debugging an application or program.

The analytic log records events that follow an issue while the operational is used for analysing and diagnosing a problem or occurrence.

2. Linux

1. **/var/log/faillog Log**

It is a binary file that records the information of the number of failed logged in attempts into a computer. The date and the number of attempts are stored in the file. Running `faillog` just in the command line will just display the list of users who have ever failed logging in. To specify a specific user, the `-u` flag must be added in the command line or to print all the users with the `-a`.

2. **/var/log/kern.log Log**

This log records information from the kernel of linux.

3. **/var/log/lpr.log Log**

This log is related to the printer. Files that get sent to be printed are recorded. Information in this log can be used by forensic to see what names of files have been printed and the date they were printed. Also information such as the computer name and the printer name can be retrieved from this log.

4. **/var/log/mail.* Log**

Contains information from the mail server running on the system. This information can be used by forensic to identify what email have been both sent and received on a device. Information such as the computer and timestamp is recorded.

3. Macintosh

/var/log log

From the following path, there is numerous log files such as `install.log`, `wifi.log`, `system.log` and `fsck_hfs.log`. Each of these files contain different information based on the system. The files record data so for example.

In the `install.log`, Information about packages will be stored in the file. The information consists of the application name, the date and time the application was installed on the device, where the package was downloaded from such as the apple store and the path where the package was installed. Other information stored in this file is any software updates.

The following image is an example from the file.

```
Sep 21 14:36:37 MacBook-Pro-3 storedownload[407]: PackageKit: Registered bundle file:///Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/Library/
```

The wifi log file contain information about the packages been sent between the Mac and

The system log file contains information about was applications or process have been used. It records a timestamp of when an application has been opened In the following image, the application iBooks was opened at 9:35:39 on the 23rd of September.

```
Sep 23 09:35:39 macbook-pro-3 iBooks[7354]: objc[7354]: Class SFUCryptoKey is implemented in both /Applications/iBooks.app/Contents/Frameworks/TSUtility.framework/Versions/A/TSUtility (0x109d61eb0) and /Applications/iBooks.app/Contents/Frameworks/IMCommonCore.framework/
```

2. /var/spool/cups

The logs recorded in this information deal with printing. Information such as what printer was used. The forensic relevance is that each file contains information about printing. The printer name that printed it and the name of the file that was printed. Each file in the cup folder is when a file was printed.

```
0Gattributes-charsetutf-8Hattributes-natural-languageen-usE
printer-uri0ipp://localhost:631/printers/Canon_MG3500_seriesBjob-originating-user-name
macbookproBjob-name0Dublin Institute of Technology Mail - DT228-2 Semester 2 Exam
Timetable
```

3. /var/vm

This path contains eight images from a sleep image file to swapfiles ranging from 0 to 8. The sleep image creates an image of your mac before the mac went to sleep, therefore when a user wakes u their make, the state will be the same before the mac went to sleep.

4. Browser.

On mac, to view Safari log, the path is /Users/macbookpro/Library/Safari/history.db

I had to open the .db file using an application called Datum. The information stored in this file is id, url, domain_expansion, visit count, daily, count and weekly count. There is also more information sited as well such as visit time.

