MAGNET VIRTUAL SUMMIT 2023
CAPTURE THE FLAG (CTF)
IOS 16 IPHONE

CTF QUESTIONS ONLY

1	A few too many ***How many email accounts did the user own? (not counting privaterelay)***	5
2	Autofill me on the deets ***Which email, other than their own, was autofilled in Chrome?***	5
3	1 fish 2 fish, red fish blue ***According to the user's email accounts, what is his favourite color?***	5
4	Q-usestion ***What Chinese networking website was associated with LinkedIn?***	5
5	Chef boyardee ***At which market was the user viewing Chef Pasquale tomato sauce?***	10
6	Staying stylish! ***What color shirt did the user choose to put their snapchat bitmoji in?***	10
7	Picking up steam ***What server was the user interested in making?***	10
8	Overlooking excellence ***What Sports stadium was the user overlooking at Camille-Houde belvedere?***	10

9	You're going to crush this one! ***What light-hearted game did the user spend the most time on?***	10
10	You are here ***Which airline lounge was viewed?***	16
11	Out of this world ***Which terms and conditions site on Tik Tok is named after a space formation?***	25
12	Which way? ***Which cardinal direction was the user turning when driving towards RHEINFAHRE?***	25
13	Boosting into a new era ***The user was trying to learn German through an application, what promotion featuring a rocket was most commonly shown to the user?***	25
14	As a river runs ***At which location did the user travel the most metres according to Apple? (City, Country)***	50
15	Lo siento senor, its going to be a cold one ***What weather front was warned to the user by YouTube?***	50

ABOUT THIS CTF CHALLENGE

This challenge was created by Magnet Forensics as part of their 2023 Virtual Summit.

Information about the next summit is available at:

- https://magnetvirtualsummit.com/
- https://magnetvirtualsummit.com/capture-the-flag/

FORENSIC IMAGE SOURCE

Download: 00008101-0010541A1130001E_files_full-001.zip (9.94 GB)

OTHER ONLINE SOLUTIONS

The following solutions can be found on the web:

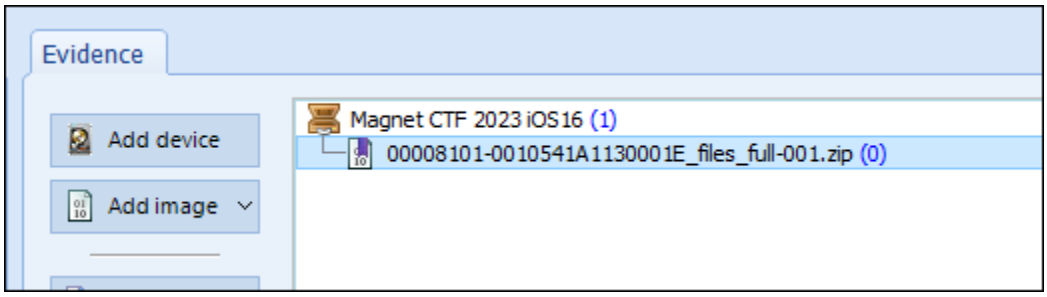
- https://www.forgottennook.com/blog/magnet-ios-2023
- https://www.stark4n6.com/2023/03/magnet-virtual-summit-2023-ctf-ios-16.html /

STARTING THIS CHALLENGE IN FORENSIC EXPLORER

In the **Evidence** module:

1. Select the **New Case** button.
2. Enter investigator details (if required) and a **case name**.
3. Click the **Add Image** button.
4. Add the evidence file: **00008101-0010541A1130001E_files_full-001.zip.**
5. In the **Evidence Processor** window use the default options.

Figure 1: Evidence Module > Add Image

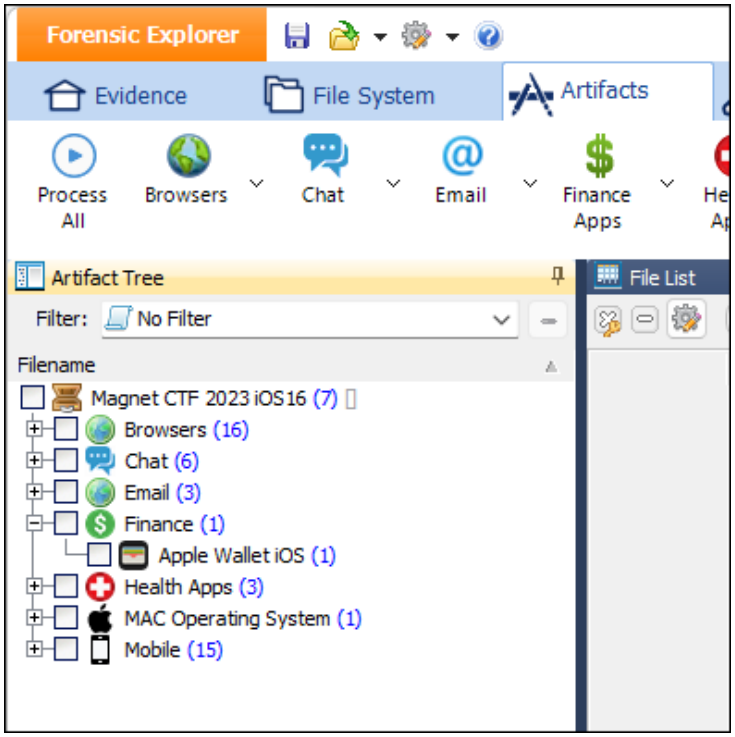


ARTIFACTS > PROCESS ALL

The Forensic Explorer **Artifacts module** extracts common forensic artifacts from SQLite, Plist, TXT, XML and other files. To populate artifacts:

1. Click the Artifacts module > **Process All** button.

Figure 2: Artifacts > Process All



QUESTION 1 - A FEW TOO MANY - (5 POINTS)

How many email accounts did the user own? (not counting privaterelay)

Q1. ANSWER

1. blueisth3best@gmail.com
2. bordardtmichael78@gmail.com
3. michaelkbordchardt@proton.me

Q1. FORENSIC EXPLORER METHODOLOGY

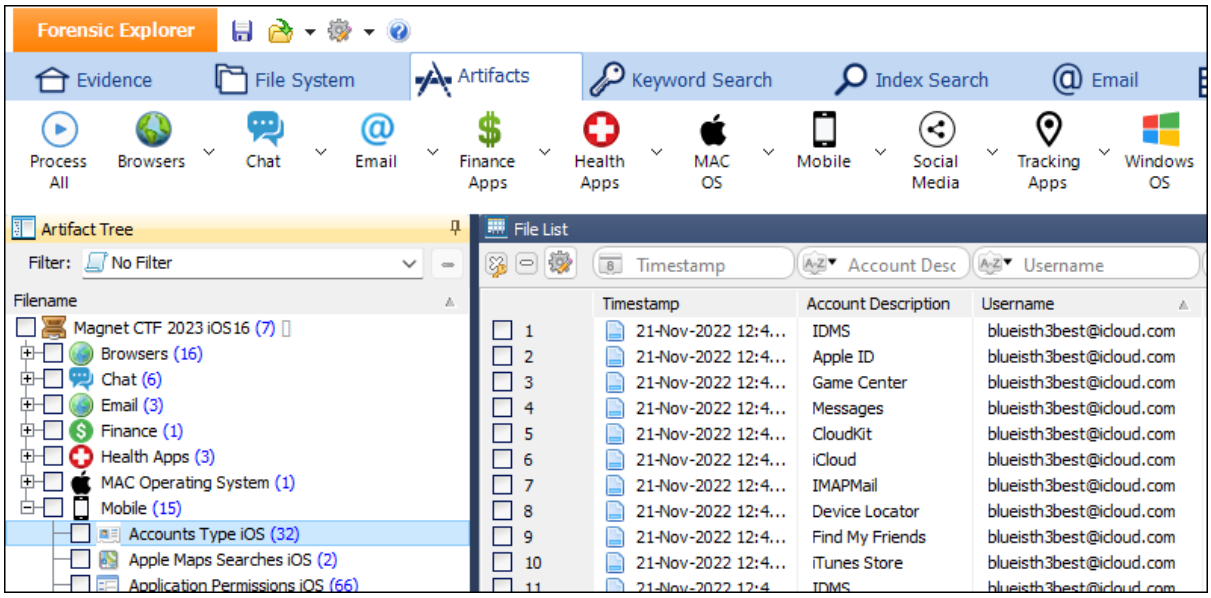
iOS account information is located in the SQLite file:

