

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

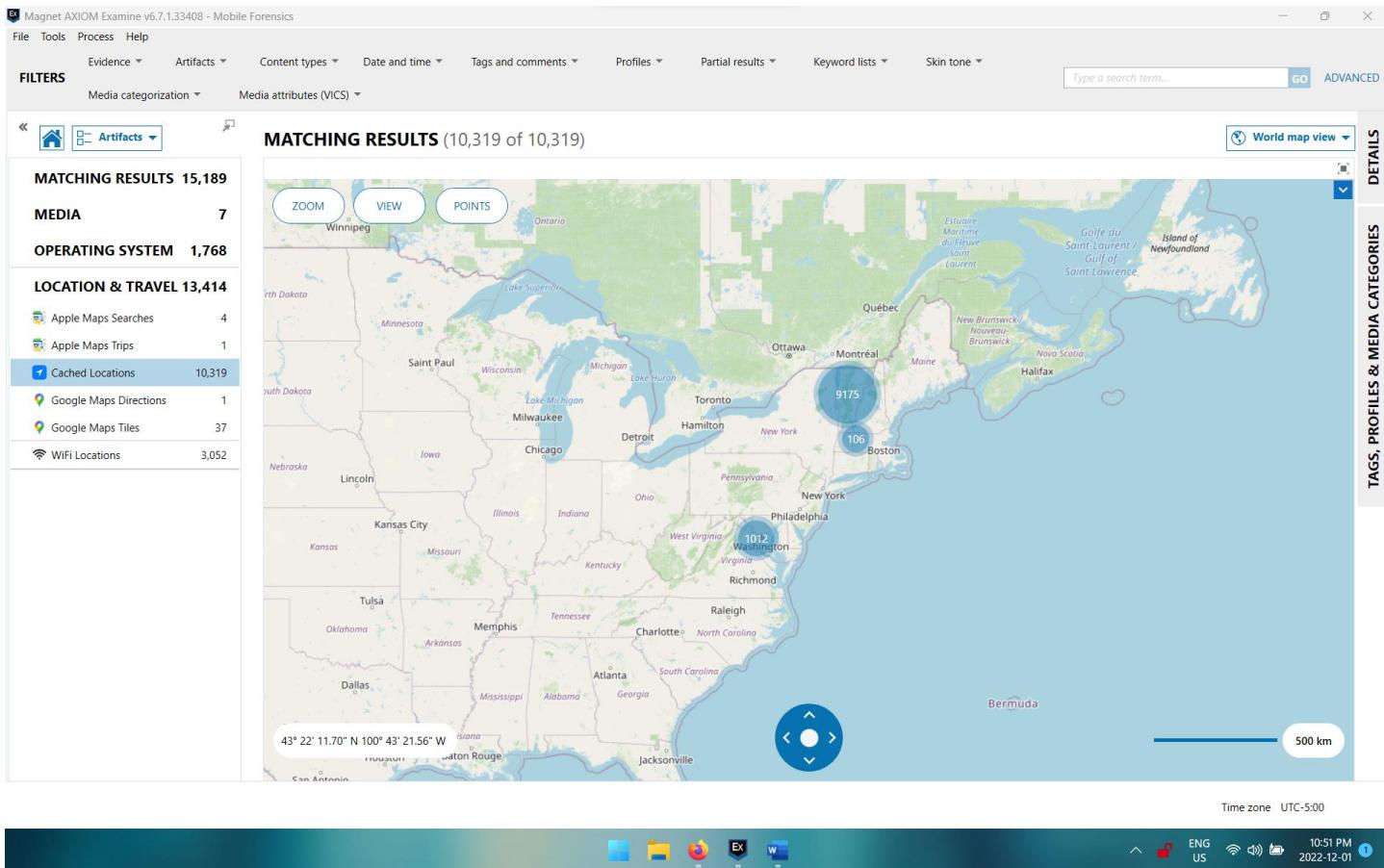
ARTIFACT INFORMATION

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

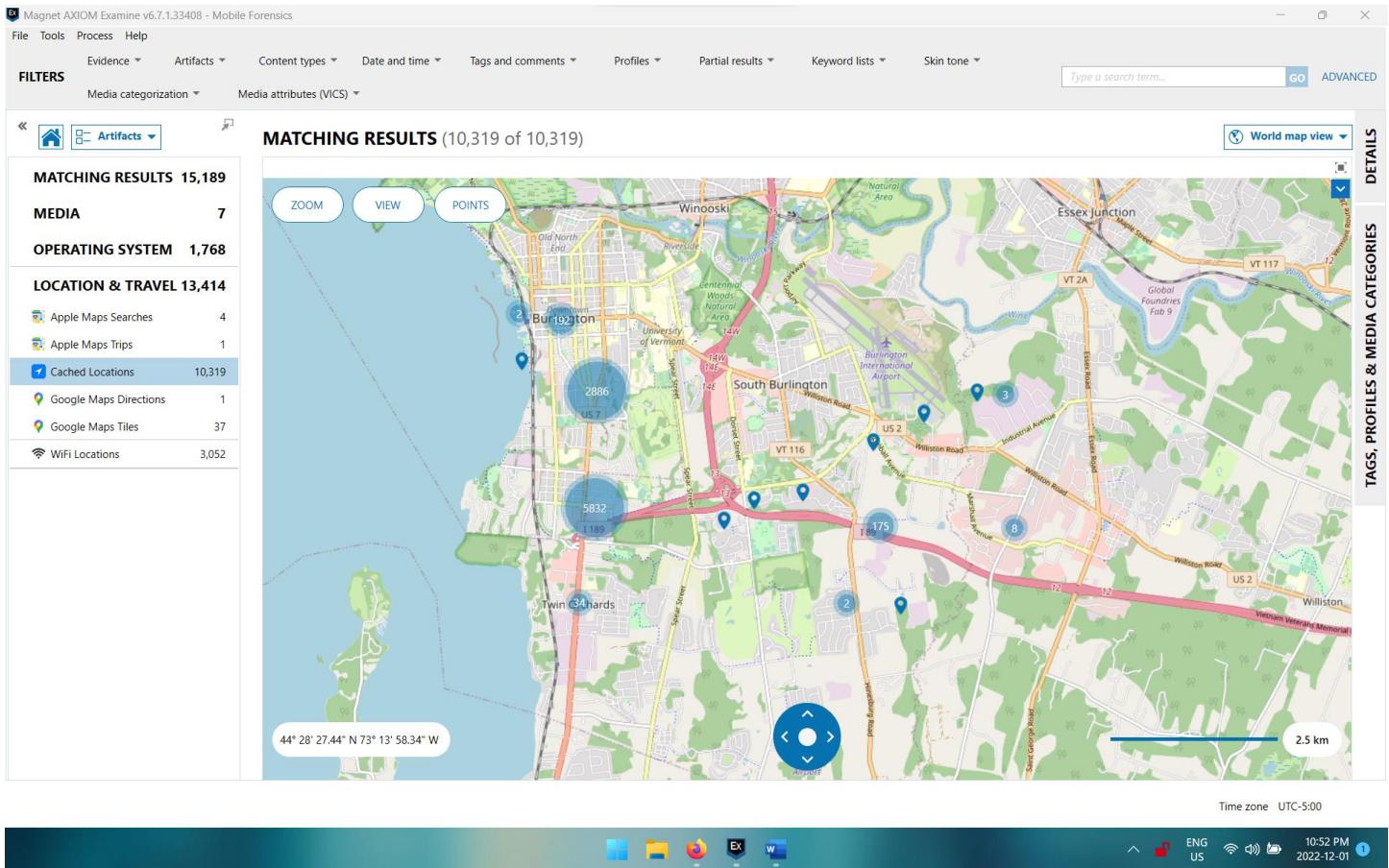
To start off the analysis, this phone is an iPhone 8 running iOS 15.0.2.

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.

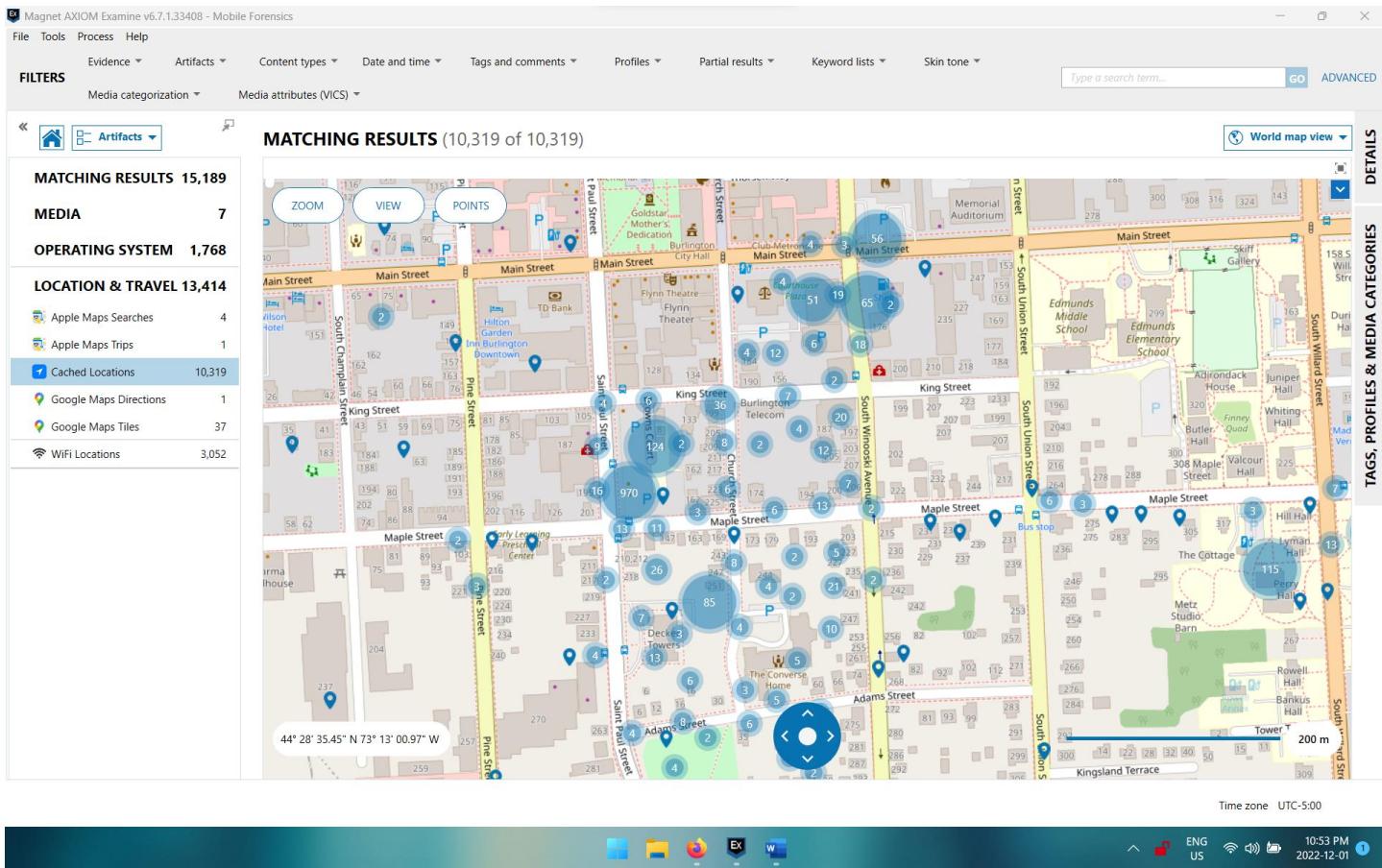


In Burlington, there are also 3 main clusters. Two big clusters appear in Downtown Burlington while a smaller one is in residential areas.

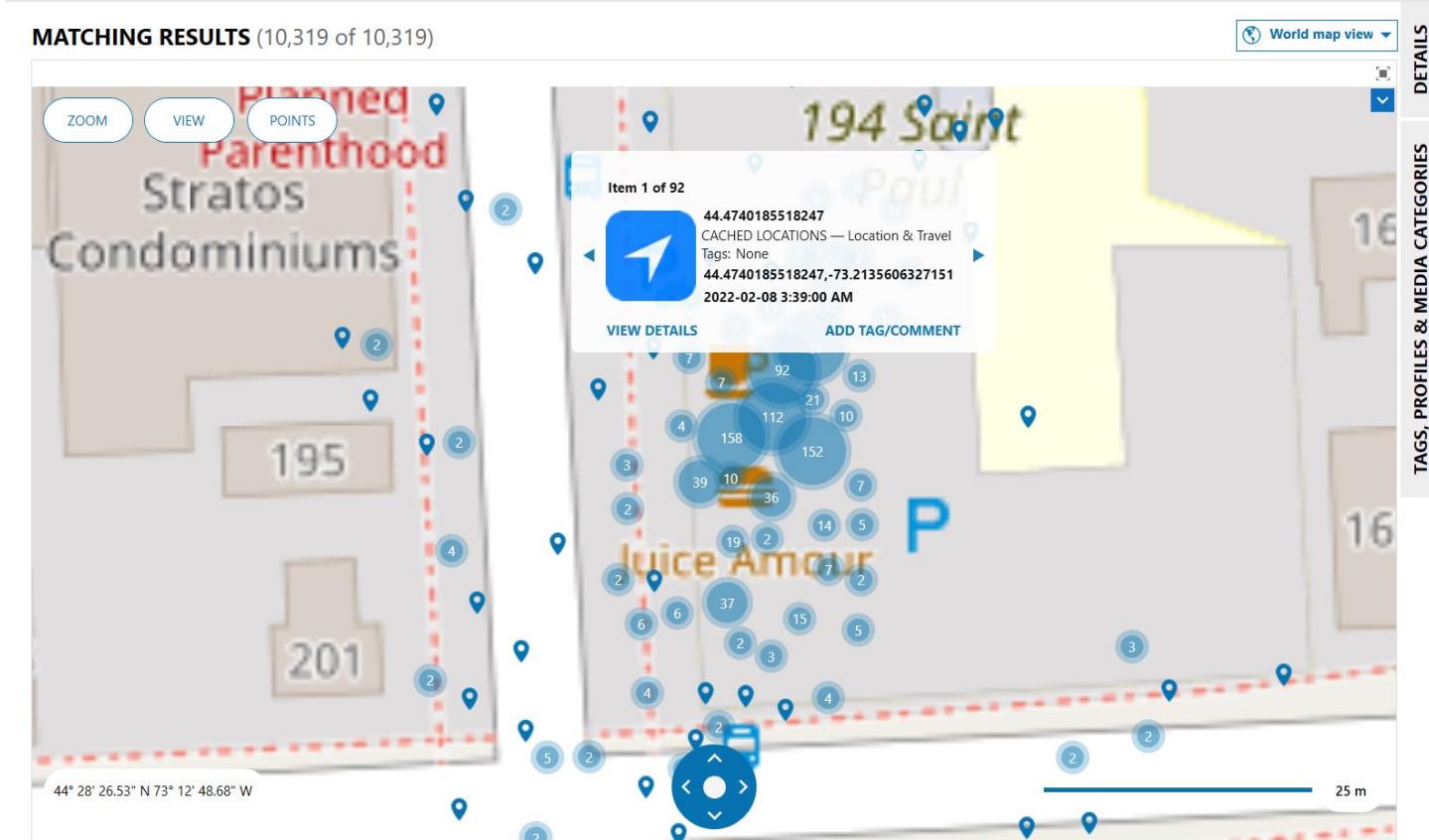
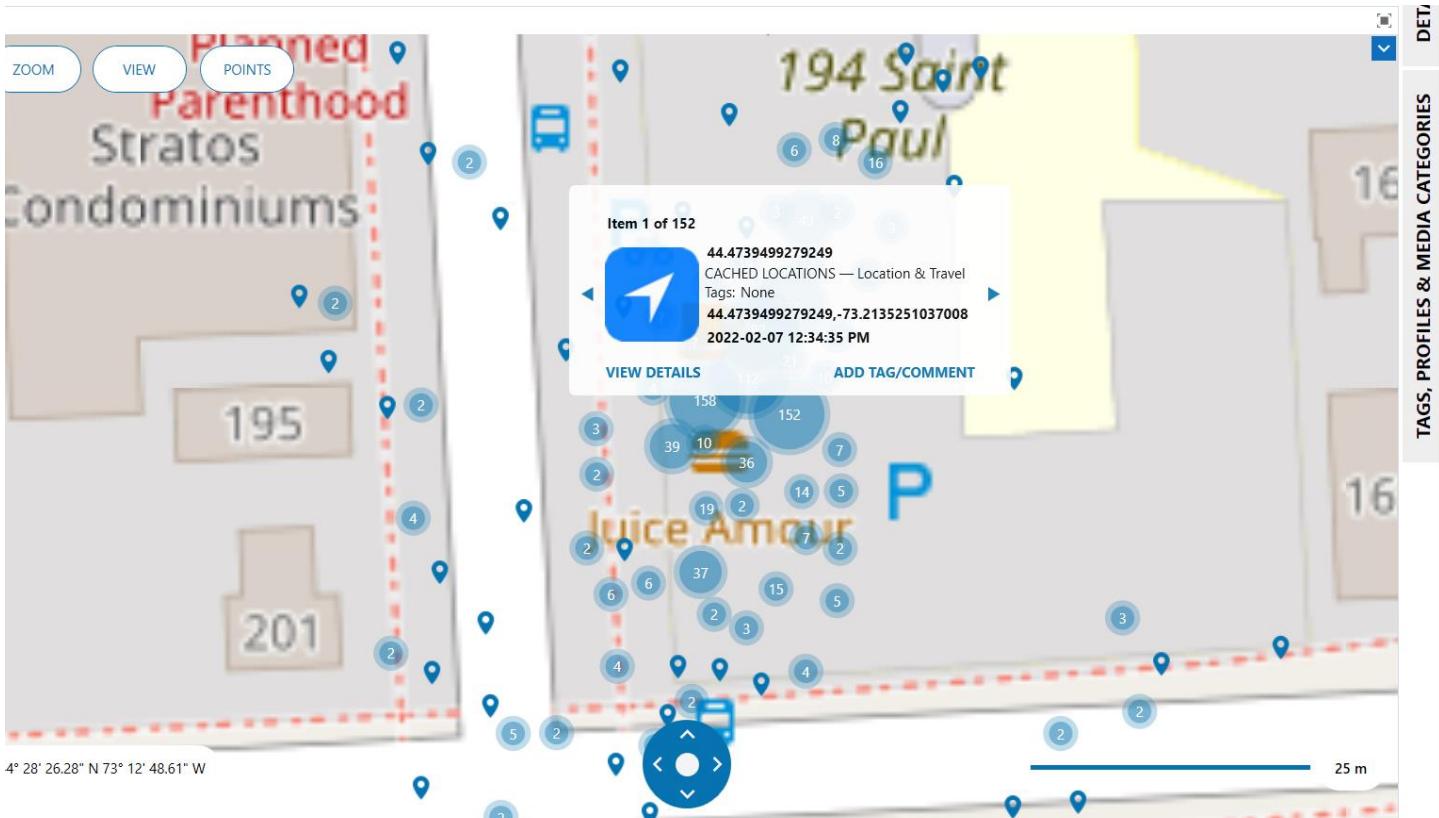


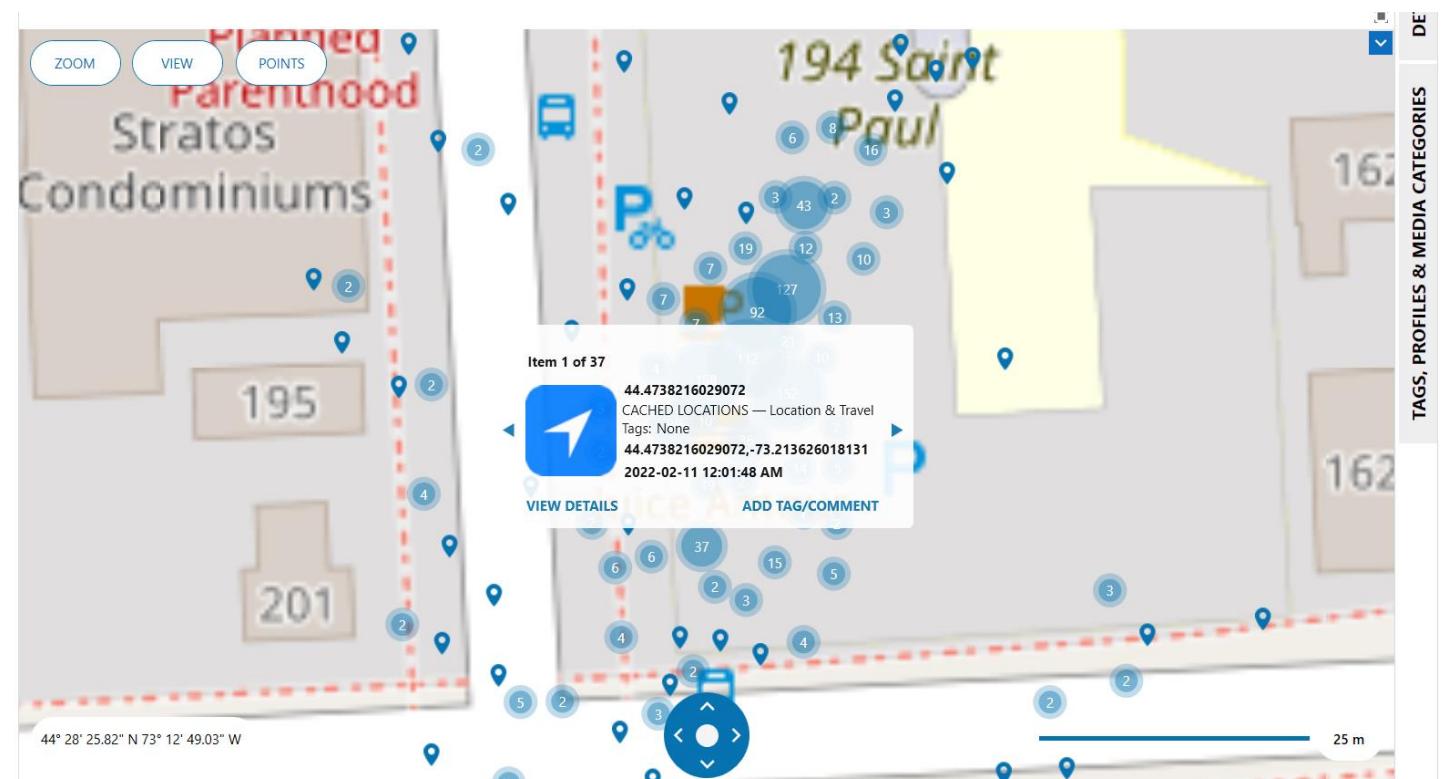
Downtown hotspot 1

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.





