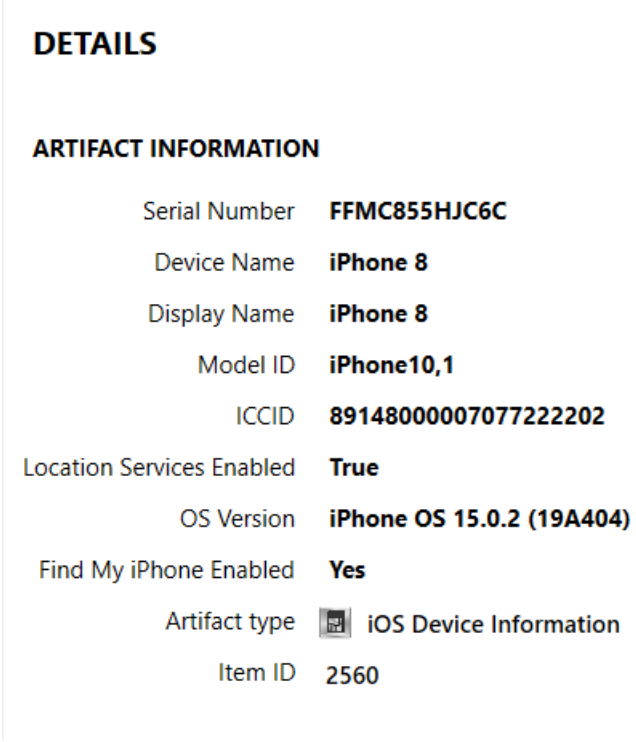
Forensics Lab

Author: Hui Nok Hang

Analysis on iPhone

In this forensics investigation, I will mainly focus on the location data extracted from the iPhone. From there, I will attempt to extrapolate the behaviours of the user of this phone, aided by the location analysis and data from other sections of Magnet Axiom.

Device Information



DETAILS

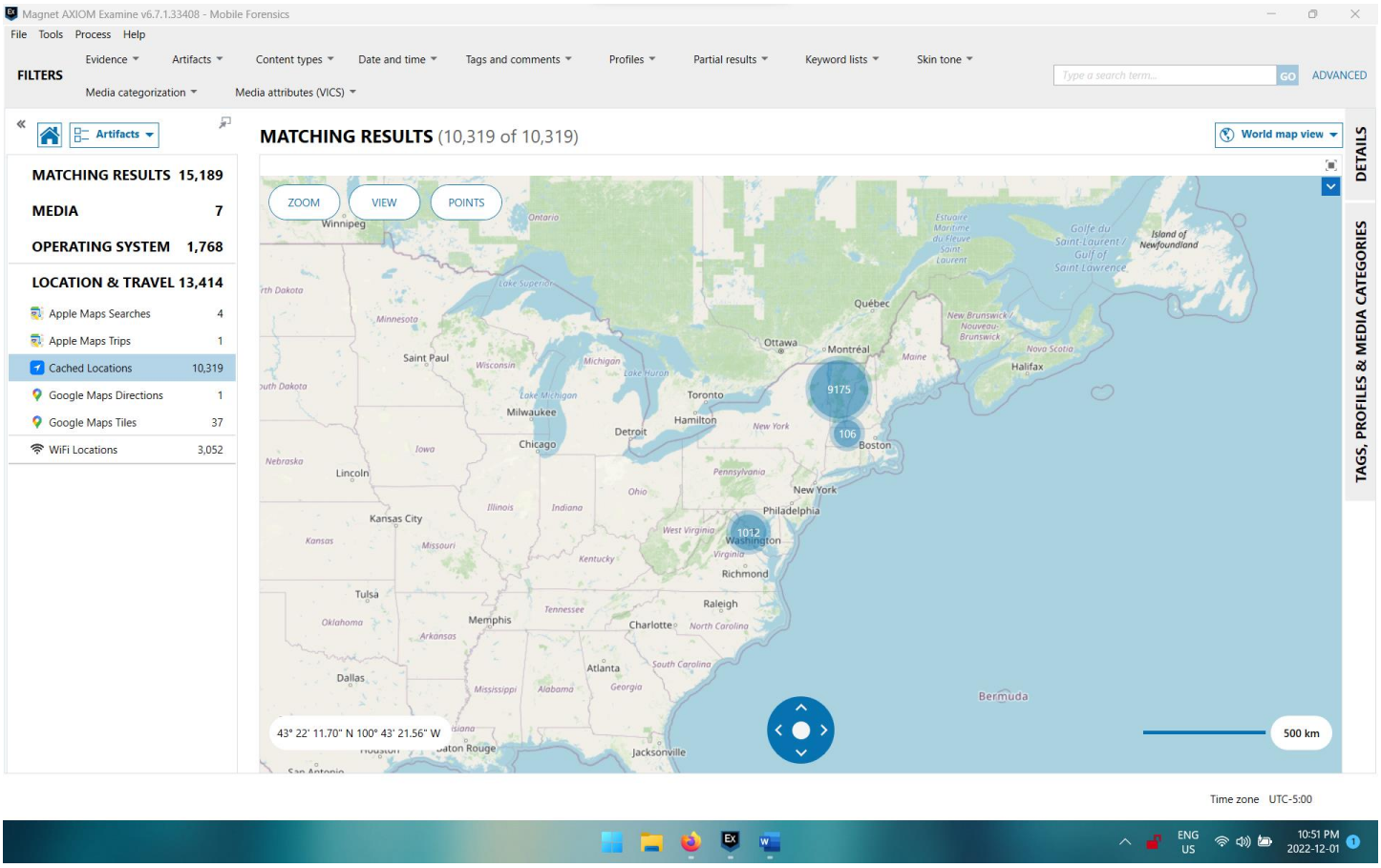
ARTIFACT INFORMATION

Serial Number	**FFMC855HJC6C**
Device Name	**iPhone 8**
Display Name	**iPhone 8**
Model ID	**iPhone10,1**
ICCID	**89148000007077222202**
Location Services Enabled	**True**
OS Version	**iPhone OS 15.0.2 (19A404)**
Find My iPhone Enabled	**Yes**
Artifact type	iOS Device Information
Item ID	2560

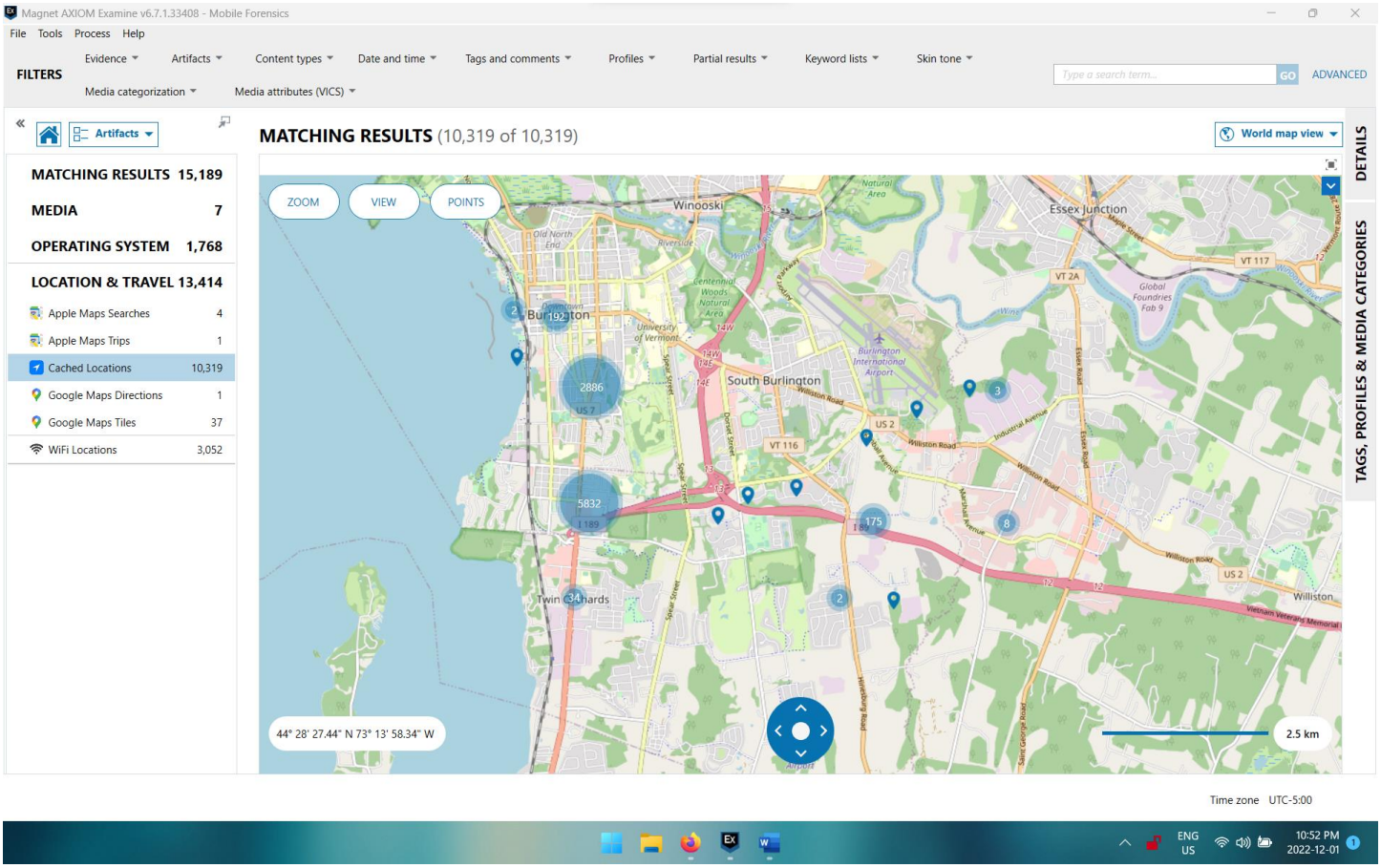
To start off the analysis, this phone is an iPhone 8 running iOS 15.0.2.

Location analysis

Cached locations is showing the there are 3 main clusters of locations on the iPhone. All 3 clusters are concentrated on the US East Coast – respectively in Burlington Vermont, Willington Massachusetts, and Fairfax Virginia. Most of the cached location data (9175) seem to be around Burlington, so we first start our investigation there.

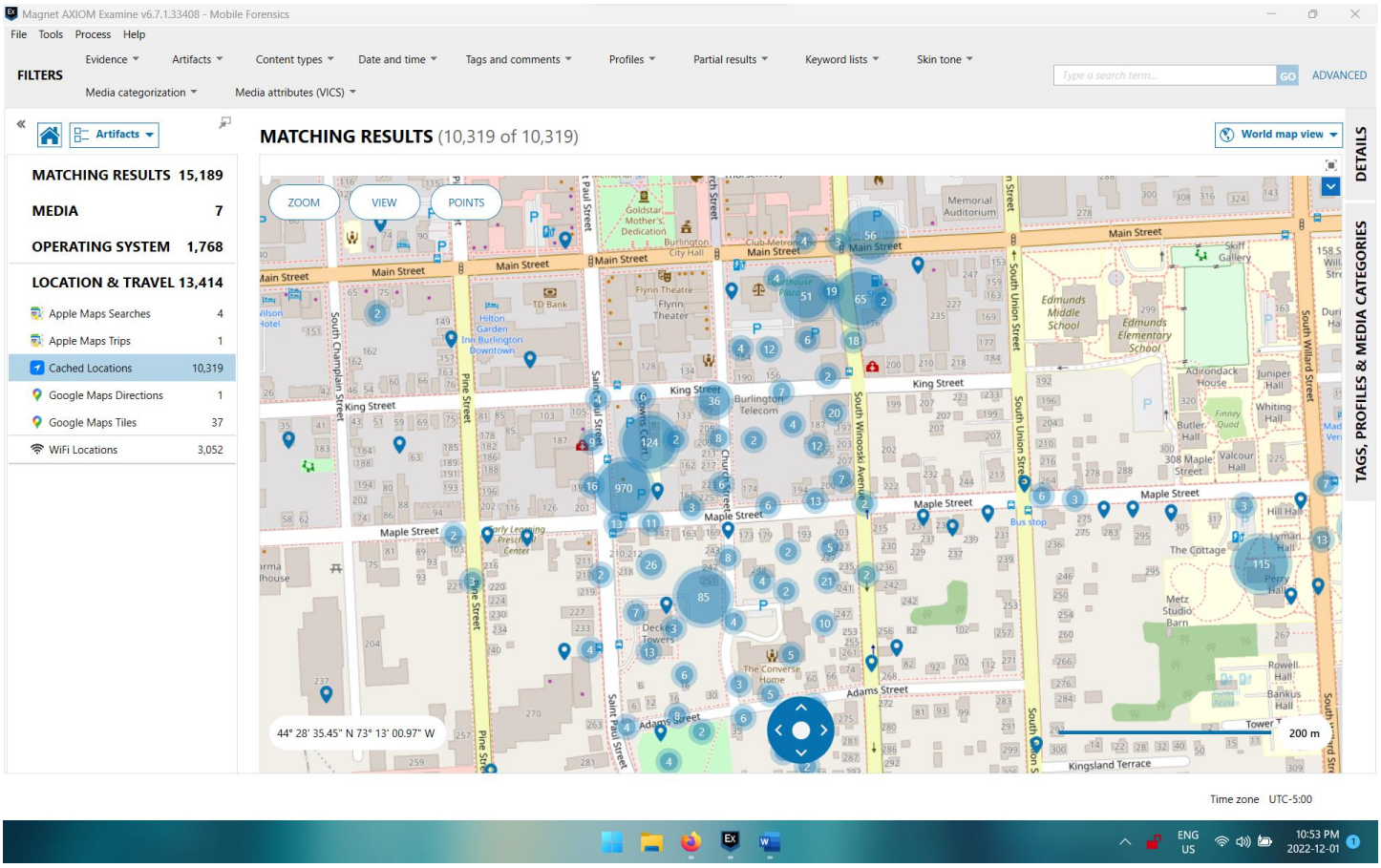


In Burlington, there are also 3 main clusters. Two big clusters appear in Downtown Burlington while a smaller one is in residential areas.

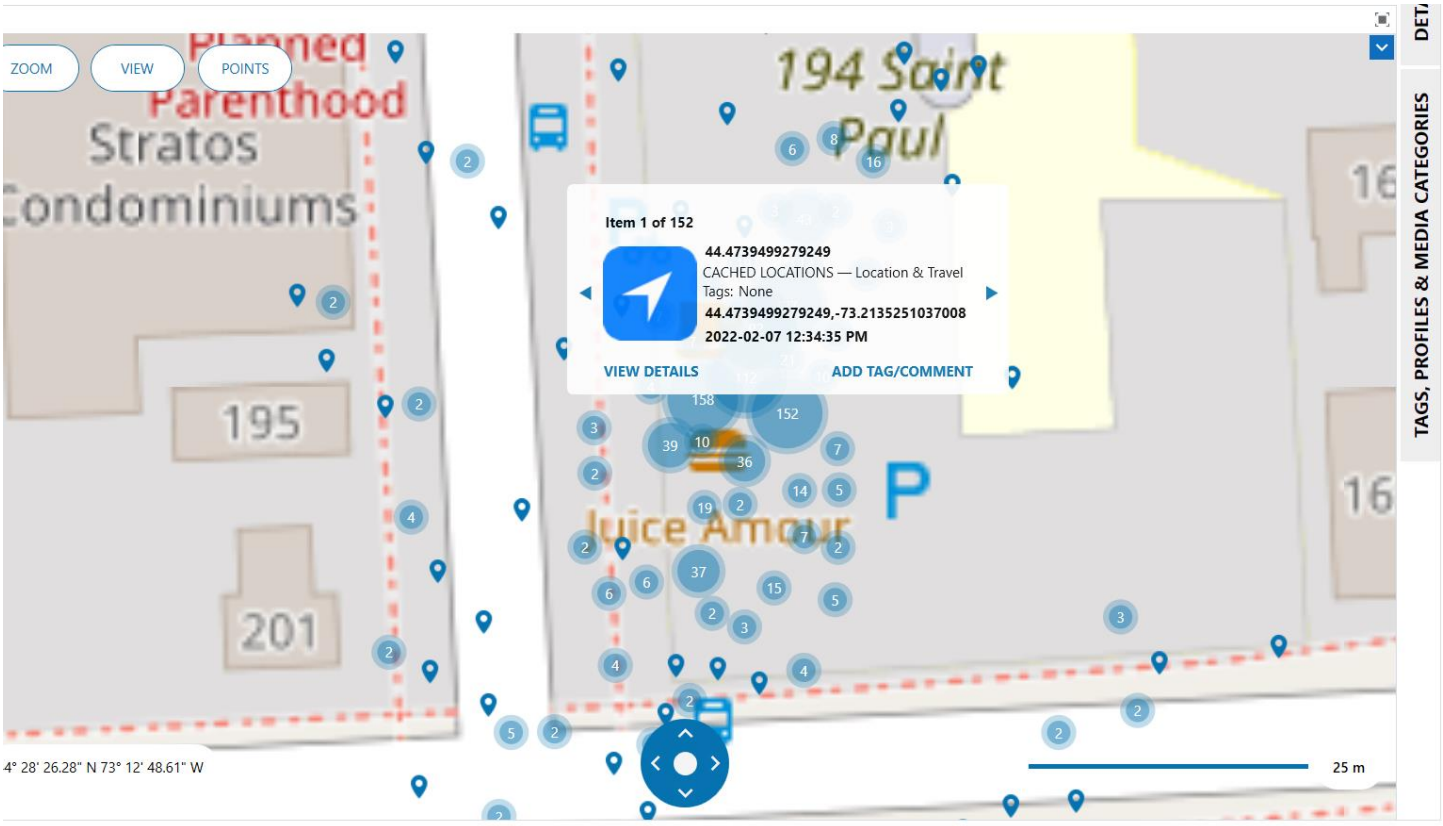


Downtown hotspot 1

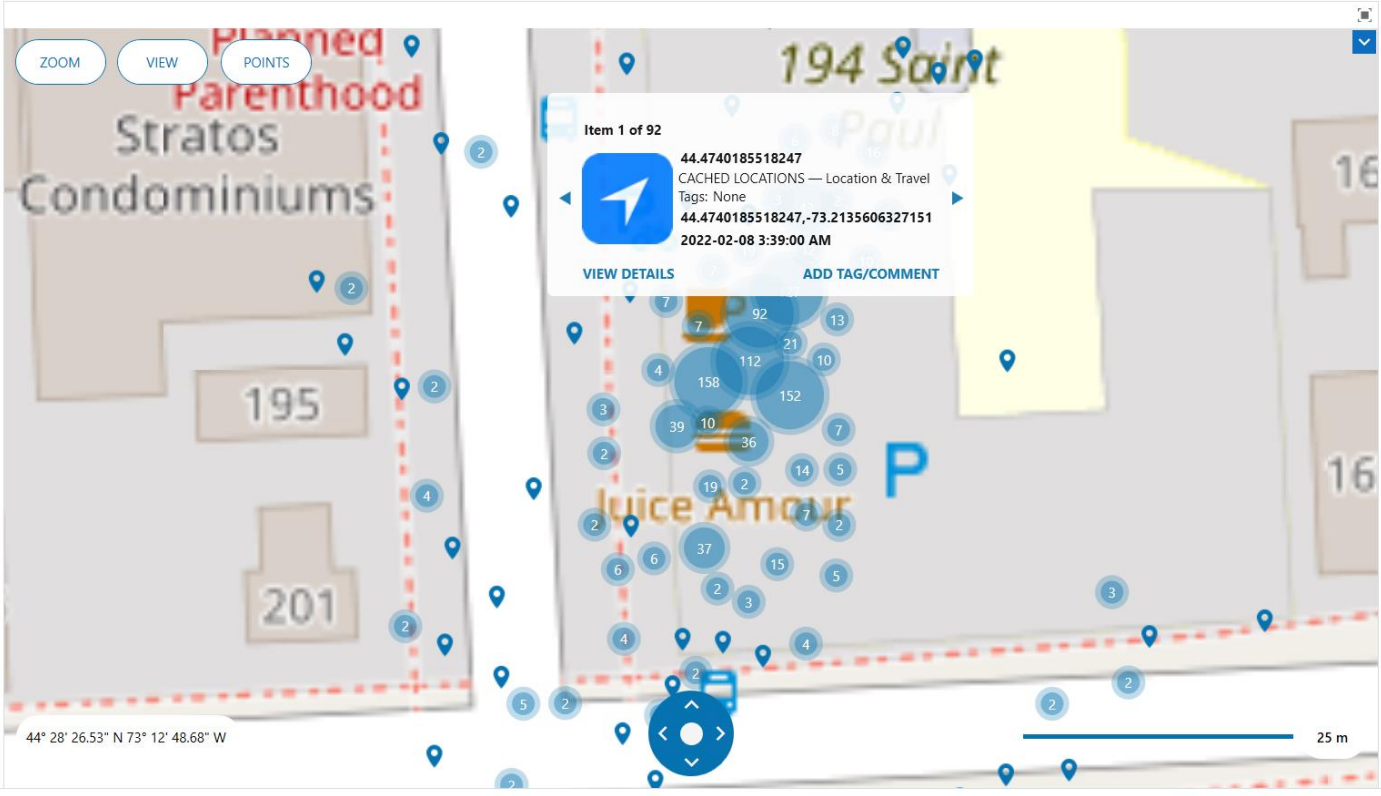
One of the Downtown Burlington locations encompass a grid around Main Street and Pine Street. The points are fairly scattered on a micro scale, therefore it is difficult to determine what the user of the iPhone was there for.

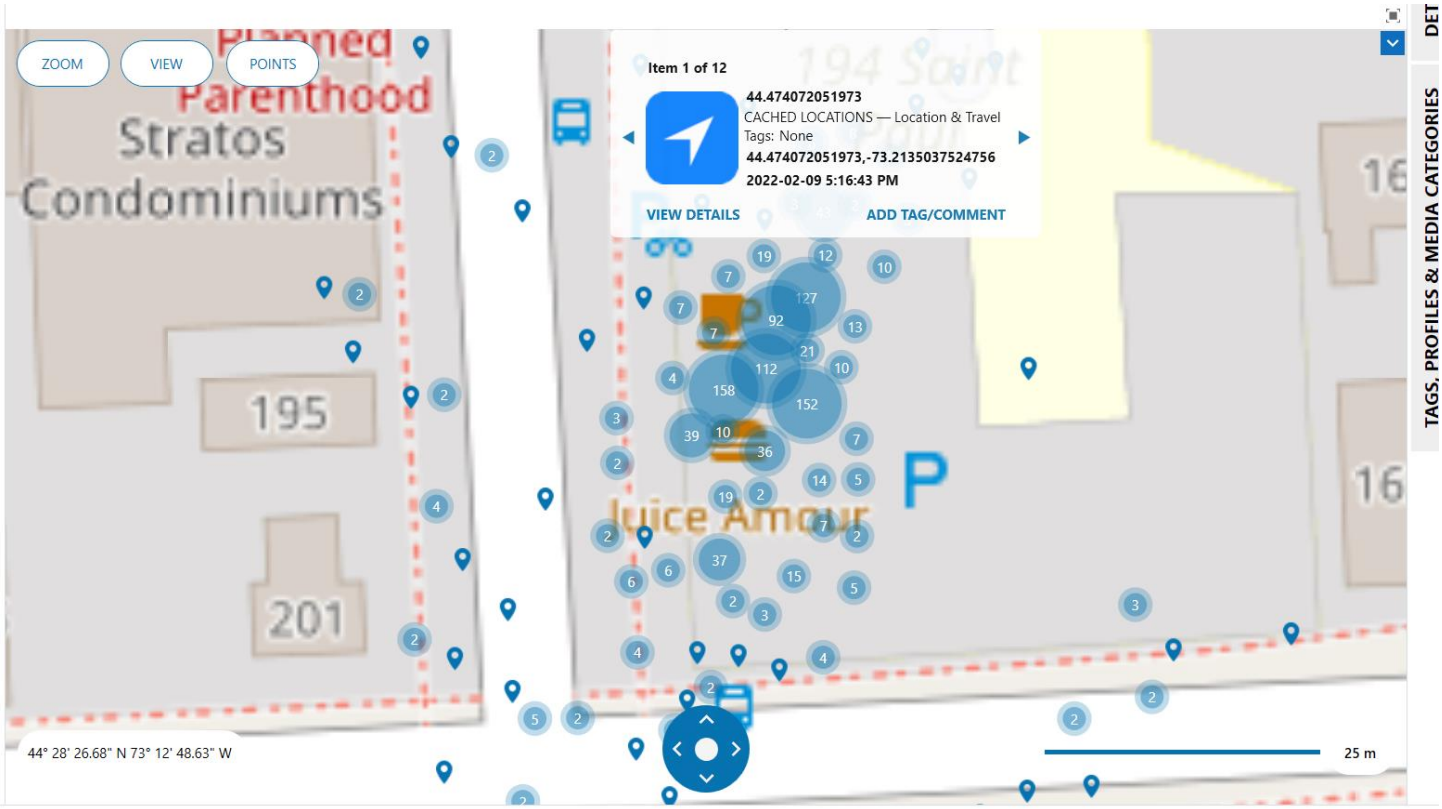


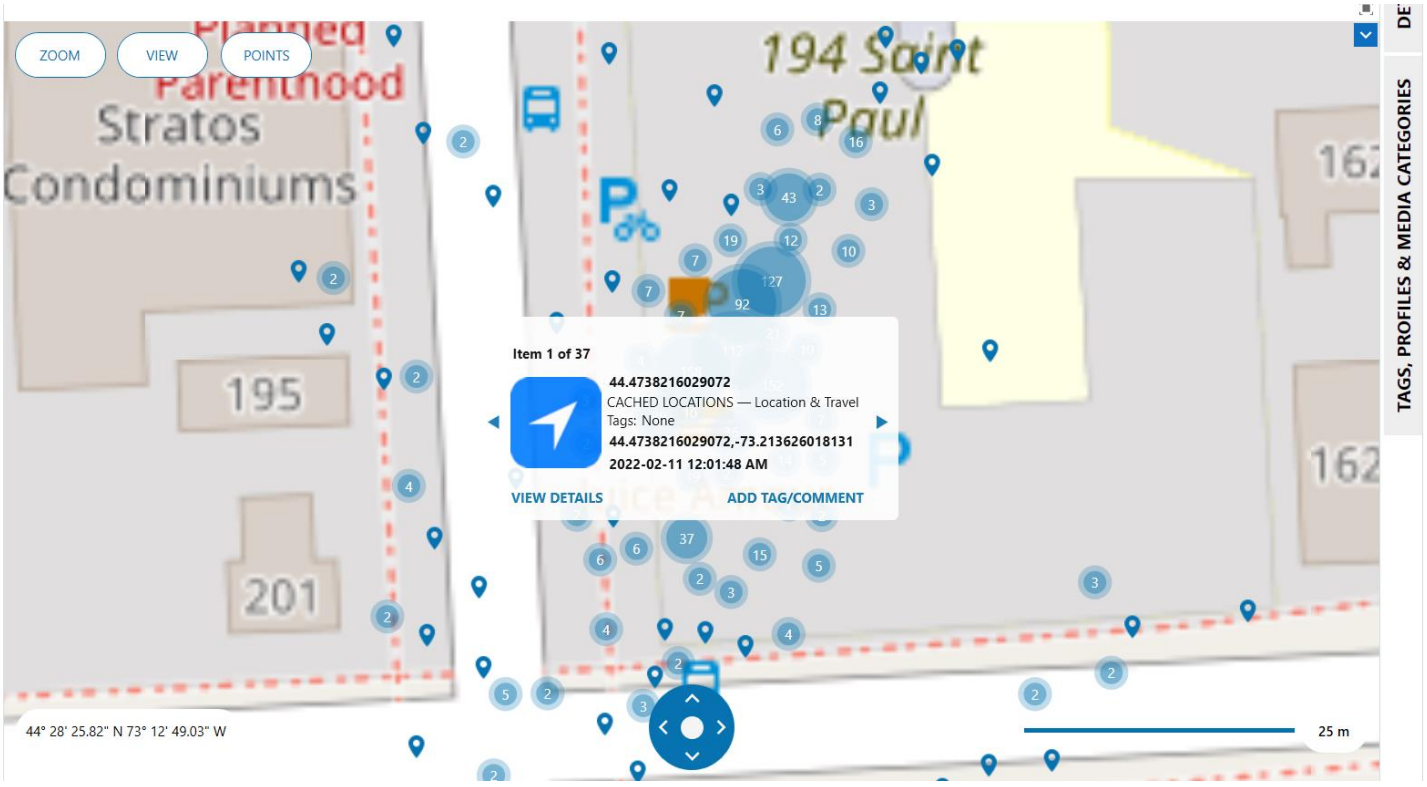
The datetime tag on the locations cover the span of a few days, from 7th February 2022 until 11th February. It can be confirmed that this area is a fairly active area of the user and (s)he likely revisits the same area frequently. Maybe it is a shopping hotspot.