> ***\private\var\mobile\Library\Accounts\Accounts3.sqlite***

This information is extract in the Forensic Explorer **Artifacts module**:

1. Mobile > Account Types iOS.
2. Double click on the Username column header to sort by Username.

Figure 3: Artifacts > Mobile > Account Types iOS



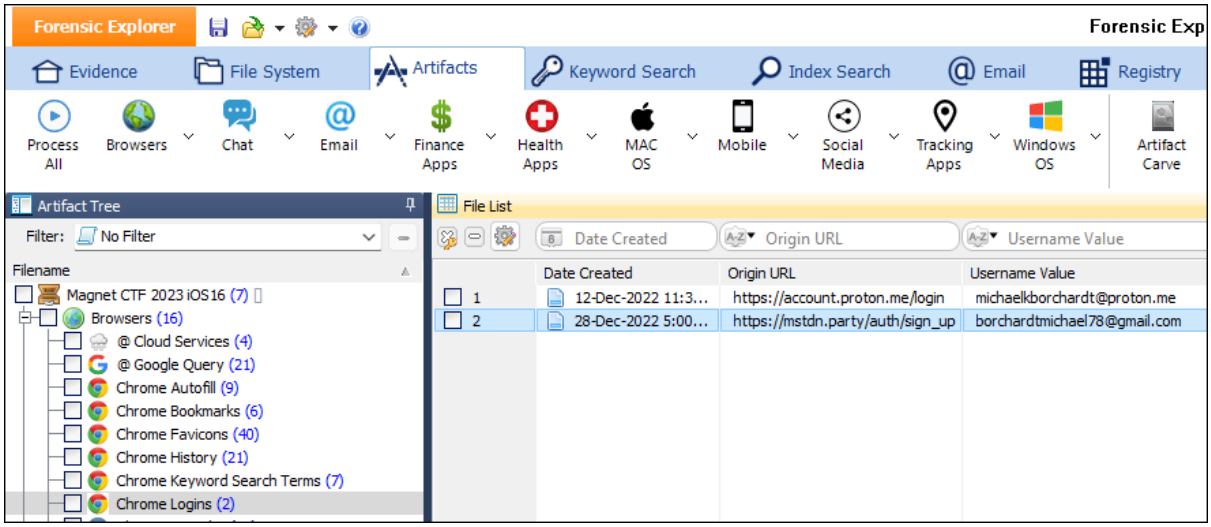
Another reliable sources of user account information are browser logins and browser autofill (see Question 3 below). For the Chrome browser, browser logins are located in the file:

> ***\private\var\mobile\Containers\Data\Application\0B468A6F-8837-4A85-BF4D-1EF523683946\Library\Application Support\Google\Chrome\Default\Login Data***

Chrome Browser Logins are extracted in the Forensic Explorer **Artifacts module**:

1. Browsers > Chrome Logins

Figure 4: Artifacts > Browsers > Chrome Logins



QUESTION 2 - AUTOFILL ME ON THE DEETS (5 POINTS)

Which email, other than their own, was autofilled in Chrome?

Q2. ANSWER

tlouis@kuravlis.com

Q2. FORENSIC EXPLORER METHODOLOGY

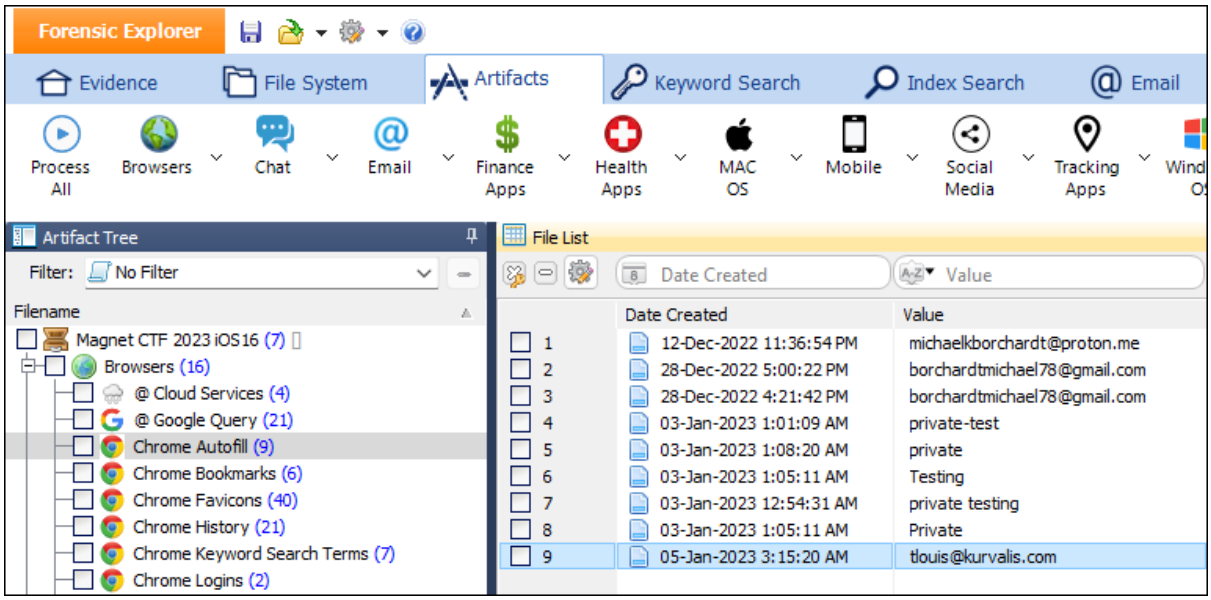
Chrome Autofill data is located in the file:

> ***\private\var\mobile\Containers\Data\Application\0B468A6F-8837-4A85-BF4D-1EF523683946\Library\Application Support\Google\Chrome\Default\Web Data***

Chrome Autofill information is extract in the Forensic Explorer **Artifacts module**:

1. Browsers > Chrome Autofill

Figure 5: Chrome Autofill



QUESTION 3 - 1 FISH 2 FISH, RED FISH BLUE (5 POINTS)

According to the user's email accounts, what is his favourite color?

Q3. ANSWER

Blue.

Q3. FORENSIC EXPLORER METHODOLOGY

This question is similar to Question 1 above. iOS account information is located in the SQLite file:

\private\var\mobile\Library\Accounts\Accounts3.sqlite

This information is extract in the Forensic Explorer Artifacts module:

1. Mobile > Account Types iOS.

Figure 6: Artifacts > Mobile > Account Types iOS

Timestamp	Account Description	Username
21/11/2022 12:18:15 AM	iTunes Store	local
21/11/2022 12:18:17 AM	iTunes Store (Sandbox)	local
21/11/2022 12:45:26 AM	IDMS	blueisth3best@icloud.com
21/11/2022 12:45:26 AM	Apple ID	blueisth3best@icloud.com
21/11/2022 12:45:31 AM	Game Center	blueisth3best@icloud.com
21/11/2022 12:45:31 AM	Messages	blueisth3best@icloud.com
21/11/2022 12:45:31 AM	CloudKit	blueisth3best@icloud.com
21/11/2022 12:45:31 AM	iCloud	blueisth3best@icloud.com
21/11/2022 12:45:41 AM	CalDAV	
21/11/2022 12:45:41 AM	IMAPNotes	
21/11/2022 12:45:41 AM	CardDAV	
21/11/2022 12:45:42 AM	IMAPMail	blueisth3best@icloud.com
21/11/2022 12:45:43 AM	Device Locator	blueisth3best@icloud.com
21/11/2022 12:45:43 AM	Find My Friends	blueisth3best@icloud.com
21/11/2022 12:45:47 AM	iTunes Store	blueisth3best@icloud.com

QUESTION 4 - Q-UESTION (5 POINTS)

What Chinese networking website was associated with LinkedIn?