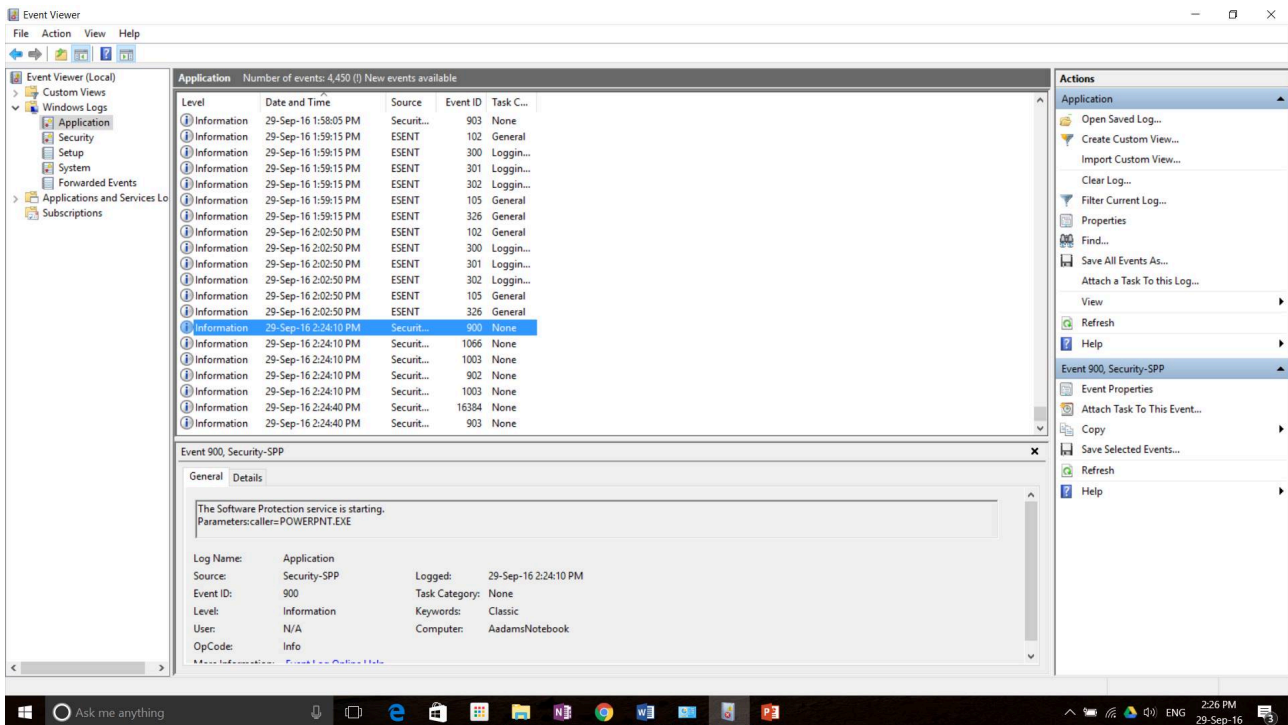
The following is an example from the history.db file.

	id	url	domain_expansion	visit_count
1	74,289	https://www.facebook.com/	facebook	2,596
2	101,028	http://google.com/	google	5
3	101,114	https://dit-bb....b_group_id=_1_1	dit-bb.blackboard	17

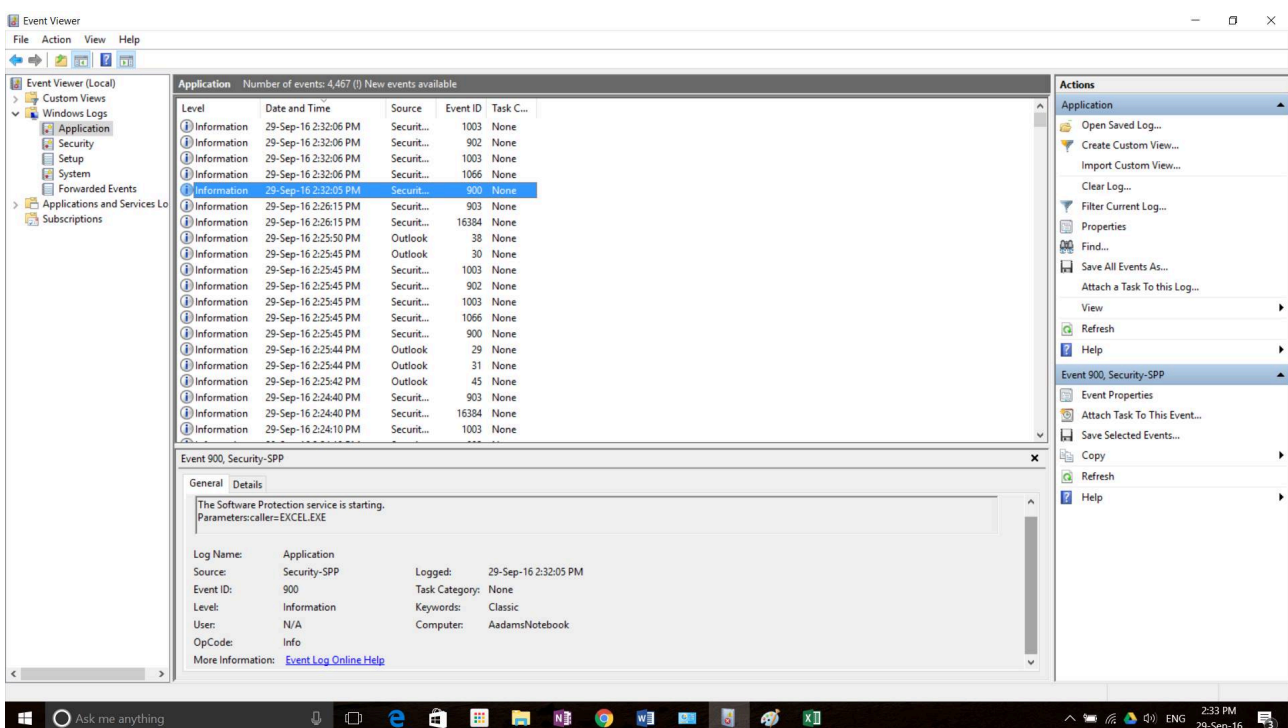
I couldn't view my last history as within that file, there is multiple tables and some of the tables such as time visited and the daily count rows are encrypted.