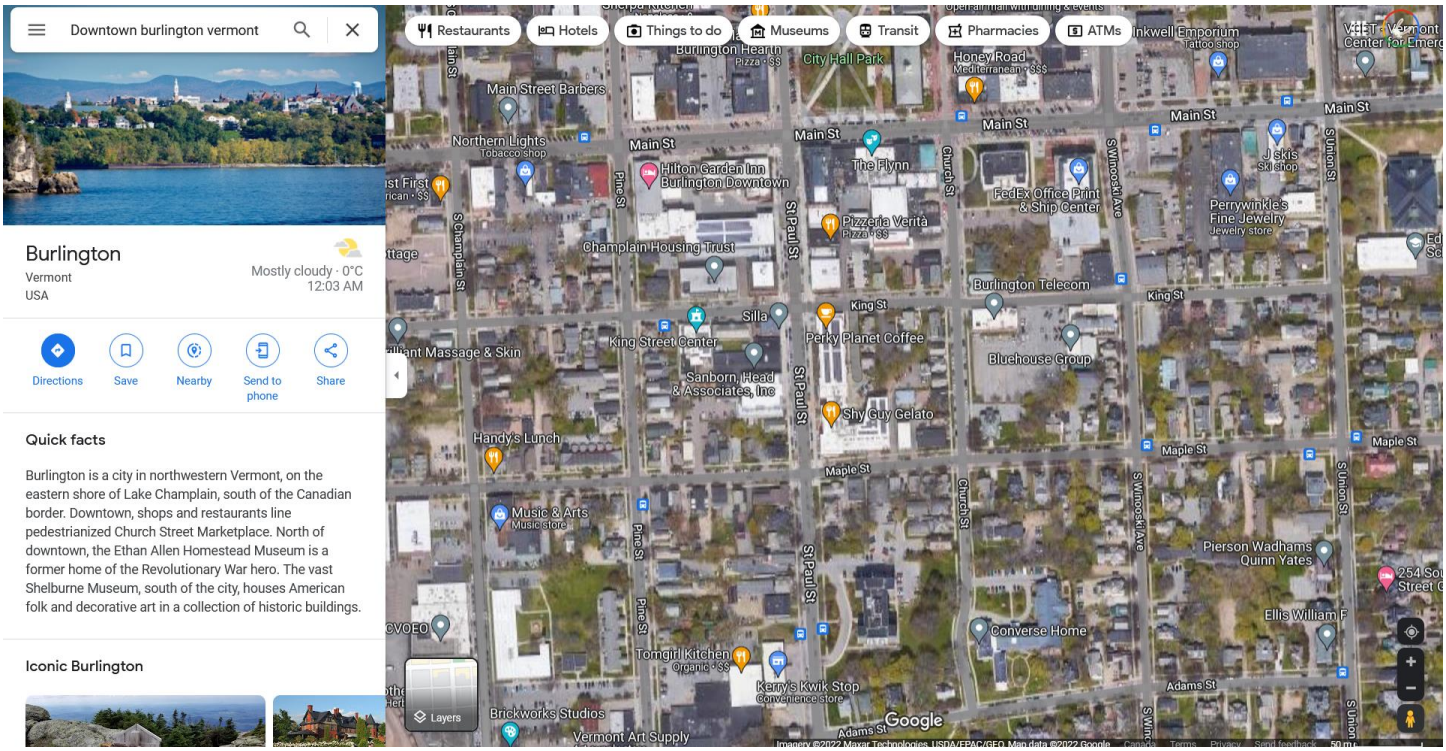


MATCHING RESULTS (10,319 of 10,319)

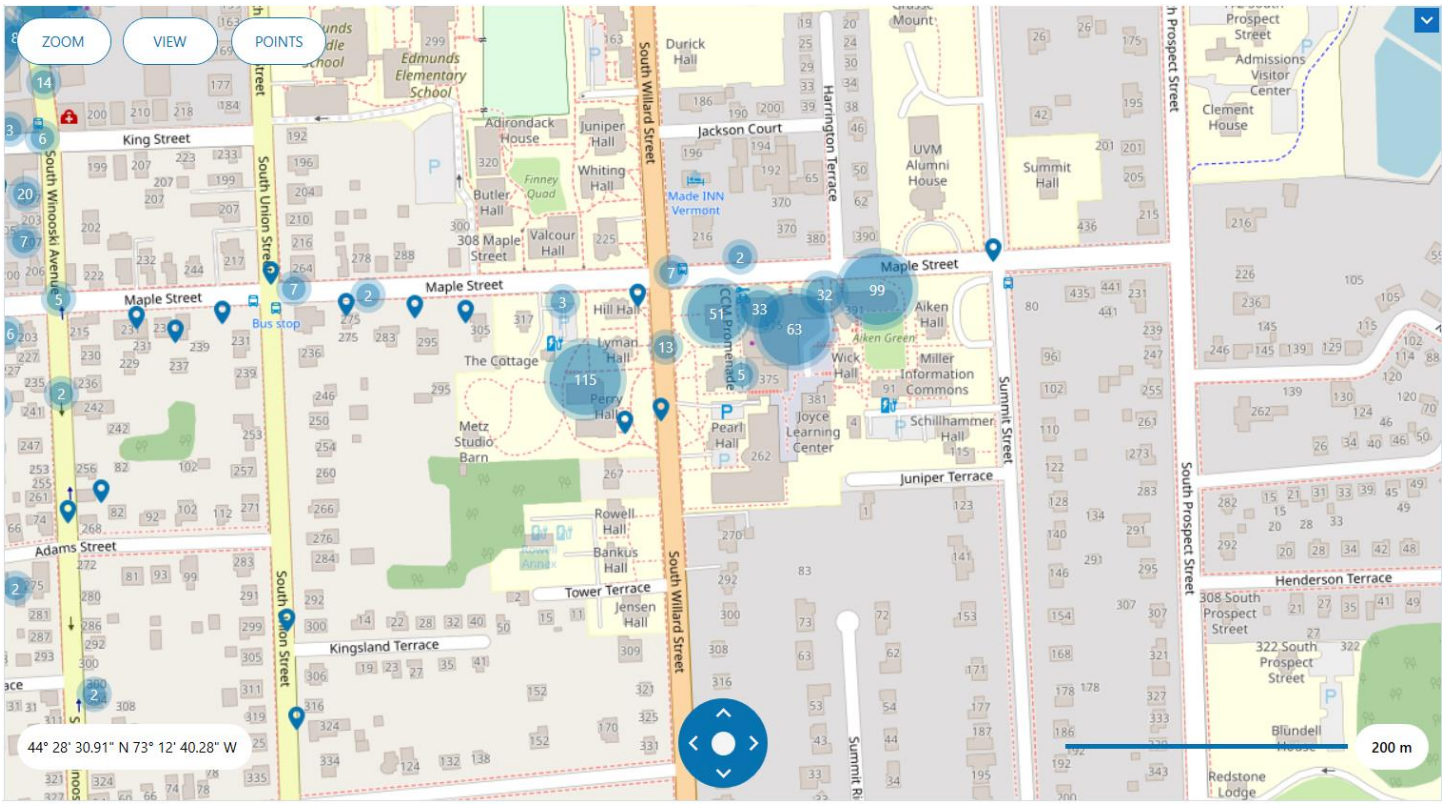



ZOOM
VIEW
POINTS
Item 1 of 12
44.474072051973
CACHED LOCATIONS — Location & Travel
Tags: None
44.474072051973,-73.2135037524756
2022-02-09 5:16:43 PM
VIEW DETAILS
ADD TAG/COMMENT
Stratos Condominiums
195
201
44° 28' 26.68" N 73° 12' 48.63" W
25 m
TAGS, PROFILES & MEDIA CATEGORIES


ZOOM
VIEW
POINTS
Item 1 of 37
44.4738216029072
CACHED LOCATIONS — Location & Travel
Tags: None
44.4738216029072,-73.213626018131
2022-02-11 12:01:48 AM
VIEW DETAILS
ADD TAG/COMMENT
Stratos Condominiums
195
201
44° 28' 25.82" N 73° 12' 49.03" W
25 m
TAGS, PROFILES & MEDIA CATEGORIES

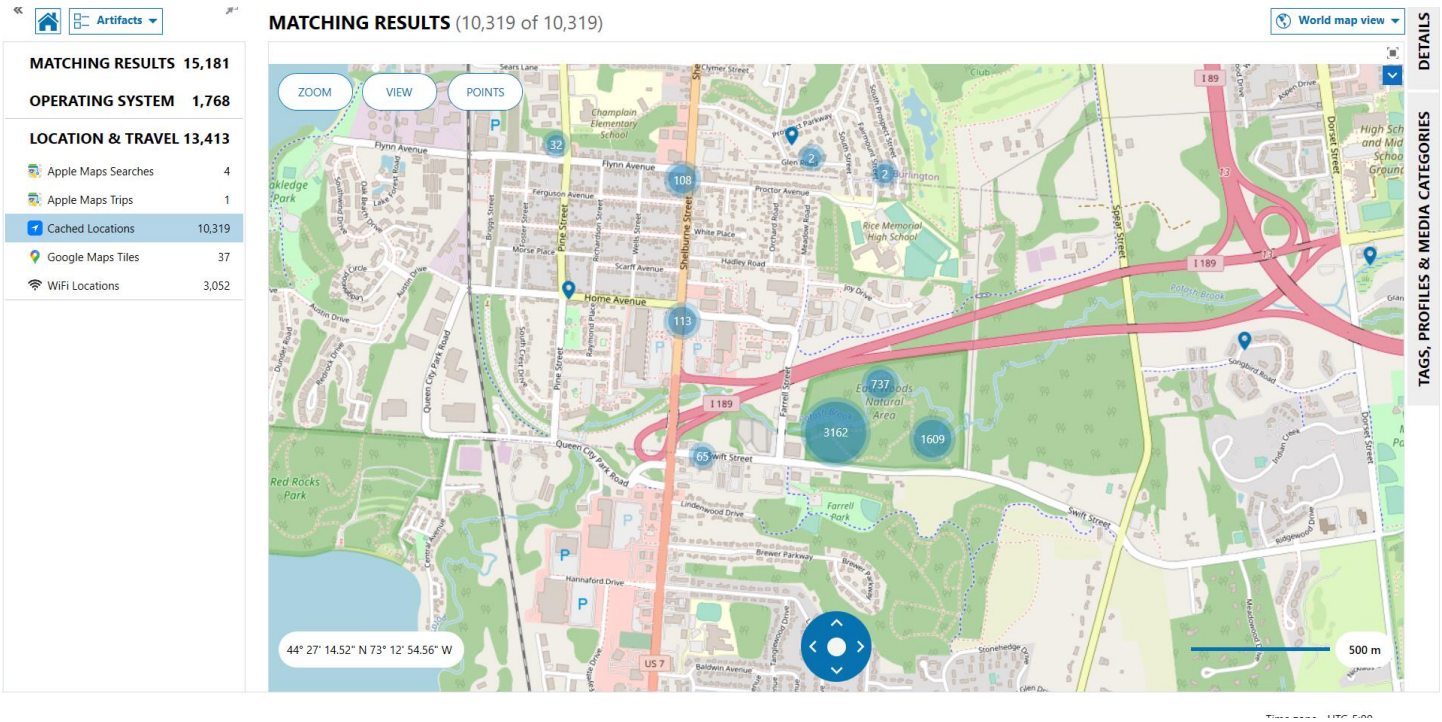


The user of a phone is potentially involved with the college affairs. One of his activity hotspots surrounds the Chaplain College in Maple & South Willard Street.



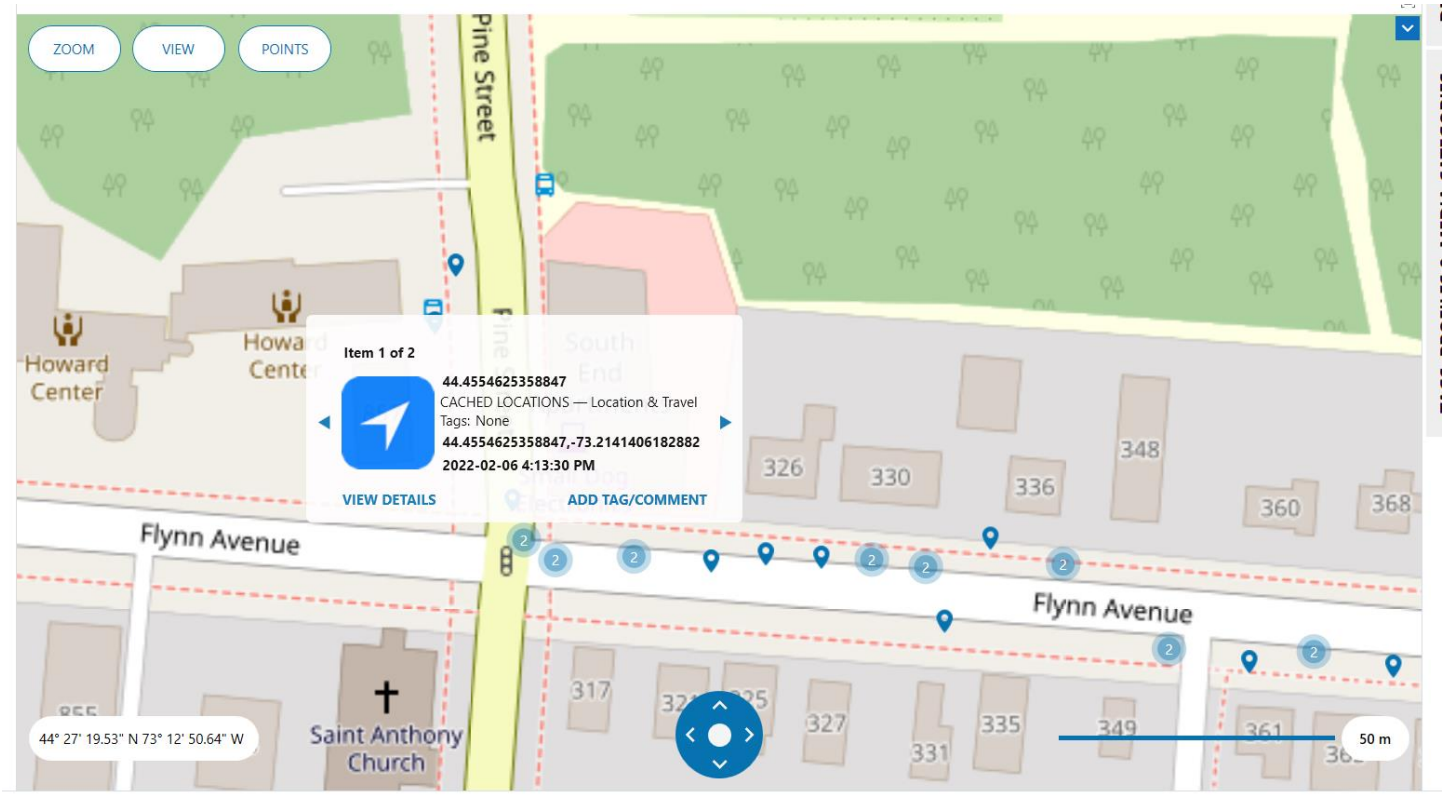
Downtown hotspot 2

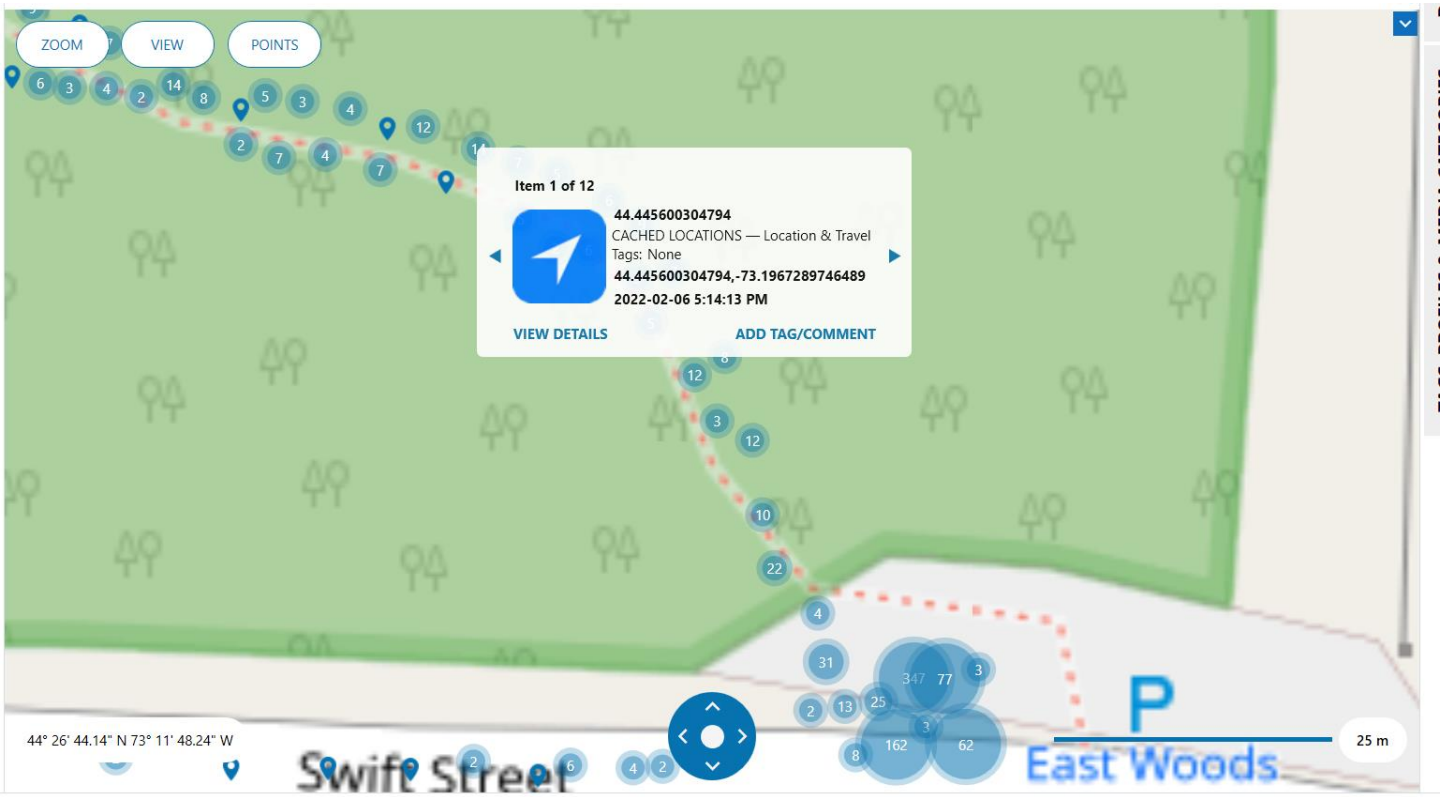
The second hotspot in Downtown would be near the East Woods Natural Area. This spot is a fairly big natural park with lush greenery by the interstate highway.

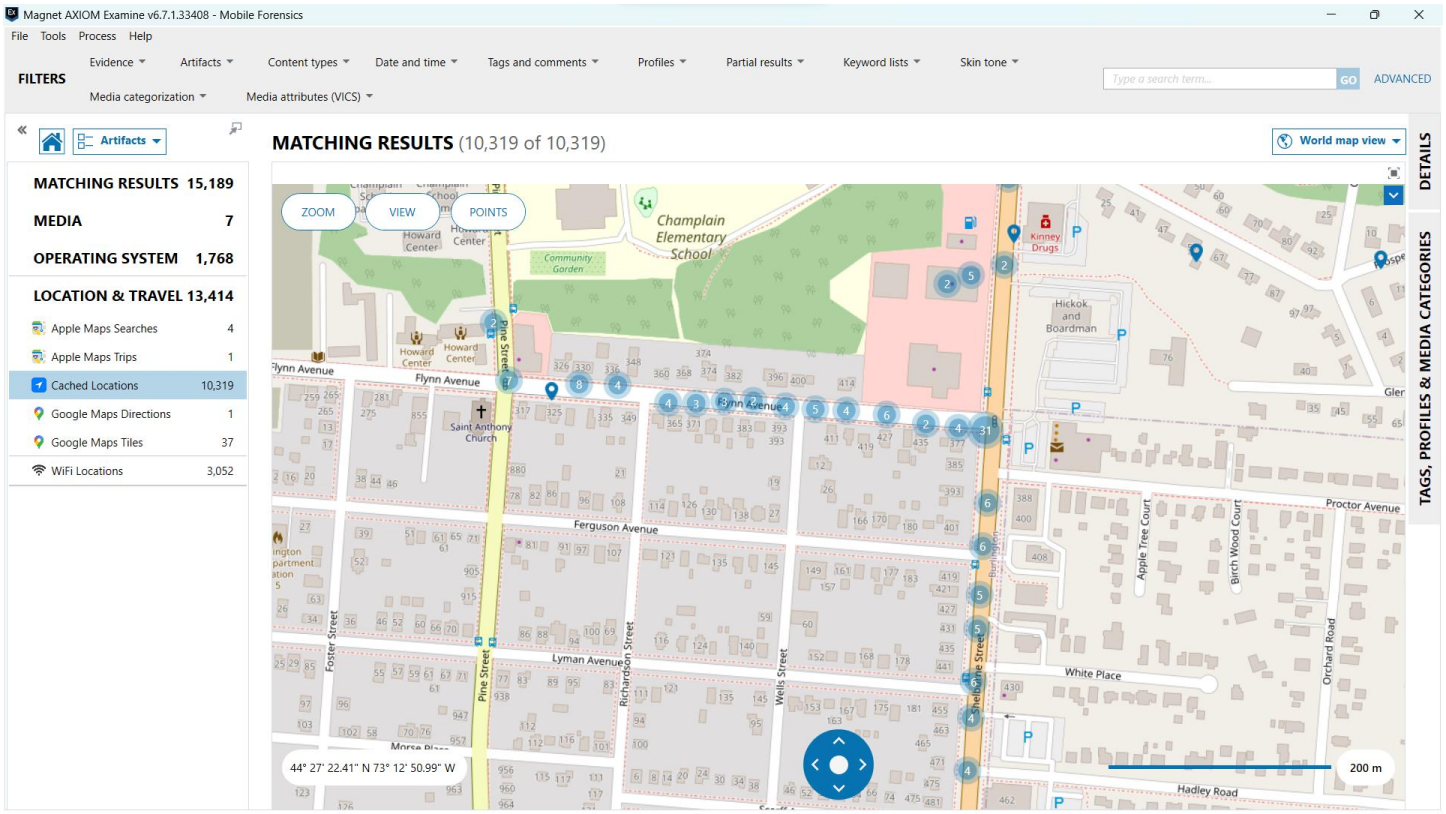


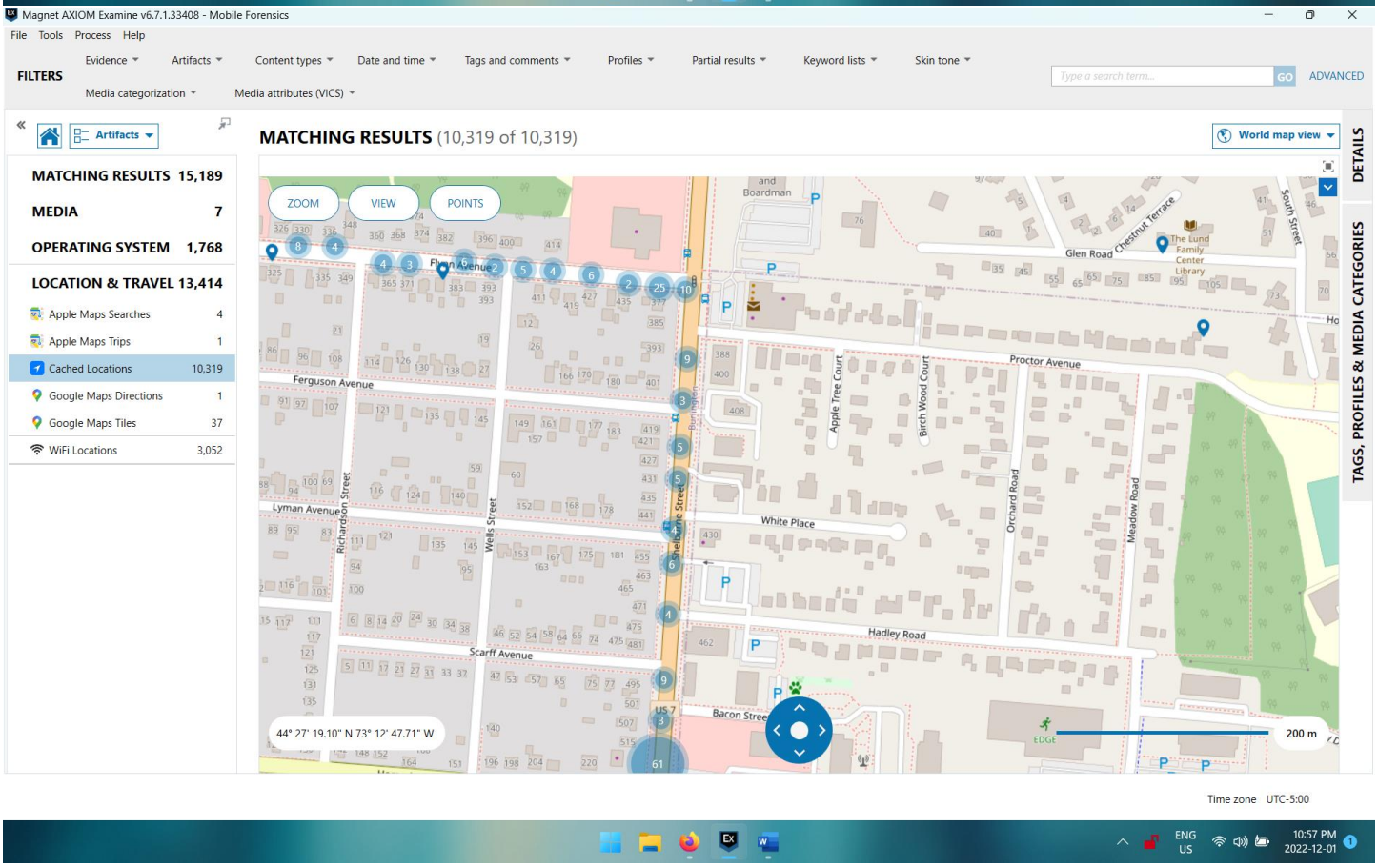
The person holding this phone seems to be following a very neat line along the trail present in the East Woods Loop area. There was a lack of off-trail activities.

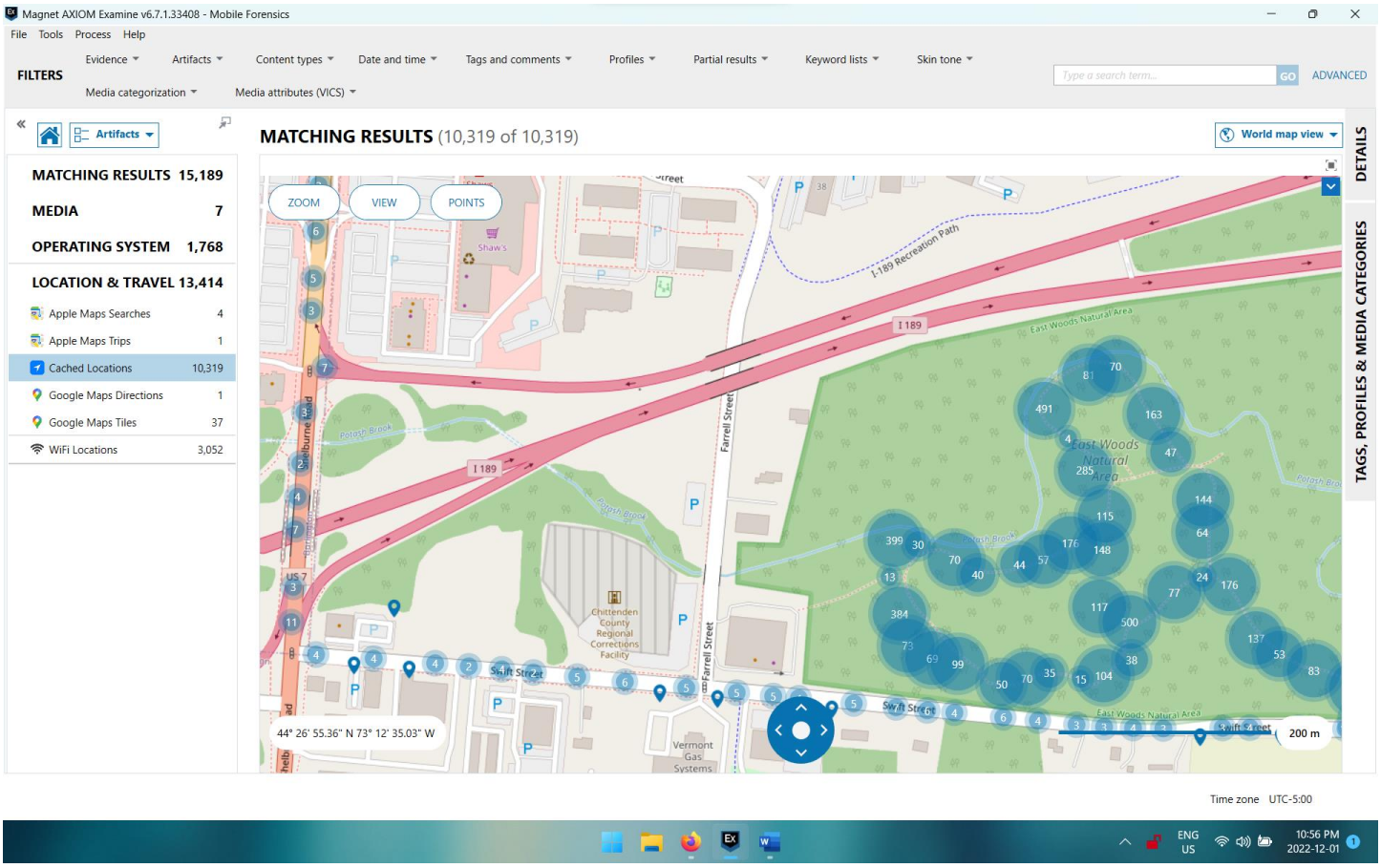
Interestingly, the high number of activities in the East Woods Natural Area is accompanied by a trail that leads to the bus stop. Since the timestamps on the bus stop appear to be earlier than the timestamps in the park, we can determine the direction of travel as going from the bus stop into the park.



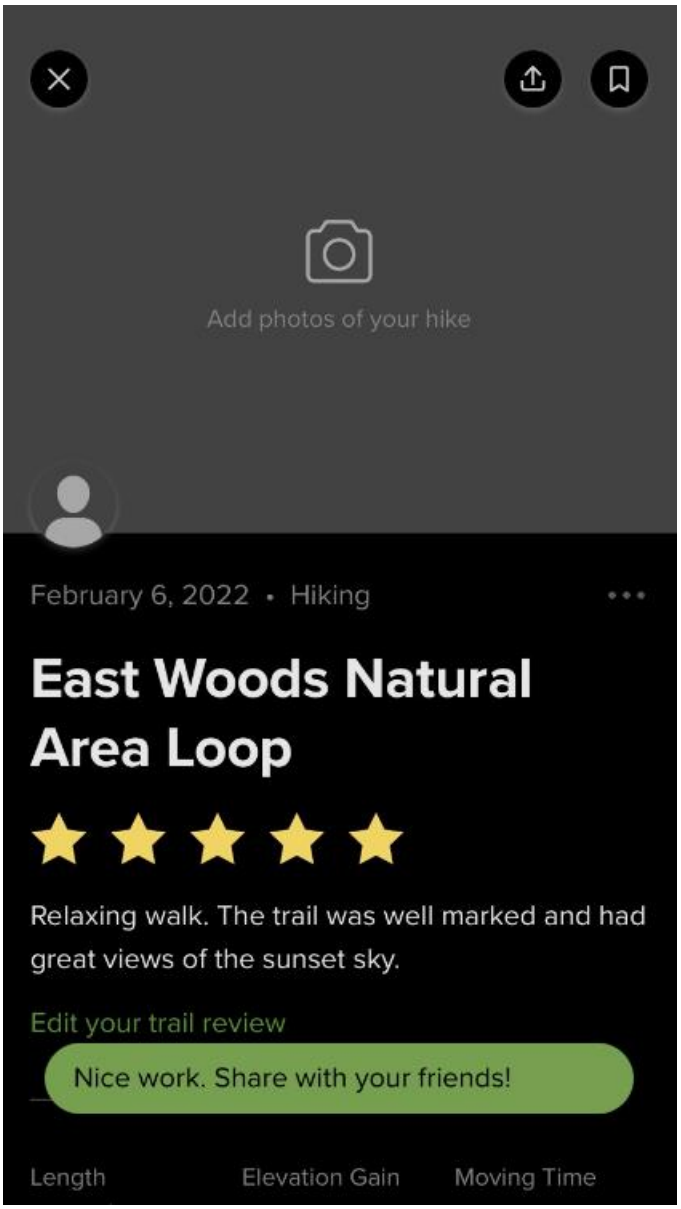

ZOOM
VIEW
POINTS
Item 1 of 12
44.445600304794
CACHED LOCATIONS — Location & Travel
Tags: None
44.445600304794,-73.1967289746489
2022-02-06 5:14:13 PM
VIEW DETAILS
ADD TAG/COMMENT
44° 26' 44.14" N 73° 11' 48.24" W
Swift Street
East Woods
25 m


Magnet AXIOM Examine v6.7.1.33408 - Mobile Forensics
File Tools Process Help
FILTERS
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone
Media categorization Media attributes (VICS)
Type a search term...
GO
ADVANCED
Artifacts
MATCHING RESULTS 15,189
MEDIA 7
OPERATING SYSTEM 1,768
LOCATION & TRAVEL 13,414
Apple Maps Searches 4
Apple Maps Trips 1
Cached Locations 10,319
Google Maps Directions 1
Google Maps Tiles 37
WiFi Locations 3,052
MATCHING RESULTS (10,319 of 10,319)
World map view
DETAILS
TAGS, PROFILES & MEDIA CATEGORIES
ZOOM
VIEW
POINTS
Champlain Elementary School
Community Garden
Howard Center
Kinney Drugs
Hickok and Boardman
Flynn Avenue
Saint Anthony Church
Ferguson Avenue
Lyman Avenue
Pine Street
Foster Street
Richardson Street
Wells Street
Shelburne Street
Apple Tree Court
Birch Wood Court
Proctor Avenue
Orchard Road
White Place
Hadley Road
44° 27' 22.41" N 73° 12' 50.99" W
200 m
Time zone UTC-5:00
ENG US
10:58 PM
2022-12-01

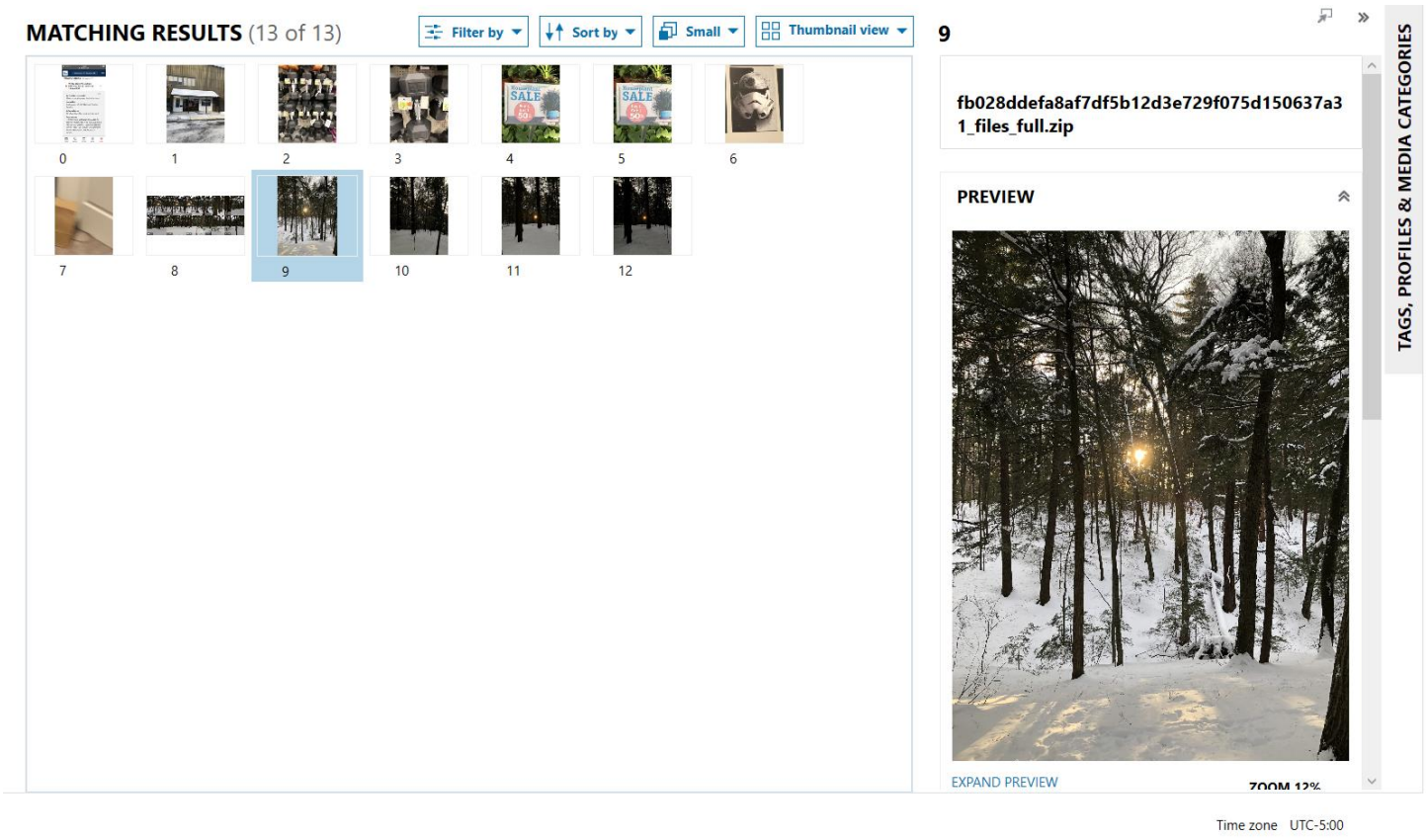

Magnet AXIOM Examine v6.7.1.33408 - Mobile Forensics
File Tools Process Help
FILTERS
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone
Media categorization Media attributes (VICS)
Type a search term...
GO
ADVANCED
Artifacts
MATCHING RESULTS 15,189
MEDIA 7
OPERATING SYSTEM 1,768
LOCATION & TRAVEL 13,414
Apple Maps Searches 4
Apple Maps Trips 1
Cached Locations 10,319
Google Maps Directions 1
Google Maps Tiles 37
WiFi Locations 3,052
MATCHING RESULTS (10,319 of 10,319)
World map view
DETAILS
TAGS, PROFILES & MEDIA CATEGORIES
ZOOM
VIEW
POINTS
Flynn Avenue
Glen Road
Chestnut Terrace
The Lund Family Center Library
South Street
Ferguson Avenue
Lyman Avenue
Richardson Street
Wells Street
Shelburne Street
Apple Tree Court
Birch Wood Court
Proctor Avenue
Orchard Road
Meadow Road
White Place
Hadley Road
Scarff Avenue
Bacon Street
US 7
EDGE
44° 27' 19.10" N 73° 12' 47.71" W
200 m
Time zone UTC-5:00
ENG US
10:57 PM
2022-12-01



