**Tools**

I used several digital forensics tools such as xplico and autopsy to investigate the given data which included photos and raw data with browser URLs.

First target was Skype info

So in this domain I used xplico to run the skype id command of the targeted account as well as the IPv6 address codes which can help us scope and obtain the raw data captured by the used device (in this case iPhone)

Graphical user interface, text, application

Description automatically generated

Results

Below are the results of the outcome after running our commands on the software

Graphical user interface, application

Description automatically generatedGraphical user interface, application, table

Description automatically generatedGraphical user interface, application

Description automatically generatedGraphical user interface, application

Description automatically generatedGraphical user interface, application

Description automatically generated

Interpretation

Its clear from the above results (check the blue arrow) that any data stored locally on the device or on cloud had been altered/tempered/deleted, although there are some recovery options to try retrieve tempered data from iCloud, these will take awhile to restore the data without the knowledge of the target

Reason is because using normal recovery procedures will result to the target being put on notice by her service iCloud providers.

Next was to identify the individual behind [jmmmy1stq40@aol.com](mailto:jmmmy1stq40@aol.com) email address

Graphical user interface, text, application, email

Description automatically generated

Although their email domain providers AOL restricted the true names (what we were after) ,we managed to obtain the general location of the individual

Note: this is something we can narrow down to, only with time since it’s a bit hectic to get into the individuals email domain servers.

Lastly was to investigate the web browsing URLs

Using colab and autopsy to investigate the network traffic of the highest frequency URLs

Graphical user interface, text, application

Description automatically generated

Text

Description automatically generated

Graphical user interface, text, application, Teams

Description automatically generated

Interpretation

Microsoft tops the most browsed url with diferent login commands at different locations,used to send in login commands but hiding the activity beyond the logins

Reason ,similar to the skype data ,the urls traffic icloud data was tempered with preventing any remote access to it,only option will be to connect direct to the hard drive of the target device to scope the data locally (since all icloud data has been tempered with)

Some more address locations connected to the target based on their IP addresses

Graphical user interface, text, application, email

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

Conclusion

Having ran some digital forensics tools to the given data and analysing it, the outcome did not provide a more detailed information behind the target since all the iCloud data which could be accessed remotely to investigate the target was intentionally altered, limiting us to connect to the hard drive of the target device to scope the data manually and use specific forensic tools specified for this type of connection to carry out the investigation