Downtown burlington vermont

Restaurants Hotels Things to do Museums Transit Pharmacies ATMs Inkwell Emporium Tattoo shop

Burlington Vermont USA

Mostly cloudy - 0°C 12:03 AM

Directions Save Nearby Send to phone Share

Quick facts

Burlington is a city in northwestern Vermont, on the eastern shore of Lake Champlain, south of the Canadian border. Downtown, shops and restaurants line pedestrianized Church Street Marketplace. North of downtown, the Ethan Allen Homestead Museum is a former home of the Revolutionary War hero. The vast Shelburne Museum, south of the city, houses American folk and decorative art in a collection of historic buildings.

Iconic Burlington

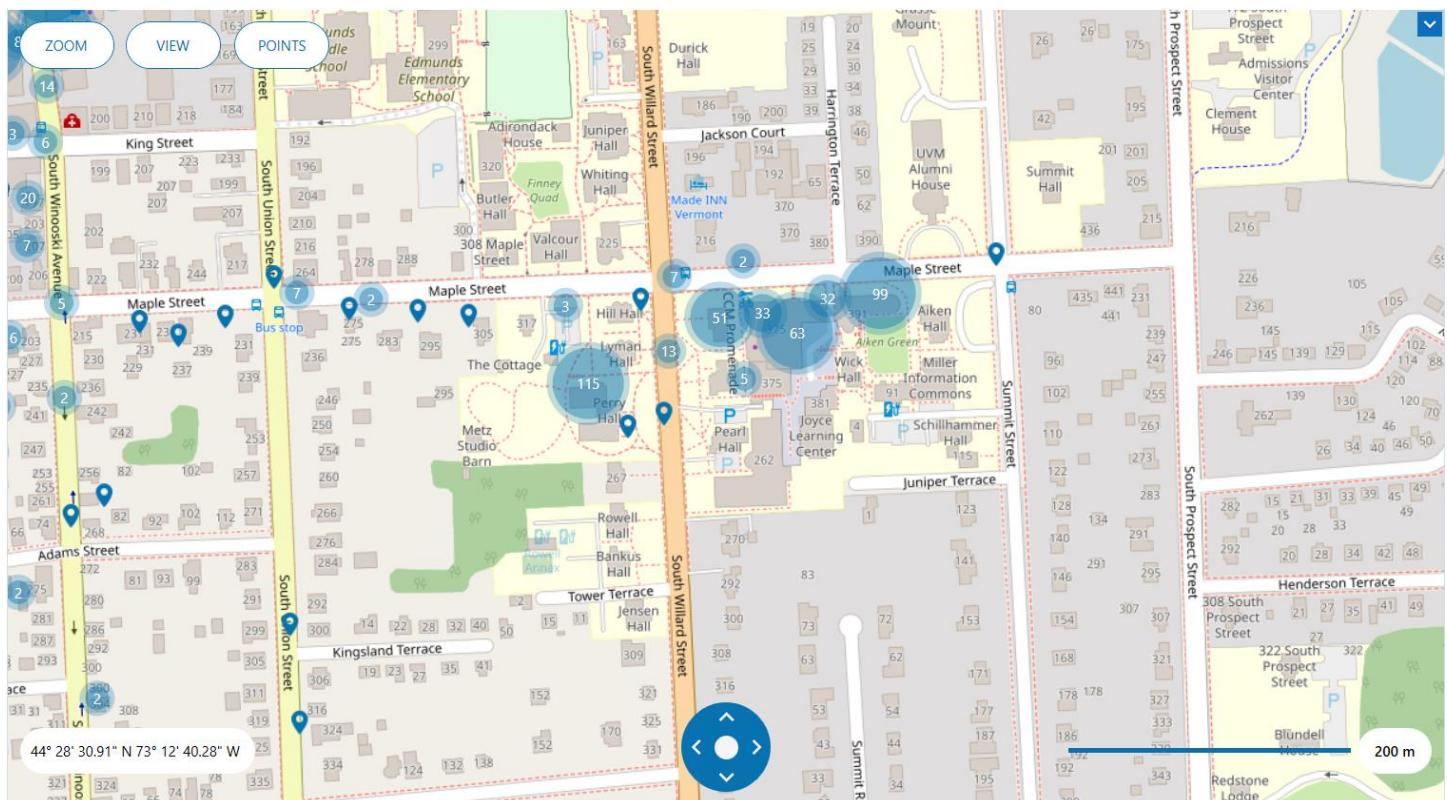
VTEdit: Vermont Center for Emergency Management

Layers

Brickworks Studios Vermont Art Supply Adams St Google

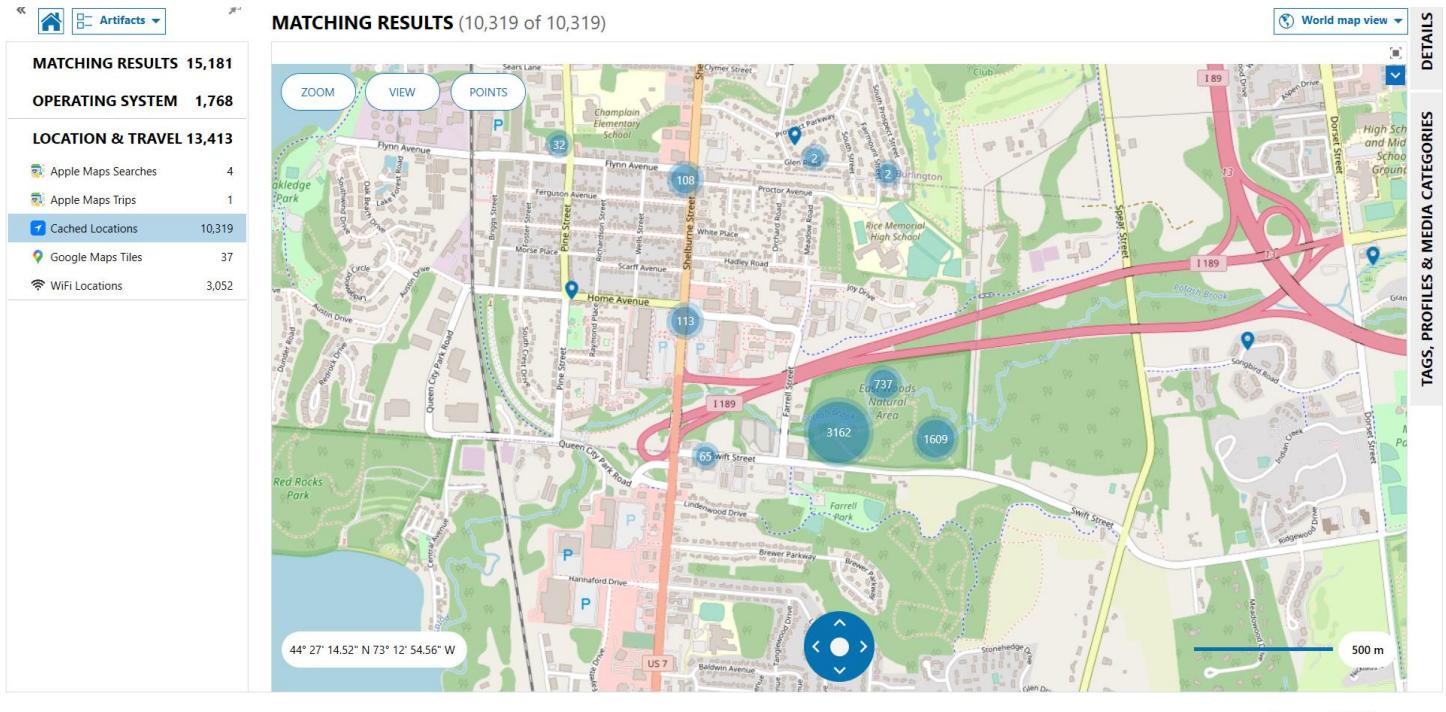
Imagery ©2022 Mayar Technologies, USDA/EPAC/GEO. Map data ©2022 Google

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.



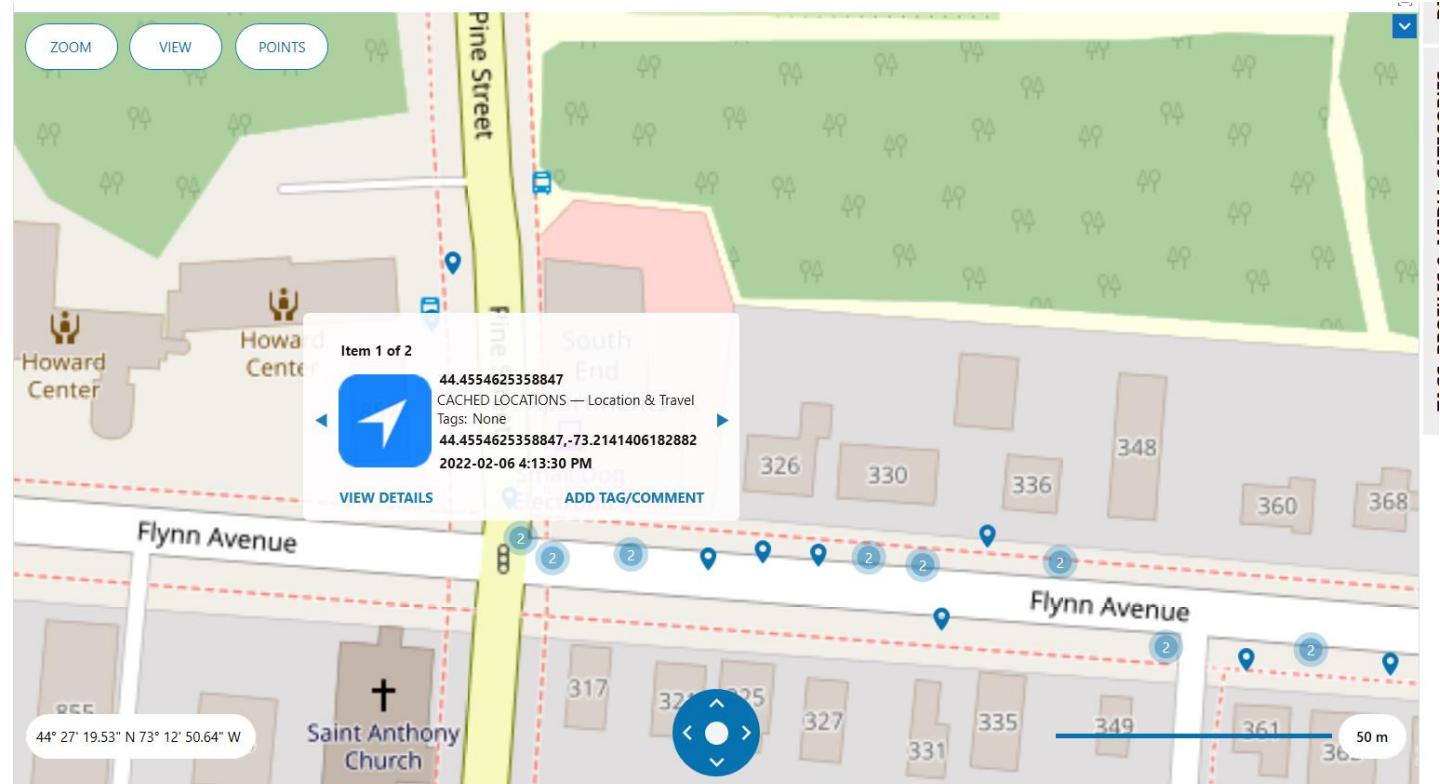
Downtown hotspot 2

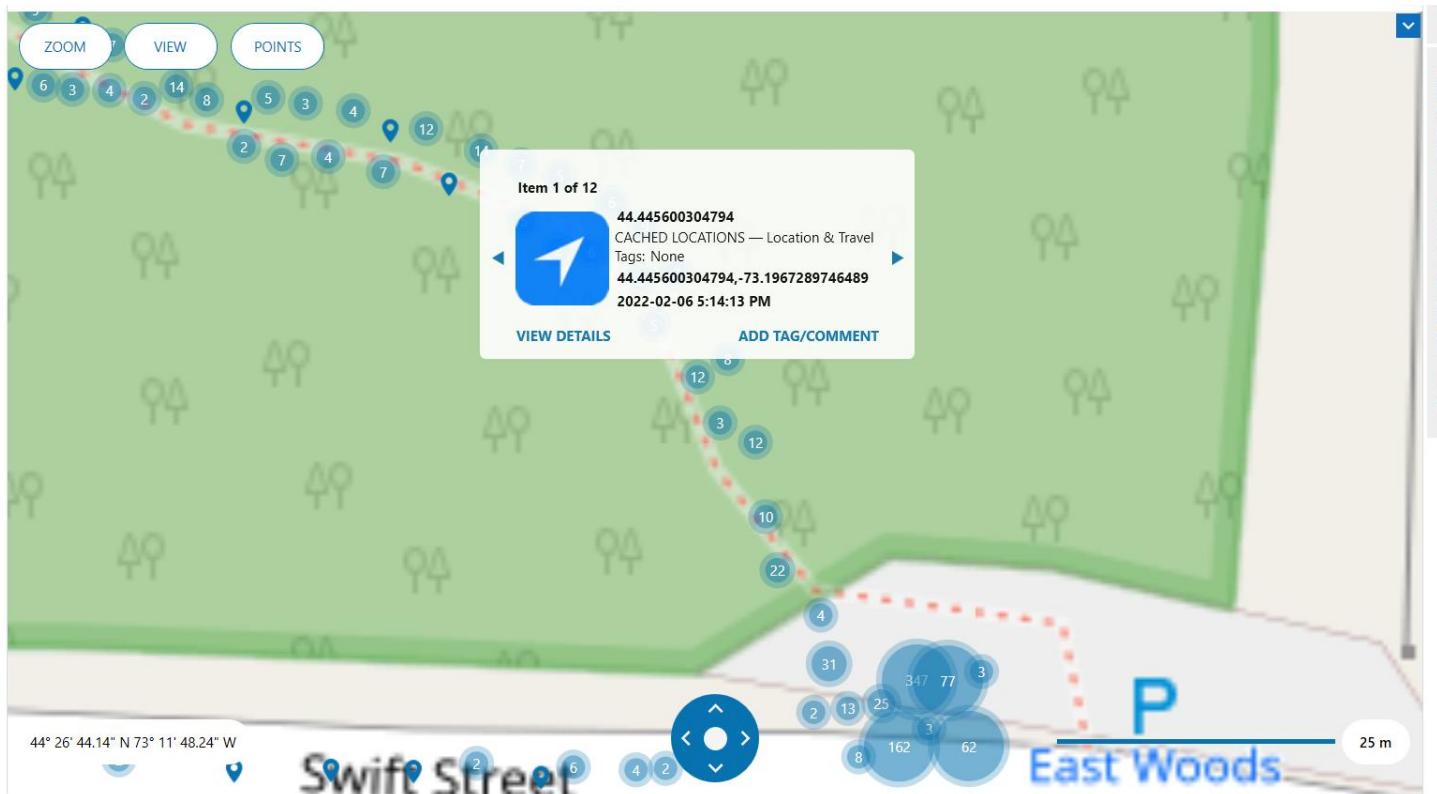
The second hotspot in Downtown would be near the East Woods Natural Area. This spot is a fairly big natural park with lush greenery by the interstate highway.