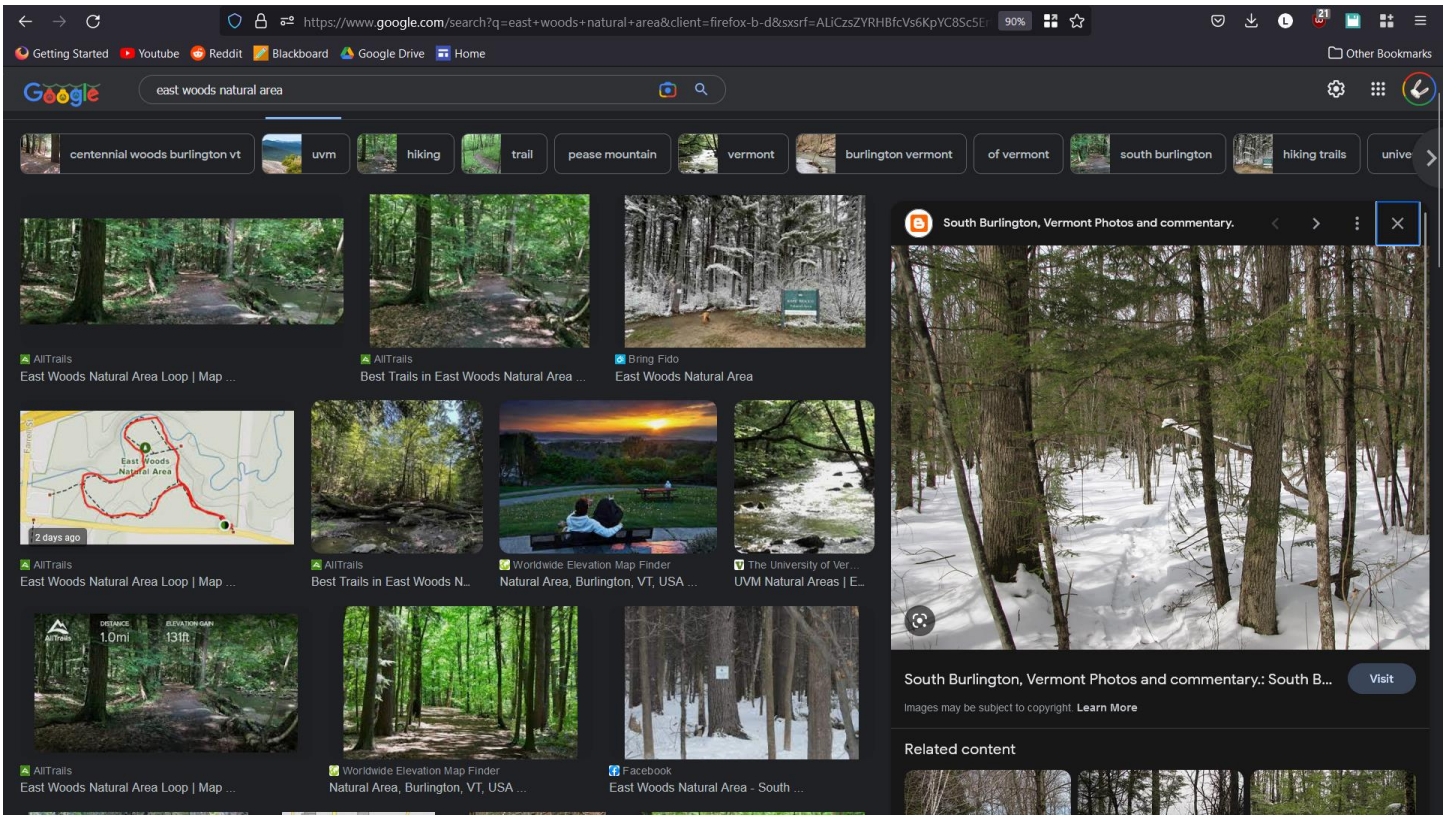
My guess is that the iPhone user is an avid park goer and have been actively planning on visiting this park for a while. Another kind of evidence also supports the claim. Let's dive into some of the web search history. This screenshot from the iOS snapshot section was found on the phone that indicates a prior interest in the park.



There are also many camera photos in the gallery that look to be taken in a natural area. Trees are packed together in the photos and the weather indicates wintertime. The metadata on this photo including location and time taken were lost so it is not possible to determine the precise coordinates.

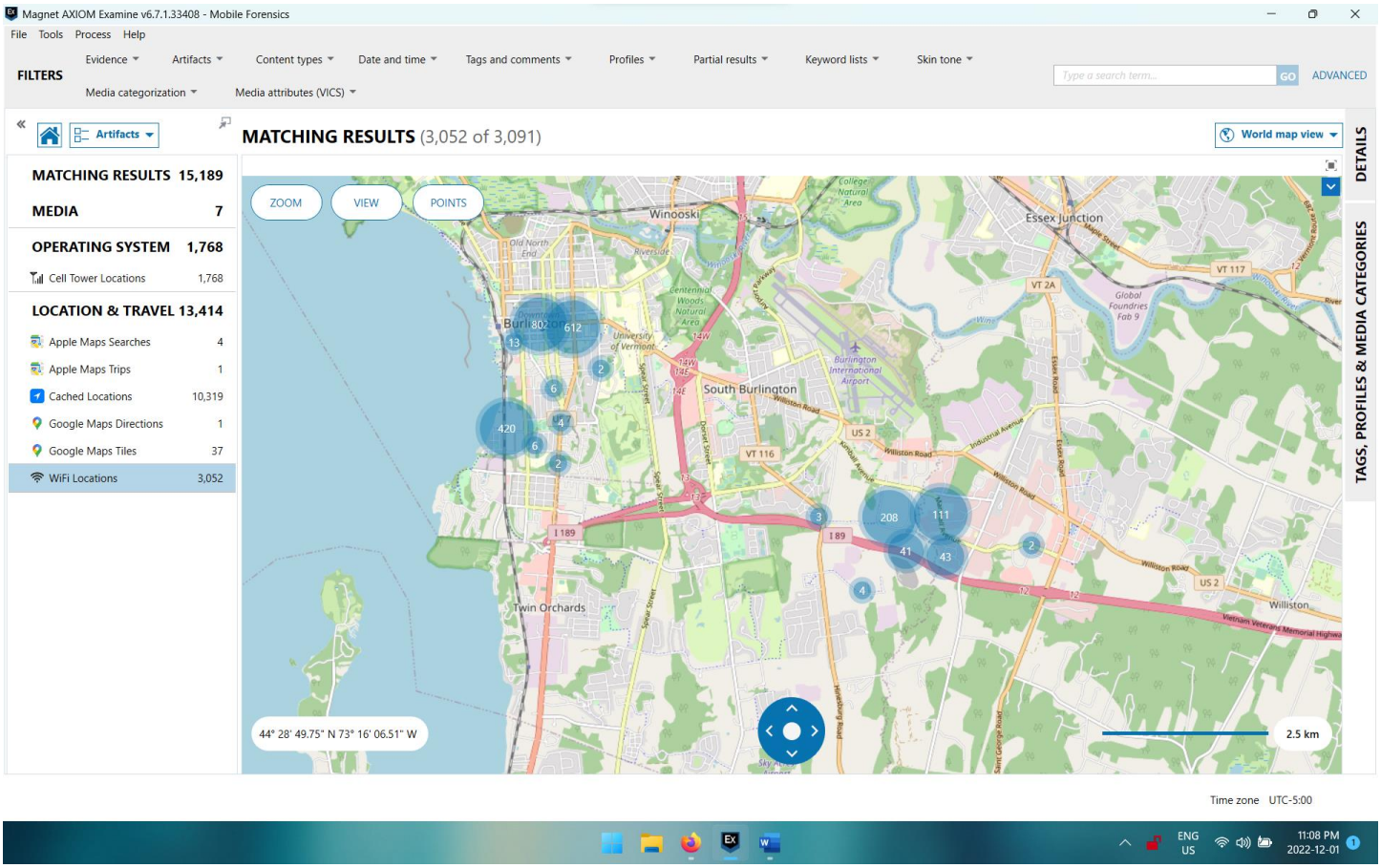


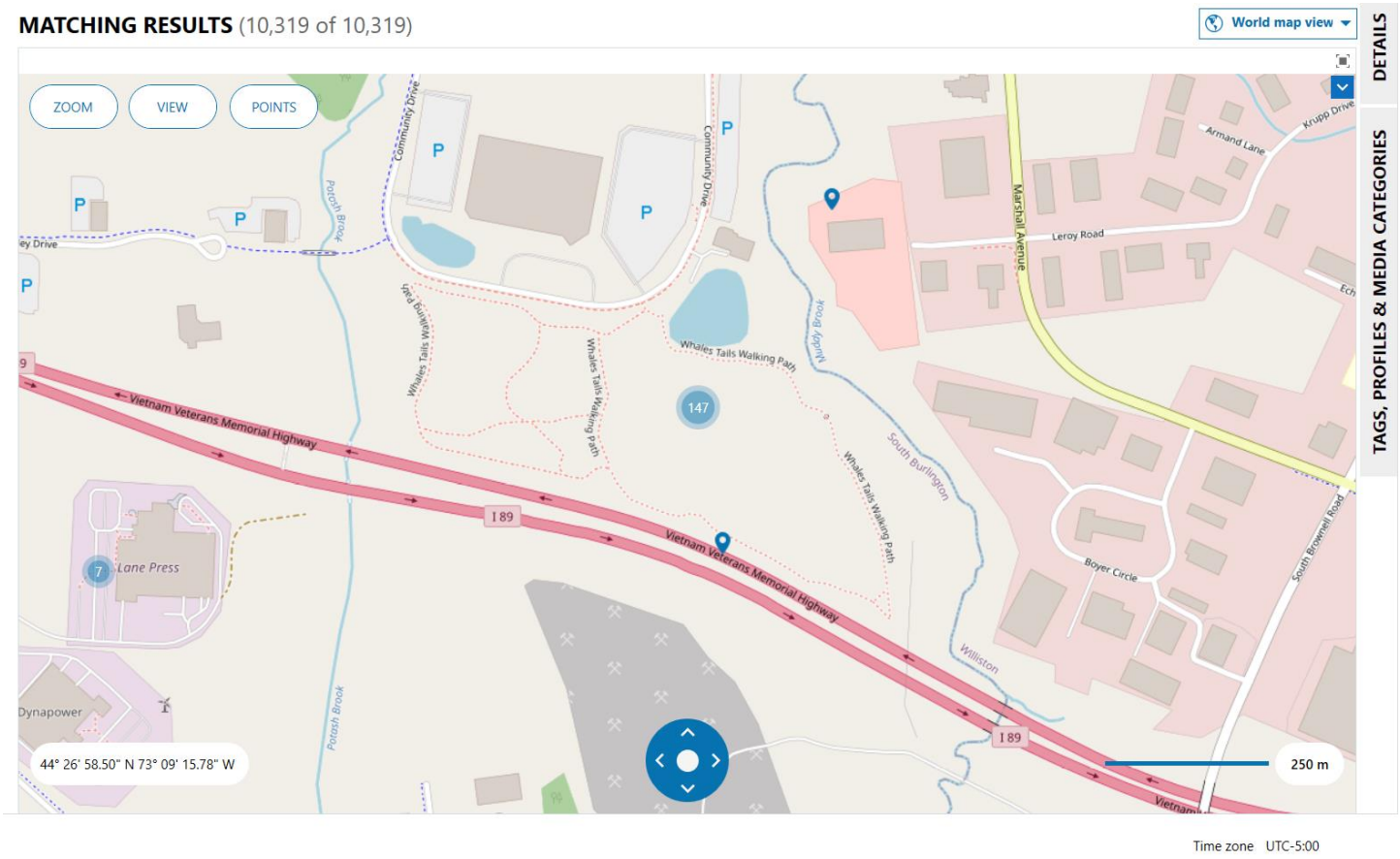
However, I suspected that these photos are related to the frequently mentioned East Woods Natural Area Loop. A quick google photo search would suggest that there is a high degree of correlation between the photos and the area as the geographical structures look very much alike.



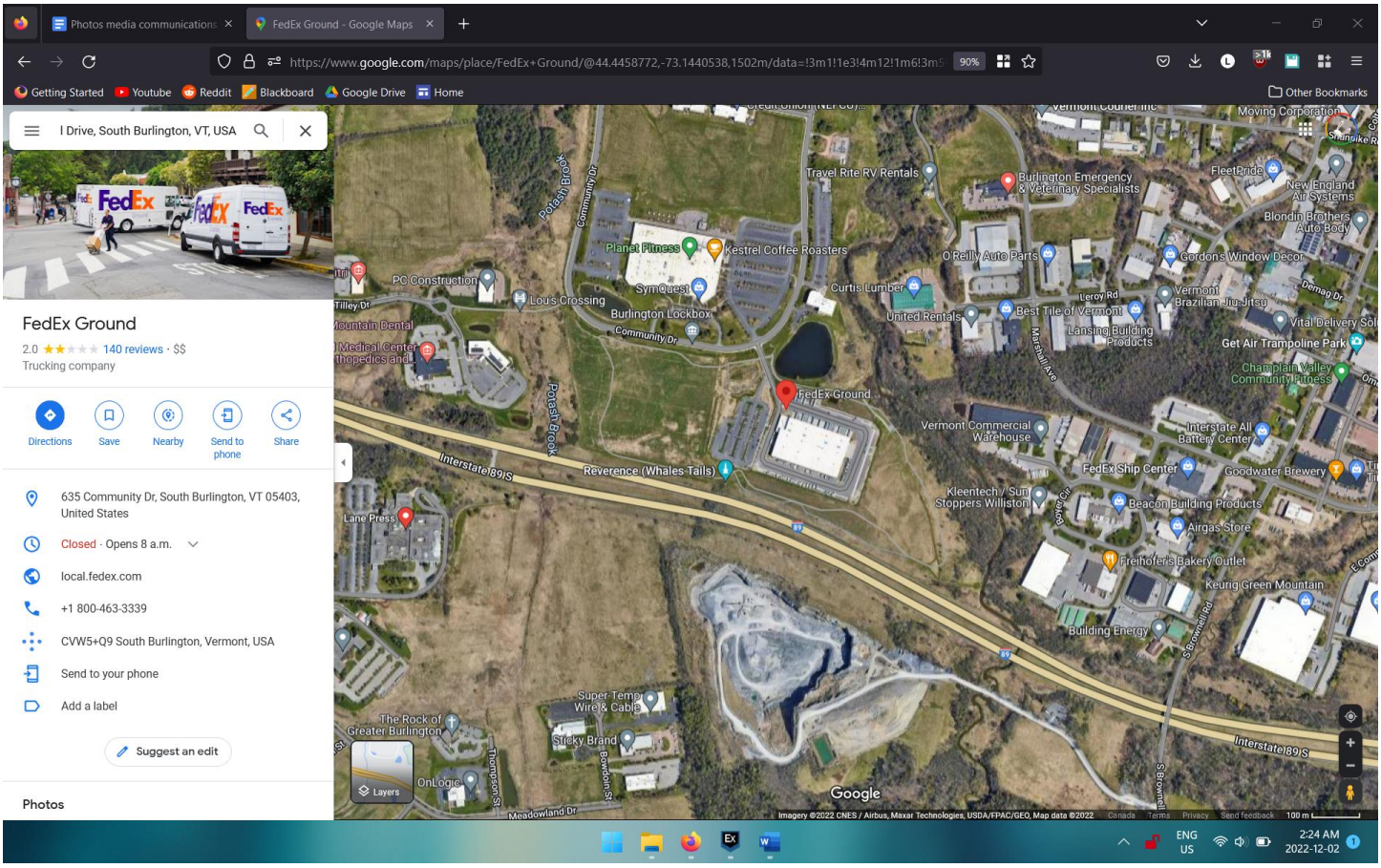
Uptown hotspot

Aside from the 2 hotspots in downtown, the iPhone also appeared many times in an uptown spot. Zooming in, the map would suggest that it is a walking path called Whales Tails Walking Path.

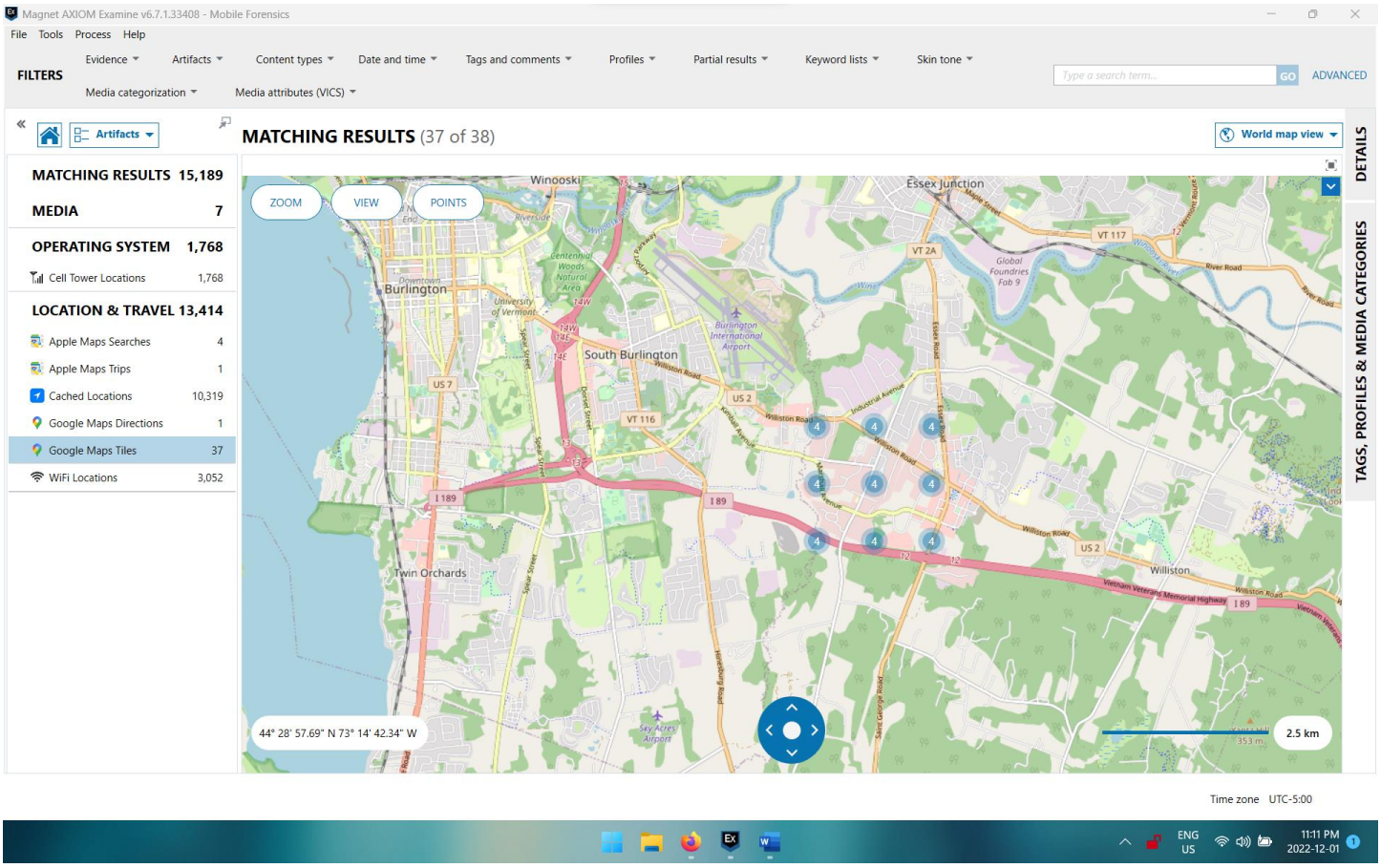




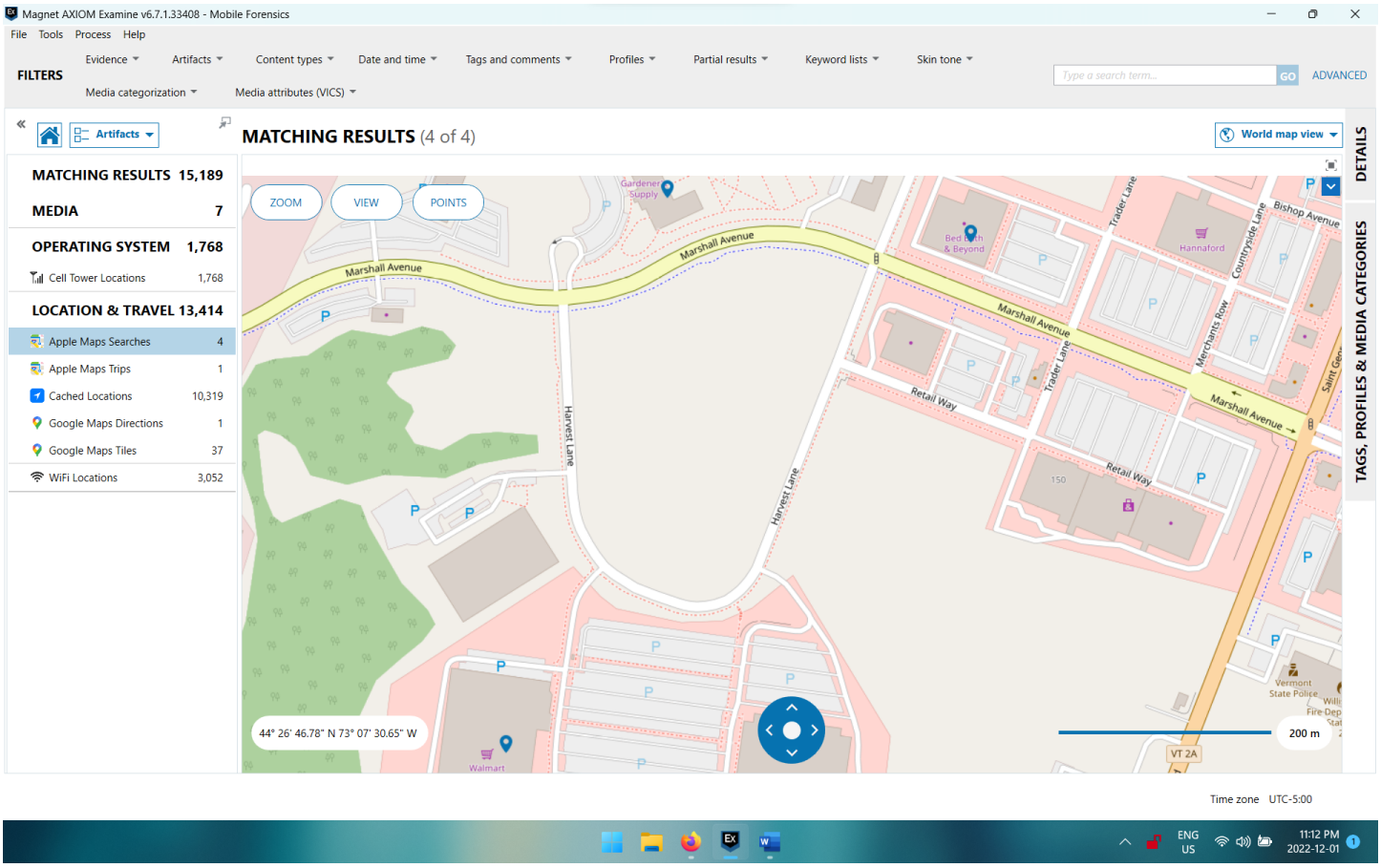
However, if we compare the location to actual satellite images on Google Maps, we will find a FedEx Ground Building in that exact hotspot location. This is something to take notes of as it is going to turn out to be very useful for our investigation and story building.



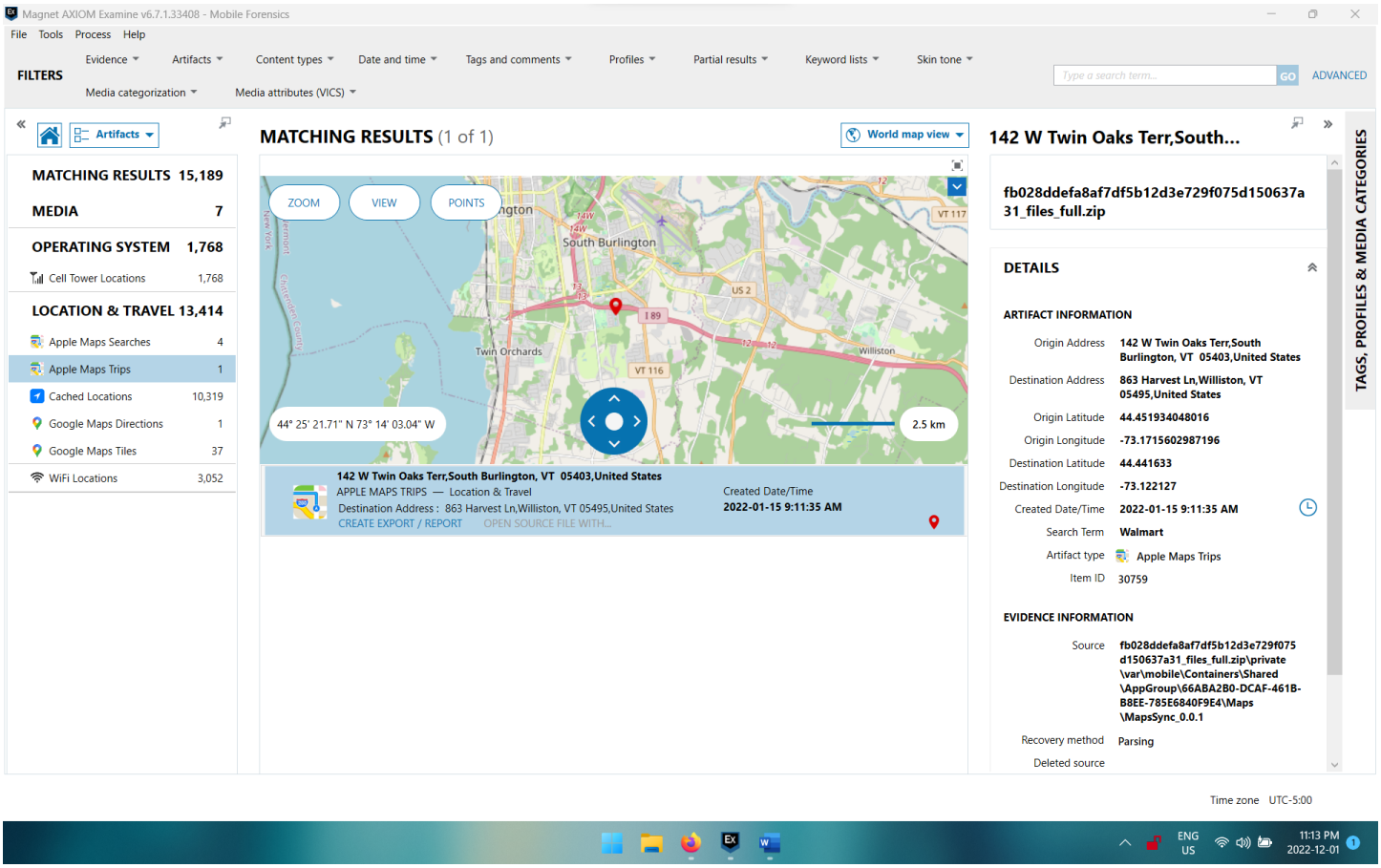
The Google Maps Tiles, which seems to indicate a cached part of the map also shows the FedEx ground vicinity area to be made offline. Usually this happens when someone frequently visit/spend a long time in a certain area, because they would want that area on Google Maps to load efficiently. In the context of a person's life, this might be their home, their school, or their workplace. In this case, a workplace seems likely.



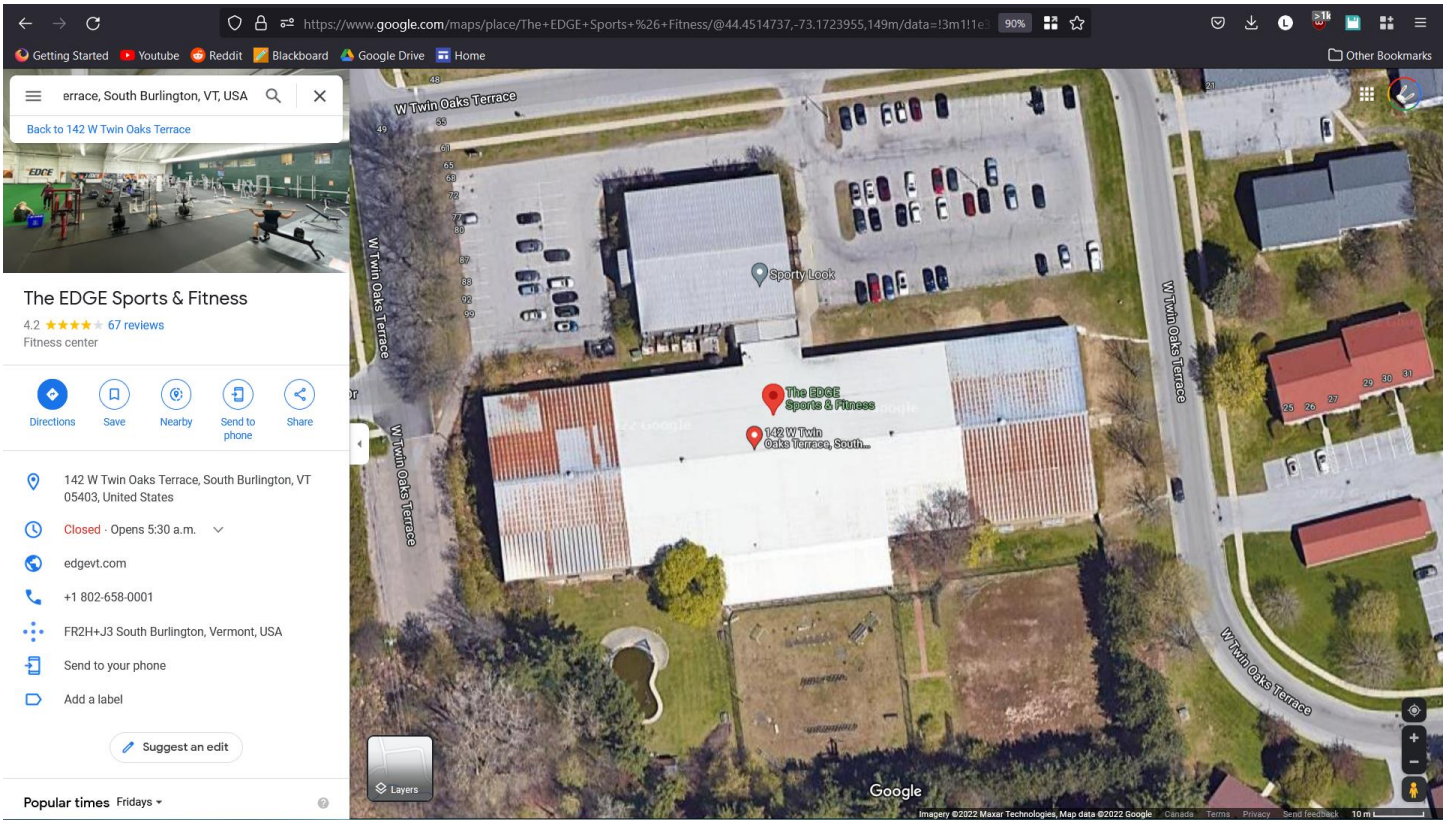
Next to the FedEx ground, a shopping area was also frequented by the iPhone user. Google Maps searches are showing that Gardener's supply, Bed Bath & Beyond and Walmart are of interests. These stores generally sell household items such as bedroom supplies, groceries or gardening items.