Q4. ANSWER

http://user.qzone.qq.com/.

Q4. FORENSIC EXPLORER METHODOLOGY

This question is a fishing expedition using the following clues provided in the question:

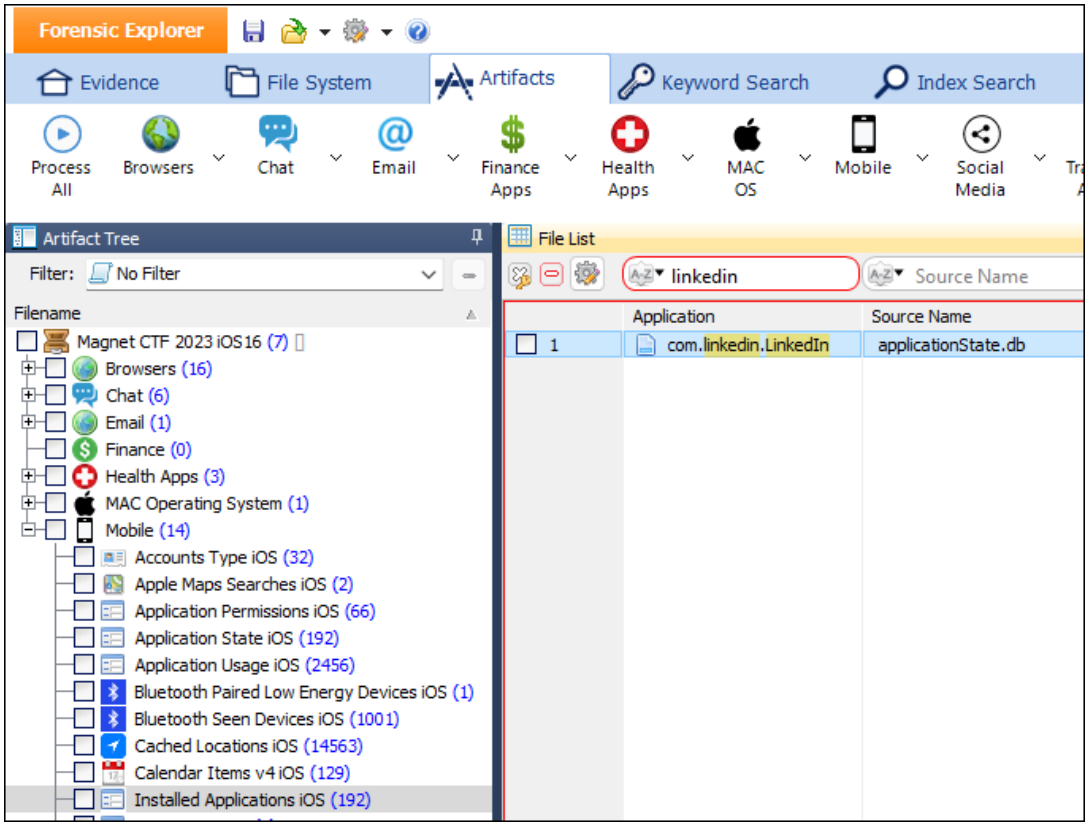
- Website: Suggests the answer is a URL.
- Chinese Networking: Suggests that the website is common only in China.

A google search for popular Chinese websites indicates the answer is likely to be one of the following:

- WeChat
- Sina Weibo
- Tencent QQ

The Artifacts module > Mobile > **Installed Applications** confirms that the LinkedIn app has been installed on the iPhone.

Figure 7: Artifacts > Mobile > Installed Applications iOS

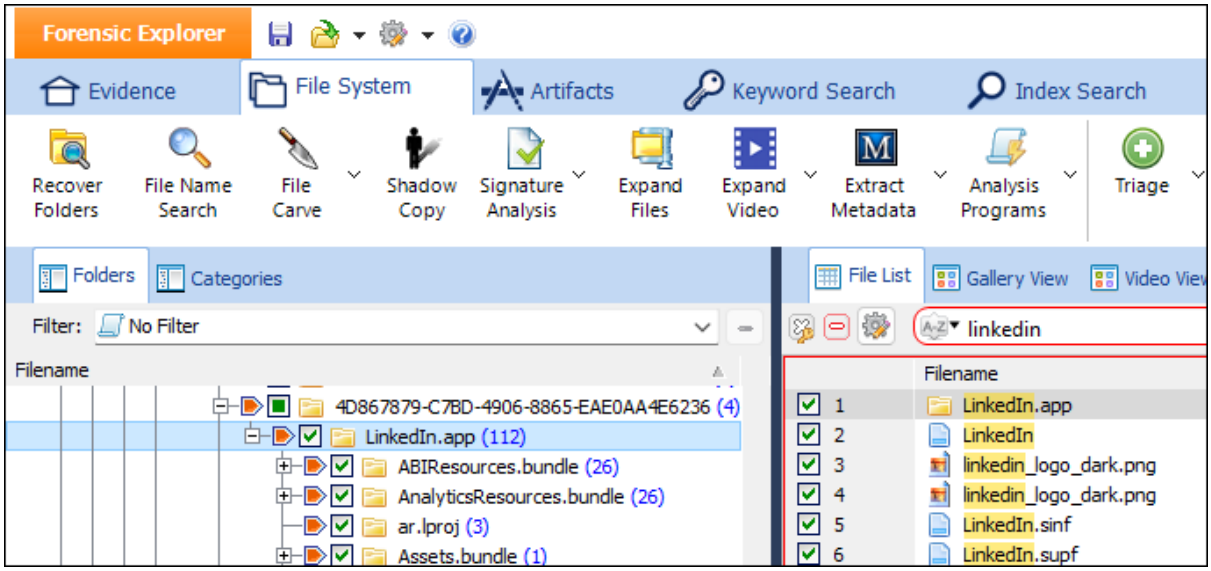


Forensic Explorer does not currently parse Linked in artifacts, so for this question we can use a **Keyword Search** as our fishing rod.

To find the **LinkedIn application root folder** in the **File System module**:

1. In the File System module, branch plate [ ] the entire case.
2. In the Filename column, filter for **LinkedIn**.

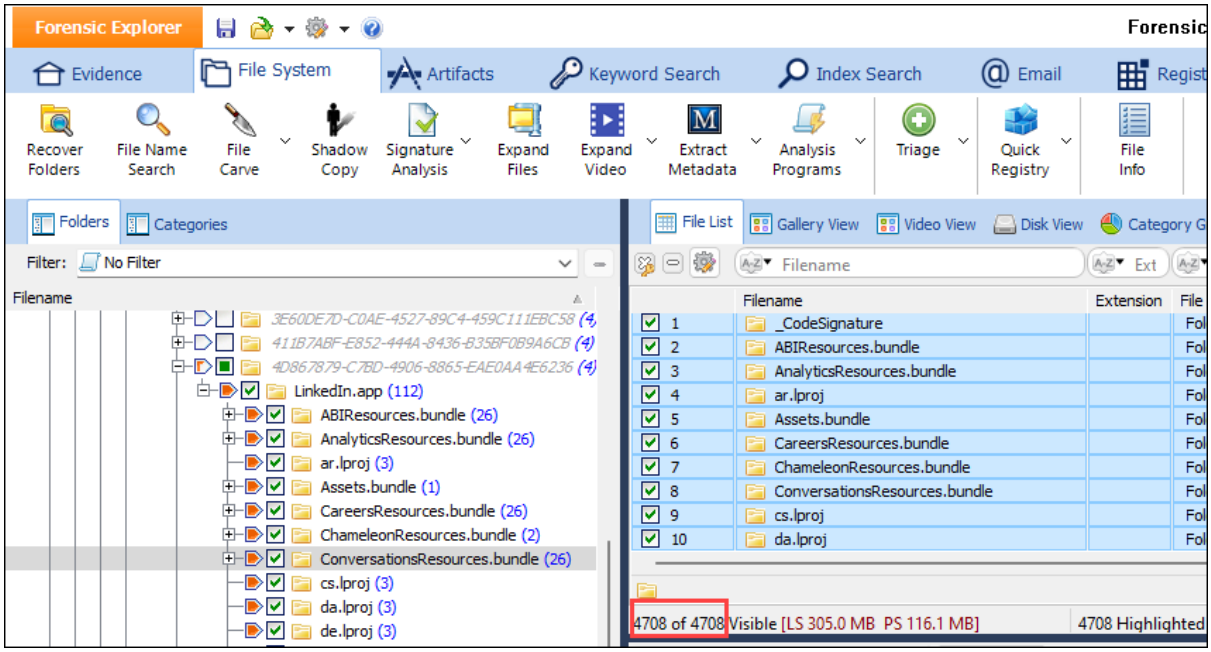
Figure 8: File System - Identifying the LinkedIn root folder



This identifies the root **LinkedIn** folder as **LinkedIn.app.**

1. A branch plate [ ] the **LinkedIn.app** folder (**4708** files).
2. CTRL-A to highlight the 4708 files.
3. Space bar to check the 4708 files.