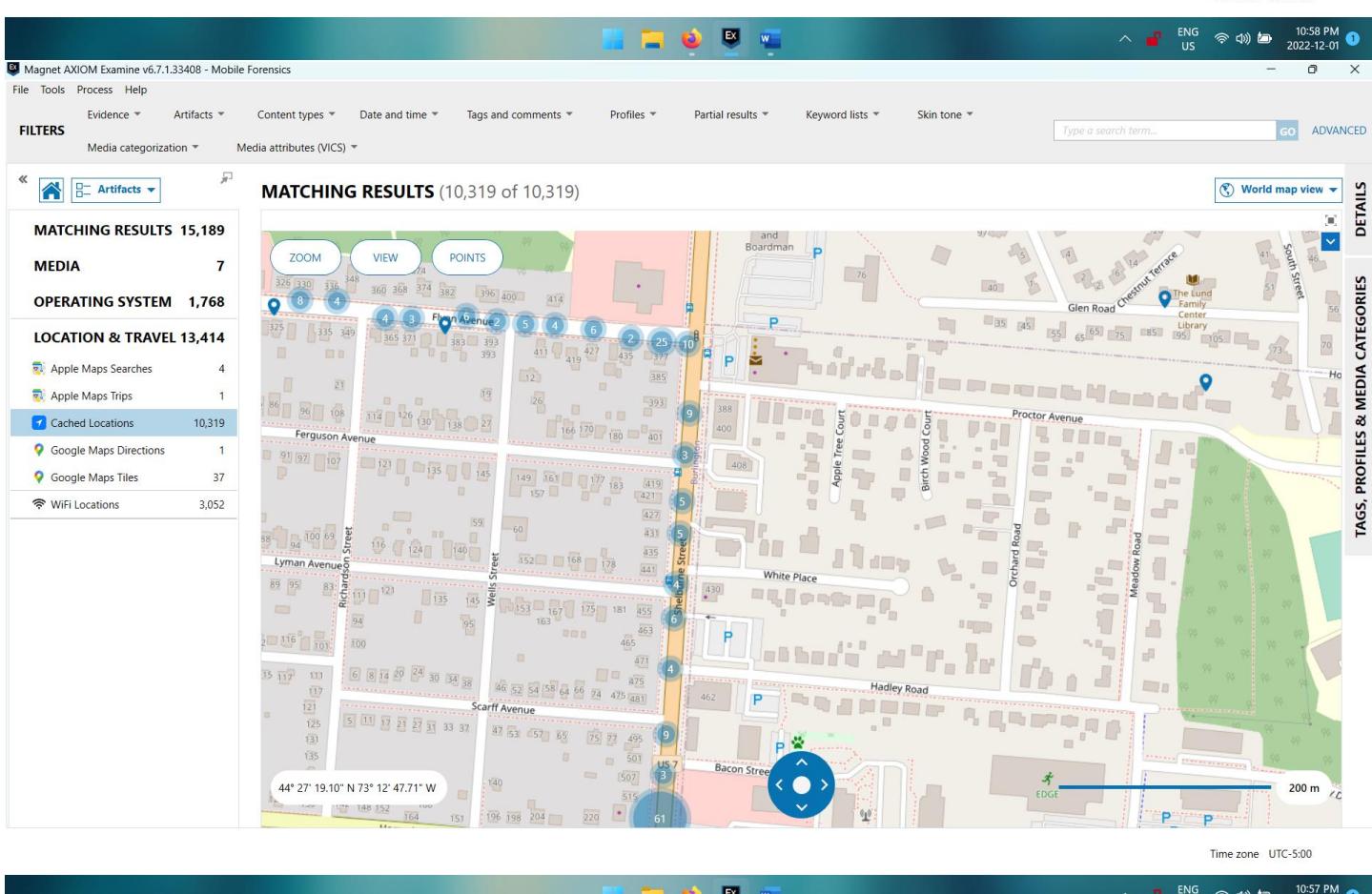
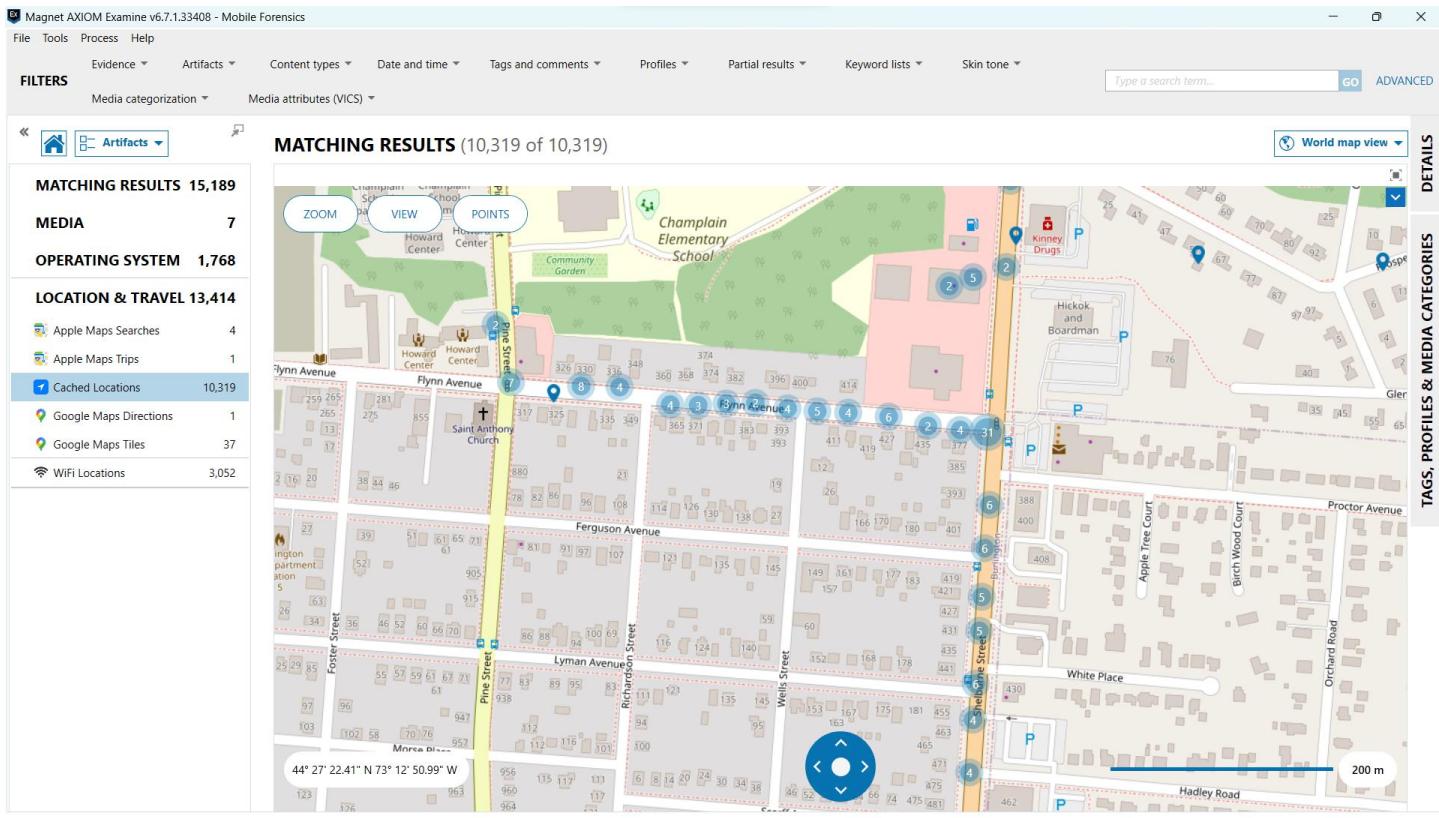


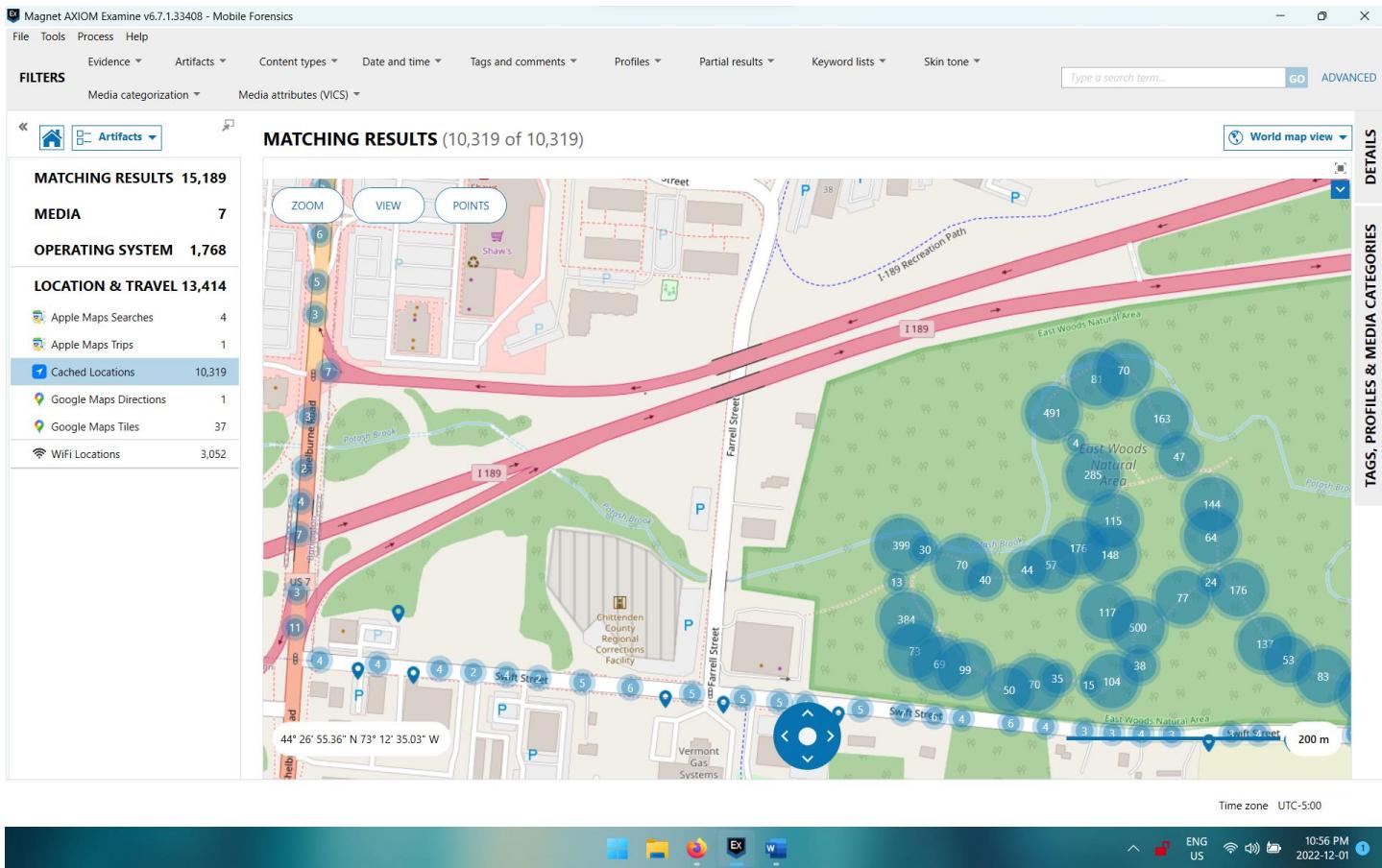
The person holding this phone seems to be following a very neat line along the trail present in the East Woods Loop area. There was a lack of off-trail activities.

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.









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.

The screenshot shows a mobile application interface for a trail review. At the top, there are three circular icons: a white 'X' on the left, an upward arrow in the middle, and a bookmark icon on the right. Below these is a camera icon with the text "Add photos of your hike". A user profile picture placeholder is shown, followed by the date "February 6, 2022 • Hiking" and a three-dot menu icon. The main title of the review is "East Woods Natural Area Loop" in large, bold, white font. Below the title is a five-star rating icon. The review text reads: "Relaxing walk. The trail was well marked and had great views of the sunset sky." A green button at the bottom says "Edit your trail review" and "Nice work. Share with your friends!". At the very bottom, there are three small, faint text links: "Length", "Elevation Gain", and "Moving Time".

February 6, 2022 • Hiking

...

East Woods Natural Area Loop

★★★★★

Relaxing walk. The trail was well marked and had great views of the sunset sky.

Edit your trail review

Nice work. Share with your friends!

Length Elevation Gain Moving Time

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.

MATCHING RESULTS (13 of 13)

[Filter by](#) [Sort by](#) [Small](#) [Thumbnail view](#)

9

fb028ddefa8af7dfb12d3e729f075d150637a3
1 files full.zip

PREVIEW



[EXPAND PREVIEW](#)

ZOOM 12%

Time zone UTC-5:00

TAGS, PROFILES & MEDIA CATEGORIES



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.

Getting Started YouTube Reddit Blackboard Google Drive Home

east woods natural area

centennial woods burlington vt uvm hiking trail pease mountain vermont burlington vermont of vermont south burlington hiking trails unive

AllTrails East Woods Natural Area Loop | Map ...

AllTrails Best Trails in East Woods Natural Area ...

Bring Fido East Woods Natural Area

AllTrails East Woods Natural Area Loop | Map ...

AllTrails Best Trails in East Woods N...

Worldwide Elevation Map Finder Natural Area, Burlington, VT, USA ...

The University of Ver... UVM Natural Areas | E...

AllTrails East Woods Natural Area Loop | Map ...

Worldwide Elevation Map Finder Natural Area, Burlington, VT, USA ...

Facebook East Woods Natural Area - South ...

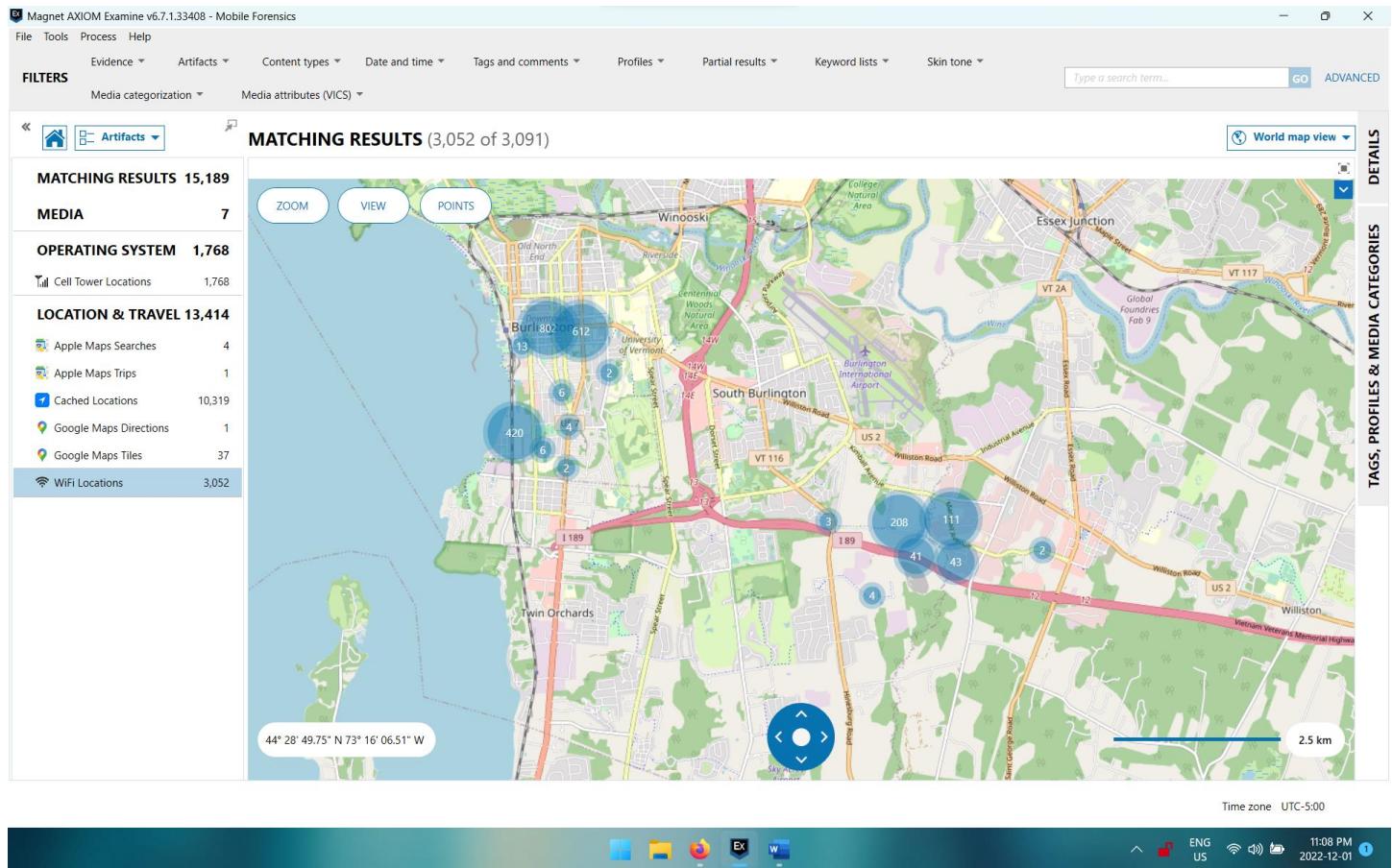
South Burlington, Vermont Photos and commentary.: South B...

Images may be subject to copyright. [Learn More](#)

Related content

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.

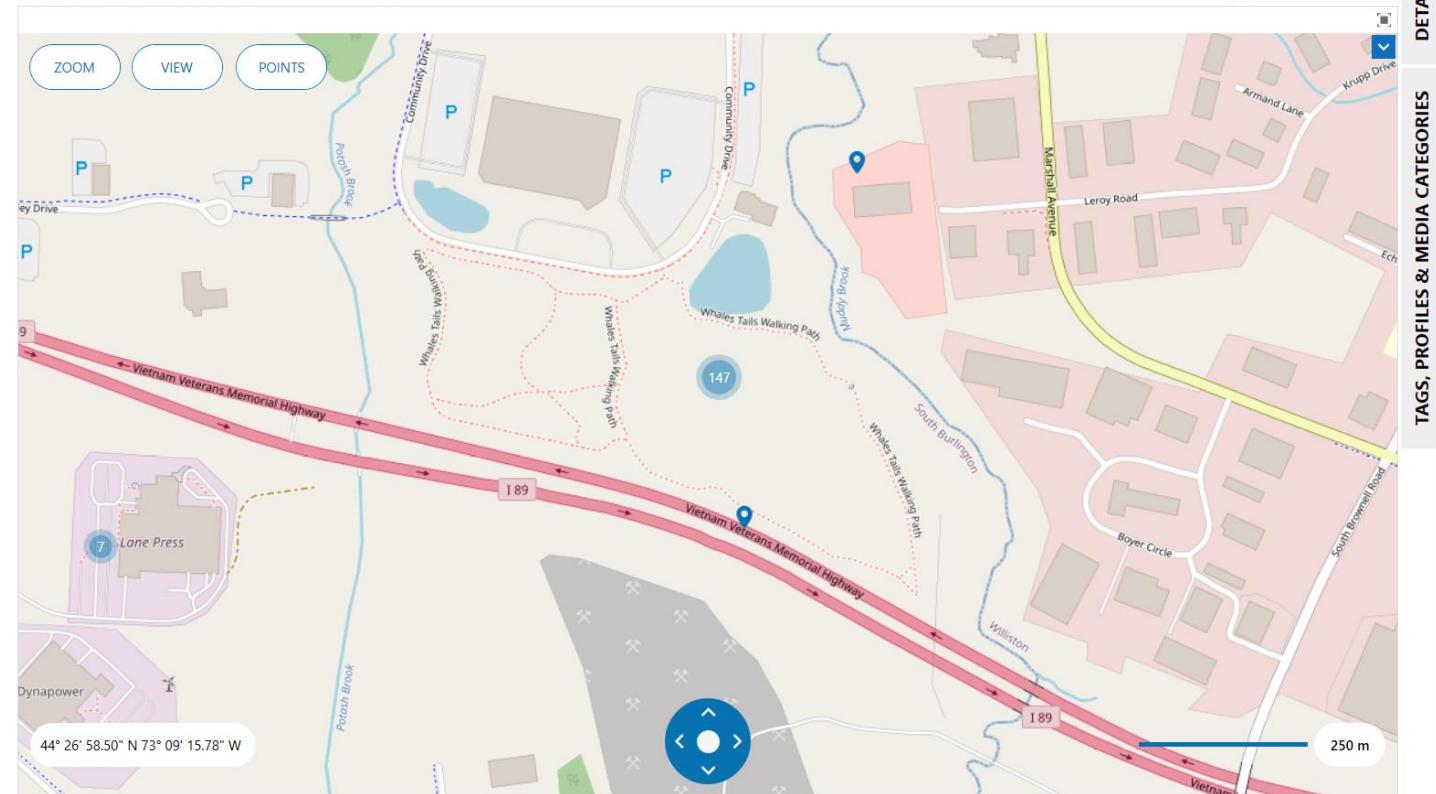


MATCHING RESULTS (10,319 of 10,319)

[World map view](#)