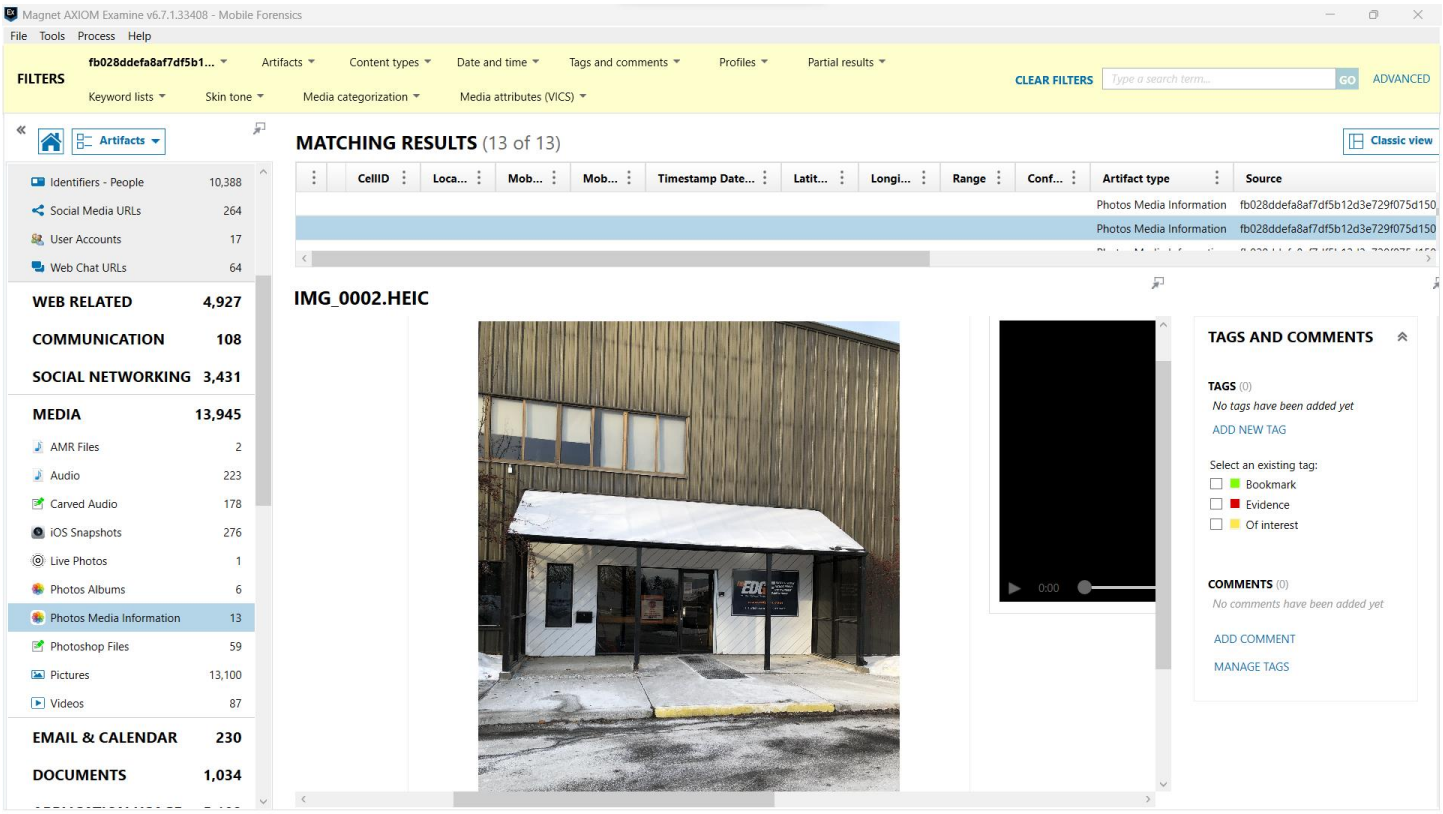
A Google Maps Trip was made to the said Walmart. The Origin address is 142 W Twin Oaks Terrace.

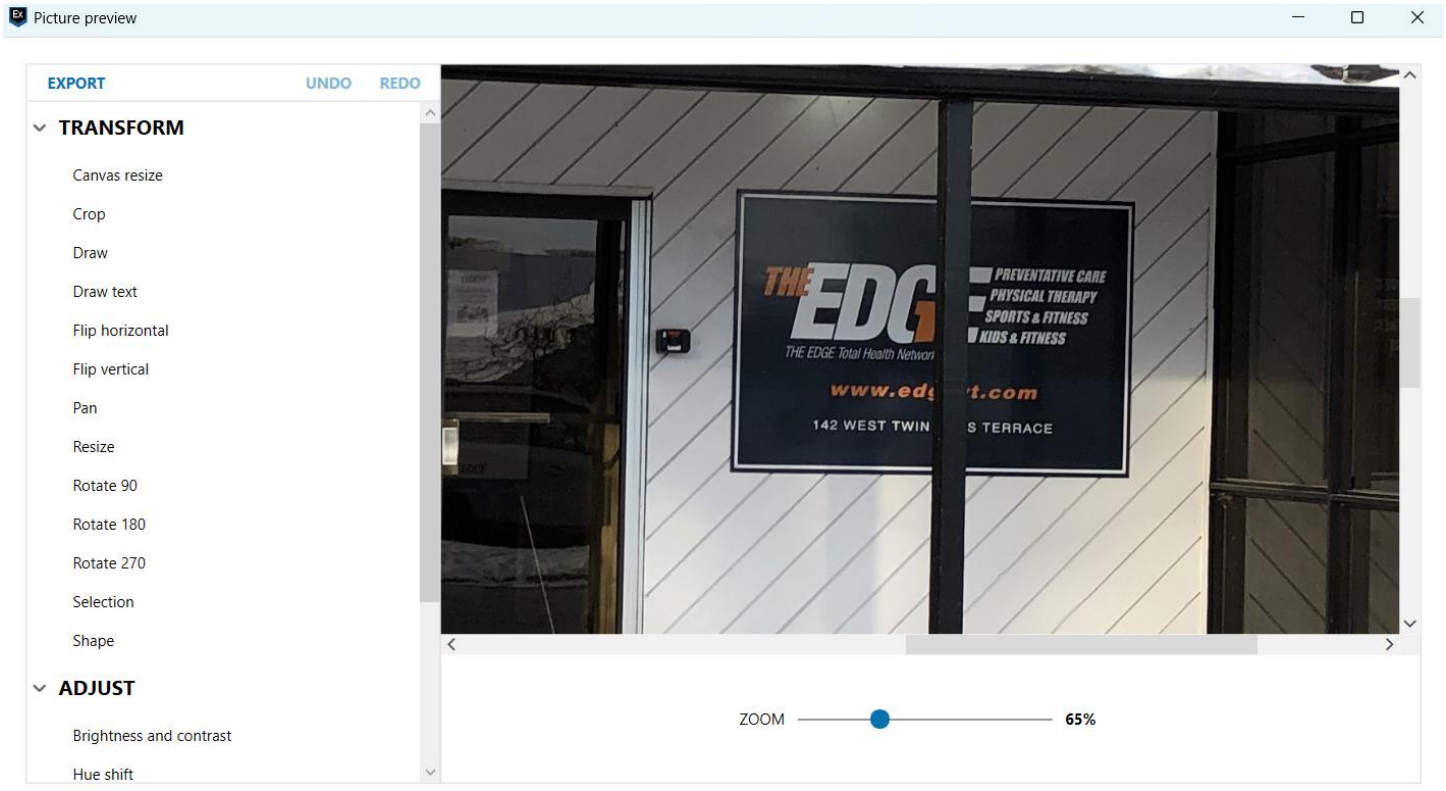


Pulling Up Google Maps Search, the address belongs to a gymnasium called the Sports & Fitness.

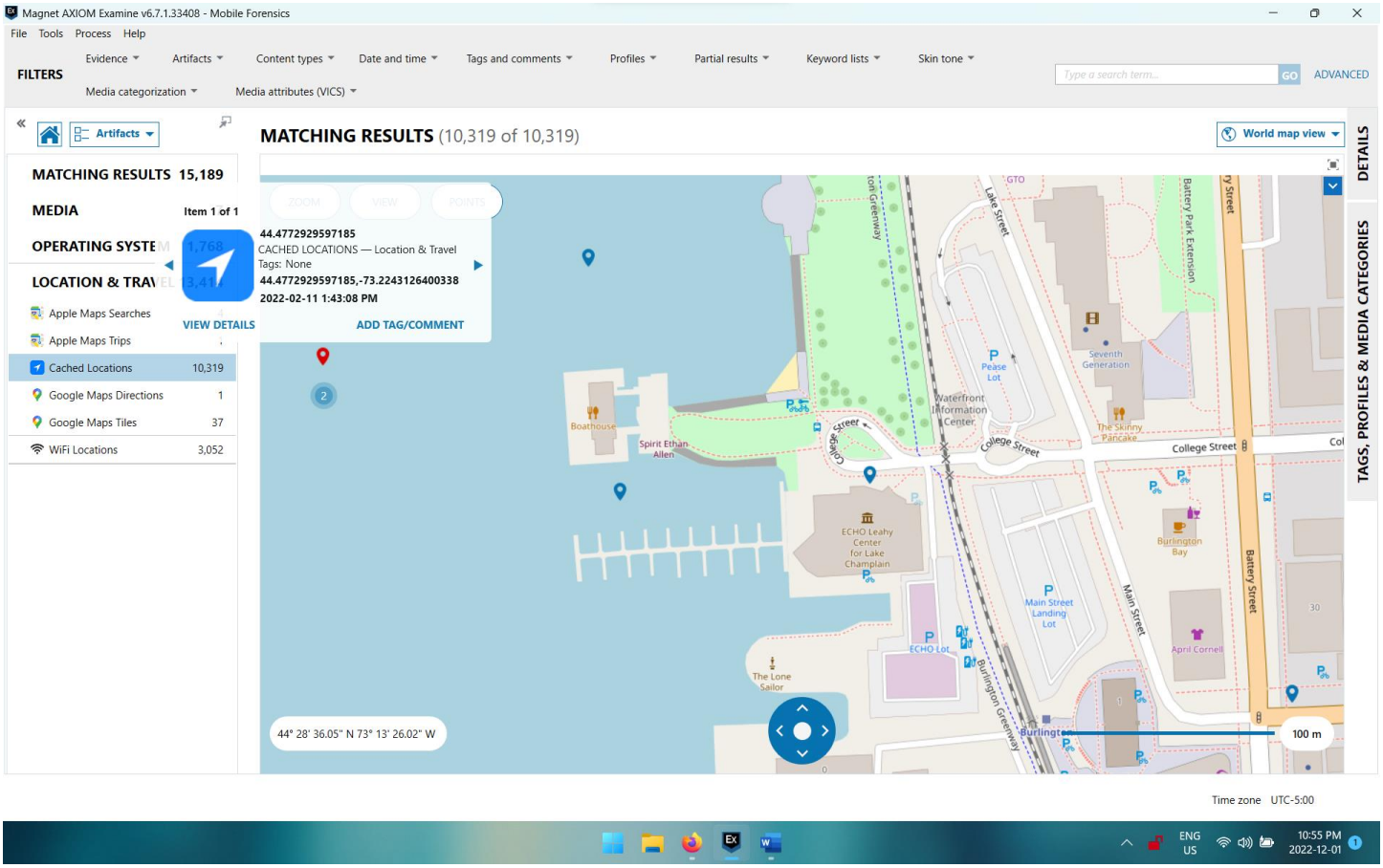


I recalled seeing a photo of the gym when first investigating the file, turns out it is in the Photos Media information section. There exists a photo of the front door of the gym. If we zoom into the name on the storefront, “the EDGE” can be seen.





On an extra note, the iPhone user had some light activity out in the water at the port of Burlington.

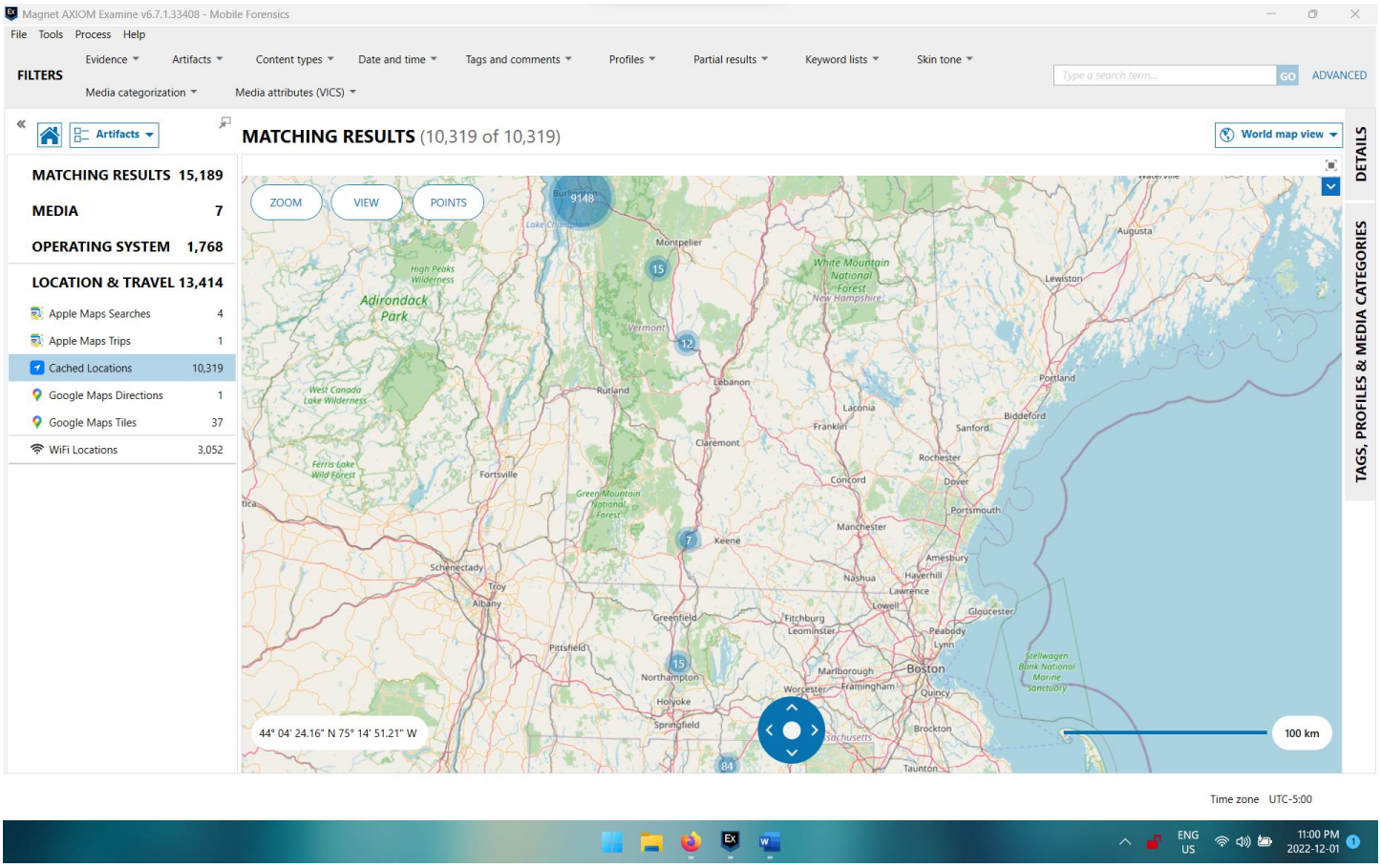


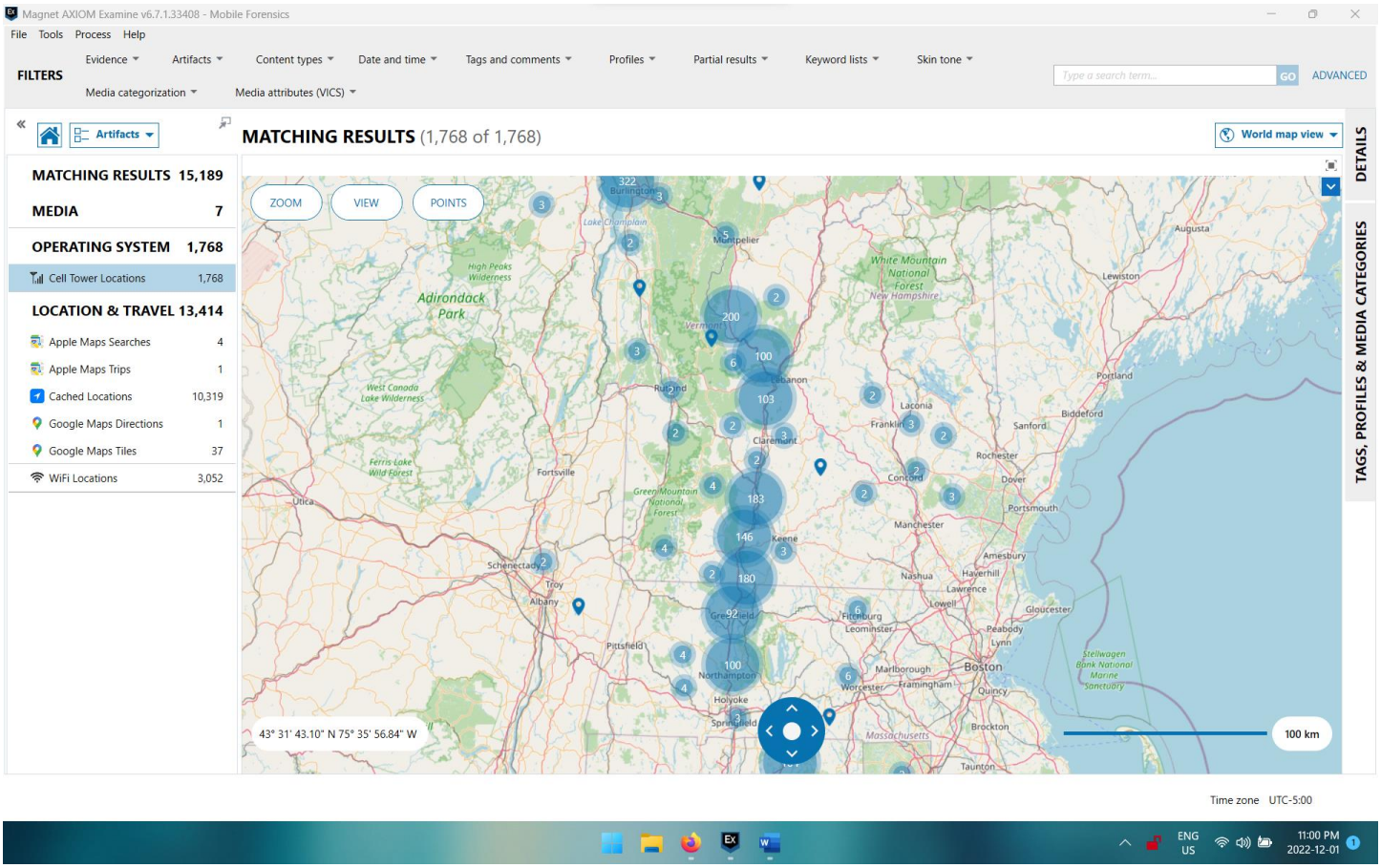
Burlington en route to Willington

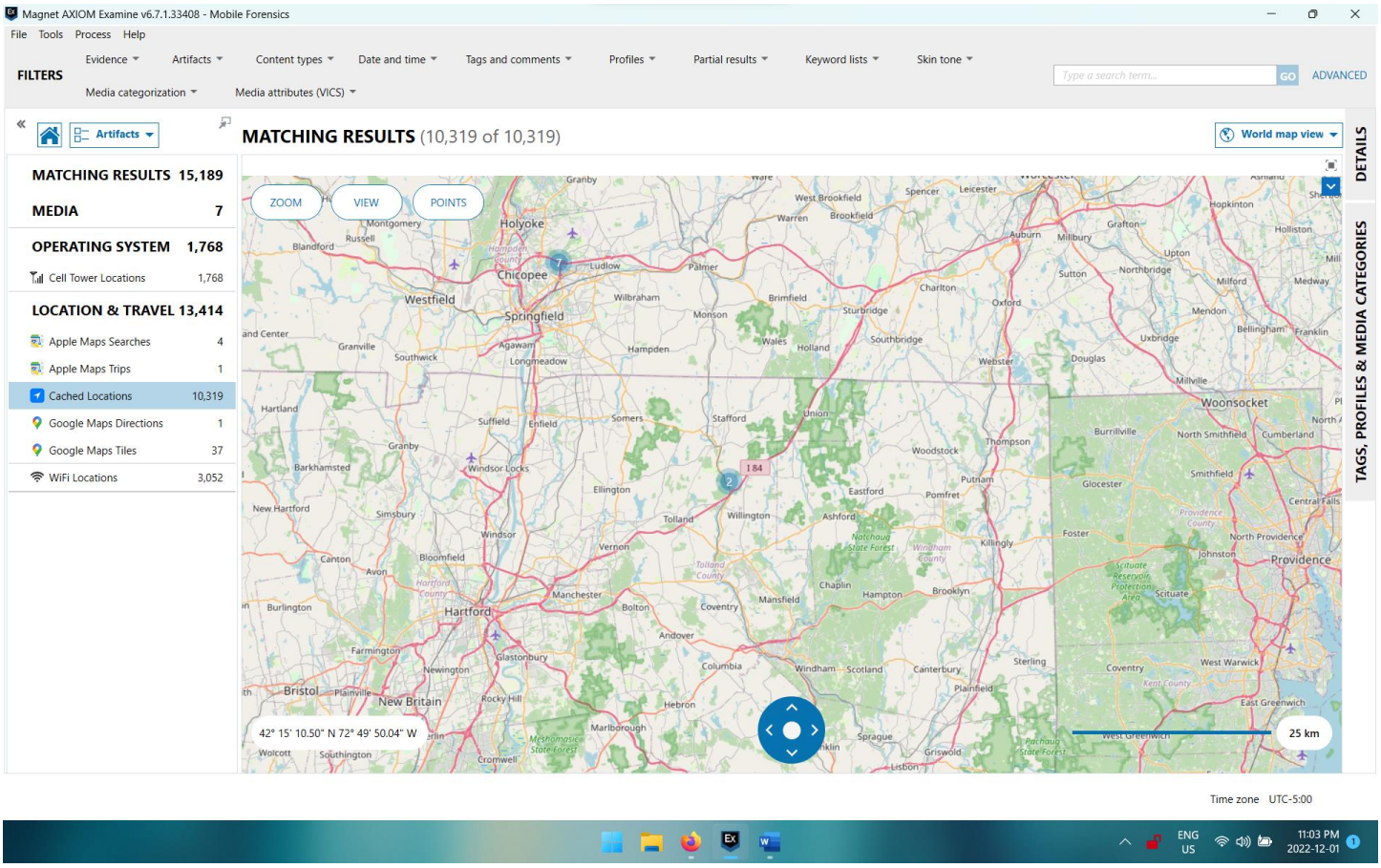
Looking at the cached locations, the data seems to suggest that the iPhone travelled away from Burlington. If we look at the location data, we can roughly make out a path leading the phone away on the highway 189. Cell tower locations seems to confirm the assumption with even clearer data showing the route.

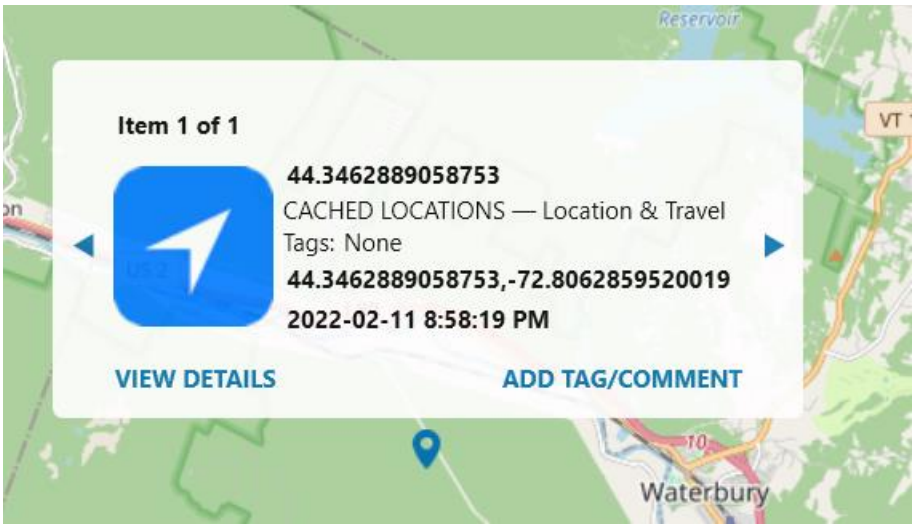
The mere presence of the data suggests that during the commute, the iPhone was on with proper reception as well as location function switched on. The phone was likely travelling on a vehicle.

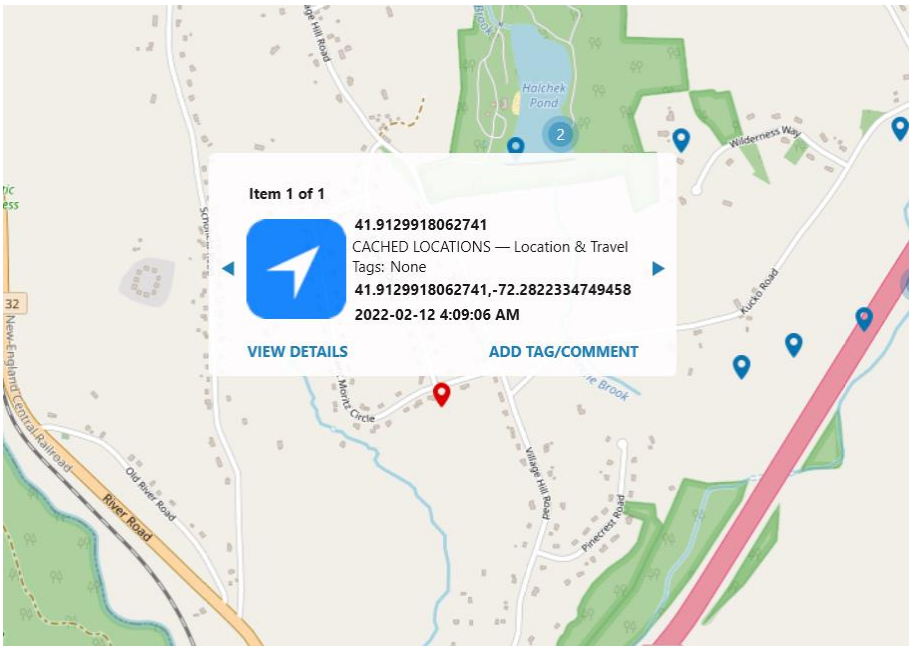
Judging from the timestamps, it appears that the phone had travelled for a little more than 7 hours to arrive at Willington, Massachusetts.


Magnet AXIOM Examine v6.7.1.33408 - Mobile Forensics
File Tools Process Help
FILTERS
Evidence
Artifacts
Content types
Date and time
Tags and comments
Profiles
Partial results
Keyword lists
Skin tone
Media categorization
Media attributes (VICS)
Type a search term...
GO
ADVANCED
Artifacts
MATCHING RESULTS (10,319 of 10,319)
World map view
DETAILS
TAGS, PROFILES & MEDIA CATEGORIES
MATCHING RESULTS 15,189
MEDIA 7
OPERATING SYSTEM 1,768
LOCATION & TRAVEL 13,414
Apple Maps Searches 4
Apple Maps Trips 1
Cached Locations 10,319
Google Maps Directions 1
Google Maps Tiles 37
WiFi Locations 3,052
ZOOM
VIEW
POINTS
44° 04' 24.16" N 75° 14' 51.21" W
100 km
Time zone UTC-5:00
ENG
US
11:00 PM
2022-12-01


Magnet AXIOM Examine v6.7.1.33408 - Mobile Forensics
File Tools Process Help
FILTERS
Evidence
Artifacts
Content types
Date and time
Tags and comments
Profiles
Partial results
Keyword lists
Skin tone
Media categorization
Media attributes (VICS)
Type a search term...
GO
ADVANCED
Artifacts
MATCHING RESULTS (1,768 of 1,768)
World map view
DETAILS
TAGS, PROFILES & MEDIA CATEGORIES
MATCHING RESULTS 15,189
MEDIA 7
OPERATING SYSTEM 1,768
Cell Tower Locations 1,768
LOCATION & TRAVEL 13,414
Apple Maps Searches 4
Apple Maps Trips 1
Cached Locations 10,319
Google Maps Directions 1
Google Maps Tiles 37
WiFi Locations 3,052
ZOOM
VIEW
POINTS
43° 31' 43.10" N 75° 35' 56.84" W
100 km
Time zone UTC-5:00
ENG
US
11:00 PM
2022-12-01

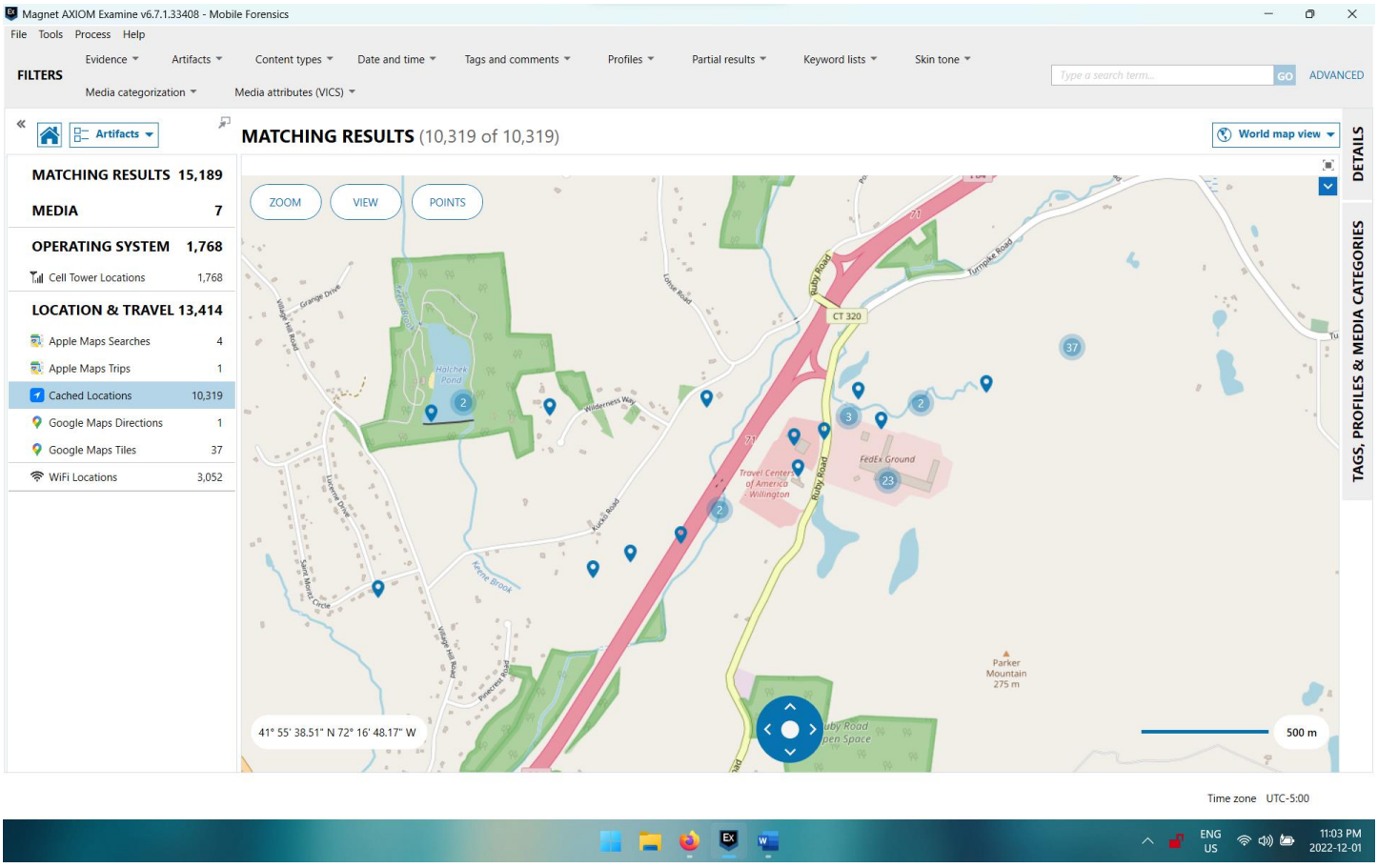

Magnet AXIOM Examine v6.7.1.33408 - Mobile Forensics
File Tools Process Help
FILTERS
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone
Media categorization Media attributes (VICS)
Type a search term...
GO
ADVANCED
Artifacts
MATCHING RESULTS (10,319 of 10,319)
World map view
DETAILS
TAGS, PROFILES & MEDIA CATEGORIES
MATCHING RESULTS 15,189
MEDIA 7
OPERATING SYSTEM 1,768
Cell Tower Locations 1,768
LOCATION & TRAVEL 13,414
Apple Maps Searches 4
Apple Maps Trips 1
Cached Locations 10,319
Google Maps Directions 1
Google Maps Tiles 37
WiFi Locations 3,052
ZOOM
VIEW
POINTS
42° 15' 10.50" N 72° 49' 50.04" W
25 km
Time zone UTC-5:00
ENG
US
11:03 PM
2022-12-01