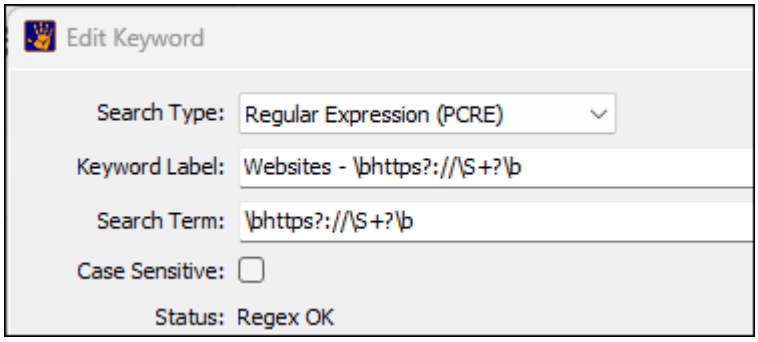
Figure 9: File System - Branch plate the LinkedIn.app root folder



In the **Keyword Search module**:

1. Add a **Regular Expression keyword** to locate websites.

Figure 10: Keyword Search module > Add Regular Expression keyword



The regular expression above is described as follows:

Figure 11: Perplexity AI - Regular expression explanation

Answer

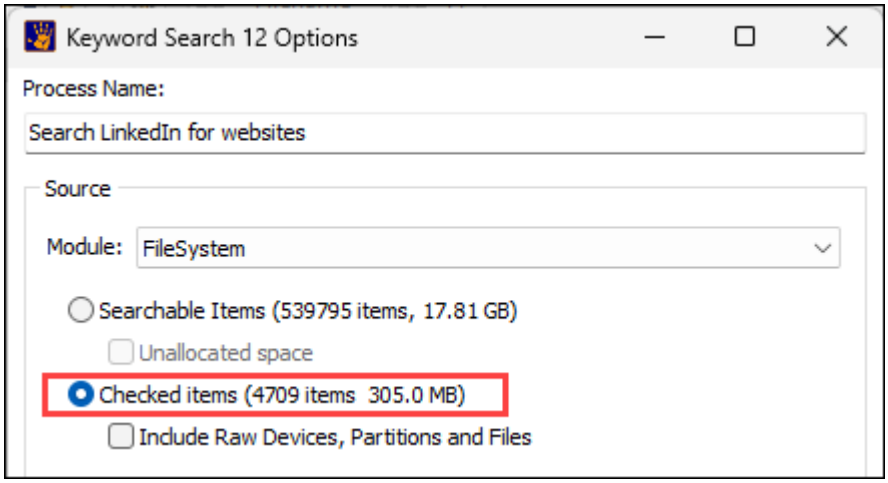
The regex \bhttps?://\S+?\b is used to match a URL within a text. Here's a breakdown of its components:

- \b: Asserts a word boundary, ensuring that the URL starts after a word character.
- https?://: Matches the http:// or https:// part of the URL.
- \S+: Matches one or more non-space characters, which represents the domain and/or path of the URL.
- \b: Asserts another word boundary, ensuring that the URL ends before a word character.

This regex is case sensitive and will match URLs that start with "http://" or "https://", followed by the domain and/or path, and it will stop at the first non-URL character, such as a space or punctuation mark [1] [3].

2. When launching the keyword search, ensure that the search is for **checked items** only:

Figure 12: Keyword Search on checked items only



166 files in the **checked items** record a **keyword match**. The primary data file appears to be:

\private\var\containers\Bundle\Application\4D867879-C7BD-4906-8865-EAE0AA4E6236\LinkedIn.app\LinkedIn

180 hits are recorded in this file, with the following entries for **qzone.com**.

Figure 13: Keyword module > Keyword search results

Hits	Hit Text	Hit Offset (File)
84/180	nding_endorsement.....https://hangouts.google.com/start.....	65604400
85/180	com/start.....http://wechat.com.volunteerCauses.inf	65604448
86/180	fView:).....http://linkedin.com/in/.....profil	65642240
87/180	//user?screen_name=.....http://twitter.com/.....profil	65642736
88/180	URLs(for:).....http://user.qzone.qq.com/.....http	65643248
89/180	user.qzone.qq.com/.....https://icq.com/people/.....http	65643280
90/180	/icq.com/people/.....http://skype.com.....[Prof	65643312
91/180	ewModel().....https://www.linkedin.com/help/linked	65674528
92/180	.....trend.....https://www.linkedin.com/creator-das	65679568

Figure 14: Perplexity AI - What is the domain qzone.com used for?

Answer

Qzone.com is a social networking website based in China, created by Tencent in 2005. It allows users to write blogs, keep diaries, send photos, listen to music, and watch videos. Users can set their Qzone background and select accessories based on their preferences so that every Qzone is customized to the individual member's taste. It is also a platform for self-expression, social networking, and content sharing among Chinese internet users. Qzone is often described as China's largest personal social networking service, providing users with a wide range of features to connect with friends, share content, and customize their online presence [1] [4].

QUESTION 5 - CHEF BOYARDEE 2.0 (10 POINTS)

At which market was the user viewing Chef Pasquale tomato sauce?

