

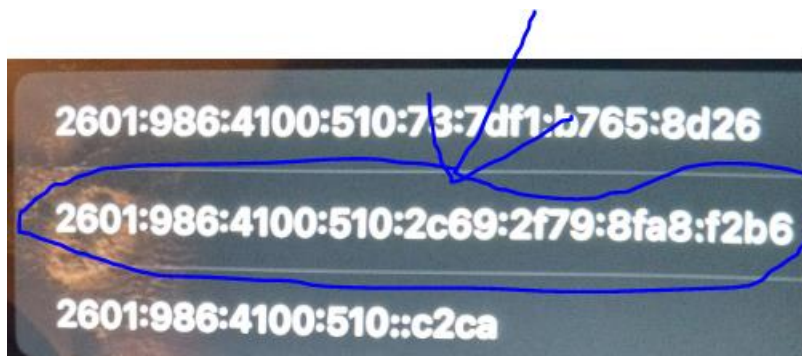
## Tools

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)

live:.cid.6e2662b5251aeaaa



## Results

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






## 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 [jimmy1stq40@aol.com](mailto:jimmy1stq40@aol.com) email address

<input checked="" type="checkbox"/> <b>Country</b>	 United States of America [US] ⓘ
<input type="checkbox"/> <b>Region</b>	Connecticut
<input type="checkbox"/> <b>City</b>	Hartford
<input type="checkbox"/> <b>Coordinates of City†</b>	41.763710, -72.685090 (41°45'49"N 72°41'6"W)
<input type="checkbox"/> <b>ISP</b>	AT&T Worldnet Services
<input type="checkbox"/> <b>Local Time</b>	13 May, 2022 05:52 AM (UTC -04:00)
<input type="checkbox"/> <b>Domain</b>	att.net
<input type="checkbox"/> <b>Net Speed</b>	(DSL) Broadband/Cable/Fiber/Mobile
<input type="checkbox"/> <b>IDD &amp; Area Code</b>	(1) 860
<input type="checkbox"/> <b>ZIP Code</b>	06101
<input type="checkbox"/> <b>Weather Station</b>	Hartford (USCT0094)

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

File Edit View Insert Runtime Tools Help All changes saved

Files

RAM 8 GB Disk 100 GB

Editing

+ Code + Text

```
[1] import pandas as pd
data=pd.read_csv('/content/drive/MyDrive/BrowsingHistory.csv')
data
```

1 to 25 of 870 entries

Filter ⓘ

index	DateTime	DeviceId	NavigatedToUri	PageTitle	SearchTerms
510	4/24/2022 7:24:10 PM +00:00	NaN	view-source:https://www.icloud.com/contacts/	NaN	NaN
400	4/27/2022 7:55:14 PM +00:00	NaN	https://www.wikihow.com/Find-Your-Apple-ID	www.wikihow.com	NaN
420	4/26/2022 12:39:39 AM +00:00	NaN	https://www.w3.org/WAI/GL/wiki/Unicode_Character_with_an_On-Screen_Text_Alternative	www.w3.org	NaN
421	4/26/2022 12:39:38 AM +00:00	NaN	https://www.w3.org/WAI/GL/wiki/Providing_an_On-Screen_Text_Alternative_for_an_Icon_Font	www.w3.org	NaN

```

▶ data['NavigatedToUrl']

0  https://ntp.msn.com/edge/ntp?locale=en-US&titl...
1  https://ntp.msn.com/edge/ntp?locale=en-US&titl...
2  https://ntp.msn.com/edge/ntp?locale=en-US&titl...
3  https://ntp.msn.com/edge/ntp?locale=en-US&titl...
4  https://ntp.msn.com/edge/ntp?locale=en-US&titl...
...
865 https://outlook.live.com/mail/0/
866 https://outlook.live.com/calendar/0/view/month
867 https://outlook.live.com/calendar/0/
868 https://www.tiktok.com/foryou?is_copy_url=1&is...
869 https://account.microsoft.com/account/privacy?...
Name: NavigatedToUrl, Length: 870, dtype: object

```

examining URL activities

```

[ ] Frequency=set_as_(high,)
review_activity_on_url(['https://account.microsoft.com/account/privacy', 'https://ntp.msn.com/edge/ntp?locale=en-US&titl'])
output=None

```

```

[ ] network_traffic=[]
for i in data['NavigatedToUrl']:
    network_traffic.append(i)
network_traffic[100:400]

```

✓ 0s completed at 12:09 PM

Tools Help All changes saved

```

X + Code + Text

[ ] 'https://www.bing.com/search?q=iforgot.apple.com+password&cvid=3c3f995560c24481a48edb28f540b043&aqs=edge.3.69i60'
    'https://www.office.com/?auth=1',
    'https://www.apple.com/',
    'https://appleid.apple.com/',
    'https://apps.microsoft.com/store/detail/icloud/9PKTQ5699M62?hl=en-us&gl=US',
    'https://support.apple.com/en-us/HT204283',
    'https://www.bing.com/search?q=icloud&cvid=2bdb82aeb99342b8b0b06f02ab1209ff&aqs=edge.2.0j69i57j0l6j69i60.7003j0j:

▶ review_activity_on_url(network_traffic)
Result= account.microsoft(sending login commands\...\b)

```

## 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

☒ **IP Address**

71.200.171.43

☒ **Country**

 [United States of America \[US\]](#) 

☐ **Region**

Delaware

☐ **City**

Dover

☐ **Coordinates of City<sup>†</sup>**

39.158170, -75.524370 (39°9'29"N 75°31'28"W)

☐ **ISP**

Comcast Cable Communications LLC

☐ **Local Time**

13 May, 2022 05:25 AM (UTC -04:00)

☐ **Domain**

comcast.net

☐ **Net Speed**

(DSL) Broadband/Cable/Fiber/Mobile

☐ **IDD & Area Code**


(1) 302

☐ **ZIP Code**

19901

☐ **Weather Station**

Dover (USDE0012)

<input checked="" type="checkbox"/> IP Address	98.18.116.164
<input checked="" type="checkbox"/> Country	 United States of America [US] ⓘ
<input type="checkbox"/> Region	Georgia
<input type="checkbox"/> City	Clayton
<input type="checkbox"/> Coordinates of City†	34.878150, -83.400990 (34°52'41"N 83°24'4"W)
<input type="checkbox"/> ISP	Windstream Communications LLC
<input type="checkbox"/> Local Time	13 May, 2022 05:28 AM (UTC -04:00)
<input type="checkbox"/> Domain	windstream.com
<input type="checkbox"/> Net Speed	(DSL) Broadband/Cable/Fiber/Mobile
<input type="checkbox"/> IDD & Area Code	(1) 706
<input type="checkbox"/> ZIP Code	30525
<input type="checkbox"/> Weather Station	Clayton (USGA0118)

## 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