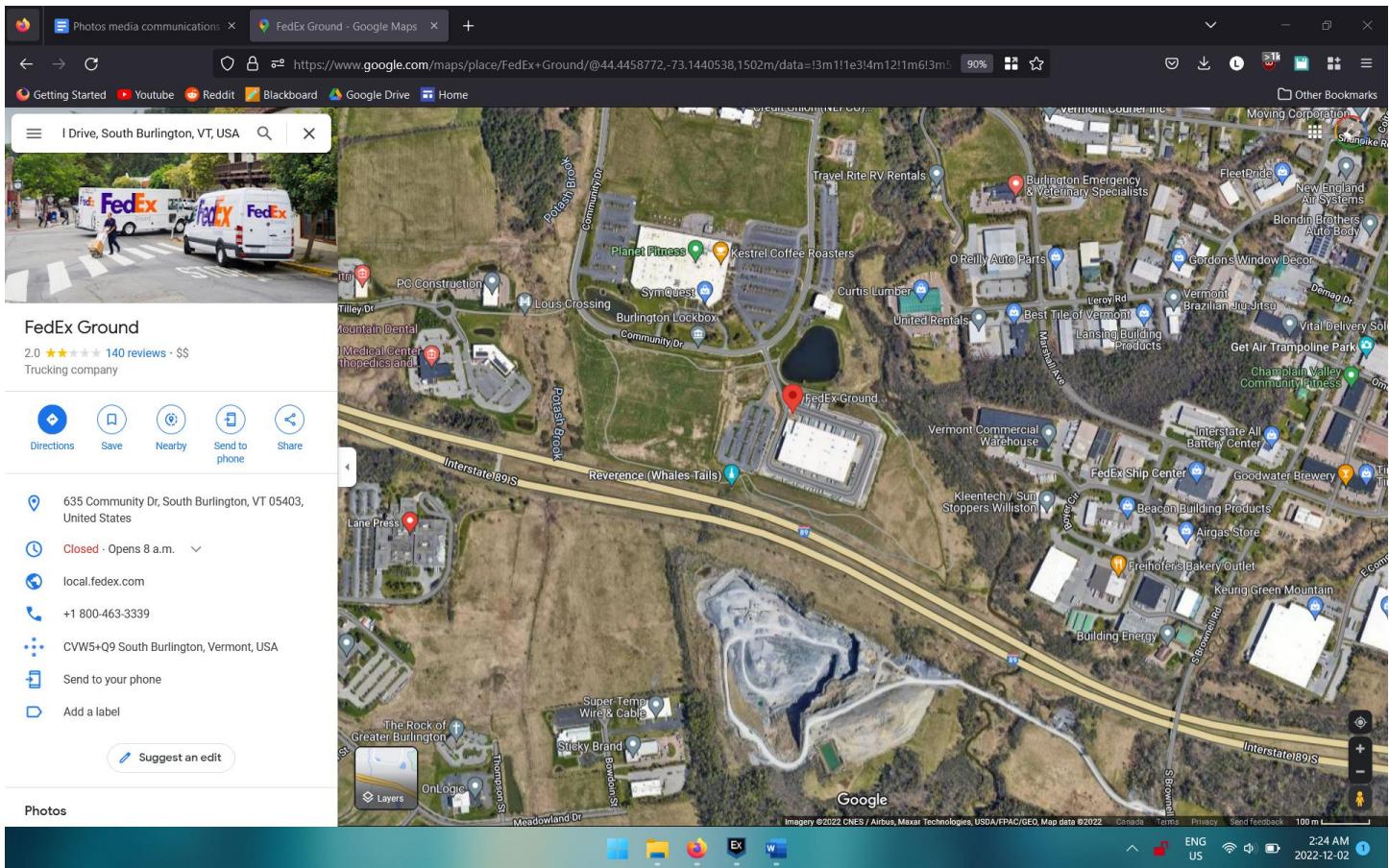
DETAILS

TAGS, PROFILES & MEDIA CATEGORIES

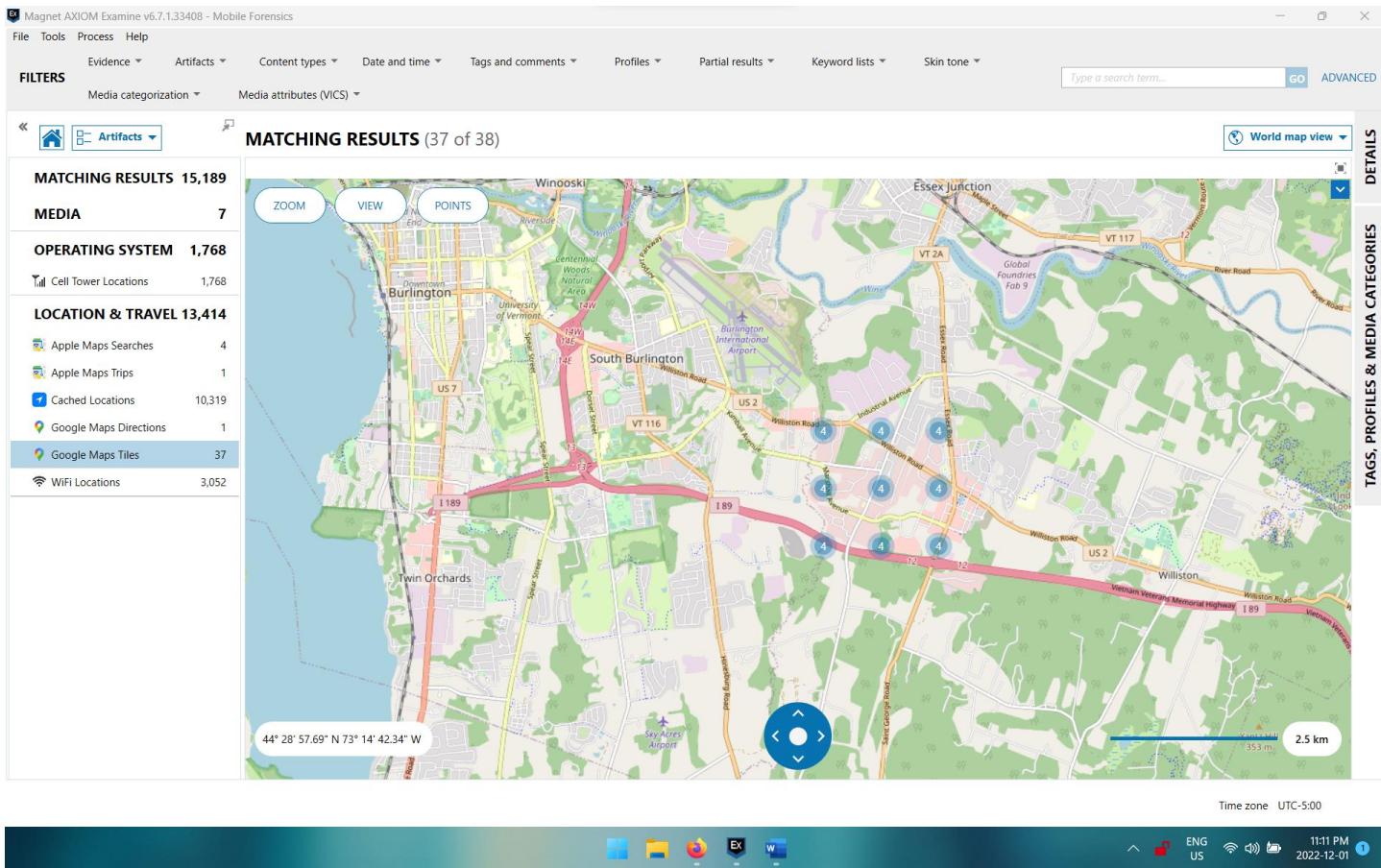


Time zone UTC-5:00

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.

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 Type a search term... GO ADVANCED

Media categorization Media attributes (VICS)

MATCHING RESULTS (4 of 4)

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

Time zone UTC-5:00

ENG US 11:12 PM 2022-12-01

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

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 Type a search term... GO ADVANCED

Media categorization Media attributes (VICS)

MATCHING RESULTS (1 of 1)

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

142 W Twin Oaks Terr, South Burlington, VT 05403, United States

APPLE MAPS TRIPS — Location & Travel

Destination Address: 863 Harvest Ln, Williston, VT 05495, United States

CREATE EXPORT / REPORT OPEN SOURCE FILE WITH...

Created Date/Time 2022-01-15 9:11:35 AM

142 W Twin Oaks Terr, South Burlington, VT 05403, United States

fb028dddefa8af7df5b12d3e729f075d150637a31_files_full.zip

DETAILS

ARTIFACT INFORMATION

- Origin Address 142 W Twin Oaks Terr, South Burlington, VT 05403, United States
- Destination Address 863 Harvest Ln, Williston, VT 05495, United States
- Origin Latitude 44.451934048016
- Origin Longitude -73.1715602987196
- Destination Latitude 44.441633
- Destination Longitude -73.122127
- Created Date/Time 2022-01-15 9:11:35 AM
- Search Term Walmart
- Artifact type Apple Maps Trips
- Item ID 30759

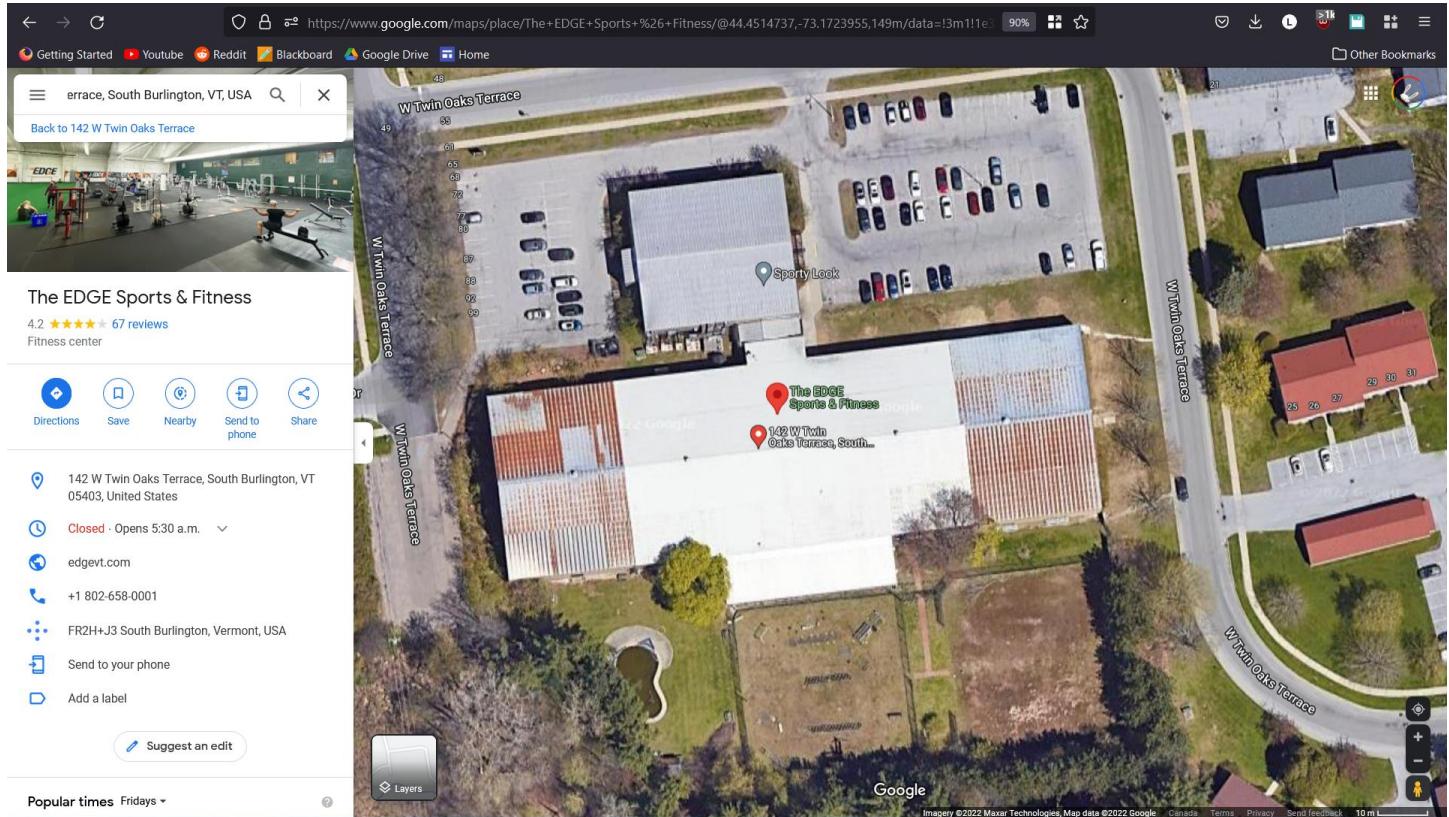
EVIDENCE INFORMATION

- Source fb028dddefa8af7df5b12d3e729f075d150637a31_files_full.zip\private\var\mobile\Containers\Shared\AppGroup-66ABA2B0-DCAF-461B-B8EE-785E6840F9E4\Maps\MapsSync_0.0.1
- Recovery method Parsing
- Deleted source

Time zone UTC-5:00

ENG US 11:13 PM 2022-12-01

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.

Magnet AXIOM Examine v6.7.1.33408 - Mobile Forensics

File Tools Process Help

FILTERS

fb028ddefa8af7df5b1... Artifacts Content types Date and time Tags and comments Profiles Partial results

CLEAR FILTERS Type a search term... GO ADVANCED

Artifacts

MATCHING RESULTS (13 of 13)

	CellID	Loca...	Mob...	Mob...	Timestamp Date...	Latit...	Longi...	Range	Conf...	Artifact type	Source
Identifiers - People	10,388									Photos Media Information	fb028ddefa8af7df5b12d3e729f075d150
Social Media URLs	264									Photos Media Information	fb028ddefa8af7df5b12d3e729f075d150
User Accounts	17										
Web Chat URLs	64										

WEB RELATED 4,927

COMMUNICATION 108

SOCIAL NETWORKING 3,431

MEDIA 13,945

- AMR Files 2
- Audio 223
- Carved Audio 178
- iOS Snapshots 276
- Live Photos 1
- Photos Albums 6
- Photos Media Information 13
- Photoshop Files 59
- Pictures 13,100
- Videos 87

EMAIL & CALENDAR 230

DOCUMENTS 1,034

IMG_0002.HEIC

TAGS AND COMMENTS

TAGS (0)
No tags have been added yet
ADD NEW TAG

Select an existing tag:
 Bookmark
 Evidence
 Of interest

COMMENTS (0)
No comments have been added yet
ADD COMMENT
MANAGE TAGS

Time zone UTC-5:00



Picture preview

EXPORT UNDO REDO

TRANSFORM

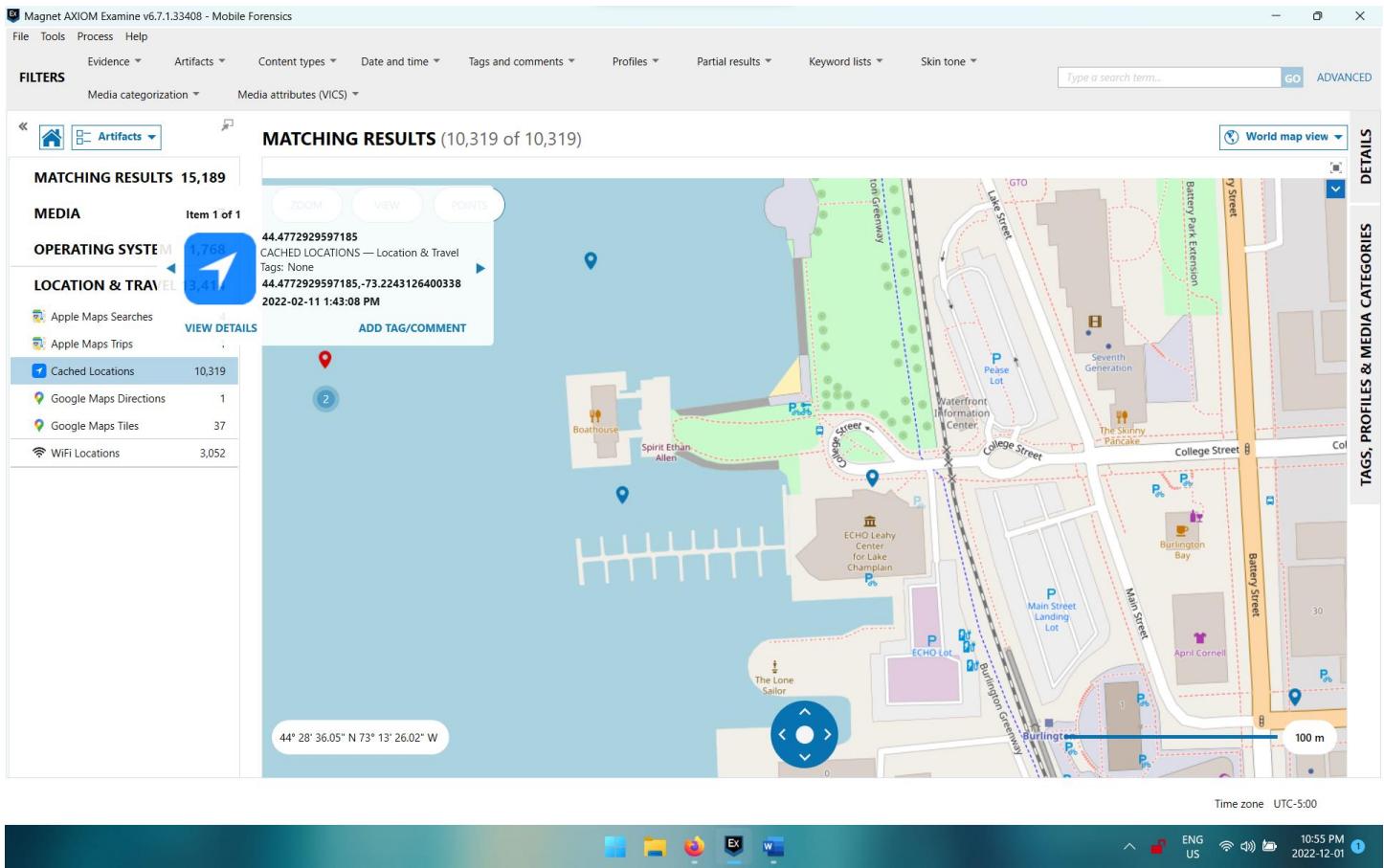
- Canvas resize
- Crop
- Draw
- Draw text
- Flip horizontal
- Flip vertical
- Pan
- Resize
- Rotate 90
- Rotate 180
- Rotate 270
- Selection
- Shape