Q5. ANSWER

IMG_0034.HEIC - near Marche Atwater

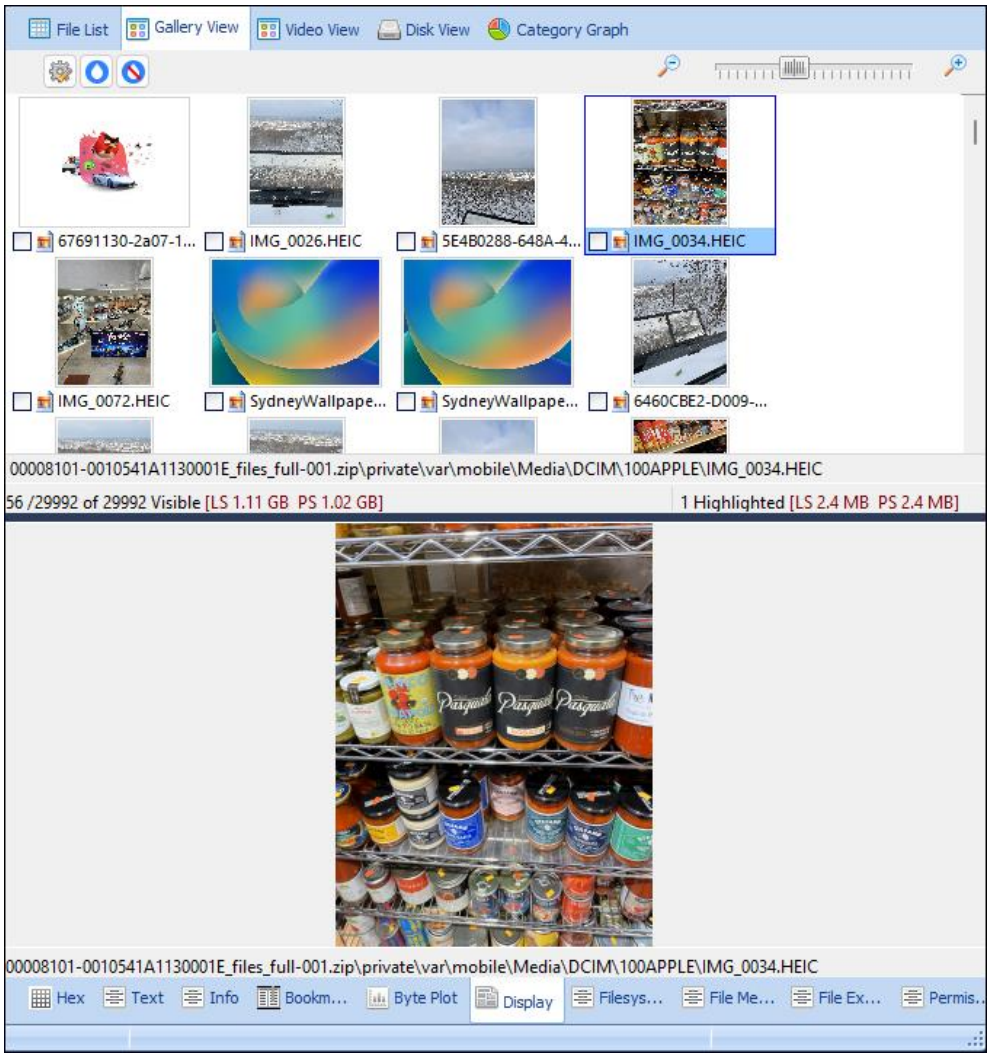
Q5. FORENSIC EXPLORER METHODOLOGY

The question suggests that the relevant file may be a photo or video. A check of the **File System** module **Gallery View** was conducted:

1. In the **File System** module, branch plate [ ] the entire case. In the **File List** window, double click on the **Logical Size column header** to sort photos by size (brings user created photos of a similar size closer together).

2. In the **File System** module, right-hand window, switch to **Gallery View** to see pictures.

Figure 15: File System > Gallery View > Display View

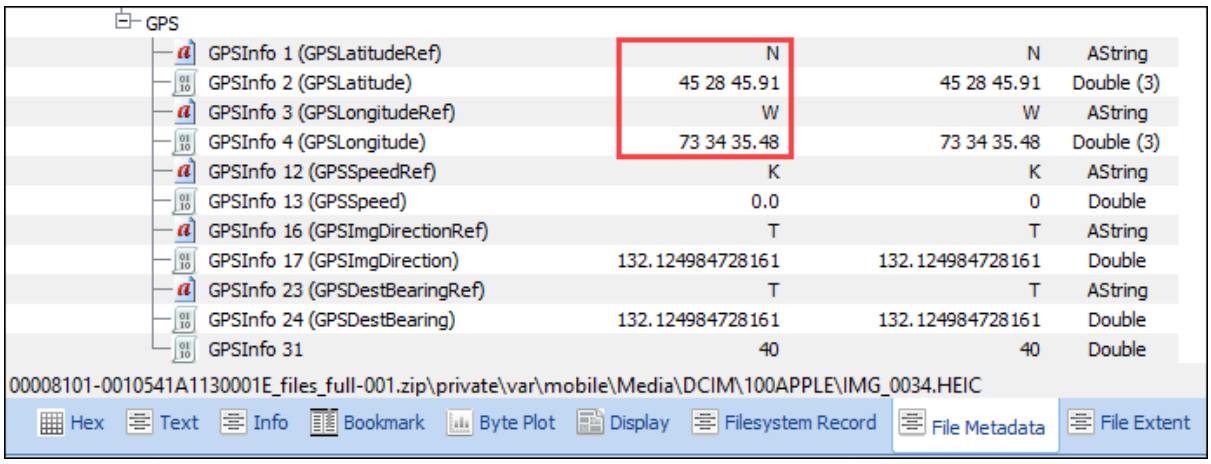


Pasquale tomato sauce was identified in the following picture:

\private\var\mobile\Media\DCIM\100APPLE\IMG_0034.HEIC

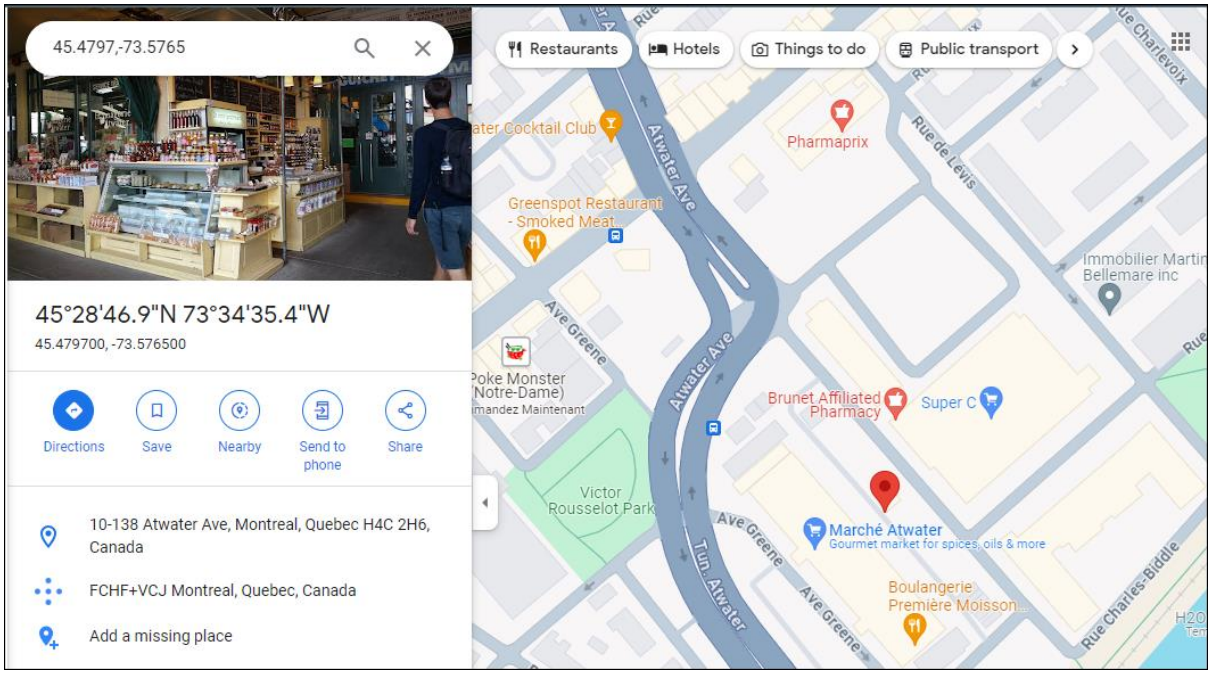
Switching to the **File Metadata** tab identifies the following GPS co-ordinates in **IMG_0034.HEIC**:

Figure 16: File System > File Metadata for IMG_0034.HEIC



Google Maps places the GPS co-ordinates near Marche Atwater, Montreal, Quebec, Canada.

Figure 17: Google Maps



QUESTION 6 - STAYING STYLISH! (10 POINTS)

What color shirt did the user choose to put their snapchat bitmoji in?

Q6. ANSWER

Green.