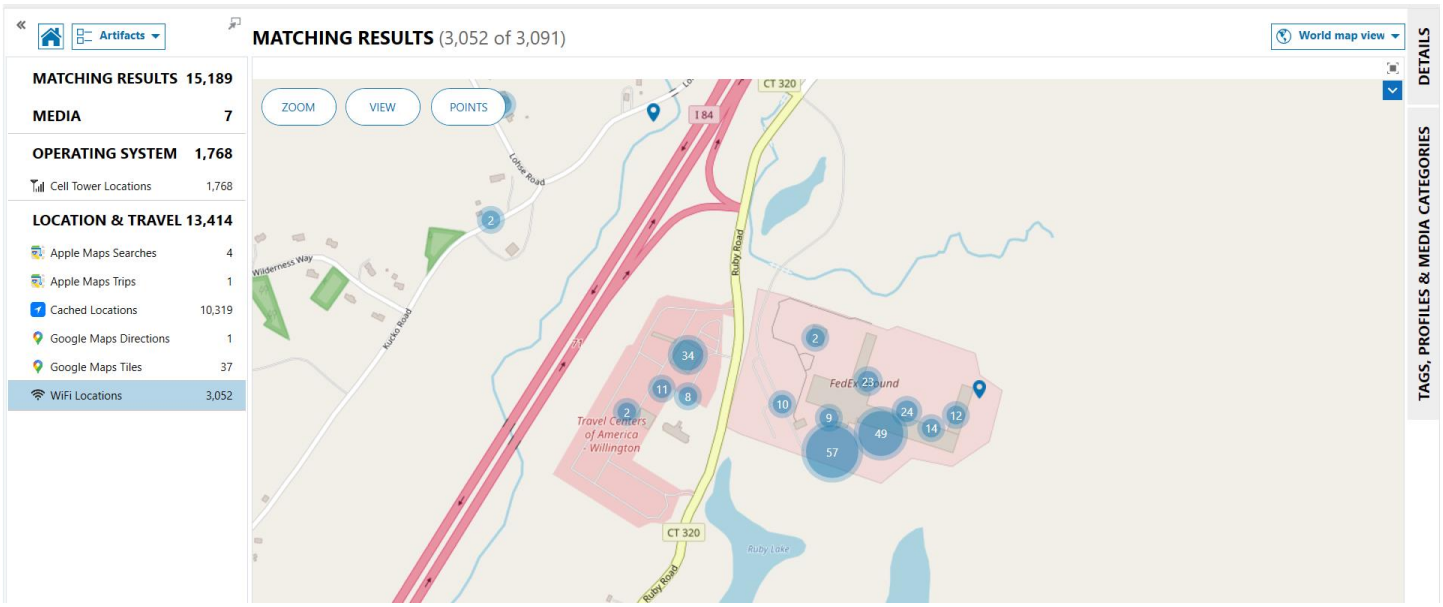

Item 1 of 1
44.3462889058753
CACHED LOCATIONS — Location & Travel
Tags: None
44.3462889058753,-72.8062859520019
2022-02-11 8:58:19 PM
VIEW DETAILS
ADD TAG/COMMENT
Waterbury



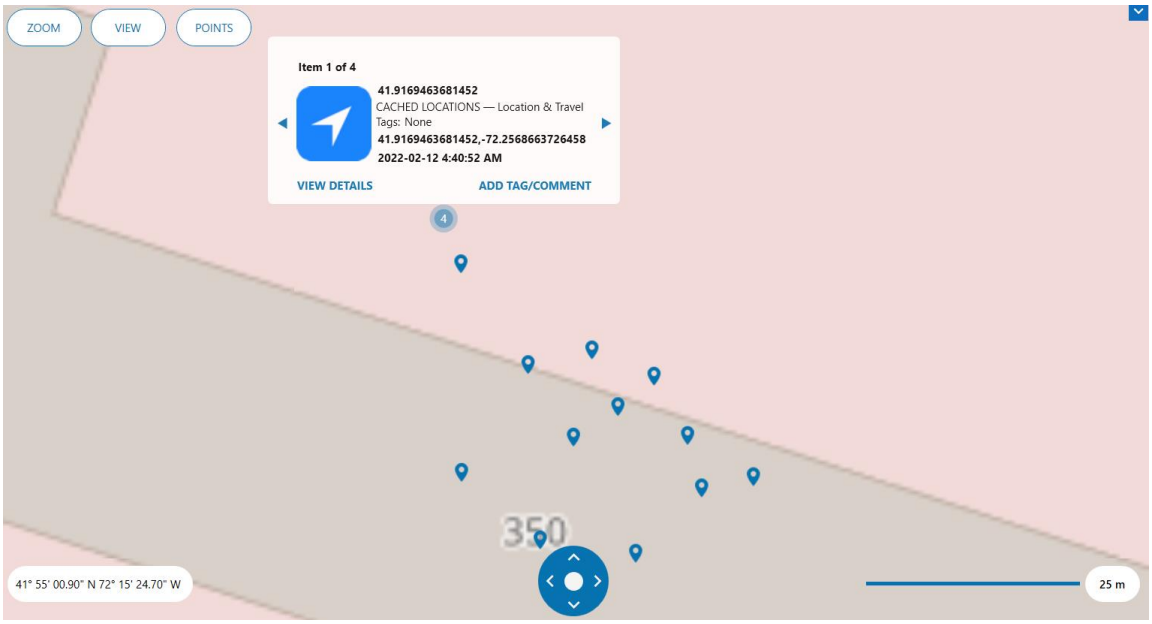
Willington, Massachusetts

The first destination of the phone in Willington is a FedEx Ground center. This coincides with our discovery that one of the location hotspots of the phone back in Burlington was also one of FedEx's centers. It is increasingly more likely that the usage of the phone is associated with FedEx services/employment.

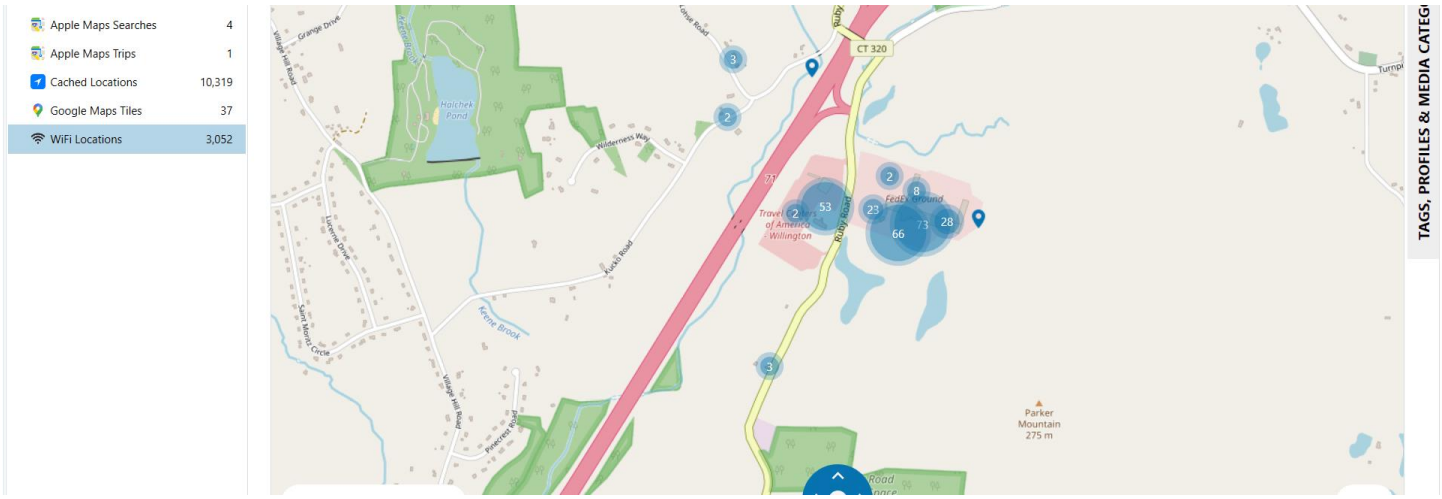




The time of arrival was 12th February 2022.



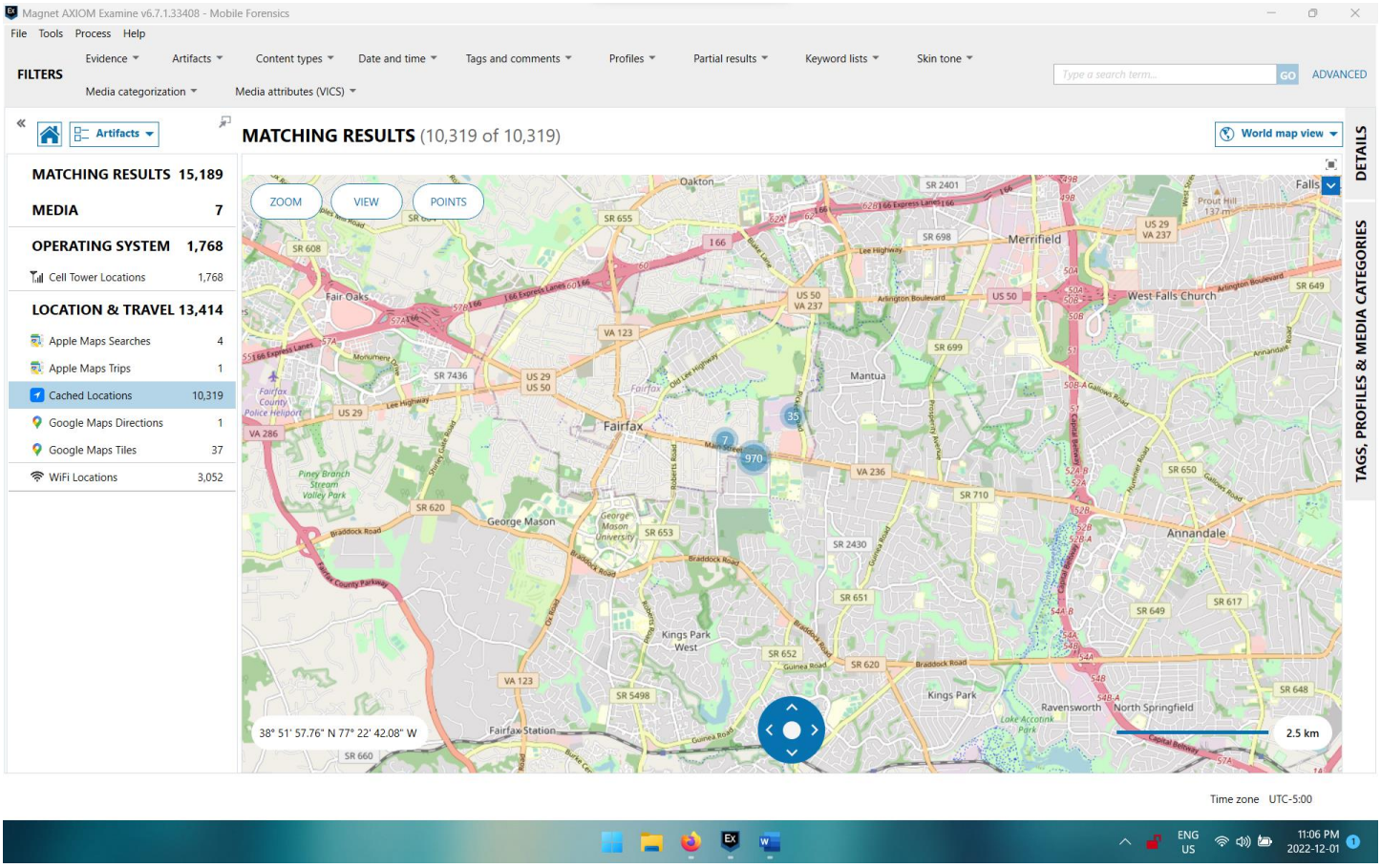
Wifi location confirms the long stay in the FedEx Ground center.

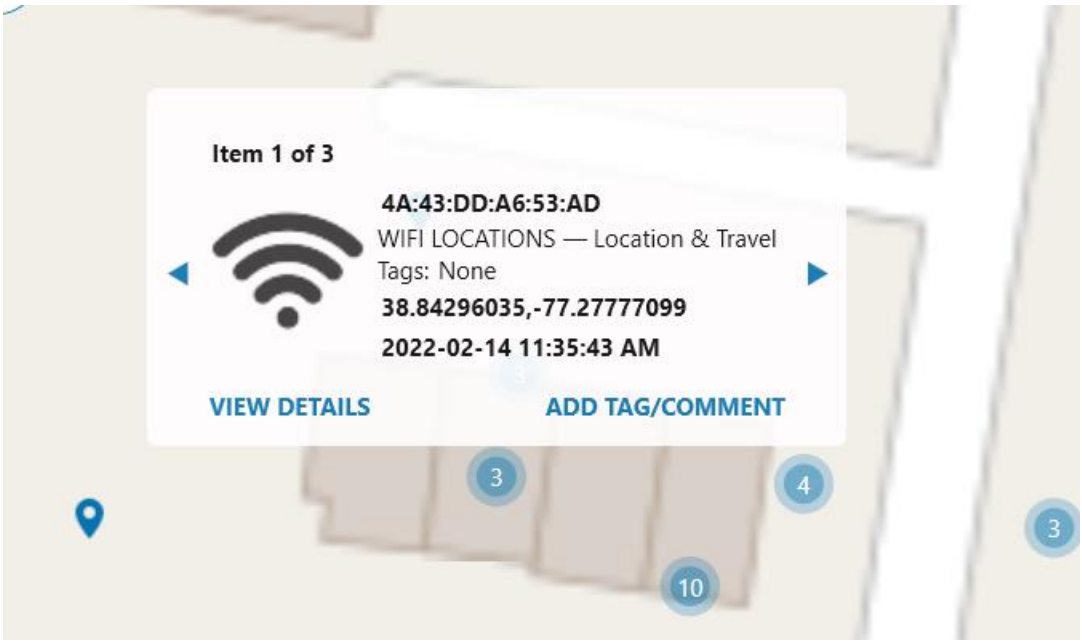


Unfortunately, there isn't sufficient data in the Willington area to make many more assumptions about its activities.

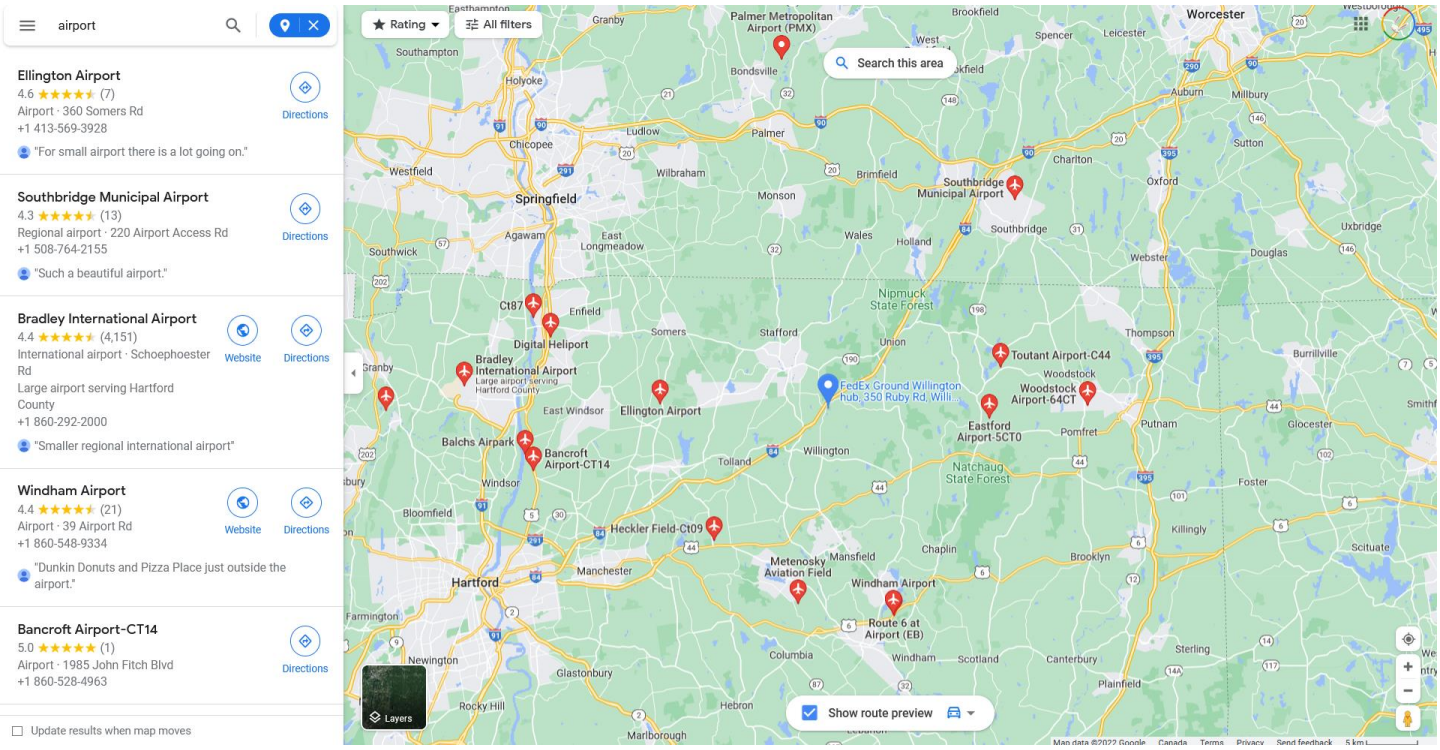
Fairfax, Virginia

The next spot with the phone's location data is Fairfax, Virginia. Unlike the road from Burlington to Willington, there isn't any data point on the map between Willington and Fairfax. It is highly likely that either the phone was turned off, without reception or it was via air travel. Time of arrival was 11:35AM, 14th February 2022.

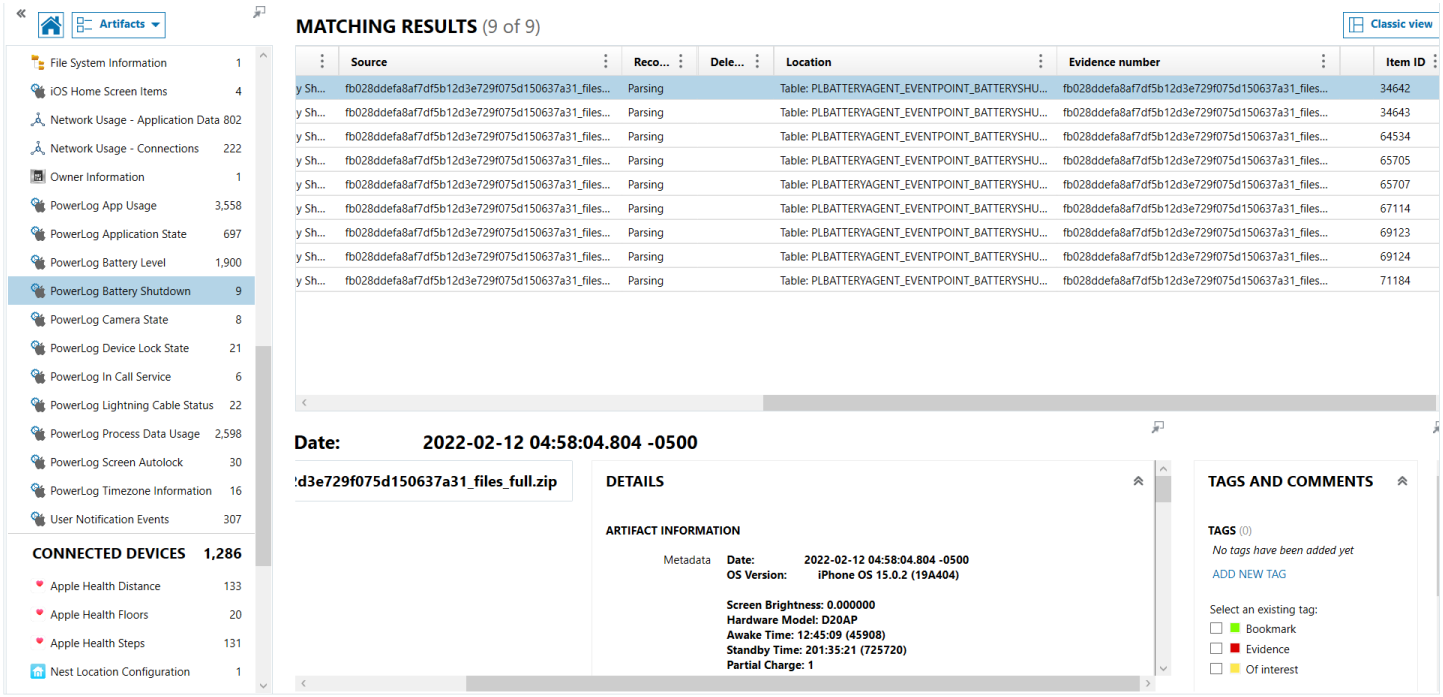


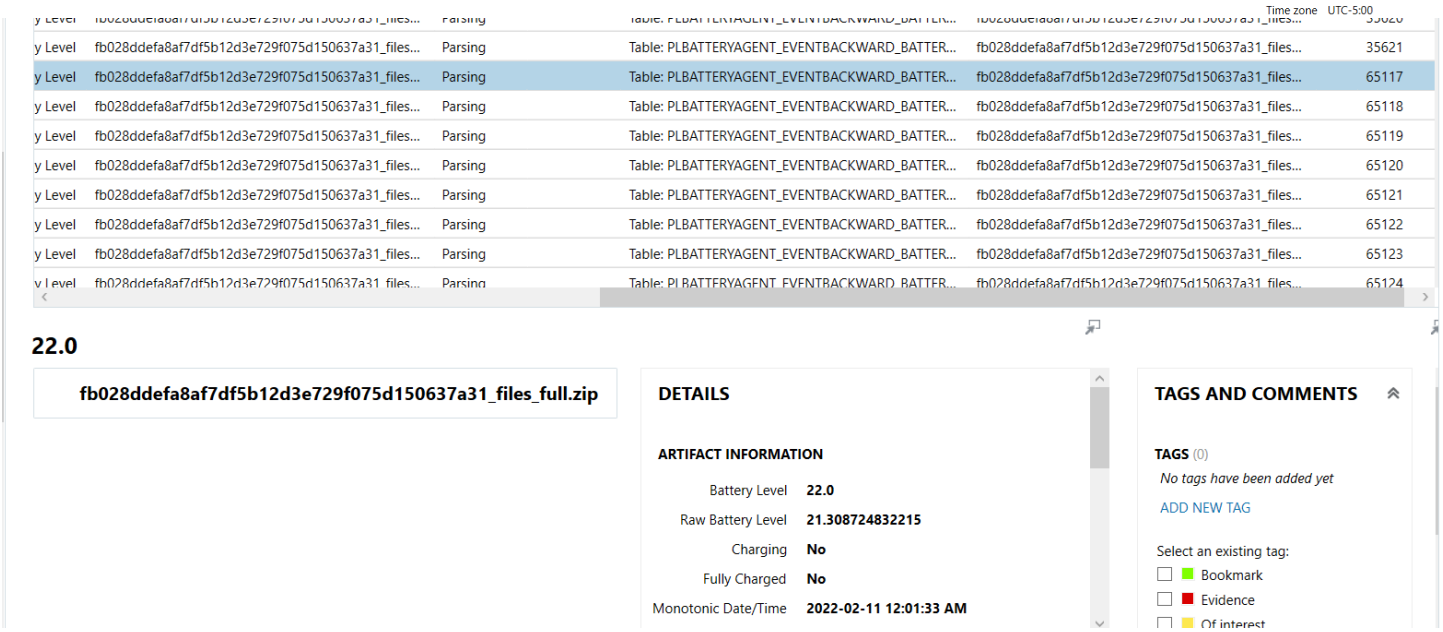


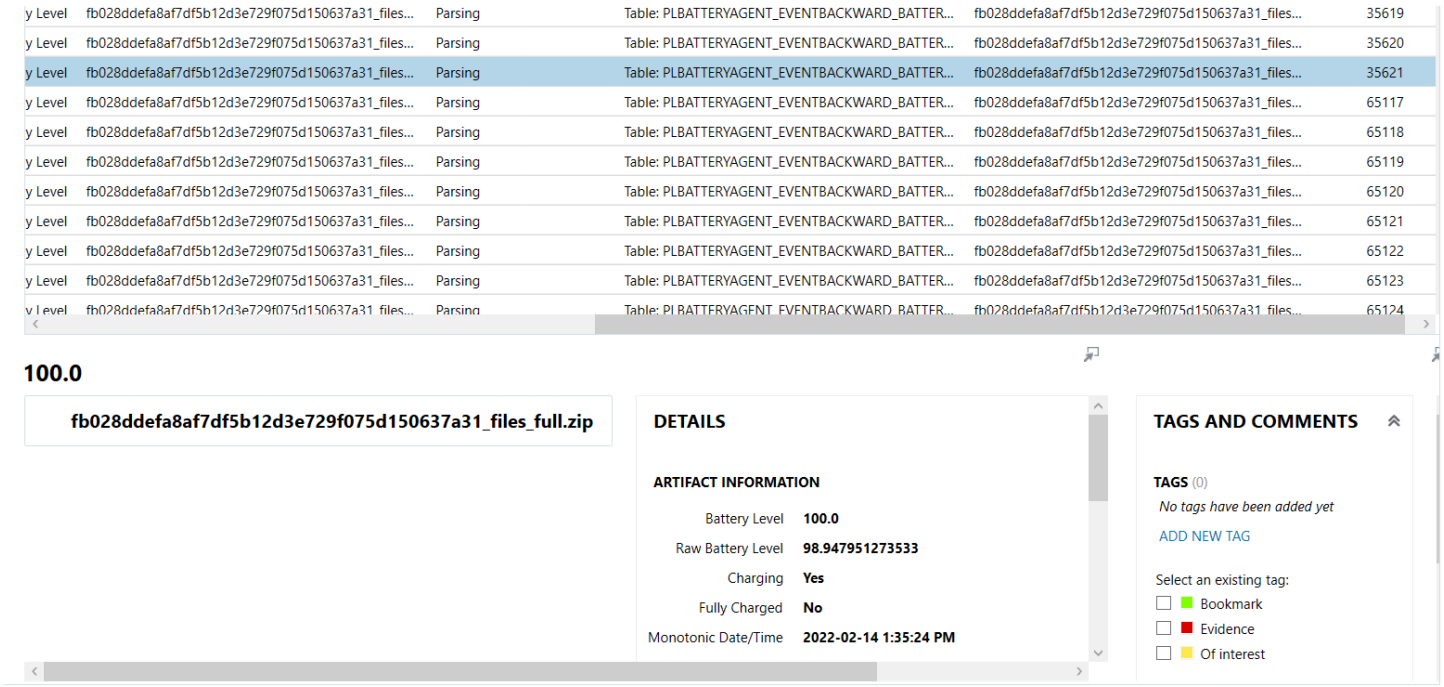
Since airports are far away from the Willington FedEx Center and the FedEx center was a Ground center, it would be fair to assume that they travelled on the road. The phone either did not have cell reception or it was powered off.



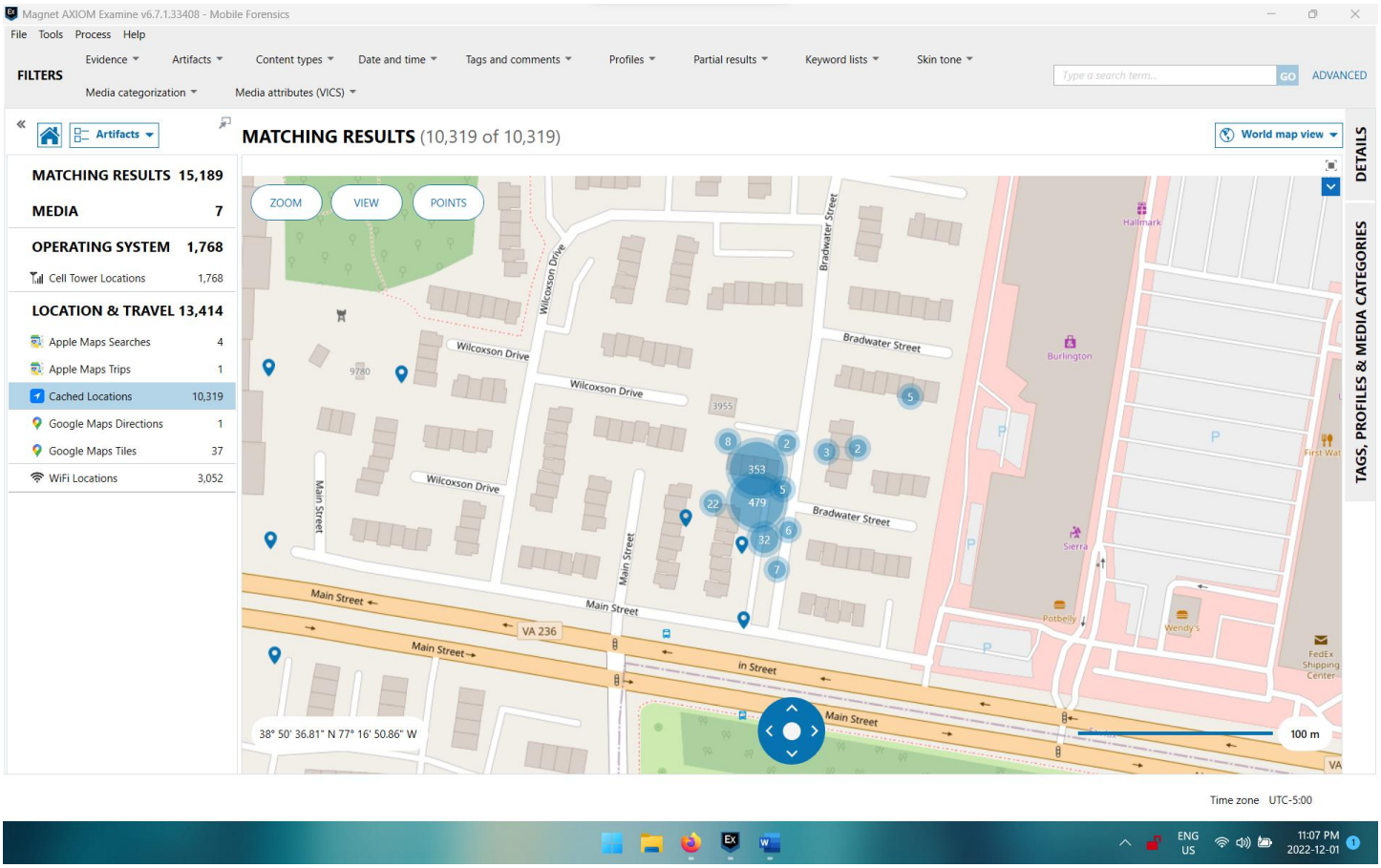
However, I have found a shutdown log on the phone that indicates it was powered off on 12th February 2022 4:58 am. That is exactly right after the phone had arrived from Burlington to Willington. The phone had no location data after this particular timestamp. In the battery levels log, there was also a disconnect of data between 11th and 14th. Therefore, it is with a high level of confidence to assume that the phone was shut off sometime when it arrived at Willington and turned back on until it reached Fairfax.