ADJUST

- Brightness and contrast
- Hue shift

ZOOM 65%

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

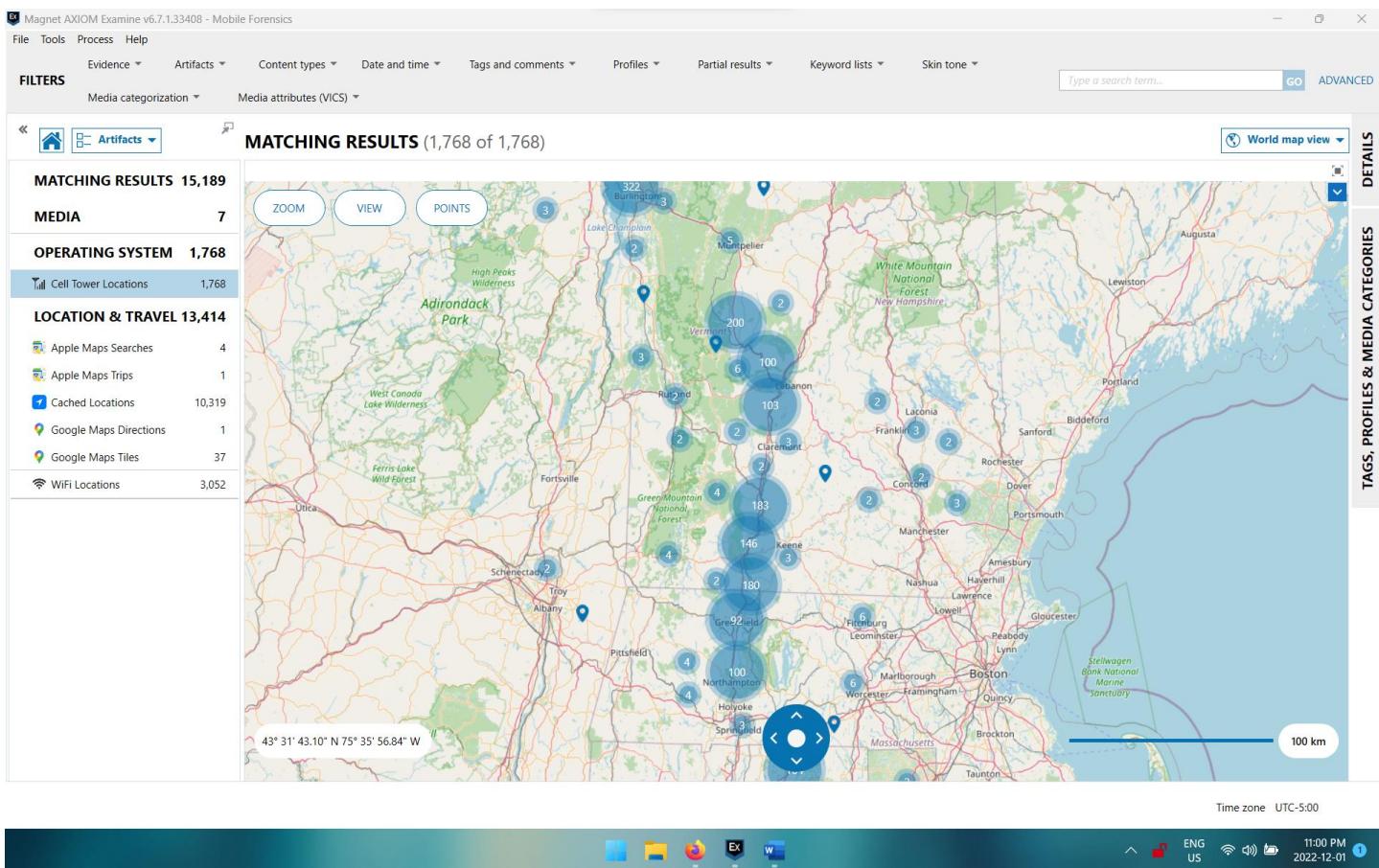
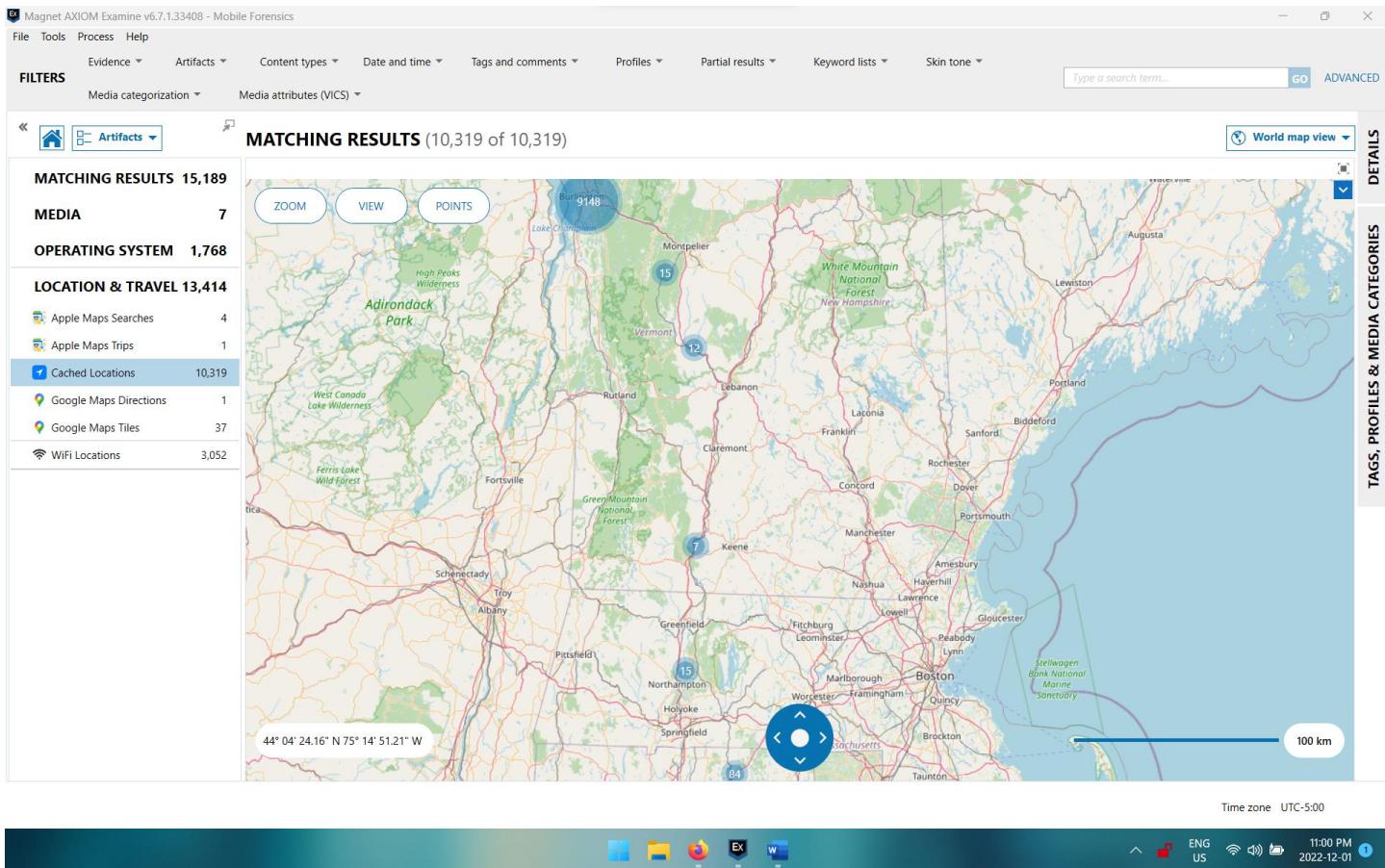


Burlington en route to Willington

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

Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

FILTERS

Media categorization Media attributes (VICs)

Type a search term... GO ADVANCED

MATCHING RESULTS (10,319 of 10,319)

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

Time zone UTC-5:00



Item 1 of 1

44.3462889058753

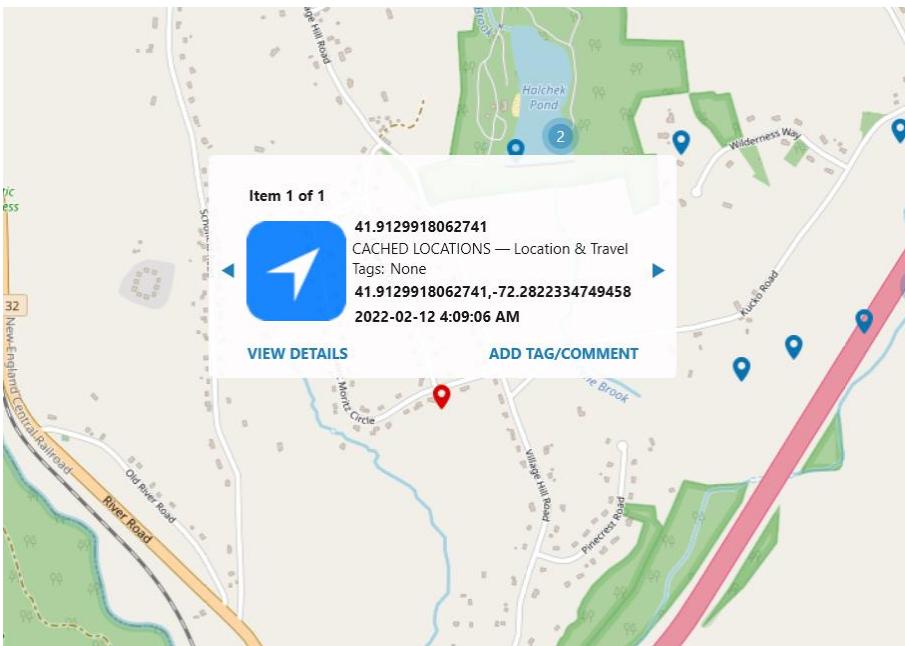
CACHED LOCATIONS — Location & Travel

Tags: None

44.3462889058753,-72.8062859520019

2022-02-11 8:58:19 PM

[VIEW DETAILS](#) [ADD TAG/COMMENT](#)



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.

Magnet AXIOM Examine v6.7.1.33408 - Mobile Forensics

FILTERS

- Evidence
- Artifacts
- Content types
- Date and time
- Tags and comments
- Profiles
- Partial results
- Keyword lists
- Skin tone

Type a search term... GO ADVANCED

MATCHING RESULTS (10,319 of 10,319)

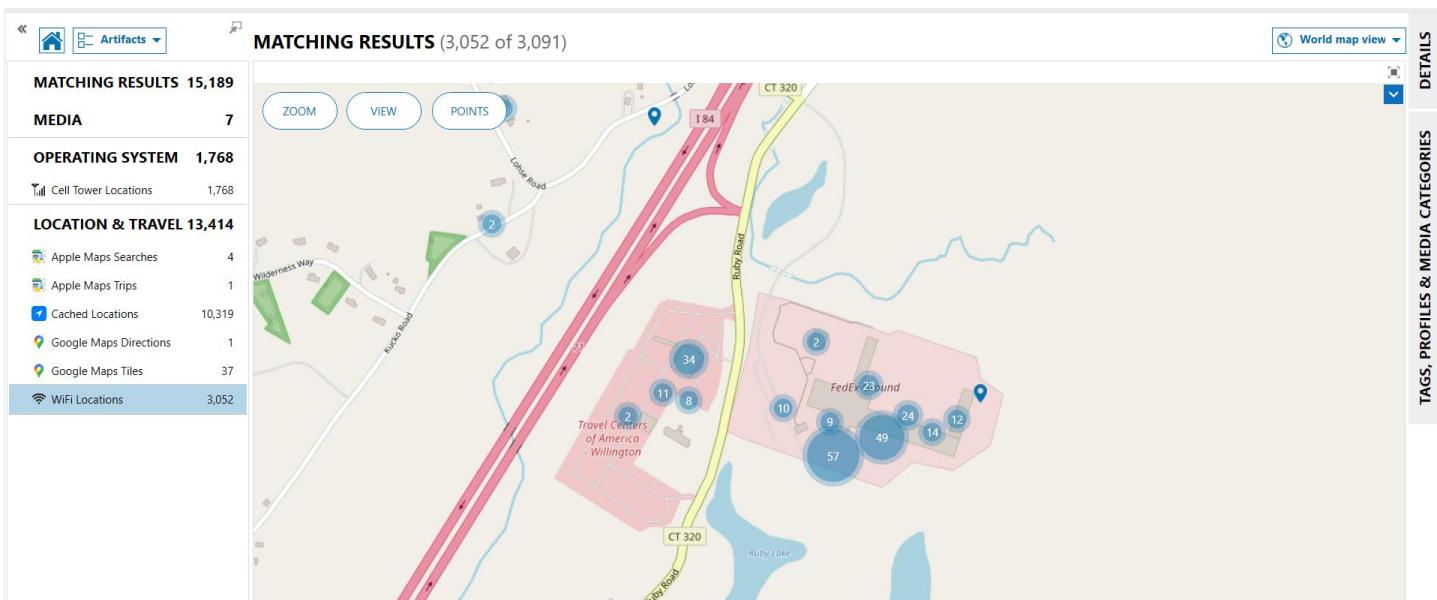
MATCHING RESULTS 15,189

MEDIA	7
OPERATING SYSTEM	1,768
Cell Tower Locations	1,768
LOCATION & TRAVEL 13,414	
Apple Maps Searches	4
Apple Maps Trips	1
<input checked="" type="checkbox"/> Cached Locations	10,319
Google Maps Directions	1
Google Maps Tiles	37
WiFi Locations	3,052

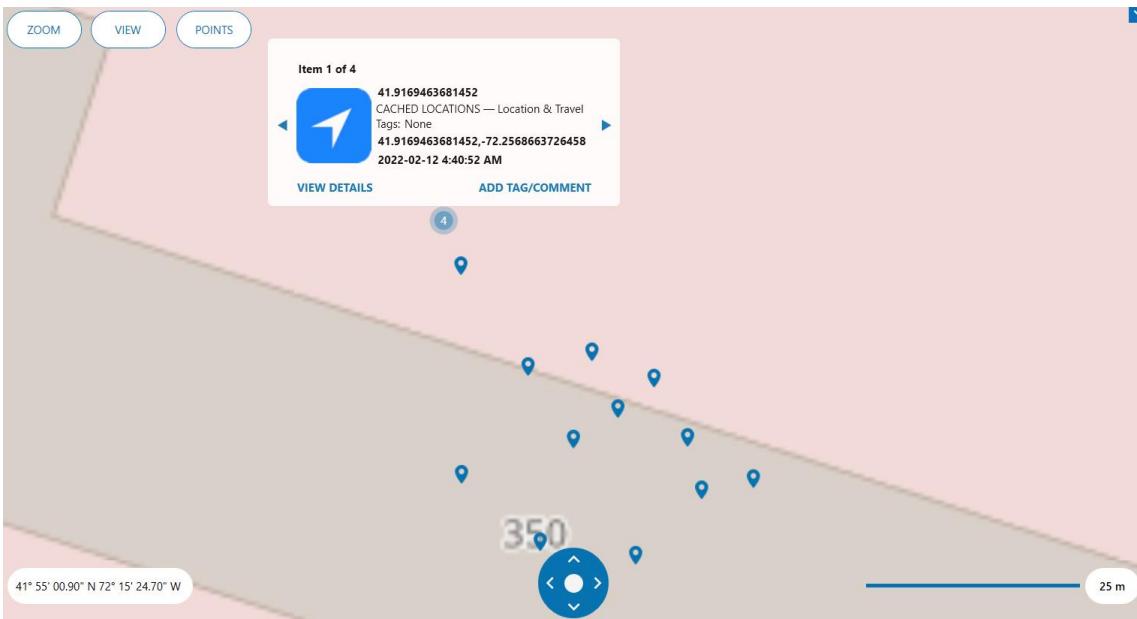
MATCHING RESULTS 10,319

Time zone UTC-5:00

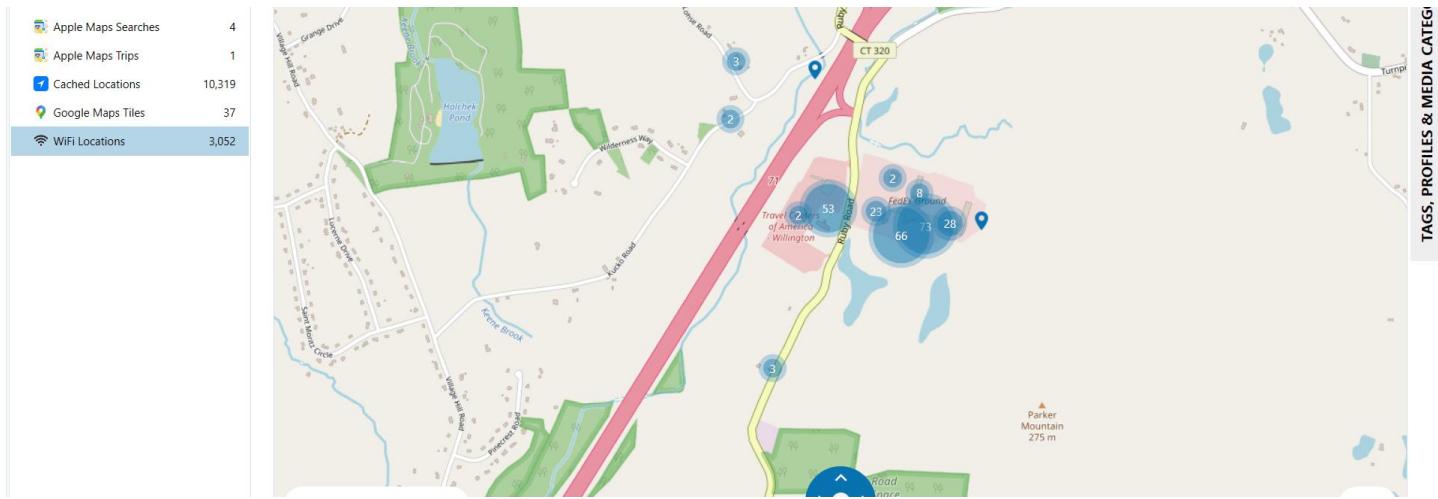
ENG US 11:03 PM 2022-12-01



The time of arrival was 12th February 2022.



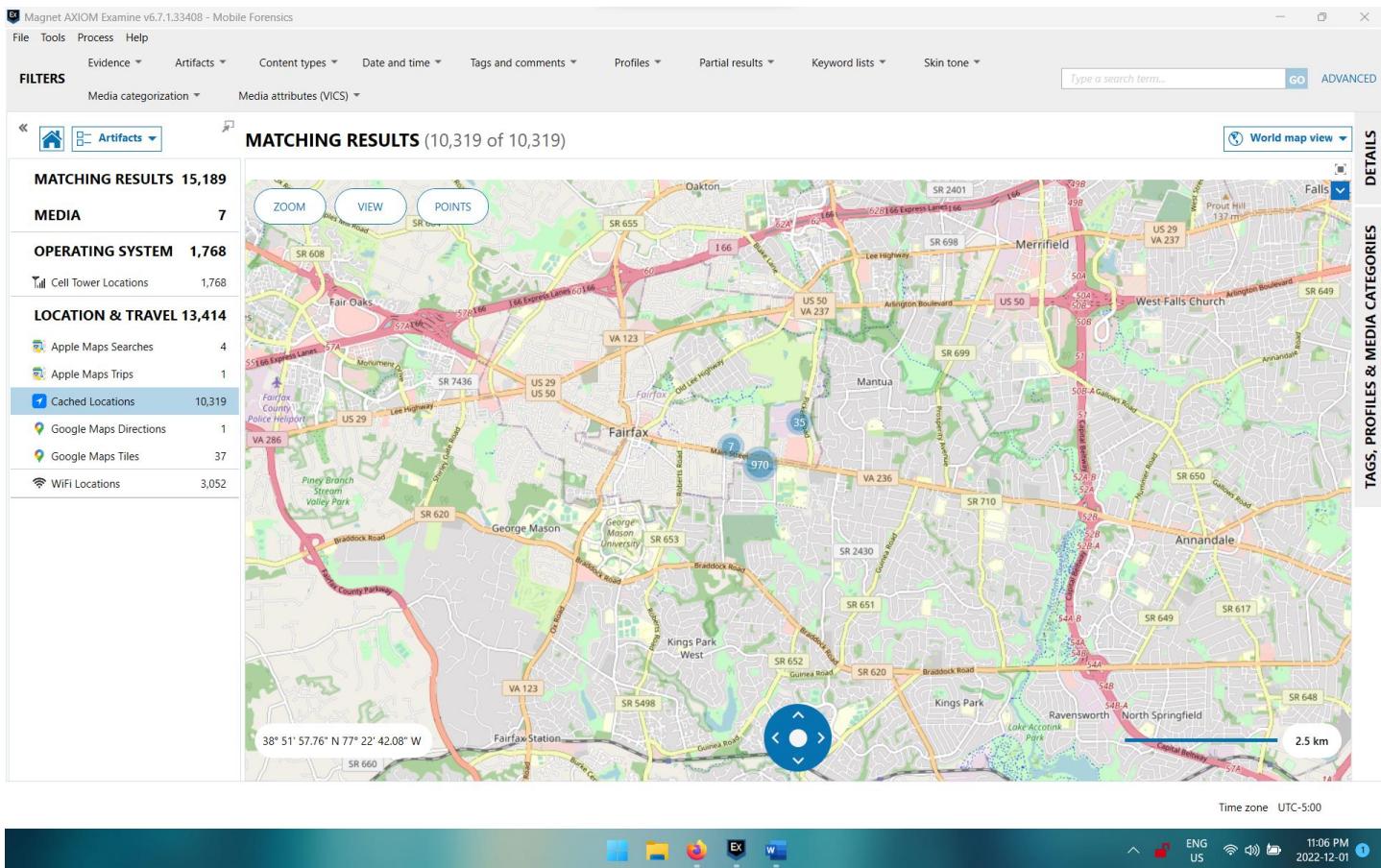
Wifi location confirms the long stay in the FedEx Ground center.

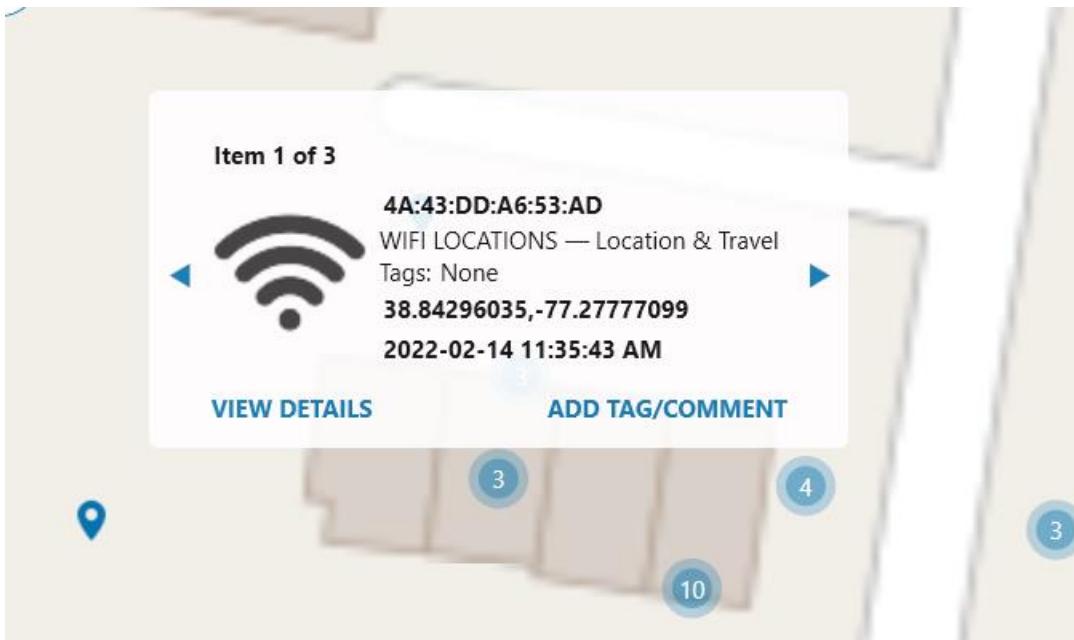


Unfortunately, there isn't sufficient data in the Willington area to make many more assumptions about its activities.