Q6. FORENSIC EXPLORER METHODOLOGY

Snapchat User Name is located in the **Artifacts module**:

- m_b227468

Figure 18: Artifacts > Snapchat User Name

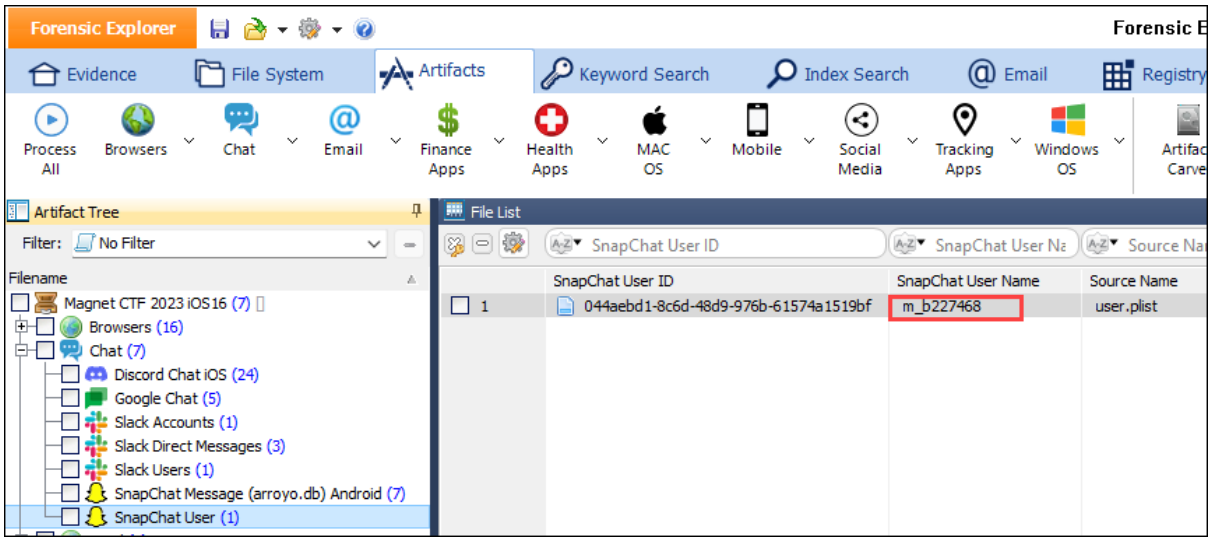
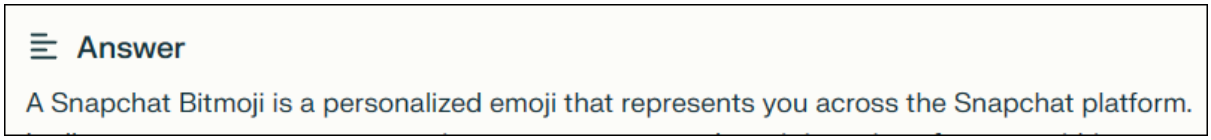


Figure 19: Perplexity - What is a Snapchat bitmoji?



A bitmoji can be access with the following URL: **https://www.snapchat.com/add/m_b227468**

Figure 20: Bitmoji - m_b227468

QUESTION 7 - PICKING UP STEAM (10 POINTS)

What server was the user interested in making?

Q7. ANSWER

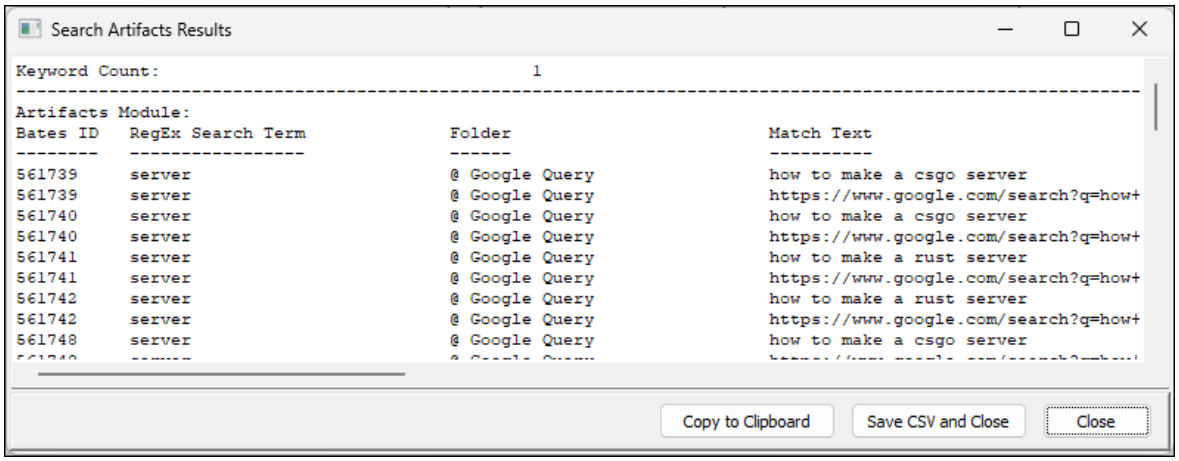
CSGO Server

Q7. FORENSIC EXPLORER METHODOLOGY

A search for the keyword server was conducted using **Search Artifact Results**.

Figure 21: Artifacts > Search Artifact Results toolbar button

Figure 22: Search Artifact Results output



Search Artifact Results identified Google browsing history and Discord chat as items of potential relevance.

Figure 23: Artifacts > Google Query

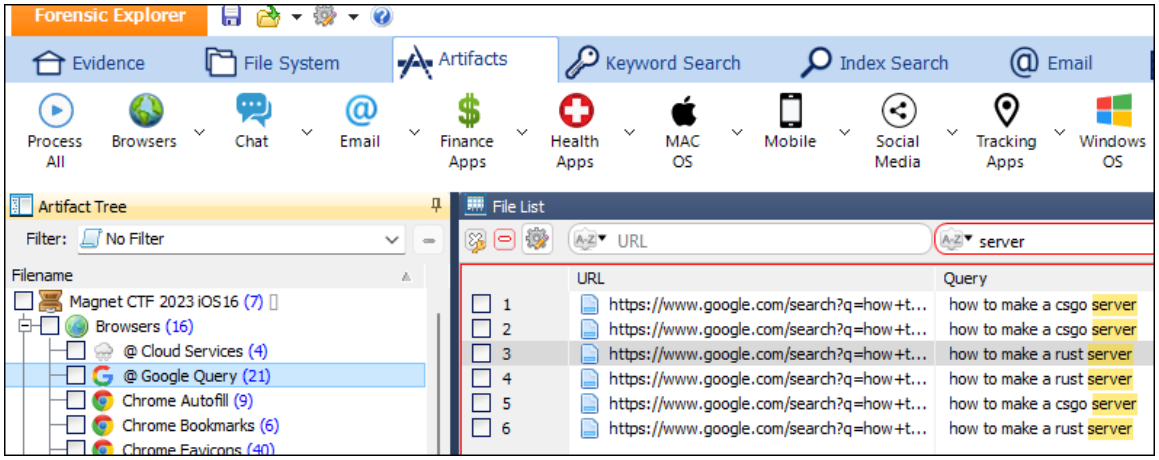
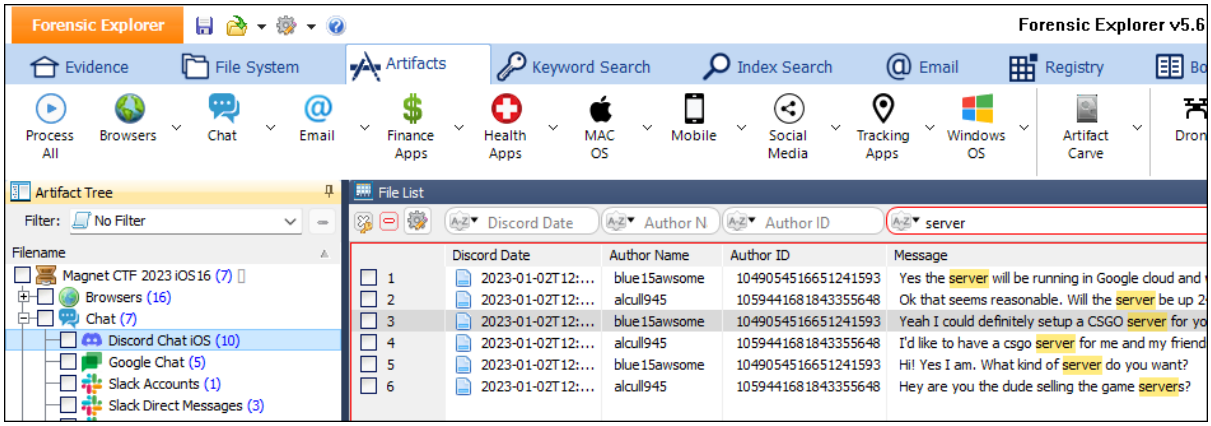


Figure 24: Artifacts > Discord Chat iOS



QUESTION 8 - OVERLOOKING EXCELLENCE (10 POINTS)

What Sports stadium was the user overlooking at Camille-Houde belvedere?