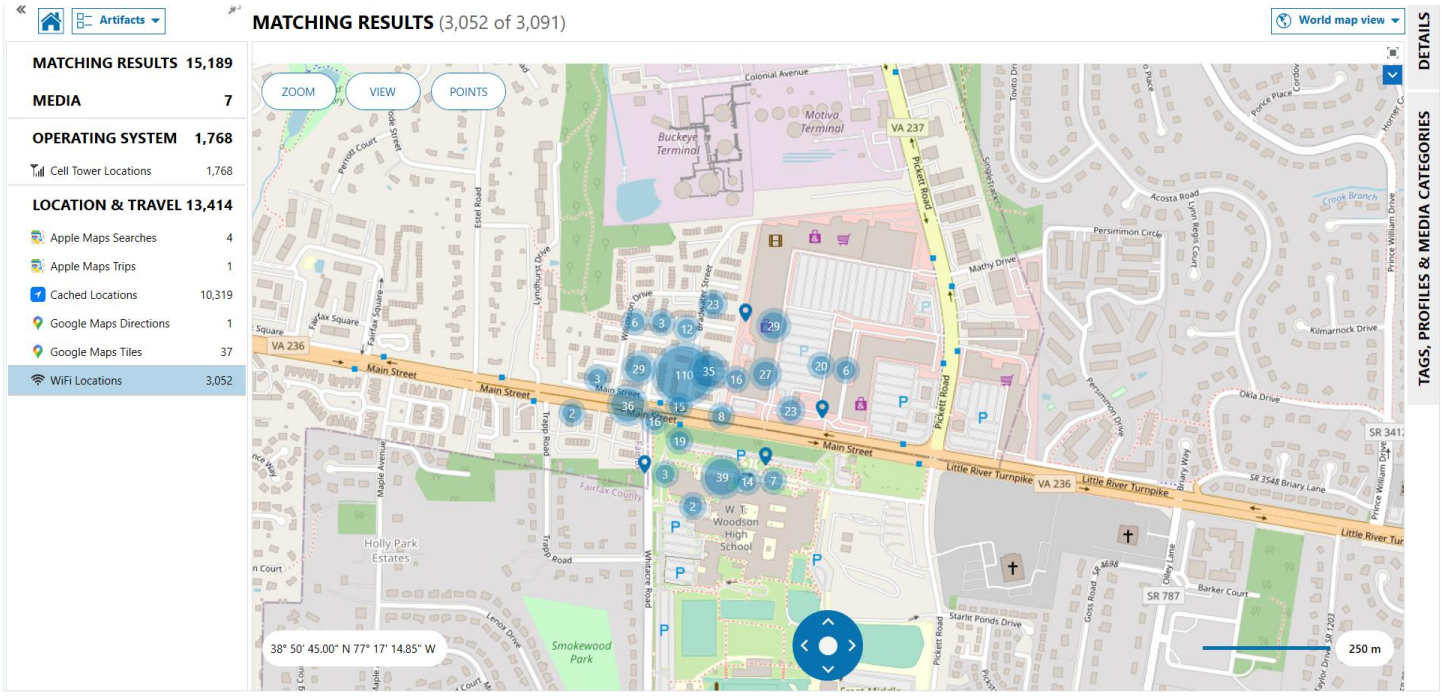

Artifacts
File System Information 1
iOS Home Screen Items 4
Network Usage - Application Data 802
Network Usage - Connections 222
Owner Information 1
PowerLog App Usage 3,558
PowerLog Application State 697
PowerLog Battery Level 1,900
PowerLog Battery Shutdown 9
PowerLog Camera State 8
PowerLog Device Lock State 21
PowerLog In Call Service 6
PowerLog Lightning Cable Status 22
PowerLog Process Data Usage 2,598
PowerLog Screen Autolock 30
PowerLog Timezone Information 16
User Notification Events 307
CONNECTED DEVICES 1,286
Apple Health Distance 133
Apple Health Floors 20
Apple Health Steps 131
Nest Location Configuration 1
MATCHING RESULTS (9 of 9)
Classic view
Source
Reco...
Dele...
Location
Evidence number
Item ID
Parsing
Table: PLBATTERYAGENT_EVENTPOINT_BATTERYSHU...
34642
34643
64534
65705
65707
67114
69123
69124
71184
Date: 2022-02-12 04:58:04.804 -0500
DETAILS
ARTIFACT INFORMATION
Metadata
Date: 2022-02-12 04:58:04.804 -0500
OS Version: iPhone OS 15.0.2 (19A404)
Screen Brightness: 0.000000
Hardware Model: D20AP
Awake Time: 12:45:09 (45908)
Standby Time: 201:35:21 (725720)
Partial Charge: 1
TAGS AND COMMENTS
TAGS (0)
No tags have been added yet
ADD NEW TAG
Select an existing tag:
Bookmark
Evidence
Of interest

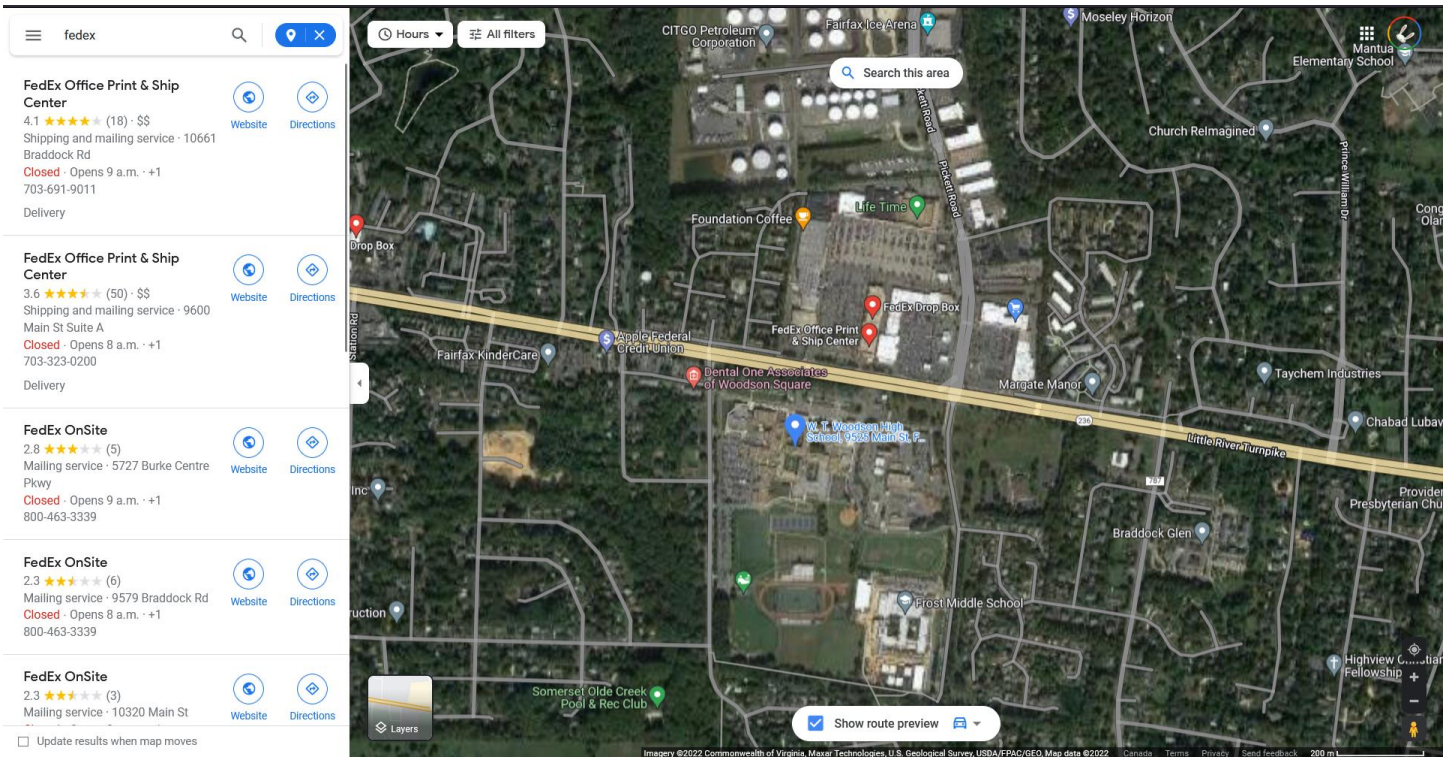

Time zone UTC-5:00
y Level fb028ddefa8af7df5b12d3e729f075d150637a31_files... Parsing Table: PLBATTERYAGENT_EVENTBACKWARD_BATTER... fb028ddefa8af7df5b12d3e729f075d150637a31_files... 35621
y Level fb028ddefa8af7df5b12d3e729f075d150637a31_files... Parsing Table: PLBATTERYAGENT_EVENTBACKWARD_BATTER... fb028ddefa8af7df5b12d3e729f075d150637a31_files... 65117
y Level fb028ddefa8af7df5b12d3e729f075d150637a31_files... Parsing Table: PLBATTERYAGENT_EVENTBACKWARD_BATTER... fb028ddefa8af7df5b12d3e729f075d150637a31_files... 65118
y Level fb028ddefa8af7df5b12d3e729f075d150637a31_files... Parsing Table: PLBATTERYAGENT_EVENTBACKWARD_BATTER... fb028ddefa8af7df5b12d3e729f075d150637a31_files... 65119
y Level fb028ddefa8af7df5b12d3e729f075d150637a31_files... Parsing Table: PLBATTERYAGENT_EVENTBACKWARD_BATTER... fb028ddefa8af7df5b12d3e729f075d150637a31_files... 65120
y Level fb028ddefa8af7df5b12d3e729f075d150637a31_files... Parsing Table: PLBATTERYAGENT_EVENTBACKWARD_BATTER... fb028ddefa8af7df5b12d3e729f075d150637a31_files... 65121
y Level fb028ddefa8af7df5b12d3e729f075d150637a31_files... Parsing Table: PLBATTERYAGENT_EVENTBACKWARD_BATTER... fb028ddefa8af7df5b12d3e729f075d150637a31_files... 65122
y Level fb028ddefa8af7df5b12d3e729f075d150637a31_files... Parsing Table: PLBATTERYAGENT_EVENTBACKWARD_BATTER... fb028ddefa8af7df5b12d3e729f075d150637a31_files... 65123
22.0
fb028ddefa8af7df5b12d3e729f075d150637a31_files_full.zip
DETAILS
ARTIFACT INFORMATION
Battery Level 22.0
Raw Battery Level 21.308724832215
Charging No
Fully Charged No
Monotonic Date/Time 2022-02-11 12:01:33 AM
TAGS AND COMMENTS
TAGS (0)
No tags have been added yet
ADD NEW TAG
Select an existing tag:
Bookmark
Evidence



Back to Willington, the phone reappeared in a residential area near WT Woodson high school. Although at first glance this may seem unimpressive and confusing, if we look to the right there are actually a FedEx Drop Box and Shipping Center. It is now almost certain the activities on the phone are associated with FedEx operations.



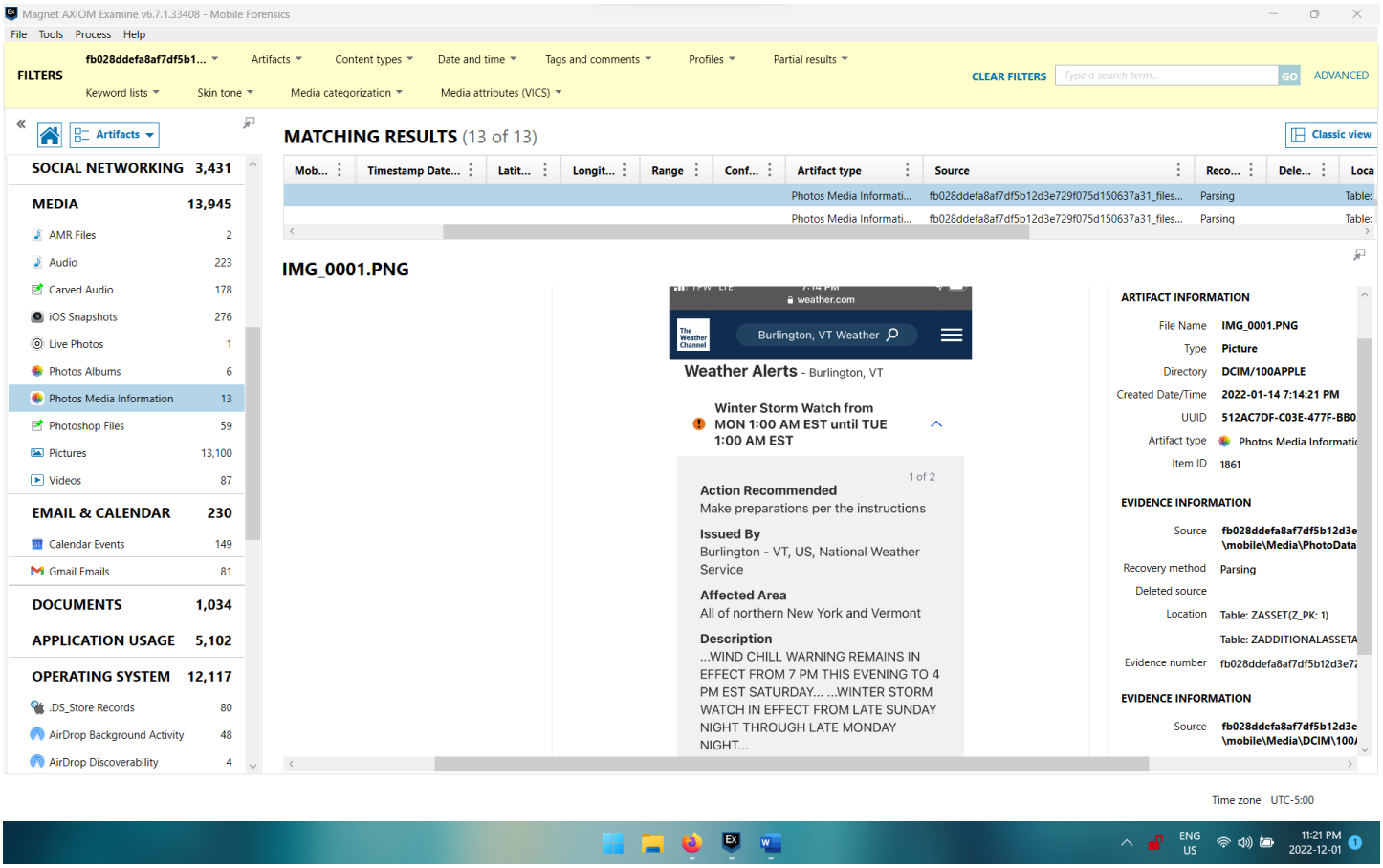




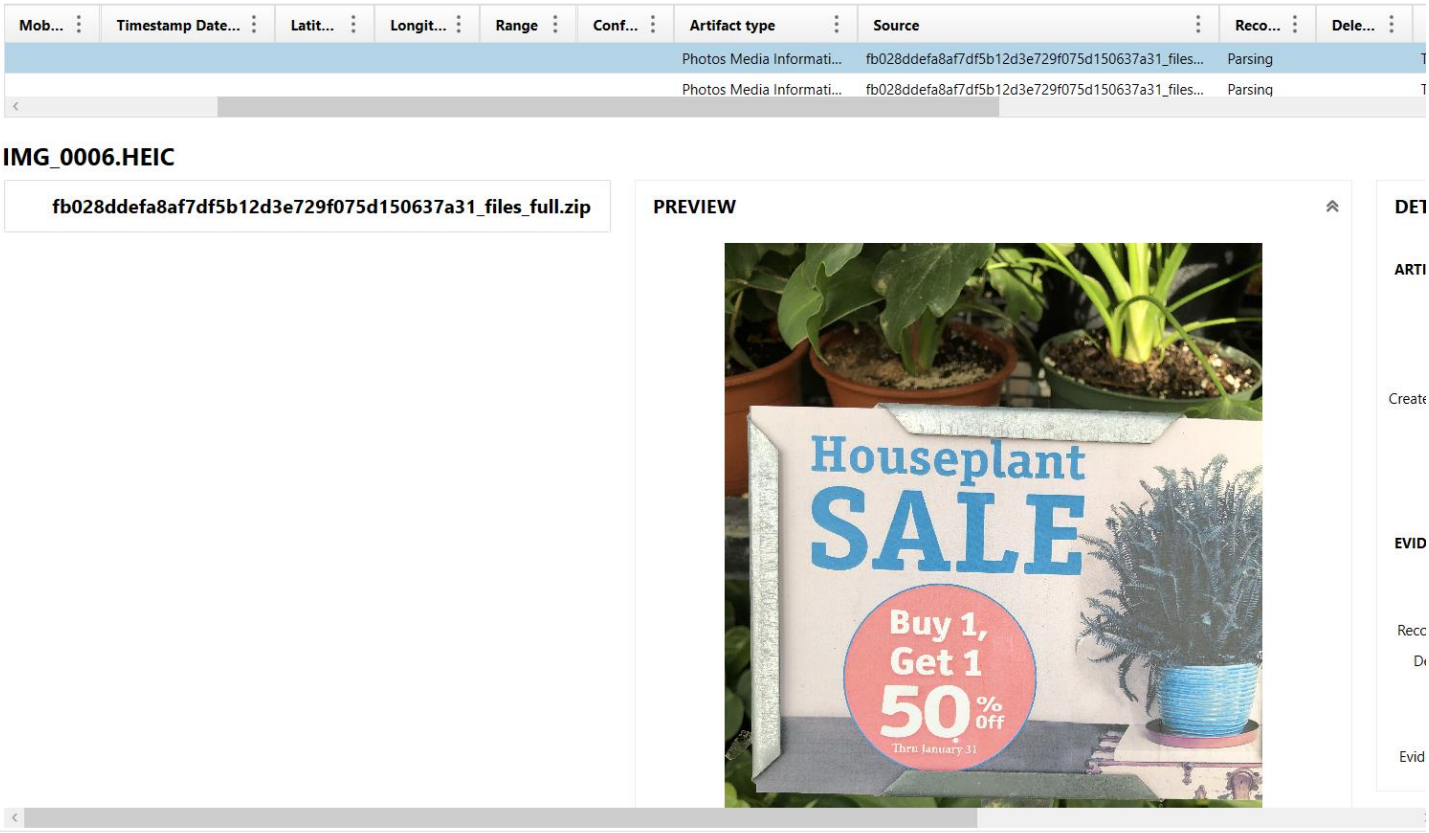
The location investigation of the iPhone ends here as there is no more meaningful data available.

Extra information from Media, iOS snapshots and photos

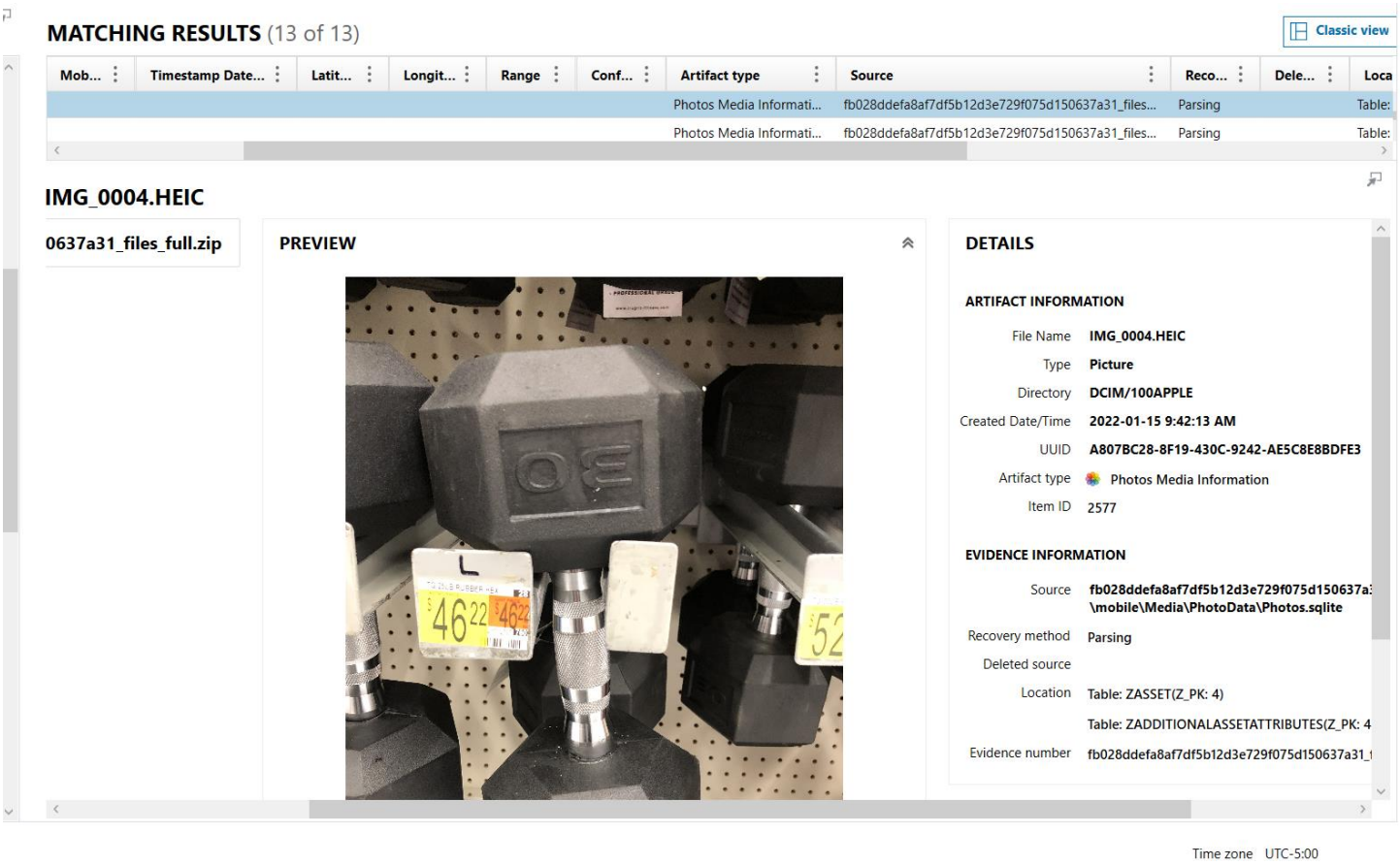
Weather search of Burlington area.



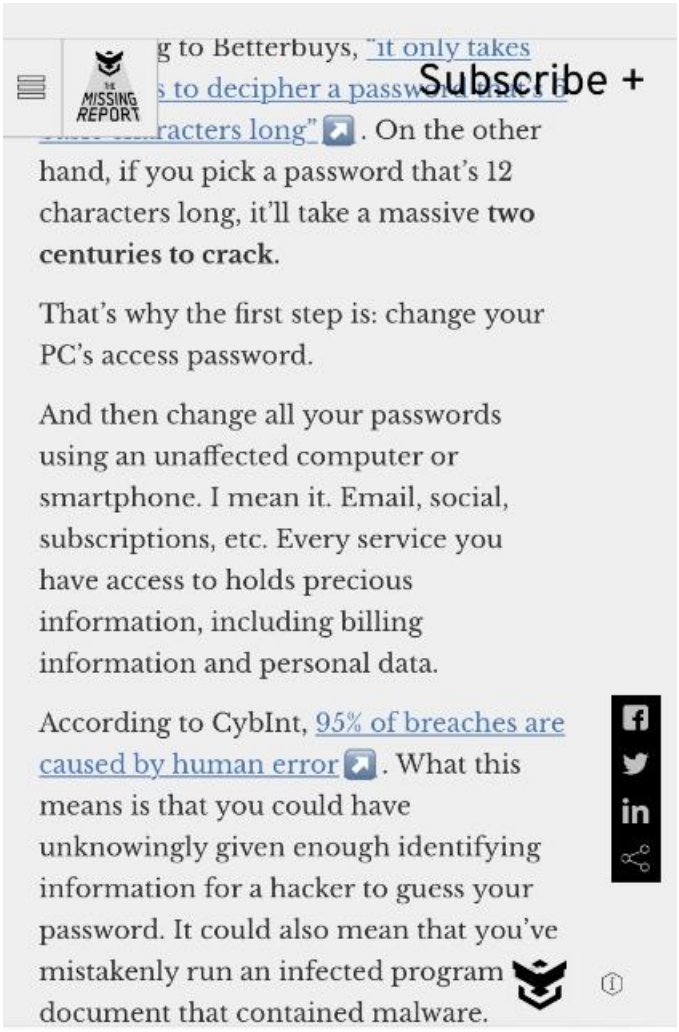
Seems like a product on sale in Gardener's supply.



Seemingly dumbbells from the EDGE gym.



This person was also searching online for what to do after they got hacked.



Conclusion

Based on the above analysis, it is very possible that the iPhone is owned by a person employed at FedEx, as the location data displayed is always in the vicinity of a FedEx facility. This employee is responsible for being on the road a lot and travelling between FedEx Centers. Therefore, the most likely occupation of the phone's owner is a FedEx driver. The driver first travelled from Burlington to Willington, then to Fairfax in the span of 3 days.

It is likely that the owner of the iPhone is based in Burlington, since frequent activities are present in the city. Not only does the person likely have a workplace there, he or she also regularly visits Downtown location including shopping mall, college, parks, gym and waterfront. He might be an avid park goer/jogger and is very active physically (Gym). He has also been possible renovating his home due to his visits to stores that sell household items.

On a side note, he or she might have suspected that their electronic devices have been compromised. Hence, they were looking up information on how to handle hacks.

Analysis on Android phone

Device Information

DETAILS

ARTIFACT INFORMATION

Device ID	**aca736026ef21682**
IMSI	**311480671778848**
Bluetooth Address	**3C:28:6D:00:8E:C8**
Bluetooth Name	**Pixel 3**
Artifact type	**Android Device Information**
Item ID	116943

EVIDENCE INFORMATION

Source	**PhysicalDrive2 - Partition 2 (Microsoft NTFS, 203.73 TB) Data [D:\]\Downloads\2022 CTF - Android-001\data\data \com.google.android.gms\shared_prefs\Checkin.xml**
Recovery method	**Parsing**
Deleted source	
Location	**n/a**
Evidence number	**iOS Keychain**

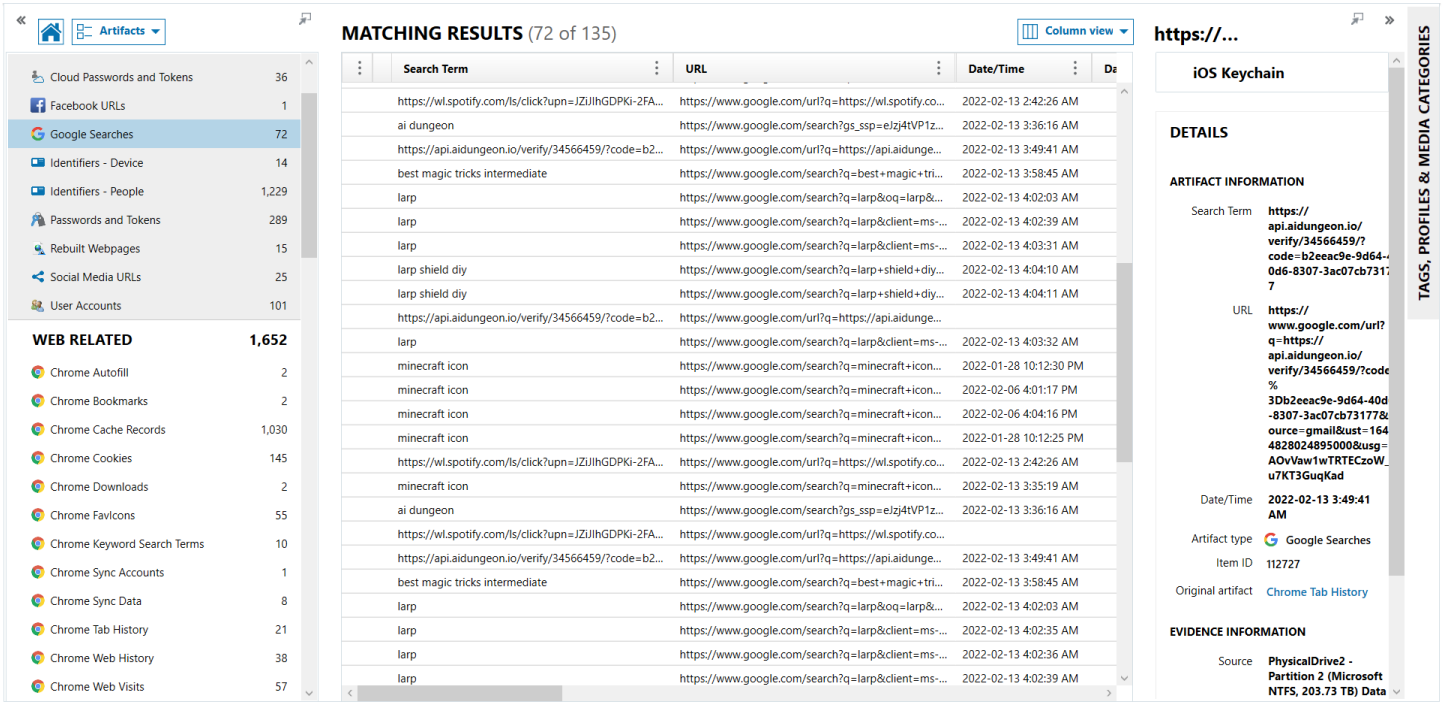
EVIDENCE INFORMATION

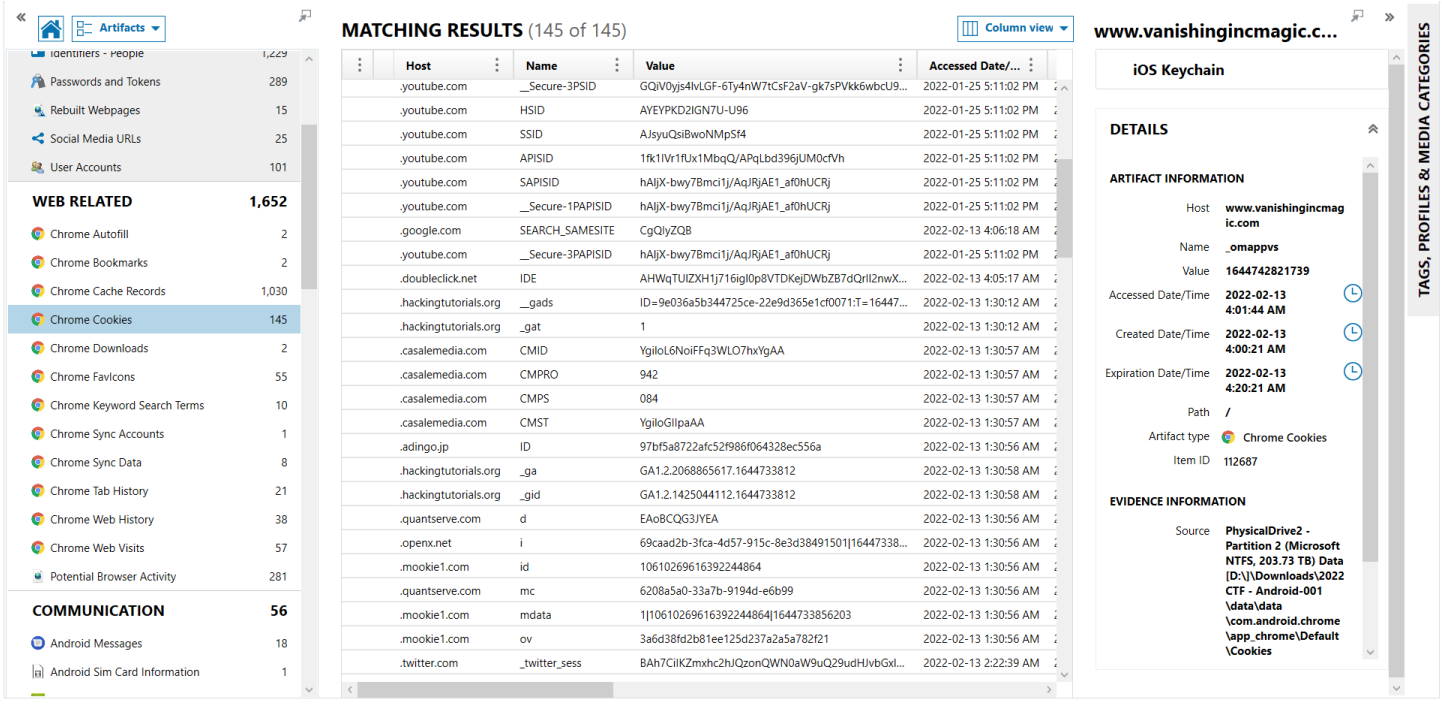
Source	**PhysicalDrive2 - Partition 2 (Microsoft NTFS, 203.73 TB) Data [D:\]\Downloads\2022 CTF - Android-001\data\system\users\0 \settings_secure.xml**
Recovery method	**Parsing**
Deleted source	
Location	**n/a**
Evidence number	**iOS Keychain**

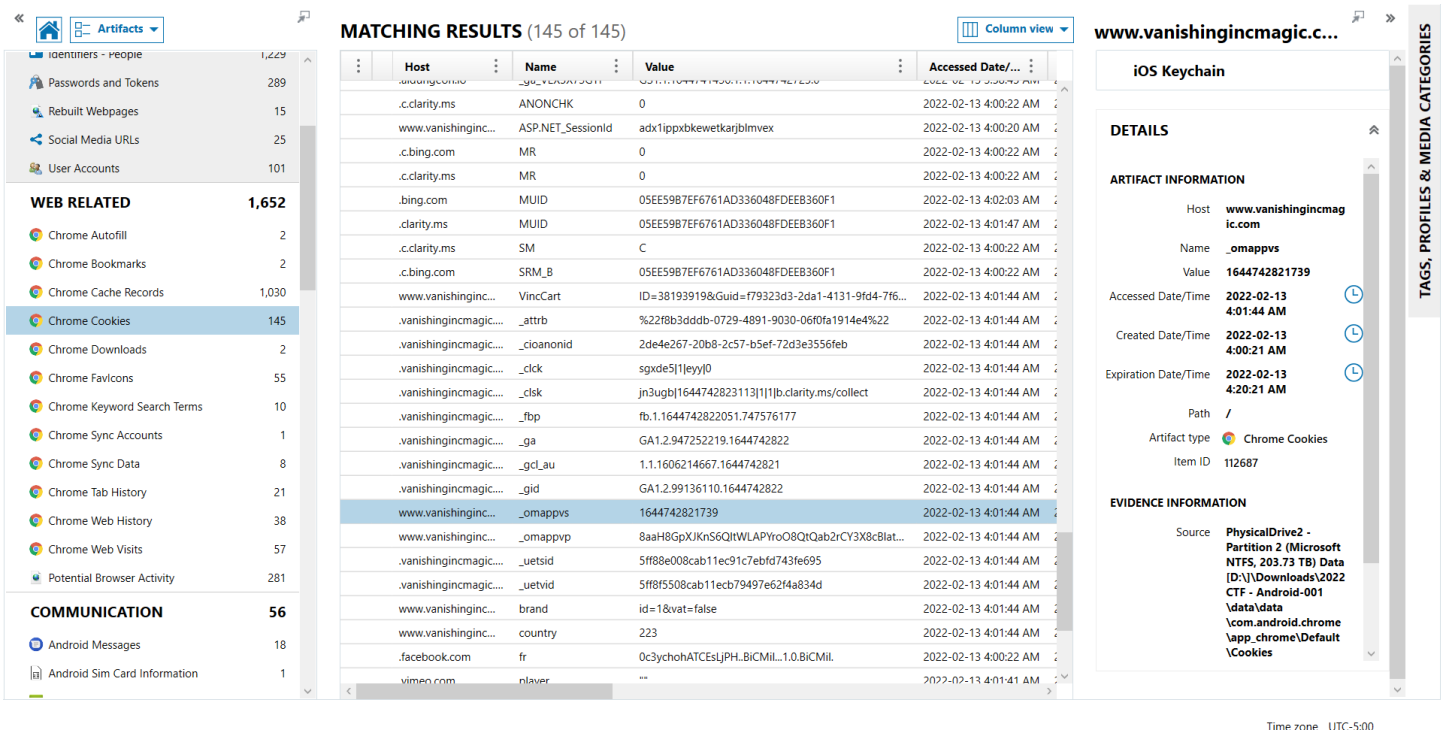
This phone is a Pixel 3 running on Android.