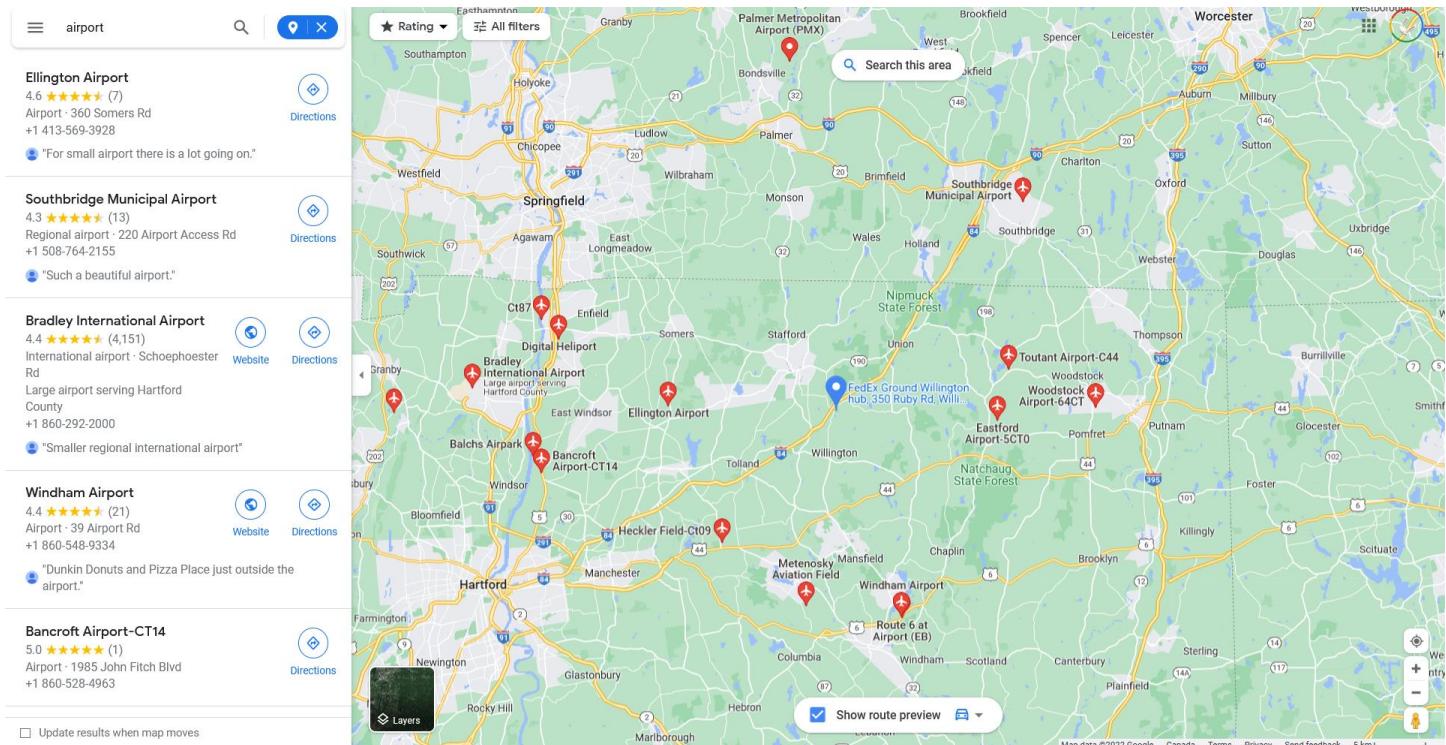
Fairfax, Virginia

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.

MATCHING RESULTS (9 of 9)

	Source	Reco...	Delete...	Location	Evidence number	Item ID
y Sh...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing		Table: PLBATTERYAGENT_EVENTPOINT_BATTERYSHU...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	34642
y Sh...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing		Table: PLBATTERYAGENT_EVENTPOINT_BATTERYSHU...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	34643
y Sh...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing		Table: PLBATTERYAGENT_EVENTPOINT_BATTERYSHU...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	64534
y Sh...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing		Table: PLBATTERYAGENT_EVENTPOINT_BATTERYSHU...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	65705
y Sh...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing		Table: PLBATTERYAGENT_EVENTPOINT_BATTERYSHU...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	65707
y Sh...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing		Table: PLBATTERYAGENT_EVENTPOINT_BATTERYSHU...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	67114
y Sh...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing		Table: PLBATTERYAGENT_EVENTPOINT_BATTERYSHU...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	69123
y Sh...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing		Table: PLBATTERYAGENT_EVENTPOINT_BATTERYSHU...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	69124
y Sh...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing		Table: PLBATTERYAGENT_EVENTPOINT_BATTERYSHU...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	71184

Date: 2022-02-12 04:58:04.804 -0500

fd3e729f075d150637a31_files_full.zip

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: D204P
	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

Y LEVEL	1002000010001/010012000/2010/0010003/021_1HES...	PARSING	1002000010001/010012000/2010/0010003/021_1HES...	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
v Level	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing	Table: PLBATTERYAGENT_EVENTBACKWARD_BATTER...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	65124

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
- Of interest

y Level	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing	Table: PLBATTERYAGENT_EVENTBACKWARD_BATTER...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	35619
y Level	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing	Table: PLBATTERYAGENT_EVENTBACKWARD_BATTER...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	35620
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
v Level	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing	Table: PLBATTERYAGENT_EVENTBACKWARD_BATTER...	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	65124

100.0

fb028ddefa8af7df5b12d3e729f075d150637a31_files_full.zip

DETAILS

ARTIFACT INFORMATION

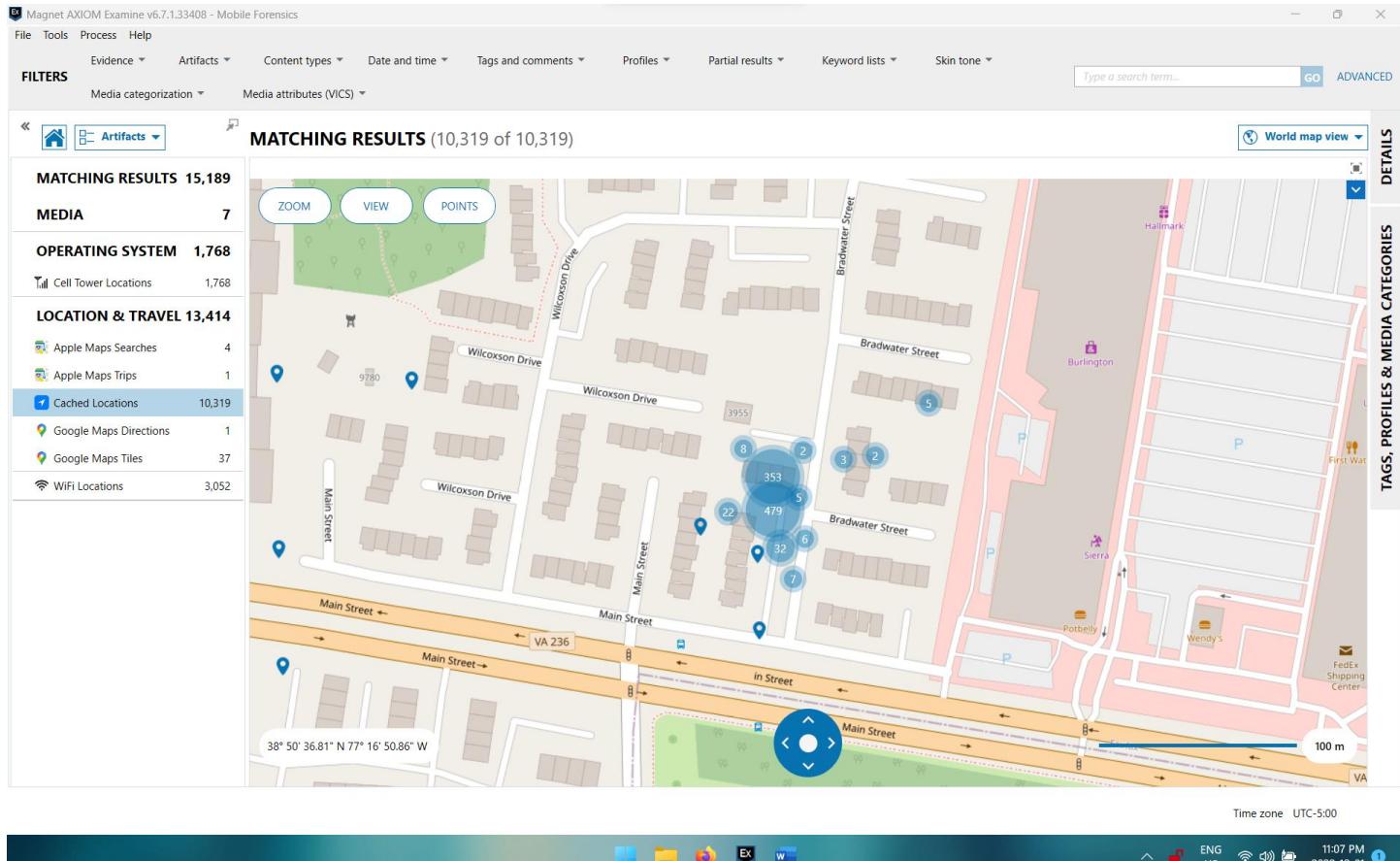
Battery Level	100.0
Raw Battery Level	98.947951273533
Charging	Yes
Fully Charged	No
Monotonic Date/Time	2022-02-14 1:35:24 PM

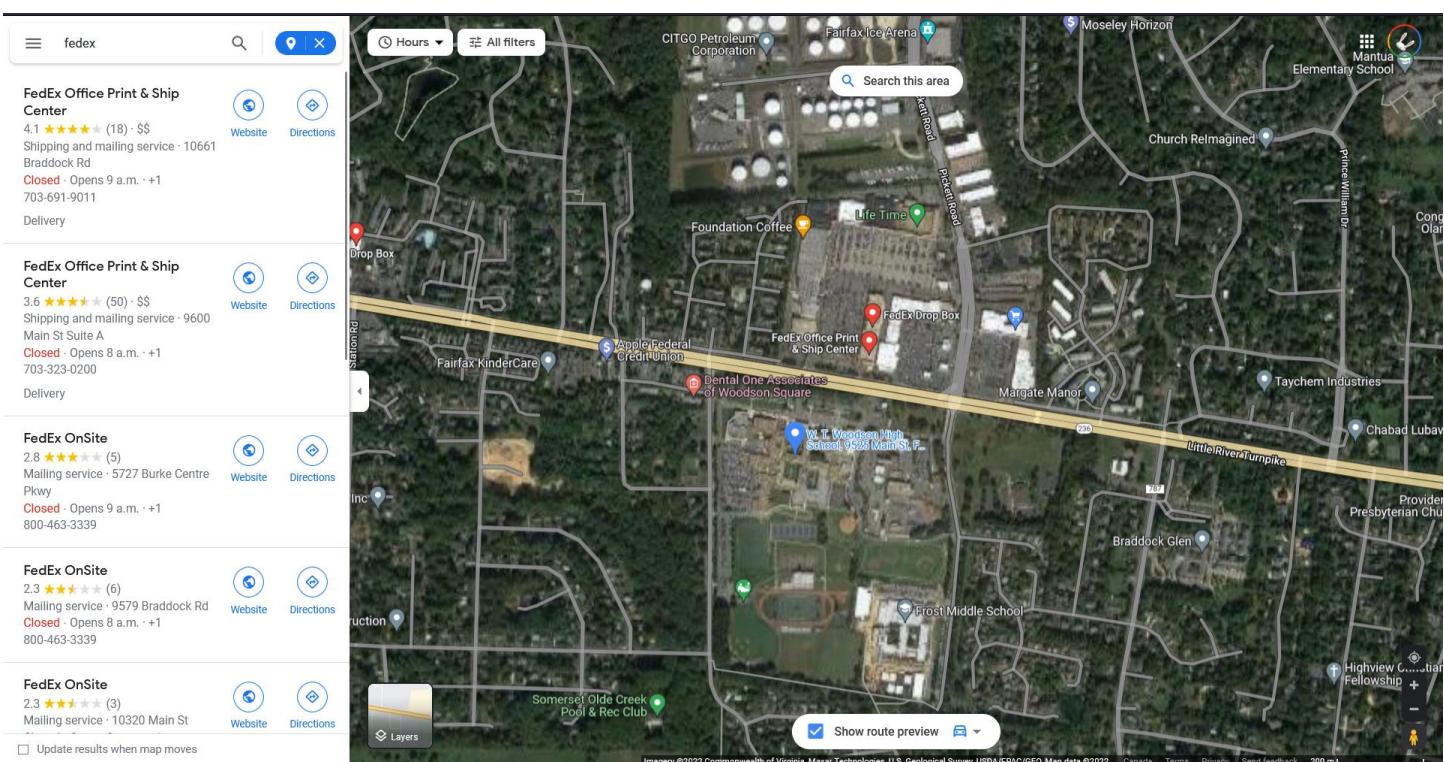
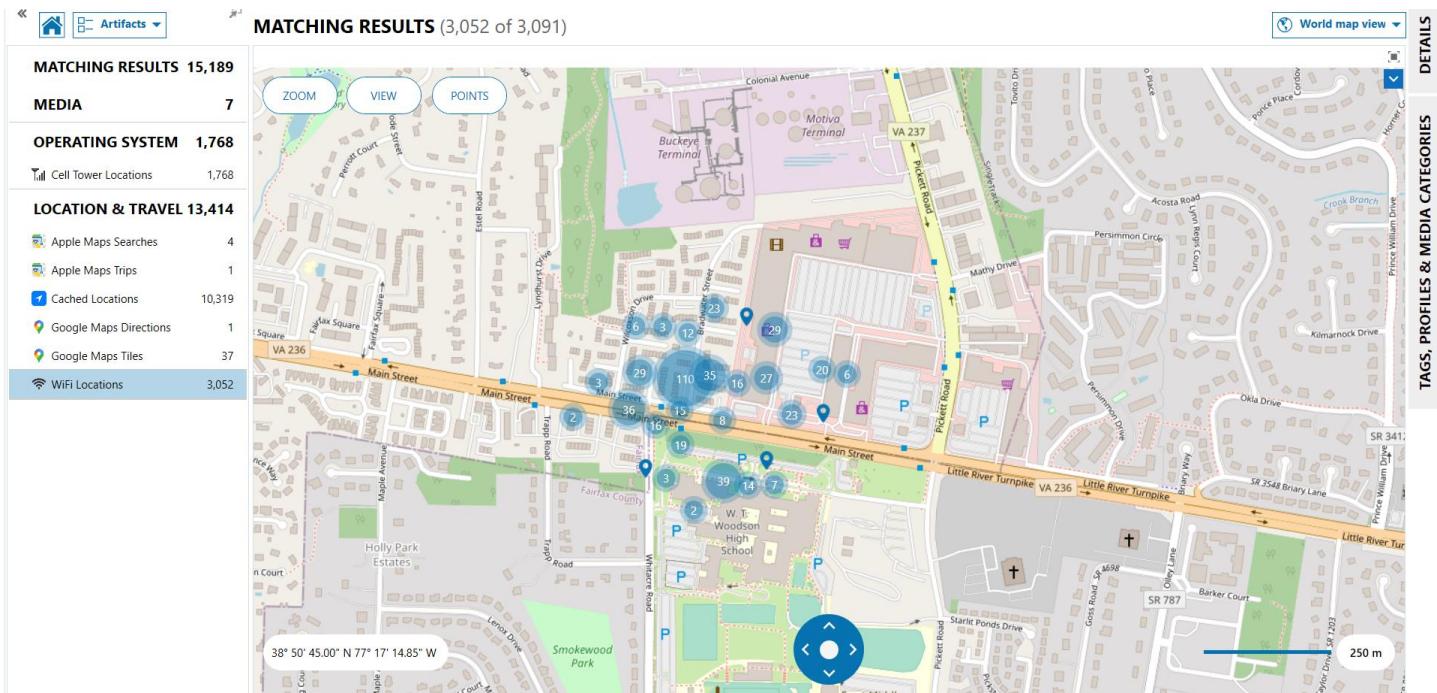
TAGS AND COMMENTS

TAGS (0)
No tags have been added yet
[ADD NEW TAG](#)

Select an existing tag:
 Bookmark
 Evidence
 Of interest

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.

Magnet AXIOM Examine v6.7.1.33408 - Mobile Forensics

File Tools Process Help

FILTERS

fb028ddefa8af7df5b1... Artifacts Content types Date and time Tags and comments Profiles Partial results

CLEAR FILTERS Type a search term... GO ADVANCED

Artifacts

MATCHING RESULTS (13 of 13)

SOCIAL NETWORKING	3,431
MEDIA	13,945
AMR Files	2
Audio	223
Carved Audio	178
iOS Snapshots	276
Live Photos	1
Photos Albums	6
Photos Media Information	13
Photoshop Files	59
Pictures	13,100
Videos	87
EMAIL & CALENDAR	230
Calendar Events	149
Gmail Emails	81
DOCUMENTS	1,034
APPLICATION USAGE	5,102
OPERATING SYSTEM	12,117
.DS_Store Records	80
AirDrop Background Activity	48
AirDrop Discoverability	4

IMG_0001.PNG

ARTIFACT INFORMATION

- File Name: IMG_0001.PNG
- Type: Picture
- Directory: DCIM/100APPLE
- Created Date/Time: 2022-01-14 7:14:21 PM
- UUID: 512AC7DF-C03E-477F-BB0
- Artifact type: Photos Media Information
- Item ID: 1861

EVIDENCE INFORMATION

- Source: fb028ddefa8af7df5b12d3e\mobile\Media\PhotoData
- Recovery method: Parsing
- Deleted source: No
- Location: Table: ZASSET(Z_PK: 1)
- Description: Table: ZADDITIONALASSETA
- Evidence number: fb028ddefa8af7df5b12d3e7;

EVIDENCE INFORMATION

- Source: fb028ddefa8af7df5b12d3e\mobile\Media\DCIM\100\

Time zone: UTC-5:00

ENG US 11:21 PM 2022-12-01

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

Mob...	Timestamp Date...	Latit...	Longit...	Range	Conf...	Artifact type	Source	Reco...	Delete...
						Photos Media Information	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing	T
						Photos Media Information	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing	T

IMG_0006.HEIC

fb028ddefa8af7df5b12d3e729f075d150637a31_files_full.zip

PREVIEW



Seemingly dumbbells from the EDGE gym.

MATCHING RESULTS (13 of 13)

Classic view

Mobile device	Timestamp Date	Latitude	Longitude	Range	Confidence	Artifact type	Source	Recovered	Deleted	Location
						Photos Media Information	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing		Table:
						Photos Media Information	fb028ddefa8af7df5b12d3e729f075d150637a31_files...	Parsing		Table:

IMG_0004.HEIC

0637a31_files_full.zip

PREVIEW



DETAILS

ARTIFACT INFORMATION

File Name **IMG_0004.HEIC**
Type **Picture**
Directory **DCIM/100APPLE**
Created Date/Time **2022-01-15 9:42:13 AM**
UUID **A807BC28-8F19-430C-9242-AE5C8E8BDFE3**
Artifact type **Photos Media Information**
Item ID **2577**

EVIDENCE INFORMATION

Source **fb028ddefa8af7df5b12d3e729f075d150637a31_files...\b**
\mobile\Media\PhotoData\Photos.sqlite
Recovery method **Parsing**
Deleted source
Location **Table: ZASSET(Z_PK: 4)**
Table: ZADDITIONALASSETATTRIBUTES(Z_PK: 4)
Evidence number **fb028ddefa8af7df5b12d3e729f075d150637a31_i**

Time zone UTC-5:00

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



g to Betterbuys, "it only takes
s to decipher a password that's
characters long"

On the other hand, if you pick a password that's 12 characters long, it'll take a massive **two centuries to crack**.

That's why the first step is: change your PC's access password.