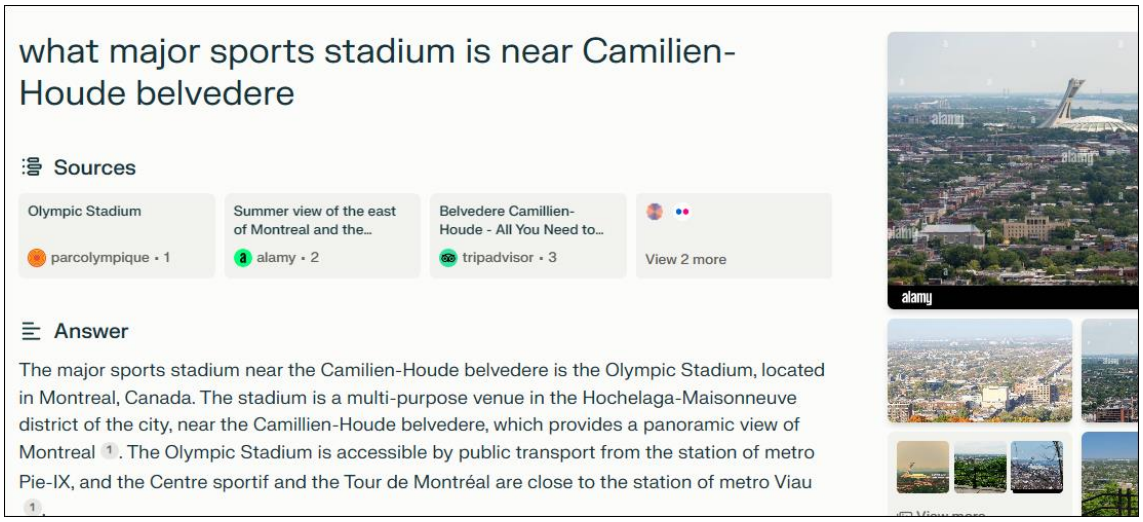
Q8. ANSWER

Stade Olympique (Montreal Olympic Stadium).

Q8. FORENSIC EXPLORER METHODOLOGY

Perplexity AI identifies that Camilien-Houde belvedere overlooks the Montreal Olympic Stadium.

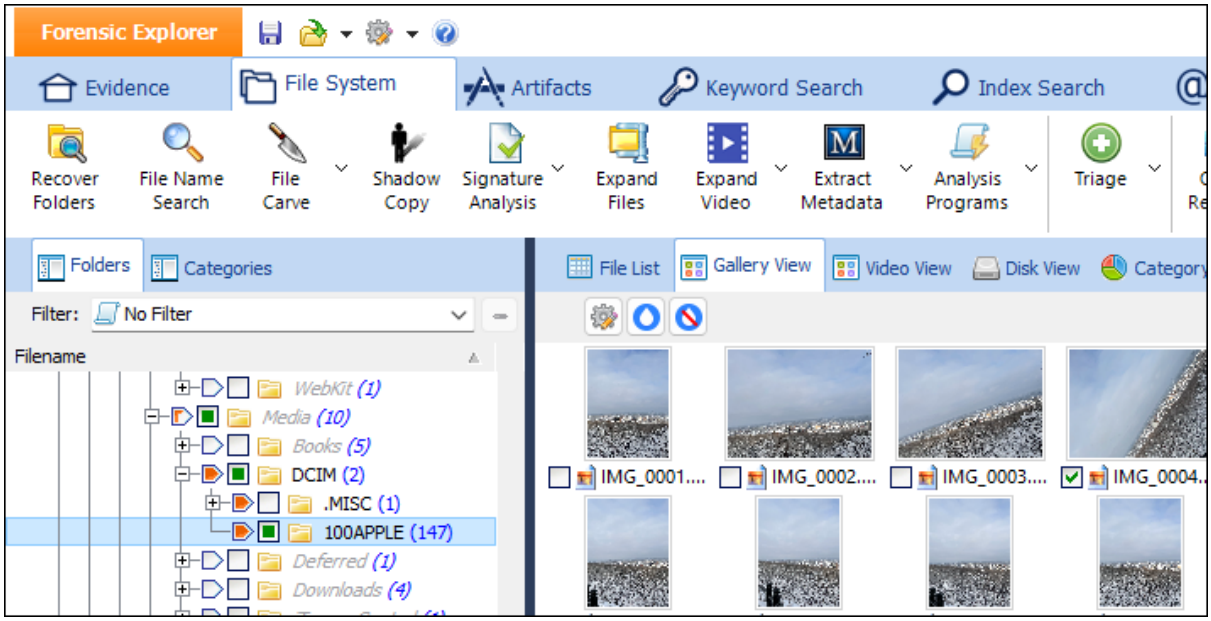
Figure 25: Perplexity AI



File System > Analysis Programs > GPS Google Earth KML Create shows that the iphone has been used to take numerous .HEIC photographs from this vantage point.

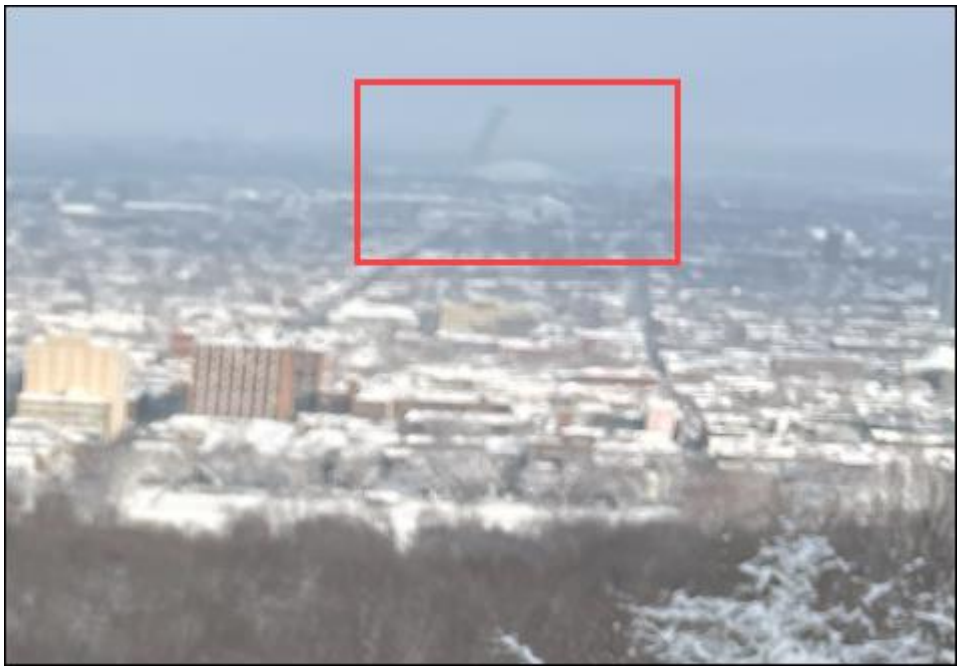
Figure 26: File System > Analysis Programs > GPS Google Earth KML Create

Figure 27: File System > Branch Plate > DCIM folder



Montreal Olympic Stadium is shown in a number of the photos.

Figure 28: Montreal Olympic Stadium



QUESTION 9 - YOU'RE GOING TO CRUSH THIS ONE! (10 POINTS)

What light-hearted game did the user spend the most time on?