Google Searches

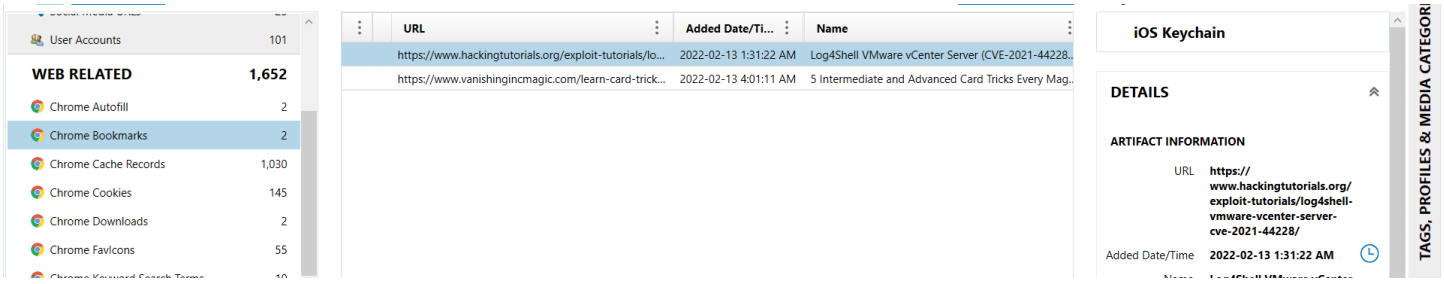
From Google searches, we can roughly make out what kind of person the user is. Looks like the user is interested in AI dungeon, LARP (maybe medieval theme since there is a shield), Minecraft, magic tricks and hacking. He also listens to a lot of music.


Artifacts
Cloud Passwords and Tokens 36
Facebook URLs 1
Google Searches 72
Identifiers - Device 14
Identifiers - People 1,229
Passwords and Tokens 289
Rebuilt Webpages 15
Social Media URLs 25
User Accounts 101
WEB RELATED 1,652
Chrome Autofill 2
Chrome Bookmarks 2
Chrome Cache Records 1,030
Chrome Cookies 145
Chrome Downloads 2
Chrome FavIcons 55
Chrome Keyword Search Terms 10
Chrome Sync Accounts 1
Chrome Sync Data 8
Chrome Tab History 21
Chrome Web History 38
Chrome Web Visits 57
MATCHING RESULTS (72 of 135)
Column view
Search Term
URL
Date/Time
https://wl.spotify.com/ls/click?upn=JZiJIhGDPKi-2FA... https://www.google.com/url?q=https://wl.spotify.co... 2022-02-13 2:42:26 AM
ai dungeon https://www.google.com/search?gs_ssp=eJzj4tVP1z... 2022-02-13 3:36:16 AM
https://api.aidungeon.io/verify/34566459/?code=b2... https://www.google.com/url?q=https://api.aidunge... 2022-02-13 3:49:41 AM
best magic tricks intermediate https://www.google.com/search?q=best+magic+tri... 2022-02-13 3:58:45 AM
larp https://www.google.com/search?q=larp&oq=larp&... 2022-02-13 4:02:03 AM
larp https://www.google.com/search?q=larp&client=ms-... 2022-02-13 4:02:39 AM
larp https://www.google.com/search?q=larp&client=ms-... 2022-02-13 4:03:31 AM
larp shield diy https://www.google.com/search?q=larp+shield+diy... 2022-02-13 4:04:10 AM
larp shield diy https://www.google.com/search?q=larp+shield+diy... 2022-02-13 4:04:11 AM
https://api.aidungeon.io/verify/34566459/?code=b2... https://www.google.com/url?q=https://api.aidunge...
larp https://www.google.com/search?q=larp&client=ms-... 2022-02-13 4:03:32 AM
minecraft icon https://www.google.com/search?q=minecraft+icon... 2022-01-28 10:12:30 PM
minecraft icon https://www.google.com/search?q=minecraft+icon... 2022-02-06 4:01:17 PM
minecraft icon https://www.google.com/search?q=minecraft+icon... 2022-02-06 4:04:16 PM
minecraft icon https://www.google.com/search?q=minecraft+icon... 2022-01-28 10:12:25 PM
https://wl.spotify.com/ls/click?upn=JZiJIhGDPKi-2FA... https://www.google.com/url?q=https://wl.spotify.co... 2022-02-13 2:42:26 AM
minecraft icon https://www.google.com/search?q=minecraft+icon... 2022-02-13 3:35:19 AM
ai dungeon https://www.google.com/search?gs_ssp=eJzj4tVP1z... 2022-02-13 3:36:16 AM
https://wl.spotify.com/ls/click?upn=JZiJIhGDPKi-2FA... https://www.google.com/url?q=https://wl.spotify.co...
https://api.aidungeon.io/verify/34566459/?code=b2... https://www.google.com/url?q=https://api.aidunge... 2022-02-13 3:49:41 AM
best magic tricks intermediate https://www.google.com/search?q=best+magic+tri... 2022-02-13 3:58:45 AM
larp https://www.google.com/search?q=larp&oq=larp&... 2022-02-13 4:02:03 AM
larp https://www.google.com/search?q=larp&client=ms-... 2022-02-13 4:02:35 AM
larp https://www.google.com/search?q=larp&client=ms-... 2022-02-13 4:02:36 AM
larp https://www.google.com/search?q=larp&client=ms-... 2022-02-13 4:02:39 AM
https://...
iOS Keychain
DETAILS
ARTIFACT INFORMATION
Search Term https://api.aidungeon.io/verify/34566459/?code=b2eeac9e-9d64-...
URL https://www.google.com/url?q=https://api.aidungeon.io/verify/34566459/?code...
Date/Time 2022-02-13 3:49:41 AM
Artifact type Google Searches
Item ID 112727
Original artifact Chrome Tab History
EVIDENCE INFORMATION
Source PhysicalDrive2 - Partition 2 (Microsoft NTFS, 203.73 TB) Data
TAGS, PROFILES & MEDIA CATEGORIES
Time zone UTC-5:00


Artifacts
Identifiers - People 1,229
Passwords and Tokens 289
Rebuilt Webpages 15
Social Media URLs 25
User Accounts 101
WEB RELATED 1,652
Chrome Autofill 2
Chrome Bookmarks 2
Chrome Cache Records 1,030
Chrome Cookies 145
Chrome Downloads 2
Chrome FavIcons 55
Chrome Keyword Search Terms 10
Chrome Sync Accounts 1
Chrome Sync Data 8
Chrome Tab History 21
Chrome Web History 38
Chrome Web Visits 57
Potential Browser Activity 281
COMMUNICATION 56
Android Messages 18
Android Sim Card Information 1
MATCHING RESULTS (145 of 145)
Column view
Host
Name
Value
Accessed Date/...
.youtube.com __Secure-3PSID GQiV0yjs4lvLGF-6Ty4nW7tCsF2aV-gk7sPVkk6wbcU9... 2022-01-25 5:11:02 PM
.youtube.com HSID AYEYPKD2IGN7U-U96 2022-01-25 5:11:02 PM
.youtube.com SSID AJsyuQsiBwoNMpSf4 2022-01-25 5:11:02 PM
.youtube.com APISID 1fk1IVr1fUx1MbqQ/APqLbd396jUM0cfVh 2022-01-25 5:11:02 PM
.youtube.com SAPISID hAljX-bwy7Bmci1j/AqJRjAE1_af0hUCRj 2022-01-25 5:11:02 PM
.youtube.com __Secure-1PAPISID hAljX-bwy7Bmci1j/AqJRjAE1_af0hUCRj 2022-01-25 5:11:02 PM
.google.com SEARCH_SAMESITE CgQIyZQB 2022-02-13 4:06:18 AM
.youtube.com __Secure-3PAPISID hAljX-bwy7Bmci1j/AqJRjAE1_af0hUCRj 2022-01-25 5:11:02 PM
.doubleclick.net IDE AHWqTUlZXH1j716igl0p8VTDKejDWbZB7dQrll2nwX... 2022-02-13 4:05:17 AM
.hackingtutorials.org __gads ID=9e036a5b344725ce-22e9d365e1cf0071:T=16447... 2022-02-13 1:30:12 AM
.hackingtutorials.org _gat 1 2022-02-13 1:30:12 AM
.casalemedia.com CMID YgiIoL6NoiFFq3WLO7hxYgAA 2022-02-13 1:30:57 AM
.casalemedia.com CMPRO 942 2022-02-13 1:30:57 AM
.casalemedia.com CMPS 084 2022-02-13 1:30:57 AM
.casalemedia.com CMST YgiIoGIIpaAA 2022-02-13 1:30:57 AM
.adingo.jp ID 97bf5a8722afc52f986f064328ec556a 2022-02-13 1:30:56 AM
.hackingtutorials.org _ga GA1.2.2068865617.1644733812 2022-02-13 1:30:58 AM
.hackingtutorials.org _gid GA1.2.1425044112.1644733812 2022-02-13 1:30:58 AM
.quantserve.com d EAoBCQG3JYEA 2022-02-13 1:30:56 AM
.openx.net i 69caad2b-3fca-4d57-915c-8e3d38491501|16447338... 2022-02-13 1:30:56 AM
.mookie1.com id 10610269616392244864 2022-02-13 1:30:56 AM
.quantserve.com mc 6208a5a0-33a7b-9194d-e6b99 2022-02-13 1:30:56 AM
.mookie1.com mdata 1|10610269616392244864|1644733856203 2022-02-13 1:30:56 AM
.mookie1.com ov 3a6d38fd2b81ee125d237a2a5a782f21 2022-02-13 1:30:56 AM
.twitter.com _twitter_sess BAh7CiIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxl... 2022-02-13 2:22:39 AM
www.vanishingincmagic.c...
iOS Keychain
DETAILS
ARTIFACT INFORMATION
Host www.vanishingincmagic.com
Name _omappvs
Value 1644742821739
Accessed Date/Time 2022-02-13 4:01:44 AM
Created Date/Time 2022-02-13 4:00:21 AM
Expiration Date/Time 2022-02-13 4:20:21 AM
Path /
Artifact type Chrome Cookies
Item ID 112687
EVIDENCE INFORMATION
Source PhysicalDrive2 - Partition 2 (Microsoft NTFS, 203.73 TB) Data (D:\)\Downloads\2022 CTF - Android-001\data\data\com.android.chrome\app_chrome\Default\Cookies
TAGS, PROFILES & MEDIA CATEGORIES
Time zone UTC-5:00

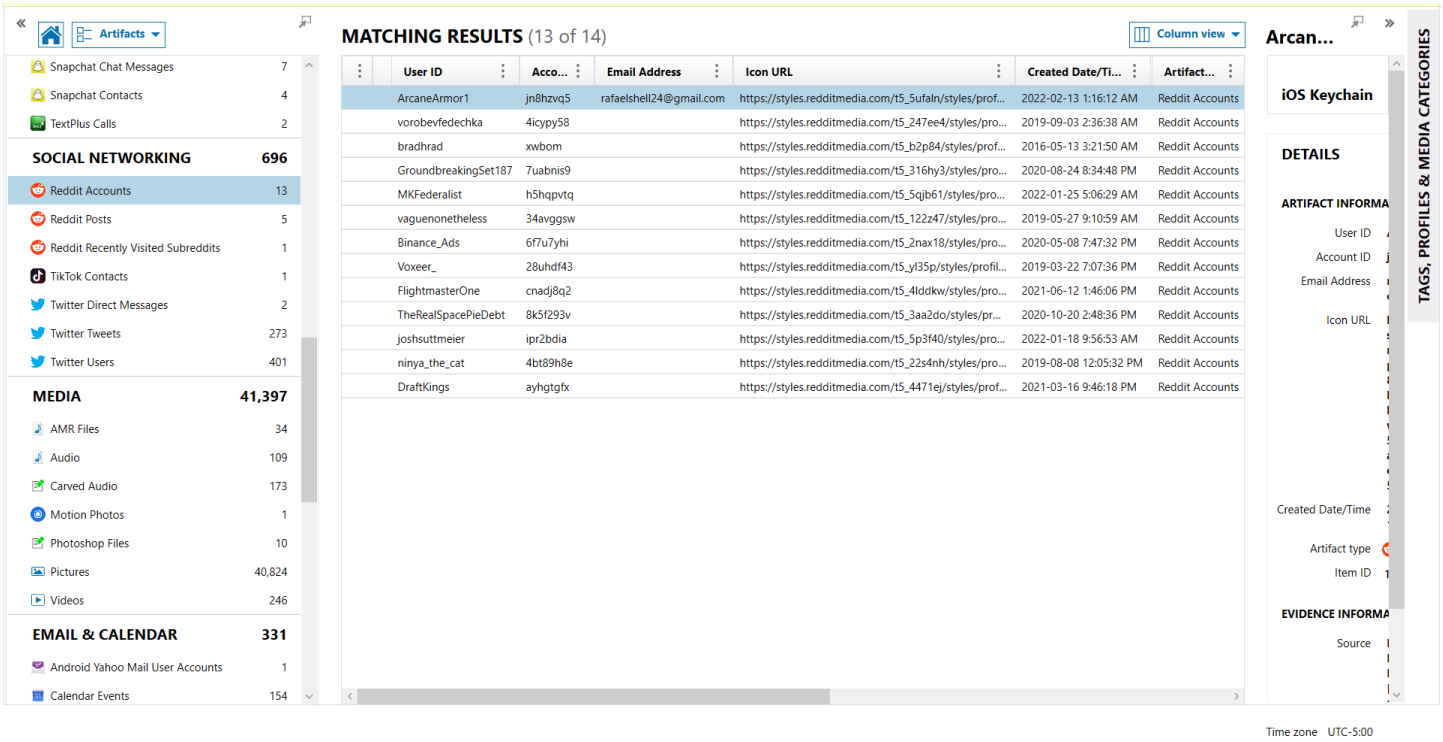


Interest in hacking can be confirmed by records in bookmark. The user bookmarked a page related to a tutorial on log4j exploit.

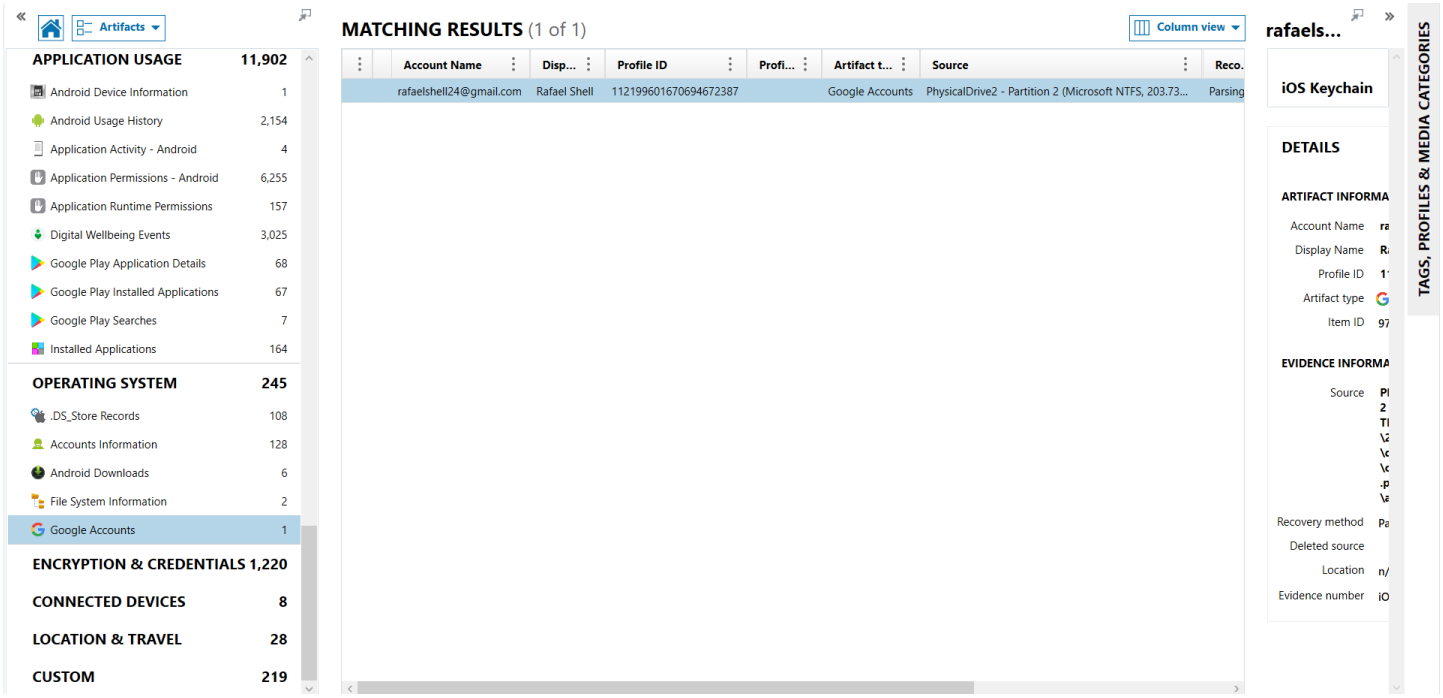


Social Media

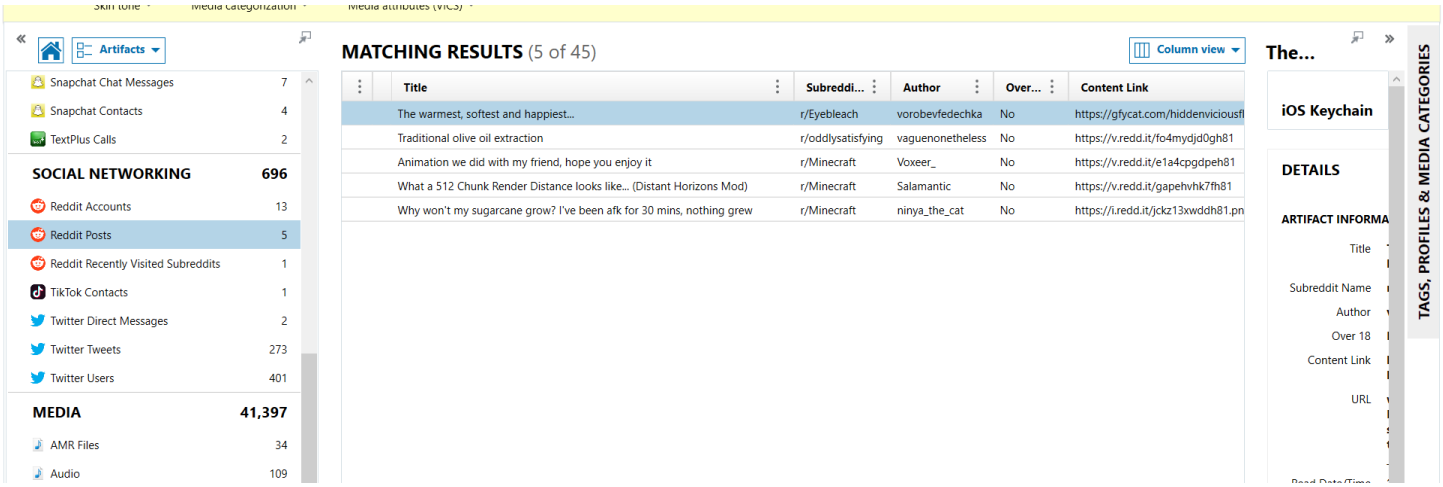
It appears that the user of the Pixel phone is an avid Reddit goer. He or she has multiple Reddit accounts, presumably for different purposes. One of his accounts has been associated with a Gmail address: rafaelshell24@gmail.co.



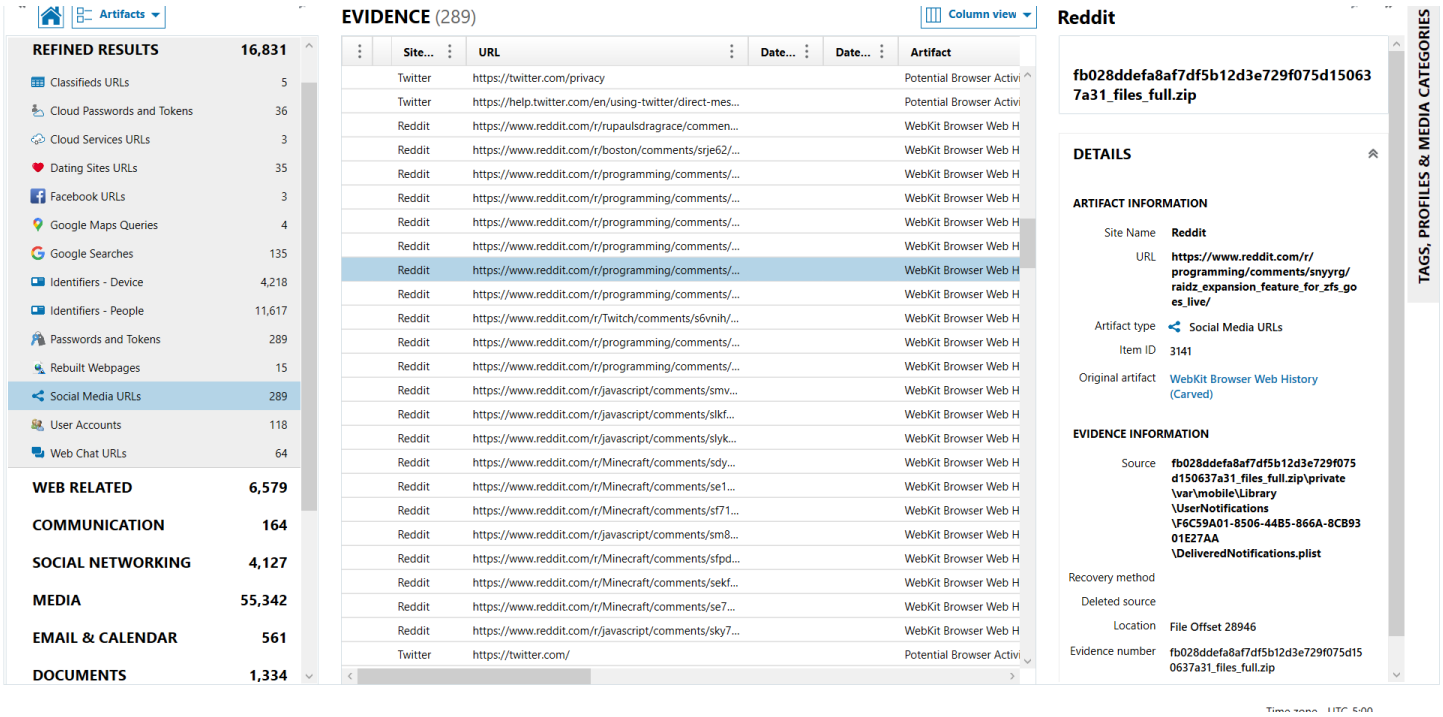
Rafaelshell24@gmail.com also shows up in the Google Account section, so presumably this is the person's main account and he is called Rafael.



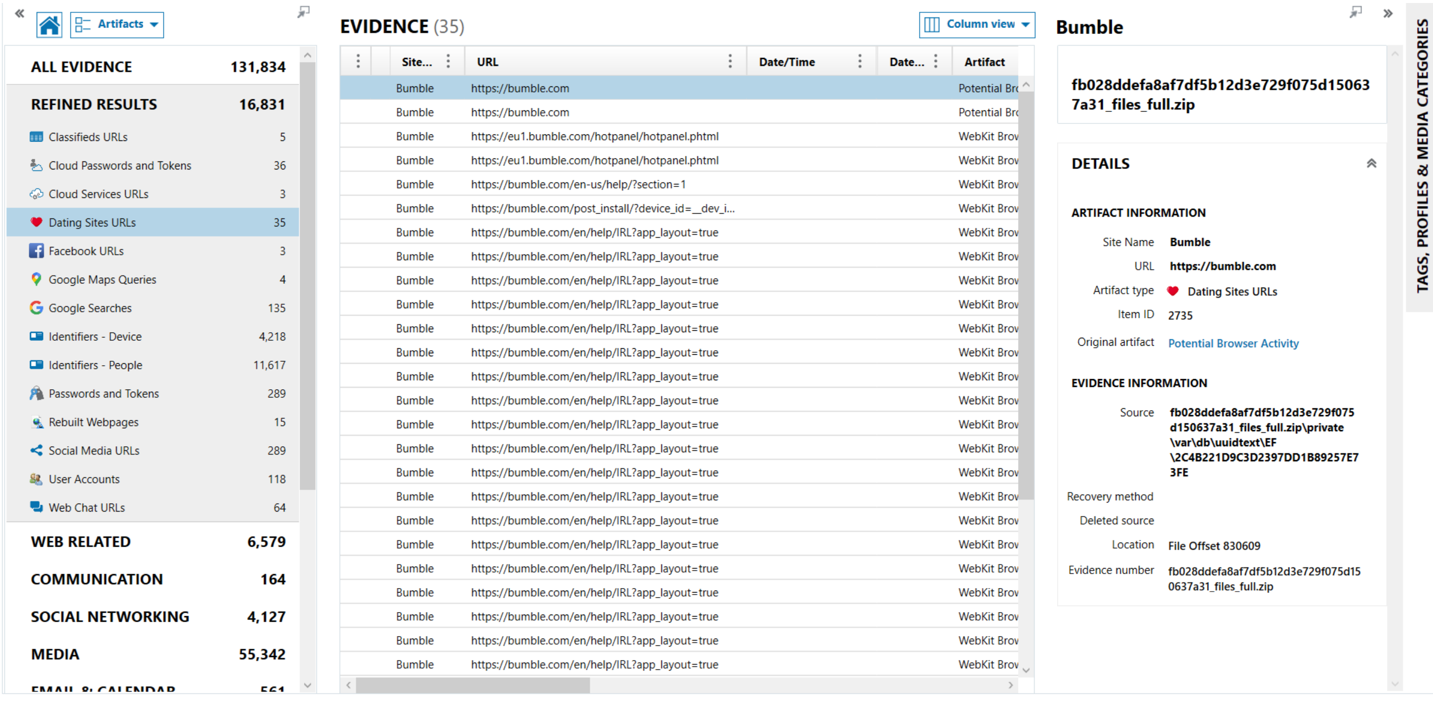
Reddit post history shows several posts. 3 of the 5 are Minecraft related, which matches with the Google search discovery. This might be one of his hobbies.



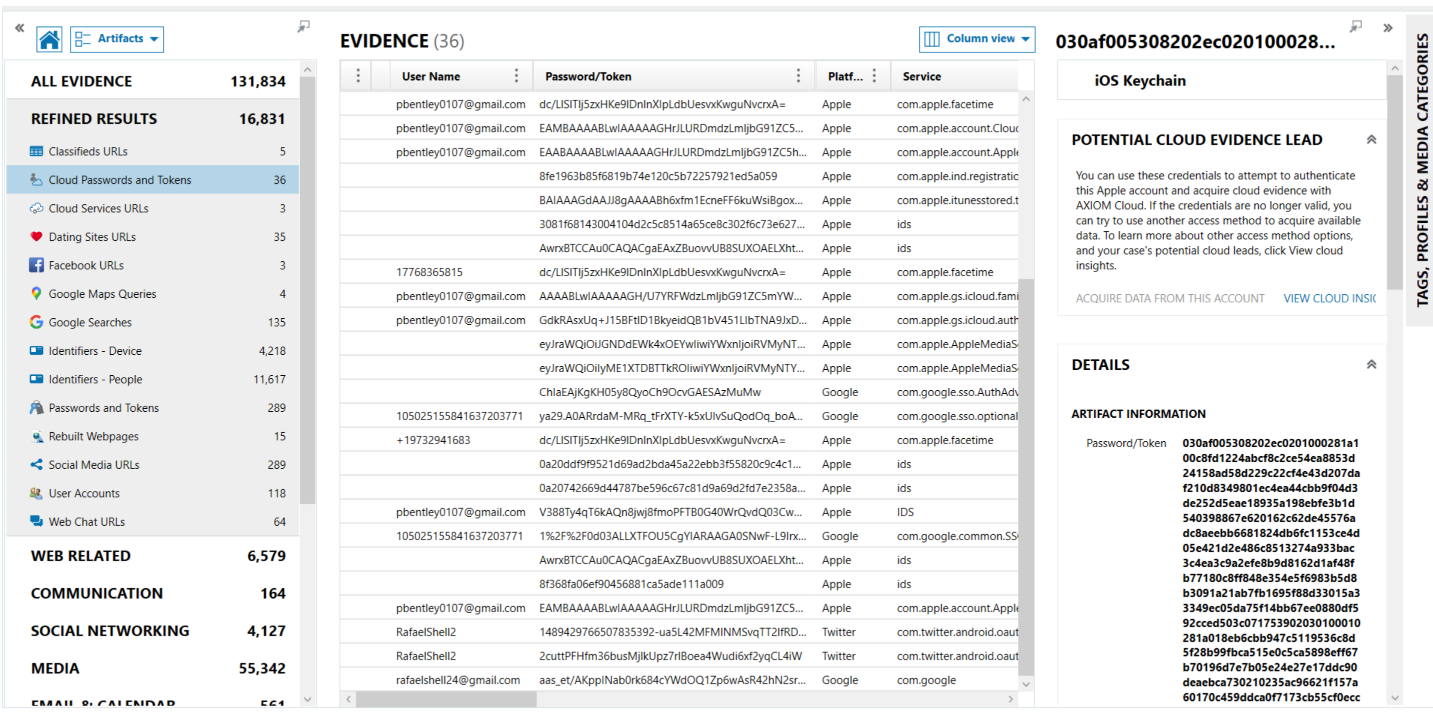
Social Media URLs show a lot more reddit posts than the previous section. Our understanding of his interests mostly stays the same, except for the addition of JavaScript posts which might indicate that he might be a JS hobbyist/developer.



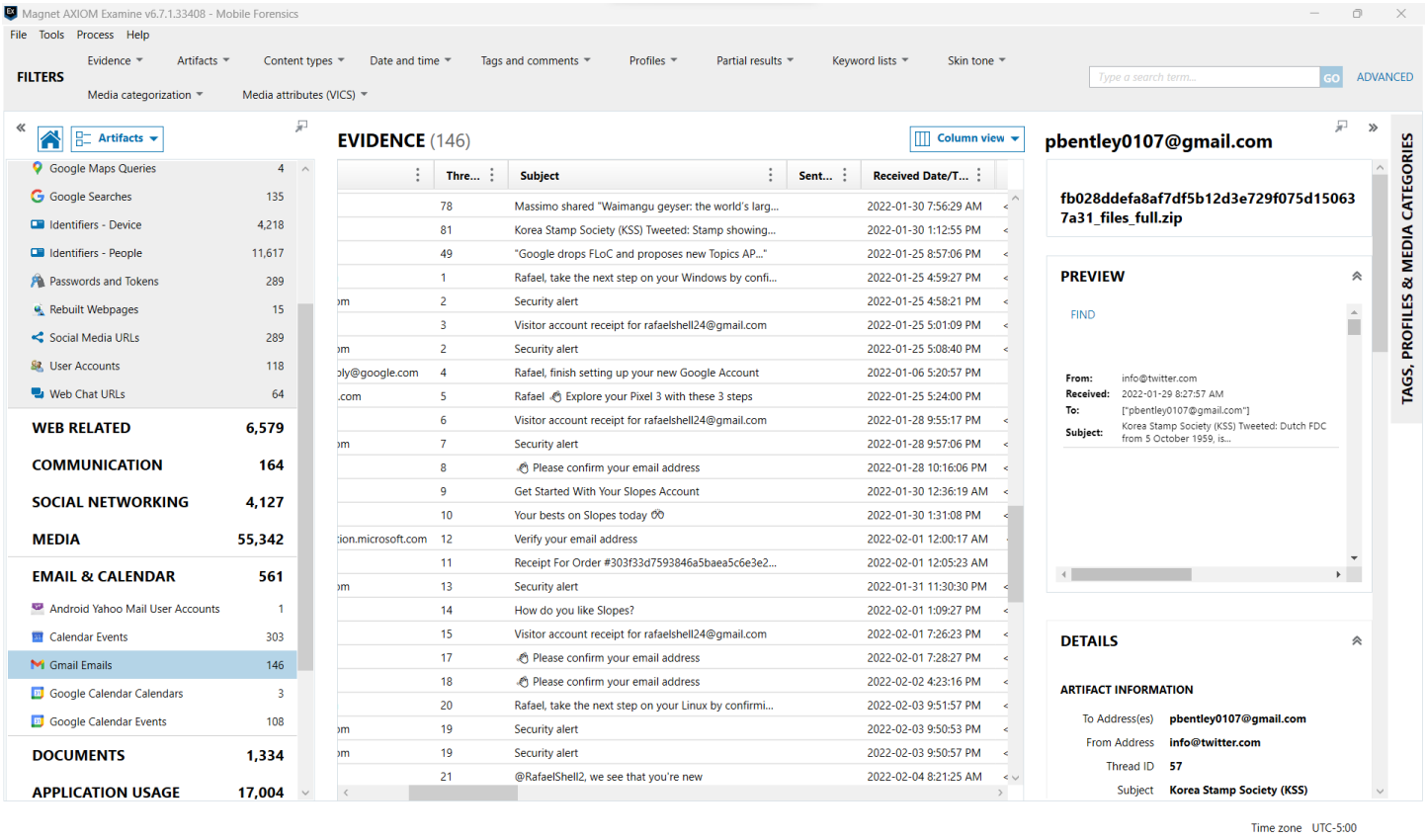
This person might be single and looking for a relationship. Results show that he frequents bumble.com which is a dating site.