And then change all your passwords using an unaffected computer or smartphone. I mean it. Email, social, subscriptions, etc. Every service you have access to holds precious information, including billing information and personal data.

According to CybInt, [95% of breaches are caused by human error](#) . What this means is that you could have unknowingly given enough identifying information for a hacker to guess your password. It could also mean that you've mistakenly run an infected program document that contained malware.



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.

MATCHING RESULTS (72 of 135)

Search Term	URL	Date/Time
https://wl.spotify.com/l...	https://www.google.com/url?q=https://wl.spotify.co...	2022-02-13 2:42:26 AM
ai dungeon	https://www.google.com/search?qs_ssp=elzj4tVP1z...	2022-02-13 3:36:16 AM
https://api.aidungeon.io/ver...	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&q=lar...	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/ver...	https://www.google.com/url?q=https://api.aidunge...	2022-02-13 4:03:22 AM
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...	2022-01-28 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/l...	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?qs_ssp=elzj4tVP1z...	2022-02-13 3:36:16 AM
https://api.aidungeon.io/ver...	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&q=lar...	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

ARTIFACT INFORMATION

Search Term: https://api.aidungeon.io/verify/34566459/?code=b2eeac9e-9d64-0d6-8307-3ac07cb73177
 URL: https://www.google.com/url?q=https://api.aidungeon.io/verify/34566459/?code=3Db2eeac9e-9d64-40d-8307-3ac07cb73177&source=gmail&ust=164828024895000&usg=AOvVaw1wTRTECzowu7KT3GuKad
 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

Time zone: UTC-5:00

MATCHING RESULTS (145 of 145)

Host	Name	Value	Accessed Date/Time
.youtube.com	_Secure-3PSID	GQIV0yjs4lvLGF-6Ty4nW7tCsF2aV-gk7sPVkk6wbU9...	2022-01-25 5:11:02 PM
.youtube.com	HSID	ALEYPKD2IGN7U-U96	2022-01-25 5:11:02 PM
.youtube.com	SSID	AJsyuQsiBwoNmPsf4	2022-01-25 5:11:02 PM
.youtube.com	APSID	1fk1Vr1fUx1MbqQ/APqLbd396jUM0cfVh	2022-01-25 5:11:02 PM
.youtube.com	SAPSID	hAljX-bwy7Bmc1j/AqjRjAE1_af0hUCRj	2022-01-25 5:11:02 PM
.youtube.com	_Secure-1PAP/SID	hAljX-bwy7Bmc1j/AqjRjAE1_af0hUCRj	2022-01-25 5:11:02 PM
google.com	SEARCH_SAMESITE	CgQlyZQB	2022-02-13 4:06:18 AM
.youtube.com	_Secure-3PAP/SID	hAljX-bwy7Bmc1j/AqjRjAE1_af0hUCRj	2022-01-25 5:11:02 PM
.doubleclick.net	IDE	AHWqTUIZXH1j716igJOp8VTDKeDWbz87dQrl2nwX...	2022-02-13 4:05:17 AM
.hackingtutorials.org	_gads	ID=9e036a5b34725ce-22e9d365e1cf0071:T=16447...	2022-02-13 1:30:12 AM
.hackingtutorials.org	_gat	1	2022-02-13 1:30:12 AM
.casalemedia.com	CMID	YgiLoL6NoiFFq3WLO7hxYgAA	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	YgiLoGlpaaAA	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-3fc4-4d57-915c-8e3d38491501 16447338...	2022-02-13 1:30:56 AM
.mookei1.com	id	10610269616392244864	2022-02-13 1:30:56 AM
.quantserve.com	mc	6208a5a0-33a7b-9194d-e6b99	2022-02-13 1:30:56 AM
.mookei1.com	mdata	I 10610269616392244864 1644733856203	2022-02-13 1:30:56 AM
.mookei1.com	ov	3a6d38fd2b81ee125d237a2a5a782f21	2022-02-13 1:30:56 AM
.twitter.com	_twitter_sess	BAh7CiiKZmxhc2hJQzonQWN0aW9uQ29udHJvbGx...	2022-02-13 2:29:39 AM

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 4:02:21 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

Time zone: UTC-5:00

MATCHING RESULTS (145 of 145)

Category	Count
Identifiers - People	1,429
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

Column view

Host	Name	Value	Accessed Date/Time
.clarity.ms	ANONCHK	0	2022-02-13 4:00:22 AM
www.vanishingincmagic.com	ASP.NET_SessionId	adx1ppxbkewetkarjblmvex	2022-02-13 4:00:20 AM
.c.bing.com	MR	0	2022-02-13 4:00:22 AM
.c.clarity.ms	MR	0	2022-02-13 4:00:22 AM
.bing.com	MUID	05EE59B7EF6761AD336048FDEEB360F1	2022-02-13 4:02:03 AM
.clarity.ms	MUID	05EE59B7EF6761AD336048FDEEB360F1	2022-02-13 4:01:47 AM
.c.clarity.ms	SM	C	2022-02-13 4:00:22 AM
.c.bing.com	SRM_B	05EE59B7EF6761AD336048FDEEB360F1	2022-02-13 4:00:22 AM
www.vanishingincmagic.com	VincCart	ID=38193919&Guid=f79323d3-2da1-4131-9fd4-7f6...	2022-02-13 4:01:44 AM
.vanishingincmagic.com	_attrb	%22f8b3ddb-0729-4891-9030-06f0fa1914e4%22	2022-02-13 4:01:44 AM
.vanishingincmagic.com	_cioanomid	2de4e267-20b8-2c57-b5ef-72d3e3556feb	2022-02-13 4:01:44 AM
.vanishingincmagic.com	_clk	sgxde5 leyjy 0	2022-02-13 4:01:44 AM
.vanishingincmagic.com	_clsk	jn3ugbj1644742823113 b.clarity.ms/collect	2022-02-13 4:01:44 AM
.vanishingincmagic.com	_fbp	fb.1.1644742822051.747576177	2022-02-13 4:01:44 AM
.vanishingincmagic.com	_ga	GA1.2.947252219.1644742822	2022-02-13 4:01:44 AM
.vanishingincmagic.com	_gd_au	1.1.1606214667.1644742821	2022-02-13 4:01:44 AM
.vanishingincmagic.com	_gid	GA1.2.99136110.1644742822	2022-02-13 4:01:44 AM
www.vanishingincmagic.com	_omappvs	1644742821739	2022-02-13 4:01:44 AM
www.vanishingincmagic.com	_omappvp	8aaH8GpXJNn6QltWLAPYroO8QtQab2rCY3X8cBlat...	2022-02-13 4:01:44 AM
.vanishingincmagic.com	_uetSID	5ff88e008cab11ec91c7ebfd743fe695	2022-02-13 4:01:44 AM
.vanishingincmagic.com	_uetvid	5ff0f508cabb11ecb79497e62f4a834d	2022-02-13 4:01:44 AM
www.vanishingincmagic.com	brand	id=1&vat=false	2022-02-13 4:01:44 AM
www.vanishingincmagic.com	country	223	2022-02-13 4:01:44 AM
facebook.com	fr	0c3ychohATCEsLjPH..BiCMil...1.0.BiCMil.	2022-02-13 4:00:22 AM
vimeo.com	rlaver	--	2022-02-13 4:01:41 AM

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 4:02:11 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

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.

Category	Count
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

URL	Added Date/Time	Name
https://www.hackingtutorials.org/exploit-tutorials/lo...	2022-02-13 1:31:22 AM	Log4Shell VMware vCenter Server (CVE-2021-44228)
https://www.vanishingincmagic.com/learn-card-trick...	2022-02-13 4:01:11 AM	5 Intermediate and Advanced Card Tricks Every Mag...

iOS Keychain

DETAILS

ARTIFACT INFORMATION

- URL: https://www.hackingtutorials.org/exploit-tutorials/log4shell-vmware-vcenter-server-cve-2021-44228/
- Added Date/Time: 2022-02-13 1:31:22 AM

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.

MATCHING RESULTS (13 of 14)

User ID	Account Name	Email Address	Icon URL	Created Date/Time	Artifact type
ArcaneArmor1	jn8hzvq5	rafaelshell24@gmail.com	https://styles.redditmedia.com/t5_5ufaln/styles/prof...	2022-02-13 1:16:12 AM	Reddit Accounts
vorobevfedecka	4icypy58		https://styles.redditmedia.com/t5_247ee4/styles/pro...	2019-09-03 2:36:38 AM	Reddit Accounts
bradhrad	xwbom		https://styles.redditmedia.com/t5_b2p84/styles/pro...	2016-05-13 3:21:50 AM	Reddit Accounts
GroundbreakingSet187	7uabnis9		https://styles.redditmedia.com/t5_316hy3/styles/pro...	2020-08-24 8:34:48 PM	Reddit Accounts
MKFederalist	h5hqvtq		https://styles.redditmedia.com/t5_5qb61/styles/pro...	2022-01-25 5:06:29 AM	Reddit Accounts
vaguenonetheless	34avggsw		https://styles.redditmedia.com/t5_122z47/styles/pro...	2019-05-27 9:10:59 AM	Reddit Accounts
Binance_Ads	6f7uzyhi		https://styles.redditmedia.com/t5_2rnax18/styles/pro...	2020-05-08 7:47:32 PM	Reddit Accounts
Voxeer_	28uhd143		https://styles.redditmedia.com/t5_yl15p/styles/profil...	2019-03-22 7:07:36 PM	Reddit Accounts
FlightmasterOne	cnadj8q2		https://styles.redditmedia.com/t5_4lkkw/styles/pro...	2021-06-12 1:46:06 PM	Reddit Accounts
TheRealSpacePieDebt	8k5f293v		https://styles.redditmedia.com/t5_3aa2do/styles/pro...	2020-10-20 2:48:36 PM	Reddit Accounts
joshuttlemeir	ipr2bdia		https://styles.redditmedia.com/t5_5p3f40/styles/pro...	2022-01-18 9:56:53 AM	Reddit Accounts
ninya_the_cat	4bt89h8e		https://styles.redditmedia.com/t5_22s4nh/styles/pro...	2019-08-08 12:05:32 PM	Reddit Accounts
DraftKings	ayhgtgfx		https://styles.redditmedia.com/t5_4471ej/styles/prof...	2021-03-16 9:46:18 PM	Reddit Accounts

SOCIAL NETWORKING **696**

Reddit Accounts	13
Reddit Posts	5
Reddit Recently Visited Subreddits	1
TikTok Contacts	1
Twitter Direct Messages	2
Twitter Tweets	273
Twitter Users	401

MEDIA **41,397**

AMR Files	34
Audio	109
Carved Audio	173
Motion Photos	1
Photoshop Files	10
Pictures	40,824
Videos	246

EMAIL & CALENDAR **331**

Android Yahoo Mail User Accounts	1
Calendar Events	154

Time zone: UTC-5:00

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.

MATCHING RESULTS (1 of 1)

Account Name	Display Name	Profile ID	Profile Name	Artifact type	Source	Reco.
rafaelshell24@gmail.com	Rafael Shell	112199601670694672387		Google Accounts	PhysicalDrive2 - Partition 2 (Microsoft NTFS, 203.73...)	Parsing

APPLICATION USAGE **11,902**

Android Device Information	1
Android Usage History	2,154
Application Activity - Android	4
Application Permissions - Android	6,255
Application Runtime Permissions	157
Digital Wellbeing Events	3,025
Google Play Application Details	68
Google Play Installed Applications	67
Google Play Searches	7
Installed Applications	164

OPERATING SYSTEM **245**

.DS_Store Records	108
Accounts Information	128
Android Downloads	6
File System Information	2
Google Accounts	1

ENCRYPTION & CREDENTIALS **1,220**

CONNECTED DEVICES **8**

LOCATION & TRAVEL **28**

CUSTOM **219**

rafaels...

iOS Keychain

DETAILS

ARTIFACT INFORMATION

EVIDENCE INFORMATION

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.

Skin white - Media categorization - Media attributes (V1CS) -

MATCHING RESULTS (5 of 45)

	Title	Subreddi...	Author	Over...	Content Link
	The warmest, softest and happiest...	r/Eyebleach	vorobevedechka	No	https://gfycat.com/hiddenviciousflame
	Traditional olive oil extraction	r/oddlysatisfying	vagueunmethless	No	https://v.redd.it/f04mydjd0gh81
	Animation we did with my friend, hope you enjoy it	r/Minecraft	Voxeer_	No	https://v.redd.it/e1a4cpgdpeh81
	What a 512 Chunk Render Distance looks like... (Distant Horizons Mod)	r/Minecraft	Salamantic	No	https://v.redd.it/gapehvhk7fh81
	Why won't my sugarcane grow? I've been afk for 30 mins, nothing grew	r/Minecraft	ninya_the_cat	No	https://i.reddit.it/jckz13kwddh81.pn

ARTIFACT INFORMATION

- Title
- Reddit Name
- Author
- Over 18
- Content Link
- URL
- Read Date/Time

TAGS, PROFILES & MEDIA CATEGORIES

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.

EVIDENCE (289)

	Site...	URL	Date...	Date...	Artifact
	Twitter	https://twitter.com/privacy			Potential Browser Activi...
	Twitter	https://help.twitter.com/en/using-twitter/direct-mes...			Potential Browser Activi...
	Reddit	https://www.reddit.com/r/rupaulsdragrace/commen...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/boston/comments/srje62/...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/programming/comments/...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/programming/comments/...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/programming/comments/...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/programming/comments/...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/programming/comments/...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/programming/comments/...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/Twitch/comments/s6vnih/...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/programming/comments/...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/programming/comments/...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/javascript/comments/sm...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/javascript/comments/slkf...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/javascript/comments/sly...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/Minecraft/comments/sdy...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/Minecraft/comments/se1...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/Minecraft/comments/sf71...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/javascript/comments/sm8...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/Minecraft/comments/sfpd...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/Minecraft/comments/sekf...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/Minecraft/comments/se7...			WebKit Browser Web H
	Reddit	https://www.reddit.com/r/javascript/comments/sky7...			WebKit Browser Web H
	Twitter	https://twitter.com/			Potential Browser Activi...

Reddit

ARTIFACT INFORMATION

- Site Name: Reddit
- URL: https://www.reddit.com/r/programming/comments/snyrg/raidz_expansion_feature_for_zfs_goes_live/
- Artifact type: Social Media URLs
- Item ID: 3141
- Original artifact: WebKit Browser Web History (Carved)

EVIDENCE INFORMATION

- Source: fb028ddefa8af7df5b12d3e729f075d150637a31_files_full.zip\private\var\mobile\Library\UserNotifications\F6C59A01-8506-44B5-866A-8CB9301E27AA\DeliveredNotifications.plist
- Recovery method: Deleted source
- Deleted source: File Offset 28946
- Location: fb028ddefa8af7df5b12d3e729f075d150637a31_files_full.zip
- Evidence number: fb028ddefa8af7df5b12d3e729f075d150637a31_files_full.zip

Tags, Profiles & Media Categories

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

EVIDENCE (35)		Column view				
		Site...	URL	Date/Time	Date...	Artifact
ALL EVIDENCE	131,834	Bumble	https://bumble.com			Potential Brow
REFINED RESULTS	16,831	Bumble	https://bumble.com			Potential Brow
Classified URLs	5	Bumble	https://eu1.bumble.com/hotpanel/hotpanel.phtml			WebKit Brow
Cloud Passwords and Tokens	36	Bumble	https://eu1.bumble.com/hotpanel/hotpanel.phtml			WebKit Brow
Cloud Services URLs	3	Bumble	https://bumble.com/en-us/help/?section=1			WebKit Brow
Dating Sites URLs	35	Bumble	https://bumble.com/post_install/?device_id=_dev_i...			WebKit Brow
Facebook URLs	3	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
Google Maps Queries	4	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
Google Searches	135	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
Identifiers - Device	4,218	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
Identifiers - People	11,617	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
Passwords and Tokens	289	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
Rebuilt Webpages	15	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
Social Media URLs	289	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
User Accounts	118	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
Web Chat URLs	64	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
WEB RELATED	6,579	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
COMMUNICATION	164	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
SOCIAL NETWORKING	4,127	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
MEDIA	55,342	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow
EMAIL & CALENDAR	564	Bumble	https://bumble.com/en/help/IRL?app_layout=true			WebKit Brow

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

ALL EVIDENCE		131,834
REFINED RESULTS		16,831
Classified URLs	5	
Cloud Passwords and Tokens	36	
Cloud Services URLs	3	
Dating Sites URLs	35	
Facebook URLs	3	
Google Maps Queries	4	
Google Searches	135	
Identifiers - Device	4,218	
Identifiers - People	11,617	
Passwords and Tokens	289	
Rebuilt Webpages	15	
Social Media URLs	289	
User Accounts	118	
Web Chat URLs	64	
WEB RELATED	6,579	
COMMUNICATION	164	
SOCIAL NETWORKING	4,127	
MEDIA	55,342	

EVIDENCE (36)			Column view	
	User Name	Password/Token	Platf...	Service
pbentley0107@gmail.com	dc/1SITj5zxHke9JdnInXlpLdbUesvxKwguNvcrxA=	Apple	com.apple.facetime	
pbentley0107@gmail.com	EAMBAAAABlwIAAAAGHrJURDmdzLmjB91ZC5...	Apple	com.apple.account.Cloud...	
pbentley0107@gmail.com	EAABAAAABlwIAAAAGHrJURDmdzLmjB91ZC5h...	Apple	com.apple.account.Apple...	
	8fe1963b85f6819b74e120c5b72257921ed5a09	Apple	com.apple.ind.registrat...	
	BAlAAAGdAAJgAAAAIh6xfm1EcneF6kUWsiBgox...	Apple	com.apple.itunesstored.t...	
	30811681430041042c5154a5ce50c302f67e2627...	Apple	ids	
	AwnrTCCAUoCAQAcgaEAzBuovvUB85UXOAELXht...	Apple	ids	
17768365815	dc/1SITj5zxHke9JdnInXlpLdbUesvxKwguNvcrxA=	Apple	com.apple.facetime	
pbentley0107@gmail.com	AAAABlwIAAAAGH/UTYRFWdlzLmjB91ZC5mW...	Apple	com.apple.gs.cloud.fami...	
pbentley0107@gmail.com	GdkRAsxUq+j15BFtD1BkyeirQ81bV451LbTNA9jD...	Apple	com.apple.gs.cloud.auth...	
	eylraWQiOjMle1XTDBTtRoiWVlyWxnljoIRVMNTy...	Apple	com.apple.AppleMedia.S...	
	eylraWQiOjMle1XTDBTtRoiWVlyWxnljoIRVMNTy...	Apple	com.apple.AppleMedia.S...	
	ChlaEAjKgKh05y8QyoCh9cvGAESzMuWm	Google	com.google.sso.AuthAd...	
105025155841637203771	ya29A0ARdRaM-MRq_tfXY-k5xUlvSuQodQo_Ba...	Google	com.google.ss.o.optional...	
+ 19732941683	dc/1SITj5zxHke9JdnInXlpLdbUesvxKwguNvcrxA=	Apple	com.apple.facetime	
	0a20ddff9f521d69ad2b2da45a22eb3f5820c94c1...	Apple	ids	
	0a20742669d44787be596c67c81d9a69d2fd7e2358a...	Apple	ids	
pbentley0107@gmail.com	V387t4qT6kaQnijwy8fmcPFTB0G40WrQvdQ03Cw...	Apple	IDS	
105025155841637203771	1%P%P2%0A186B2UQG9jYIARAAGOSNwf-L9lx...	Google	com.google.common.SS...	
	AwnrTCCAUoCAQAcgaEAzBuovvUB85UXOAELXht...	Apple	ids	
	8f368f60e690456881ca5ade111a09	Apple	ids	
pbentley0107@gmail.com	EAMBAAAABlwIAAAAGHrJURDmdzLmjB91ZC5...	Apple	com.apple.account.Apple...	
RafaelShell2	148942976650783593-ua5L42MFMINMSvqTT2fIRD...	Twitter	com.twitter.android.oauth...	
RafaelShell2	2cuttFHfm36busMjlkUpz7rBoea4Wudi6xfzyCl4iW	Twitter	com.twitter.android.oauth...	
rafaelshell24@gmail.com	aas,et/Akppn00rlks84cYWhOOd1Zp6wsR42hN2sr...	Google	com.google	

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

Magnet AXIOM Examine v6.7.1.33408 - Mobile Forensics

File Tools Process Help

Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

FILTERS Media categorization Media attributes (VICS)

Type a search term... GO ADVANCED

EVIDENCE (146)

Column view

	Thre...	Subject	Sent...	Received Date/T...
78	Massimo shared "Waimangu geyser: the world's larg...	2022-01-30 7:56:29 AM	<	
81	Korea Stamp Society (KSS) Tweeted: Stamp showing...	2022-01-30 1:12:55 PM	<	
49	"Google drops FloC and proposes new Topics AP..."	2022-01-25 8:57:06 PM	<	
1	Rafael, take the next step on your Windows by confi...	2022-01-25 4:59:27 PM	<	
2	Security alert	2022-01-25 4:58:21 PM	<	
3	Visitor account receipt for rafaelshell24@gmail.com	2022-01-25 5:01:09 PM	<	
2	Security alert	2022-01-25 5:08:40 PM	<	
4	Rafael, finish setting up your new Google Account	2022-01-06 5:20:57 PM		
5	Rafael 📸 Explore your Pixel 3 with these 3 steps	2022-01-25 5:24:00 PM		
6	Visitor account receipt for rafaelshell24@gmail.com	2022-01-28 9:55:17 PM	<	
7	Security alert	2022-01-28 9:57:06 PM	<	
8	✉️ Please confirm your email address	2022-01-28 10:16:06 PM	<	
9	Get Started With Your Slopes Account	2022-01-30 12:36:19 AM	<	
10	Your bests on Slopes today 🎉	2022-01-30 1:31:08 PM	<	
12	Verify your email address	2022-02-01 12:00:17 AM		
11	Receipt For Order #303f33d7593846a5baea5c6e3e2...	2022-02-01 12:05:23 AM		
13	Security alert	2022-01-31 11:30:30 PM	<	
14	How do you like Slopes?	2022-02-01 1:09:27 PM	<	
15	Visitor account receipt for rafaelshell24@gmail.com	2022-02-01 7:26:23 PM	<	
17	✉️ Please confirm your email address	2022-02-01 7:28:27 PM	<	
18	✉️ Please confirm your email address	2022-02-02 4:23:16 PM	<	
20	Rafael, take the next step on your Linux by confi...	2022-02-03 9:51:57 PM	<	
19	Security alert	2022-02-03 9:50:53 PM	<	
19	Security alert	2022-02-03 9:50:57 PM	<	
21	@RafaelShell2, we see that you're new	2022-02-04 8:21:25 AM	<	

pbentley0107@gmail.com

fb028dddefa8af7df5b12d3e729f075d15063
7a31_files_full.zip

PREVIEW

FIND

From: info@twitter.com
Received: 2022-01-29 8:27:57 AM
To: ["pbentley0107@gmail.com"]
Subject: Korea Stamp Society (KSS) Tweeted: Dutch FDC from 5 October 1959, is...