5. Application

The following is a log been recorded for Microsoft powerpoint running on a Windows machine. As we can see from the image, the timestamp, Computer name event ID and the executable file is recorded.



The following is an example of Microsoft Excel been logged into the application folder. as previously before, the timestamp, computer name, event ID and executable file is recorded.



6. Password

The hash value for the file is: bce793a19d80e648b579d0521eb51d9

I got this value using the md5 command in the command line on mac.

```
[MacBook-Pro-3:~ Jonathan$ md5 Dublin-Break.docx  
MD5 (Dublin-Break.docx) = bce793a19d80e648b579d0521eb51d9c
```

The password for the Dublin-break.docx file is: 1234

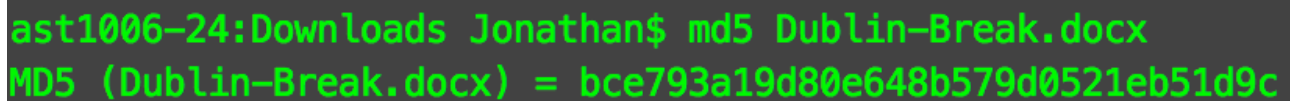
I retrieved the password by just doing brute force. I tested multiple password from the website <http://www.passwordrandom.com/most-popular-passwords>. Eventually password 4 worked from the site.

This website contains the most common password.

#:	Password	MD5	Length	L	U	N	Meter
1	password	5f4dcc3b5aa765d61d8327deb882cf99	8	8	0	0	check
2	123456	e10adc3949ba59abbe56e057f20f883e	6	0	0	6	check
3	12345678	25d55ad283aa400af464c76d713c07ad	8	0	0	8	check
4	1234	81dc9bdb52d04dc20036dbd8313ed055	4	0	0	4	check
5	qwerty	d8578edf8458ce06fbc5bb76a58c5ca4	6	6	0	0	check
6	12345	827ccb0eea8a706c4c34a16891f84e7b	5	0	0	5	check
7	dragon	8621ffdbc5698829397d97767ac13db3	6	6	0	0	check

The following is a screenshot of the dublin-break file.

After opening the file, I checked the hash value. The hash value after getting the password was:

A screenshot of a terminal window with a dark background and green text. The text shows a file path and its MD5 hash.

```
ast1006-24:Downloads Jonathan$ md5 Dublin-Break.docx  
MD5 (Dublin-Break.docx) = bce793a19d80e648b579d0521eb51d9c
```

The hash vales are the same.

The following image is a screen shot of the contents in the file.

Forensics – DT228-4 and DT211-4

Lab Sheet 2

Is memory forensics a forensics discipline all its own? Not really. You're unlikely to work an entire case using only memory artifacts (although you will learn how). To be a true forensics professional though, you have to understand what's available in the different forensics disciplines. Memory is definitely one of those disciplines. If you think that running half a dozen volatility plugins is all there is to memory forensics, we have much to teach you. Just as disk forensics practitioners understand filesystem layouts, we'll teach you memory layouts and how to interpret key structures in memory.

7. Auditpol/ Winzapper

I tried to do auditpol on windows virtual machine, but I was unable as my user didn't have the right privileges. "A required privilege is not held by the client.". I spent a while searching the web on how to grant my self privileges for deleting files on the C drive but was unsuccessful.

Also Auditpol isn't on Mac, therefore I couldn't do it and I couldn't find a stable version of Winzapper online without been prompted that the software I downloaded may have a virus.

I did look up what auditpol does, it logs the deletion of a file or folder by a user. To view the log, the user would have to go to their security log on their device and search for the event ID: 560.

This would be used by forensic to identify what files have been deleted and when. The only problem with this is that a user must enable auditing for a specific folder in their C drive.

References.

1. [https://technet.microsoft.com/en-us/library/cc722404\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc722404(v=ws.11).aspx)
2. http://windows.tips.net/T012886_What_is_the_Purpose_of_the_Application_Event_Log.html
3. <https://help.ubuntu.com/community/LinuxLogFiles>
4. <http://www.computerhope.com/unix/ulpr.htm>
5. <http://www.passwordrandom.com/most-popular-passwords>