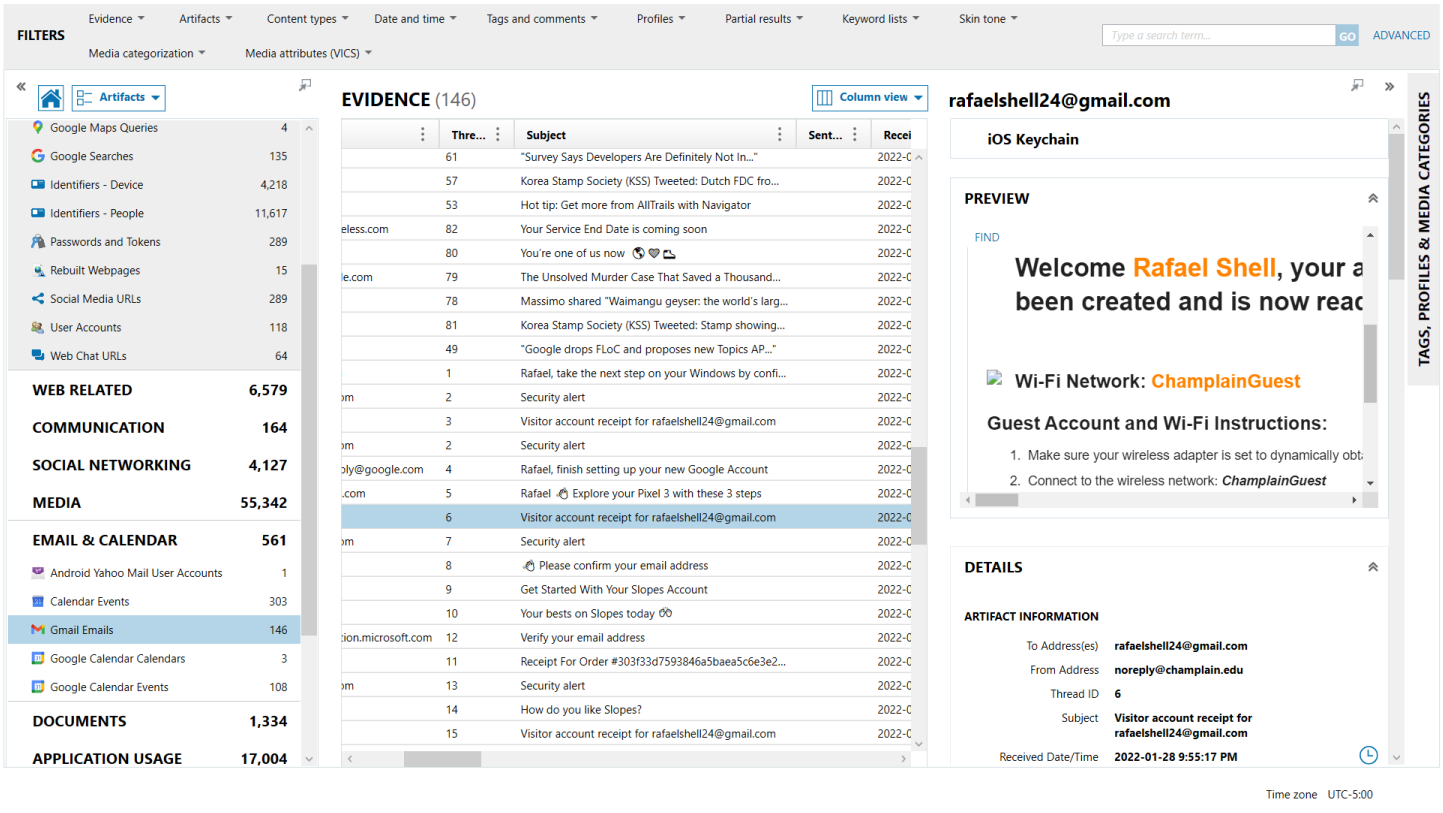
There are also some accounts on apple cloud. A new email address that pops up is pbentley0107@gmail.com registered on apple.com.



From his gmail history, he uses twitter and is interested in Politics, Bitcoin, Korea, gaming.

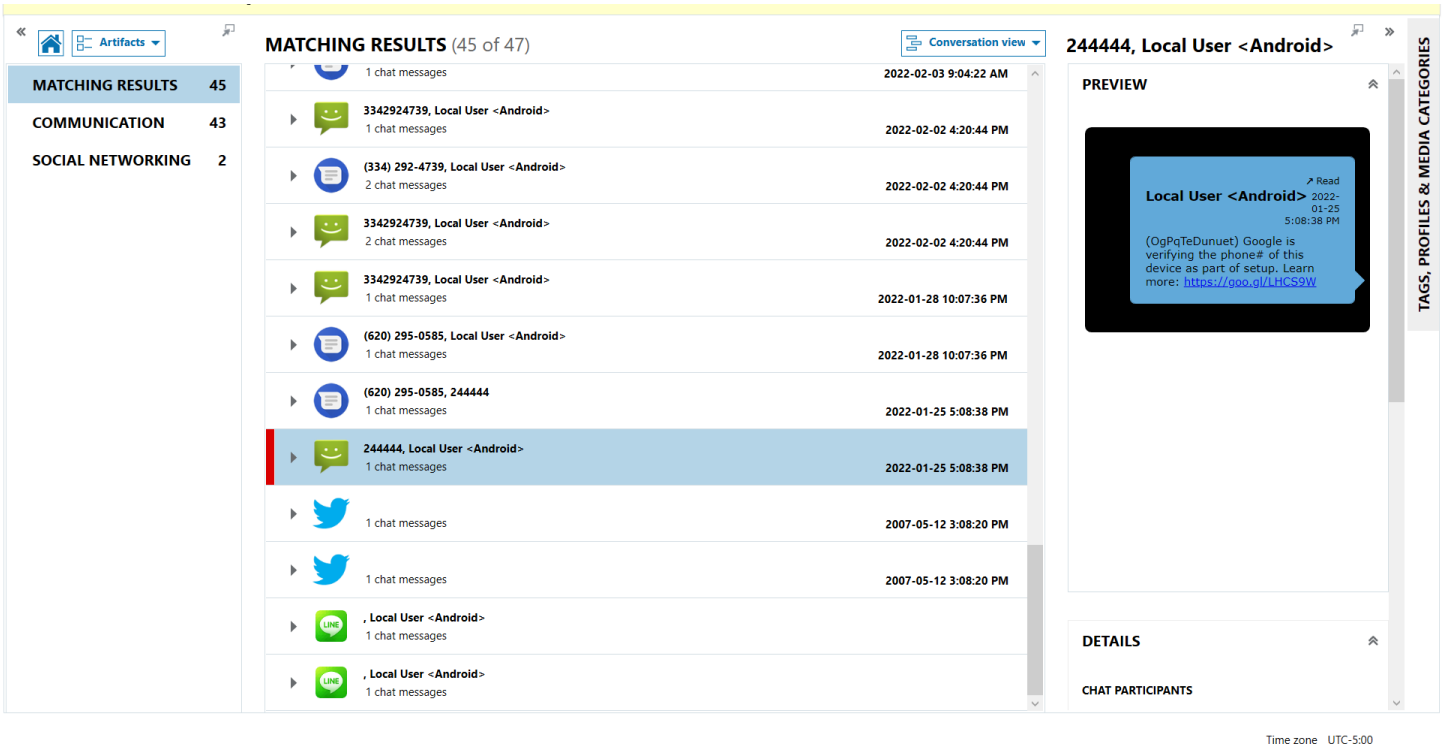


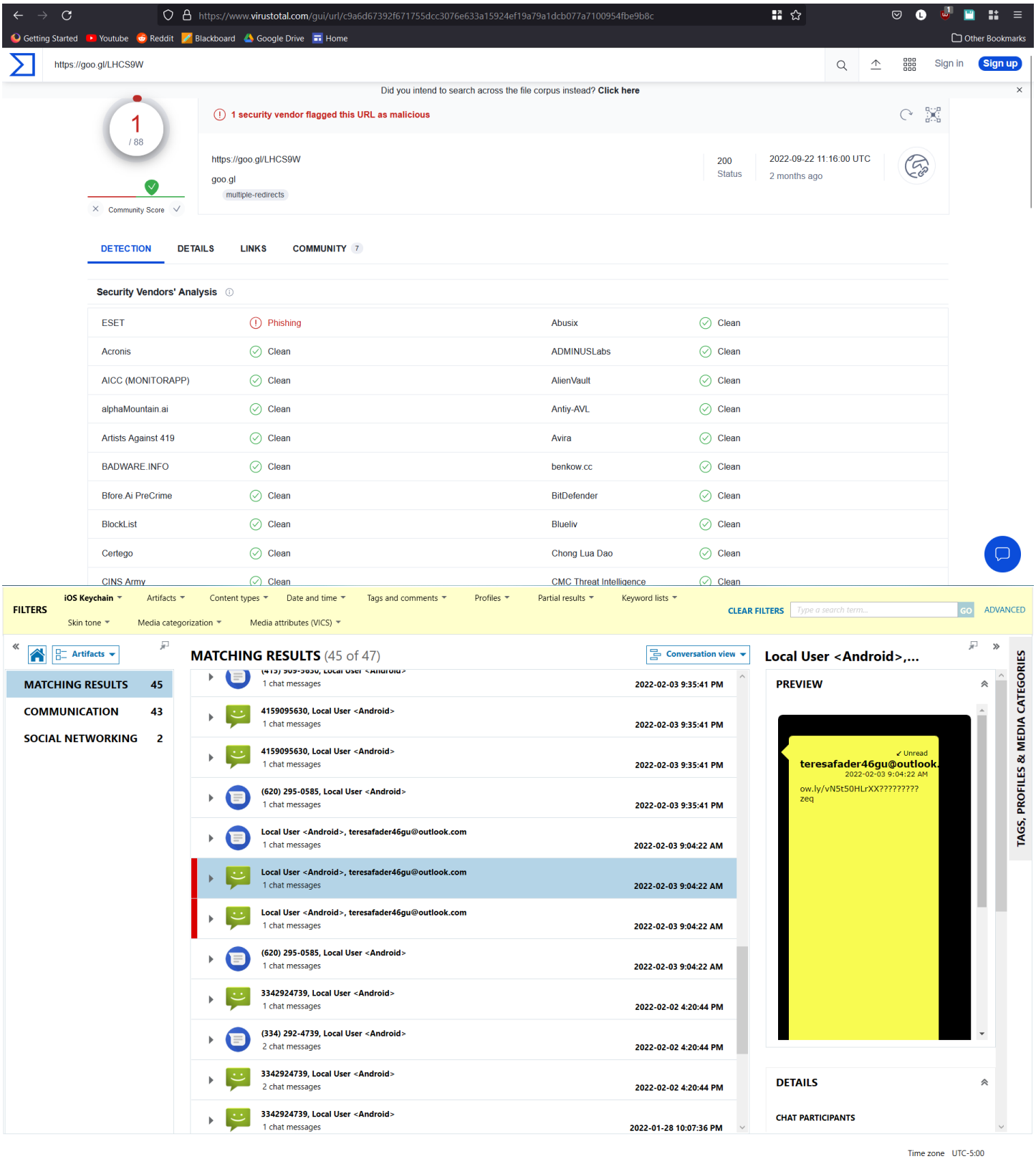
I also noticed that he connected to Chaplain College's wifi which is in Burlington. This is one of the hotspots of the previous iPhone.

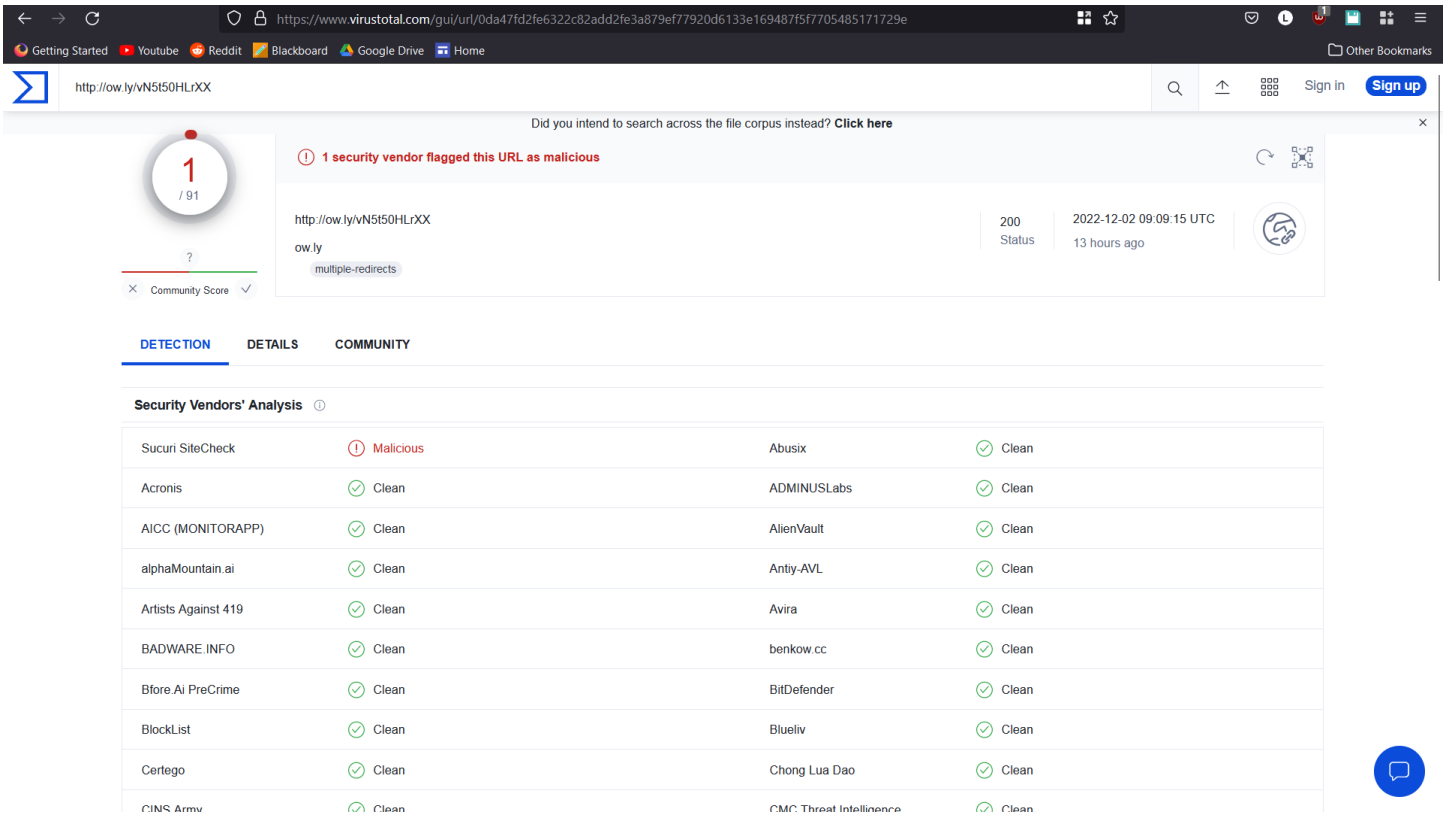


Conversations and text messages

In the conversation view, we can see conversations from different applications on the phone. Most of the texts are related to verification code or marketing messages. However, there are a number of phishing links in the texts.

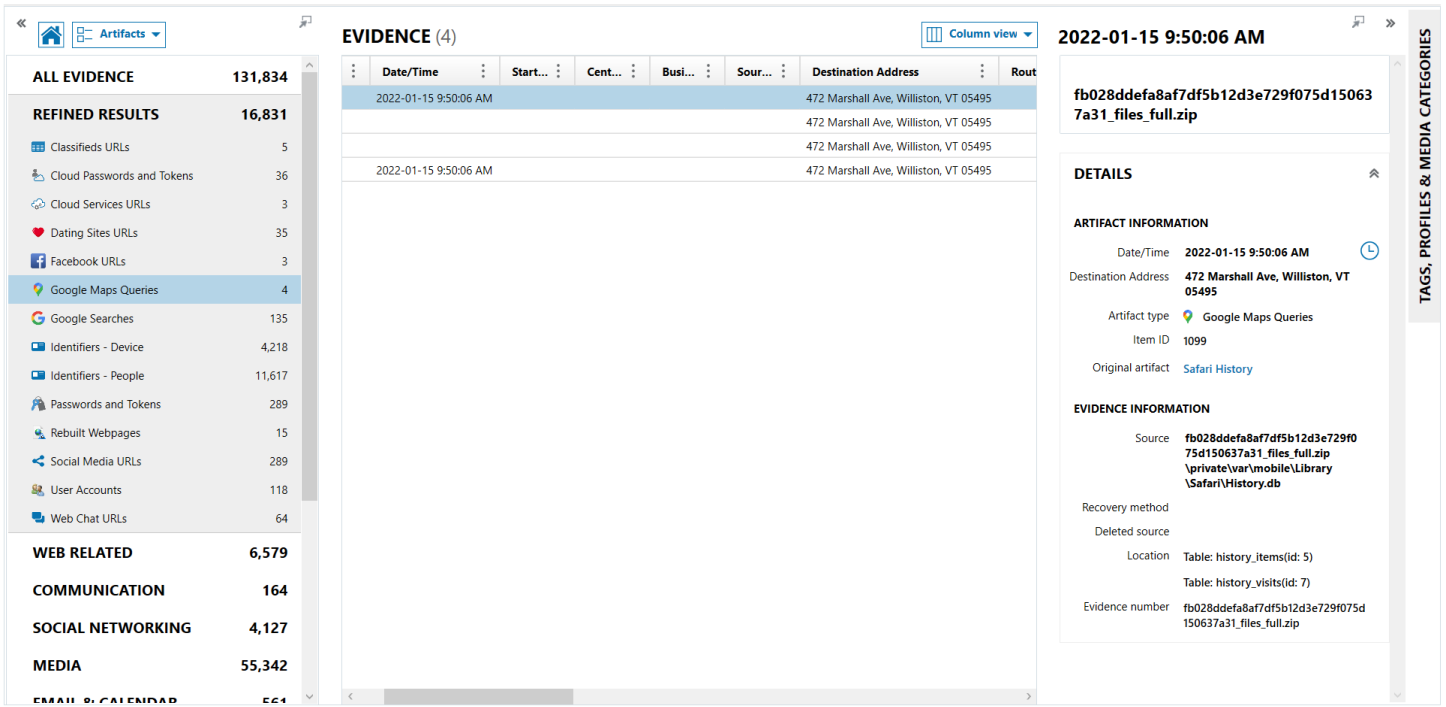


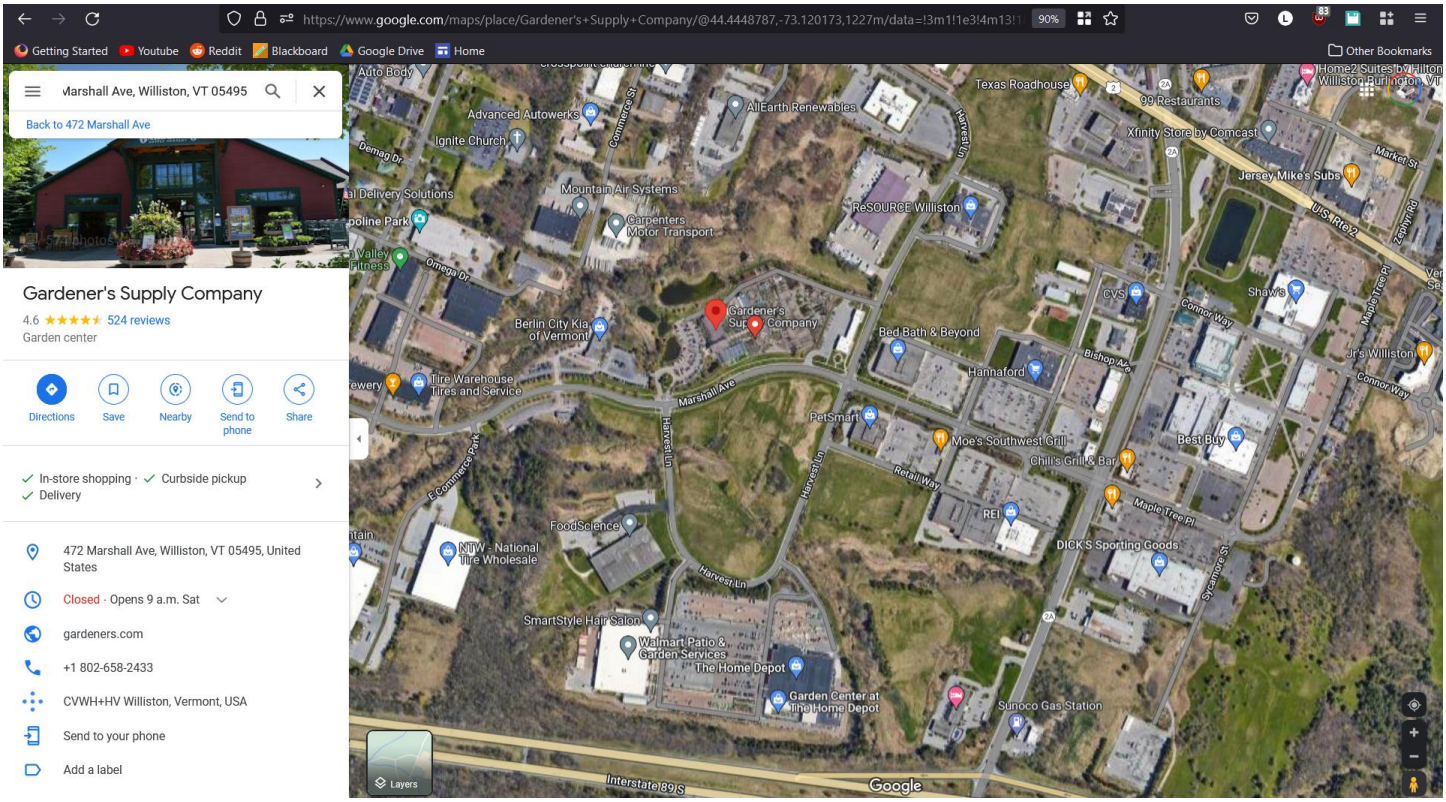

https://www.virustotal.com/gui/url/c9a6d67392f671755dcc3076e633a15924ef19a79a1dcb077a7100954fbe9b8c
Getting Started
Youtube
Reddit
Blackboard
Google Drive
Home
Other Bookmarks
https://goo.gl/LHCS9W
Sign in
Sign up
Did you intend to search across the file corpus instead? Click here
1
/ 88
Community Score
1 security vendor flagged this URL as malicious
https://goo.gl/LHCS9W
goo.gl
multiple-redirects
200
Status
2022-09-22 11:16:00 UTC
2 months ago
DETECTION
DETAILS
LINKS
COMMUNITY 7
Security Vendors' Analysis
ESET Phishing
Abusix Clean
Acronis Clean
ADMINUSLabs Clean
AICC (MONITORAPP) Clean
AlienVault Clean
alphaMountain.ai Clean
Antiy-AVL Clean
Artists Against 419 Clean
Avira Clean
BADWARE.INFO Clean
benkow.cc Clean
Bfore.Ai PreCrime Clean
BitDefender Clean
BlockList Clean
Blueliv Clean
Certego Clean
Chong Lua Dao Clean
CINS Army Clean
CMC Threat Intelligence Clean
FILTERS
iOS Keychain
Artifacts
Content types
Date and time
Tags and comments
Profiles
Partial results
Keyword lists
Skin tone
Media categorization
Media attributes (VICS)
CLEAR FILTERS
Type a search term...
GO
ADVANCED
Artifacts
MATCHING RESULTS 45
COMMUNICATION 43
SOCIAL NETWORKING 2
MATCHING RESULTS (45 of 47)
Conversation view
1 chat messages 2022-02-03 9:35:41 PM
4159095630, Local User <Android>
1 chat messages 2022-02-03 9:35:41 PM
4159095630, Local User <Android>
1 chat messages 2022-02-03 9:35:41 PM
(620) 295-0585, Local User <Android>
1 chat messages 2022-02-03 9:35:41 PM
Local User <Android>, teresafader46gu@outlook.com
1 chat messages 2022-02-03 9:04:22 AM
Local User <Android>, teresafader46gu@outlook.com
1 chat messages 2022-02-03 9:04:22 AM
Local User <Android>, teresafader46gu@outlook.com
1 chat messages 2022-02-03 9:04:22 AM
(620) 295-0585, Local User <Android>
1 chat messages 2022-02-03 9:04:22 AM
3342924739, Local User <Android>
1 chat messages 2022-02-02 4:20:44 PM
(334) 292-4739, Local User <Android>
2 chat messages 2022-02-02 4:20:44 PM
3342924739, Local User <Android>
2 chat messages 2022-02-02 4:20:44 PM
3342924739, Local User <Android>
1 chat messages 2022-01-28 10:07:36 PM
Local User <Android>,...
PREVIEW
Unread
teresafader46gu@outlook.
2022-02-03 9:04:22 AM
ow.ly/vN5t50HLrXX????????
zeq
DETAILS
CHAT PARTICIPANTS
TAGS, PROFILES & MEDIA CATEGORIES
Time zone UTC-5:00



Locations

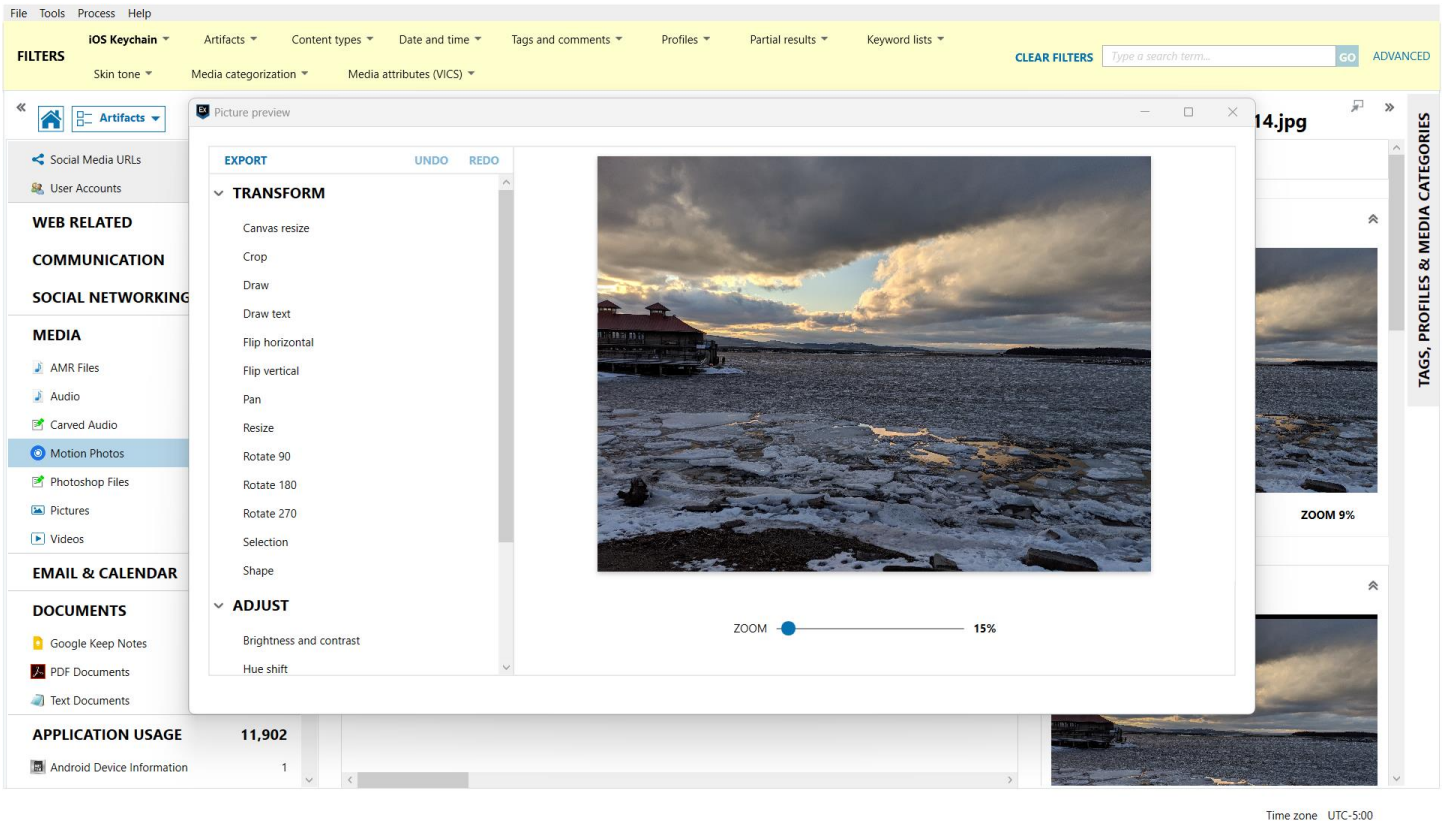
This pixel phone seems to have less location history compared to the previous iPhone we investigated. However, tracks of the phone's whereabouts are still present. First, we can see a Google Map search on the device. The address turns out to be Gardener's Supply in Burlington which is the same store in the iPhone's location history.



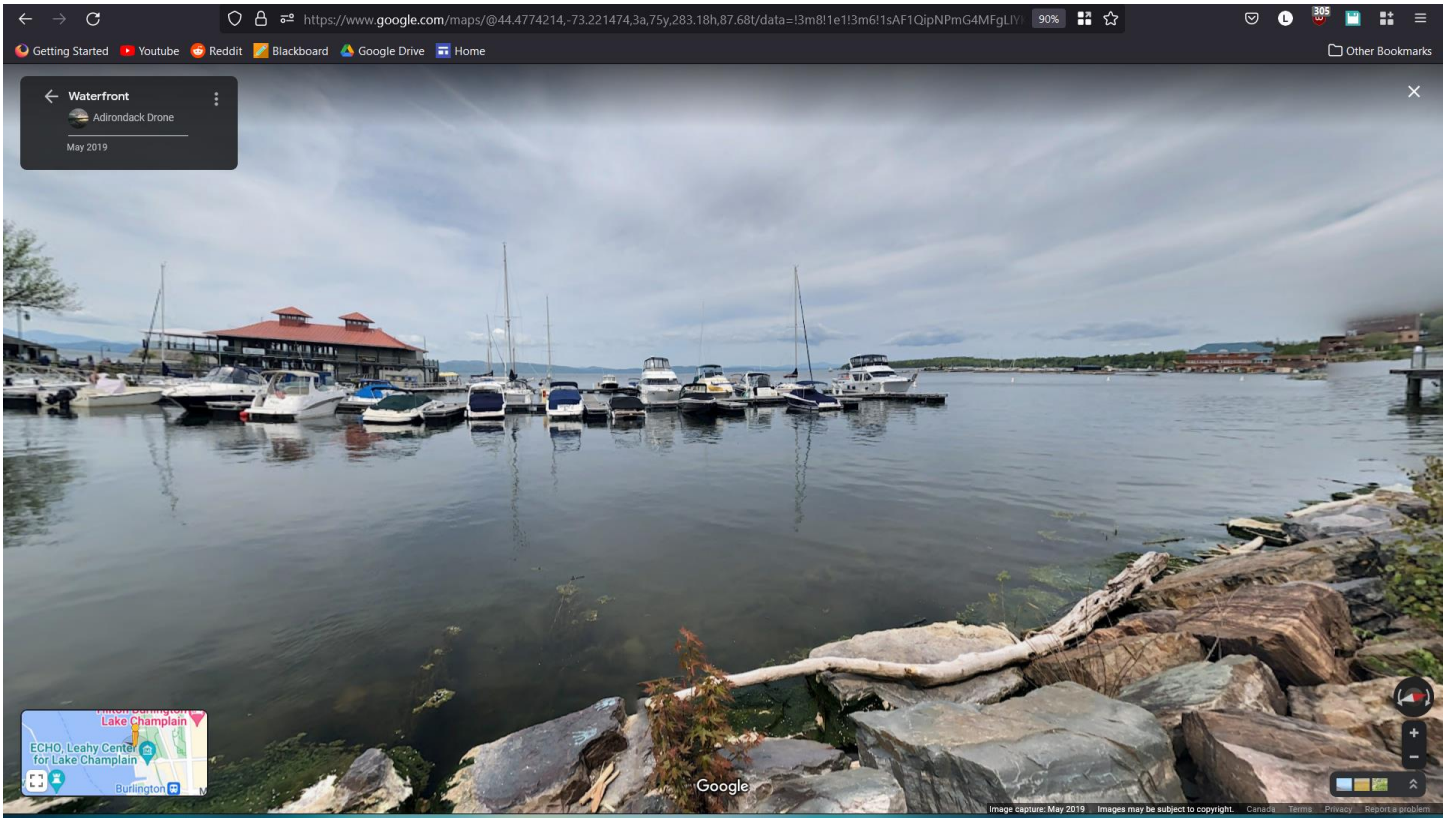


Media and photos

One of the camera pictures we can find on the phone shows a temple like structure on a body of water.



Based on his location history in Burlington, I found the location to be by the port of Burlington.



From the angle of the photo, it was likely that he was on a boat at the time of the picture taken.