DETAILS

ARTIFACT INFORMATION

To Address(es) pbentley0107@gmail.com
From Address info@twitter.com
Thread ID 57
Subject Korea Stamp Society (KSS)

Time zone UTC-5:00

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.

Magnet AXIOM Examine v6.7.1.33408 - Mobile Forensics

File Tools Process Help

Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

FILTERS Media categorization Media attributes (VICS)

Type a search term... GO ADVANCED

EVIDENCE (146)

Column view

	Thre...	Subject	Sent...	Received Date/T...
61	"Survey Says Developers Are Definitely Not In..."	2022-C	<	
57	Korea Stamp Society (KSS) Tweeted: Dutch FDC fro...	2022-C	<	
53	Hot tip: Get more from AllTrails with Navigator	2022-C	<	
82	Your Service End Date is coming soon	2022-C	<	
80	You're one of us now 🌐🌐🌐	2022-C	<	
79	The Unsolved Murder Case That Saved a Thousand...	2022-C	<	
78	Massimo shared "Waimangu geyser: the world's larg...	2022-C	<	
81	Korea Stamp Society (KSS) Tweeted: Stamp showing...	2022-C	<	
49	"Google drops FloC and proposes new Topics AP..."	2022-C	<	
1	Rafael, take the next step on your Windows by confi...	2022-C	<	
2	Security alert	2022-C	<	
3	Visitor account receipt for rafaelshell24@gmail.com	2022-C	<	
2	Security alert	2022-C	<	
4	Rafael, finish setting up your new Google Account	2022-C	<	
5	Rafael 📸 Explore your Pixel 3 with these 3 steps	2022-C	<	
6	Visitor account receipt for rafaelshell24@gmail.com	2022-C	<	
7	Security alert	2022-C	<	
8	✉️ Please confirm your email address	2022-C	<	
9	Get Started With Your Slopes Account	2022-C	<	
10	Your bests on Slopes today 🎉	2022-C	<	
12	Verify your email address	2022-C	<	
11	Receipt For Order #303f33d7593846a5baea5c6e3e2...	2022-C	<	
13	Security alert	2022-C	<	
14	How do you like Slopes?	2022-C	<	
15	Visitor account receipt for rafaelshell24@gmail.com	2022-C	<	

rafaelshell24@gmail.com

iOS Keychain

PREVIEW

FIND

Welcome Rafael Shell, your account has been created and is now ready to use.

Wi-Fi Network: ChamplainGuest

Guest Account and Wi-Fi Instructions:

1. Make sure your wireless adapter is set to dynamically obtain an IP address.
2. Connect to the wireless network: **ChamplainGuest**

DETAILS

ARTIFACT INFORMATION

To Address(es) rafaelshell24@gmail.com
From Address noreply@champlain.edu
Thread ID 6
Subject Visitor account receipt for rafaelshell24@gmail.com

Received Date/Time 2022-01-28 9:55:17 PM

Time zone UTC-5:00

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.

The screenshot shows a digital forensic interface with two main panes. On the left, a 'MATCHING RESULTS' list is displayed, showing 45 items under 'COMMUNICATION' and 2 under 'SOCIAL NETWORKING'. On the right, a detailed view of a specific conversation is shown for '244444, Local User <Android>'. The conversation view includes a preview of a message from 'Local User <Android>' containing a Google verification link, details about the message (timestamp, recipient), and participant information.

MATCHING RESULTS (45 of 47)

Category	Count
MATCHING RESULTS	45
COMMUNICATION	43
SOCIAL NETWORKING	2

244444, Local User <Android>

PREVIEW

Local User <Android> 2022-01-25 5:08:38 PM
(OgPqTeDunuet) Google is verifying the phone# of this device as part of setup. Learn more: <https://goo.gl/LHCS9W>

DETAILS

CHAT PARTICIPANTS

Time zone UTC-5:00

Getting Started YouTube Reddit Blackboard Google Drive Home Other Bookmarks

https://goo.gl/LHCS9W

Did you intend to search across the file corpus instead? [Click here](#)

1 / 88

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

[Community Score](#)

DETECTION DETAILS LINKS COMMUNITY

Security Vendors' Analysis

ESET	① 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 [CLEAR FILTERS](#) Type a search term... GO ADVANCED

Skin tone Media categorization Media attributes (VICS)

MATCHING RESULTS 45 [Conversation view](#)

COMMUNICATION 43

SOCIAL NETWORKING 2

MATCHING RESULTS (45 of 47)

- (612) 295-0550, 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
- 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.com 2022-02-03 9:04:22 AM ow.ly/vN5t50HLrXX????????? zeq

TAGS, PROFILES & MEDIA CATEGORIES

Time zone UTC-5:00

Getting Started YouTube Reddit Blackboard Google Drive Home Other Bookmarks

http://ow.ly/vN5t50HLrXX

Did you intend to search across the file corpus instead? [Click here](#)

1 security vendor flagged this URL as malicious

http://ow.ly/vN5t50HLrXX
ow.ly
multiple-redirects

200 Status 2022-12-02 09:09:15 UTC 13 hours ago

Community Score ? ✓

DETECTION DETAILS COMMUNITY

Security Vendors' Analysis

Sucuri SiteCheck	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Anti-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 Arms	Clean	CMC Threat Intelligence	Clean

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.

EVIDENCE (4)

ALL EVIDENCE 131,834

REFINED RESULTS 16,831

- Classified URLs 5
- Cloud Passwords and Tokens 36
- Cloud Services URLs 3
- Dating Sites URLs 35
- Facebook URLs 3
- Google Maps Queries 4
- Google Searches 135
- Identifiers - Device 4,218
- Identifiers - People 11,617
- Passwords and Tokens 289
- Rebuilt Webpages 15
- Social Media URLs 289
- User Accounts 118
- Web Chat URLs 64

WEB RELATED 6,579

COMMUNICATION 164

SOCIAL NETWORKING 4,127

MEDIA 55,342

2022-01-15 9:50:06 AM

fb028ddefa8af7df5b12d3e729f075d15063
7a31_files_full.zip

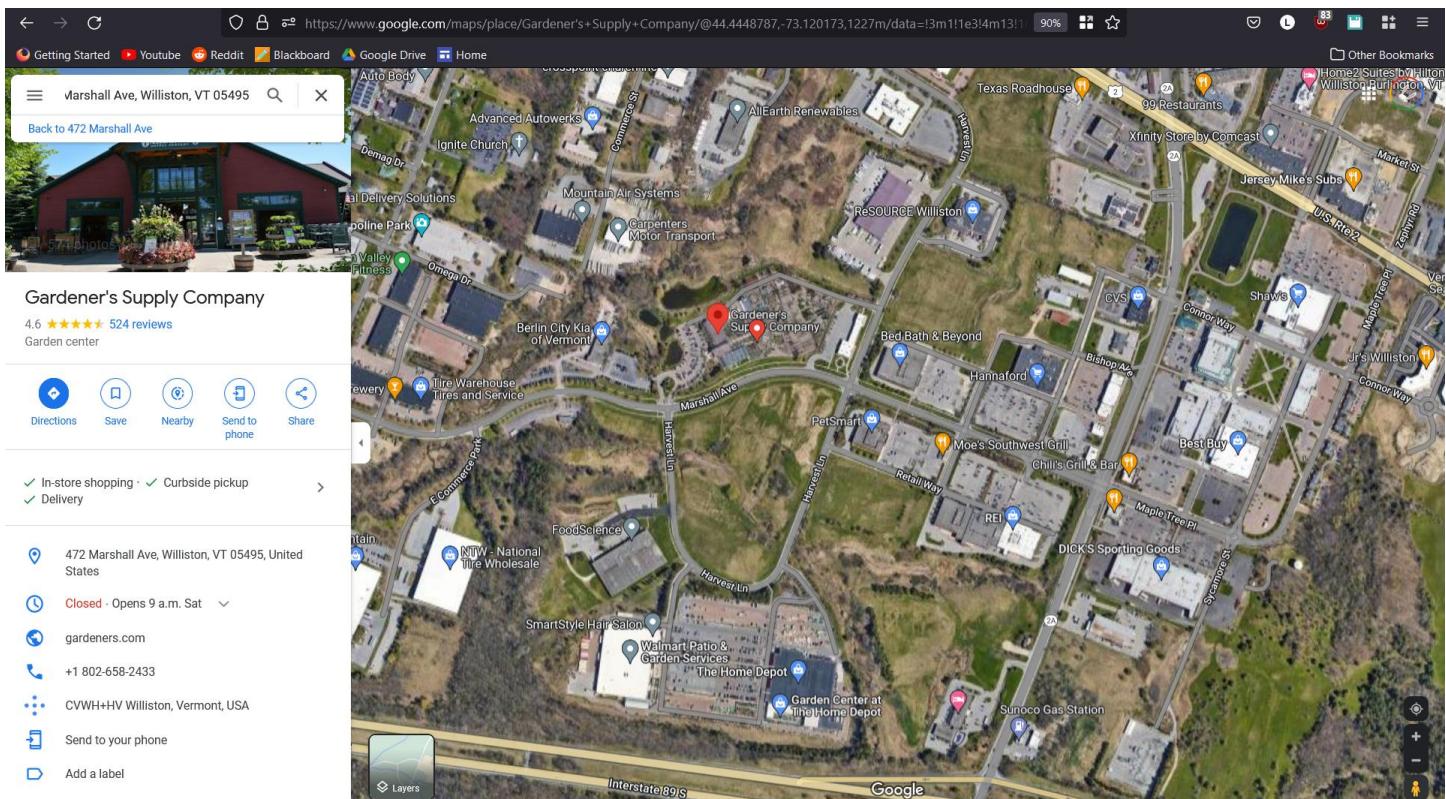
DETAILS

ARTIFACT INFORMATION

- Date/Time 2022-01-15 9:50:06 AM
- Destination Address 472 Marshall Ave, Williston, VT 05495
- Artifact type Google Maps Queries
- Item ID 1099
- Original artifact Safari History

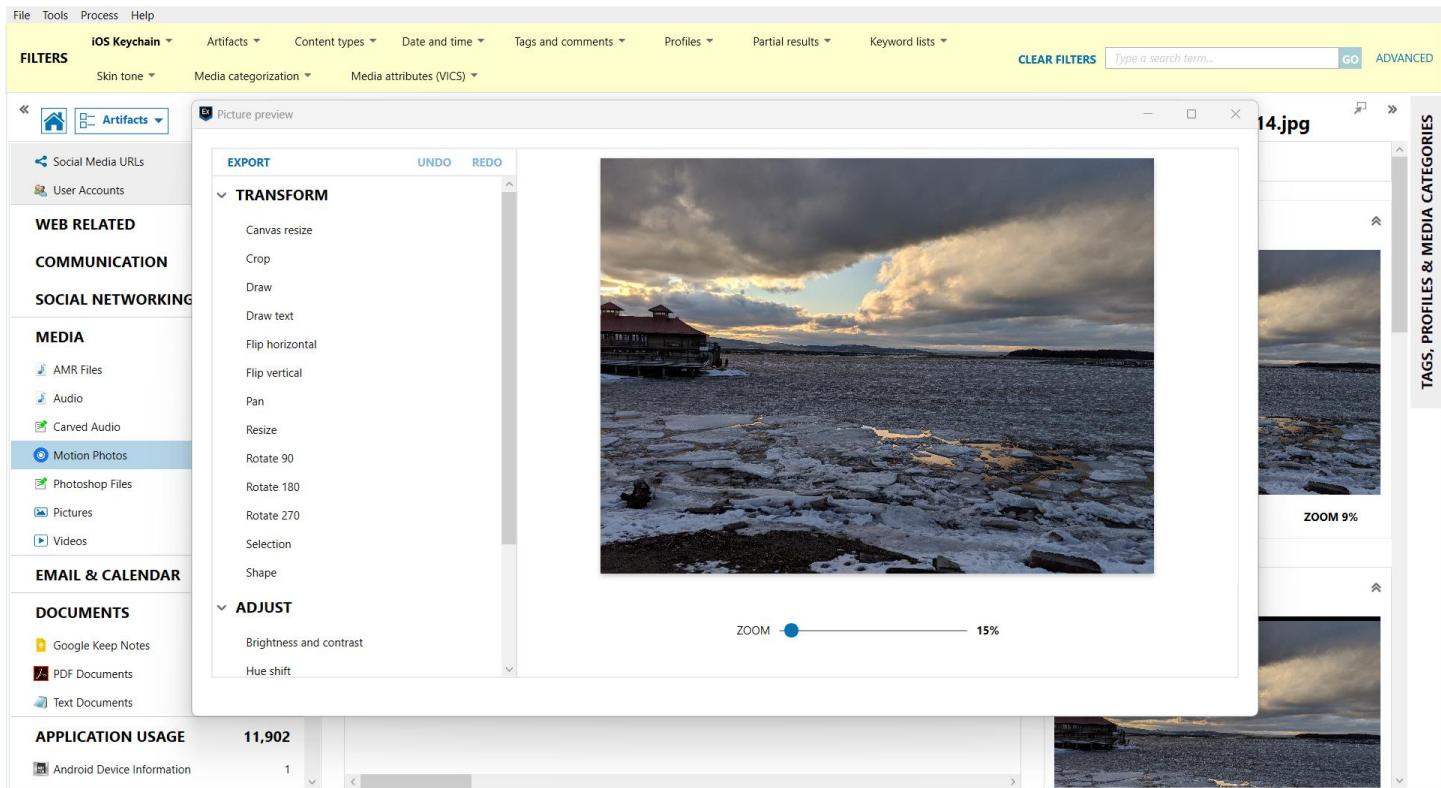
EVIDENCE INFORMATION

- Source fb028ddefa8af7df5b12d3e729f075d15063
7a31_files_full.zip
\private\var\mobile\Library
\Safari\History.db
- Recovery method
- Deleted source
- Location Table: history_items(id: 5)
Table: history_visits(id: 7)
- Evidence number fb028ddefa8af7df5b12d3e729f075d15063
7a31_files_full.zip

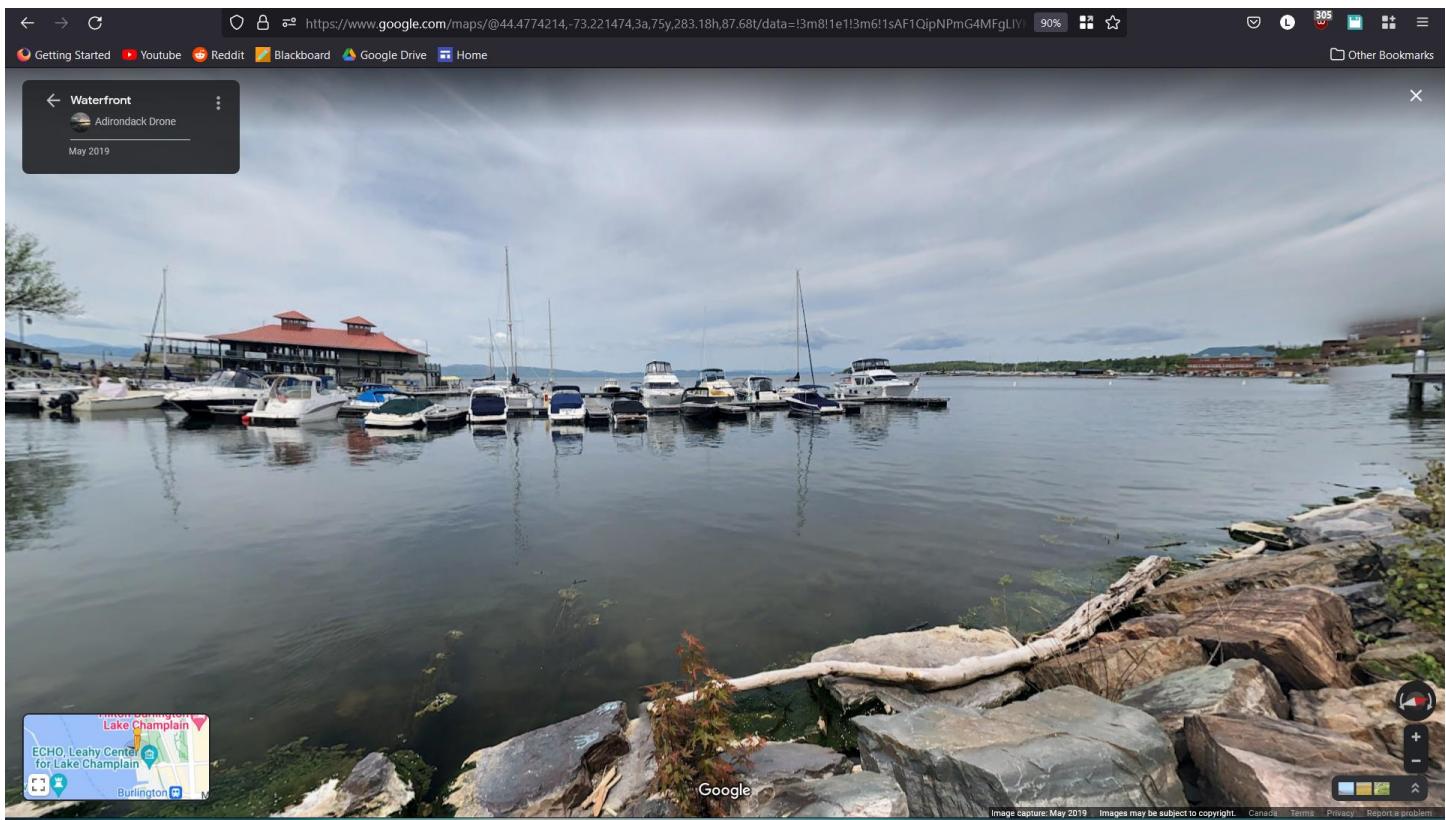


Media and photos

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.