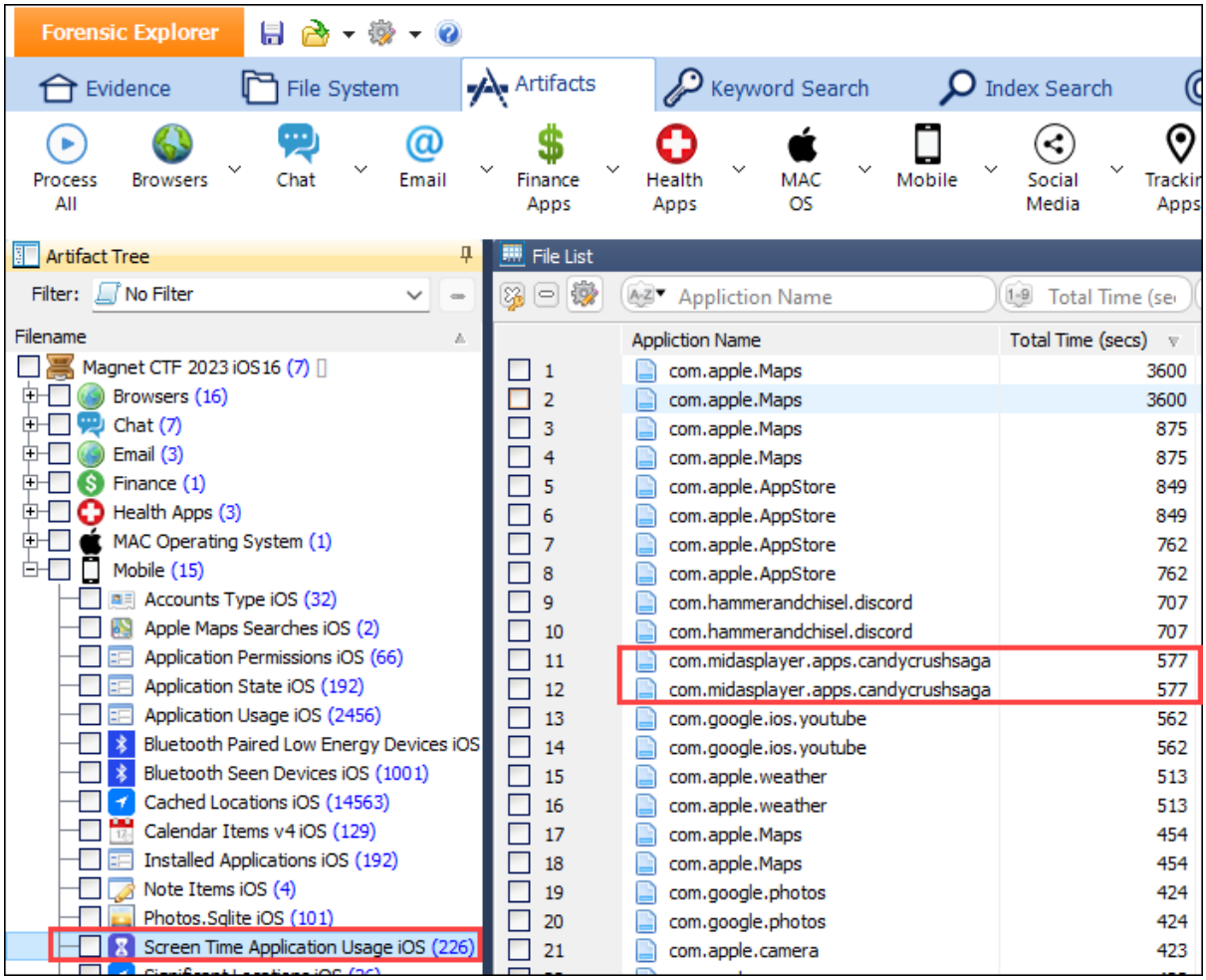
Q9. ANSWER

Candy Crush

Q9. FORENSIC EXPLORER METHODOLOGY

In the Artifacts module:

1. Mobile > Screen Time application Usage iOS.
2. Double click on the Total Time (secs) column header to sort by second.



The first light-hearted game listed is **candycrushsaga**.

QUESTION 10 - YOU ARE HERE (15 POINTS)

Which airline lounge was viewed?

Q10. ANSWER

Lufthansa.

Q10. FORENSIC EXPLORER METHODOLOGY

Artifacts > Search Artifact Results was used to search for the keyword **lounge**.

Figure 29: Artifacts > Search Artifact Results toolbar button

Figure 30: Figure 28: Artifacts > Search Artifact Results for "lounge"

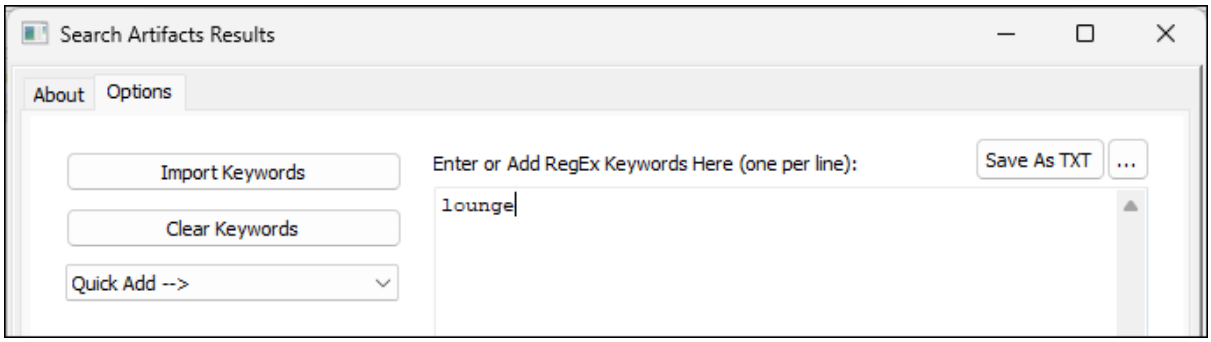
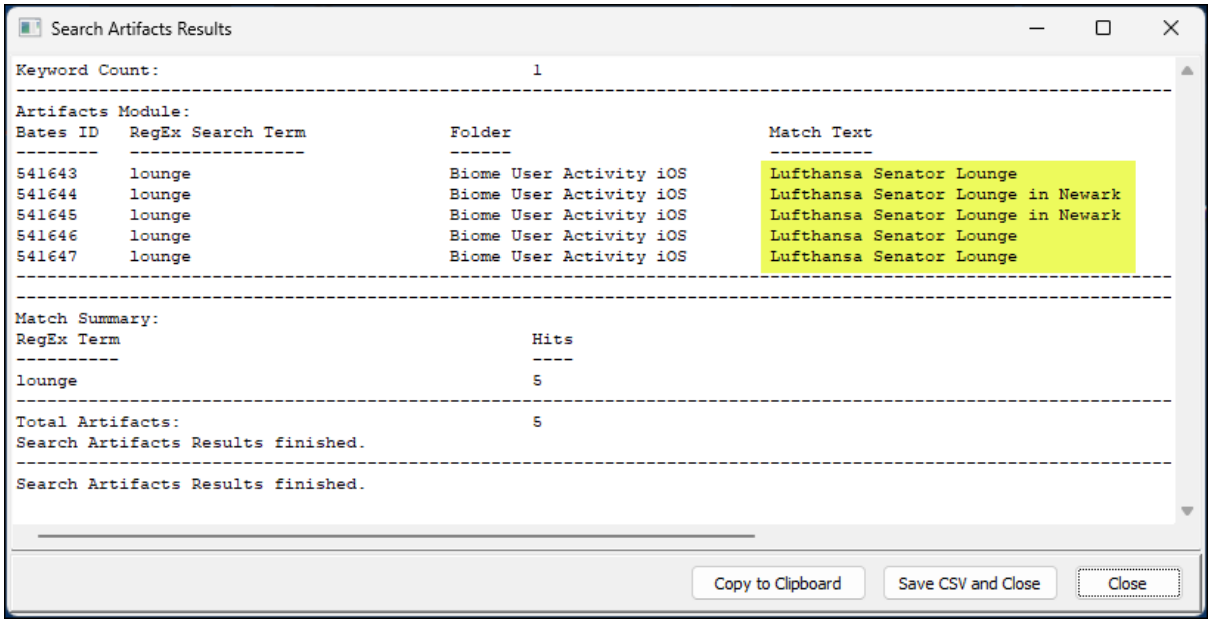
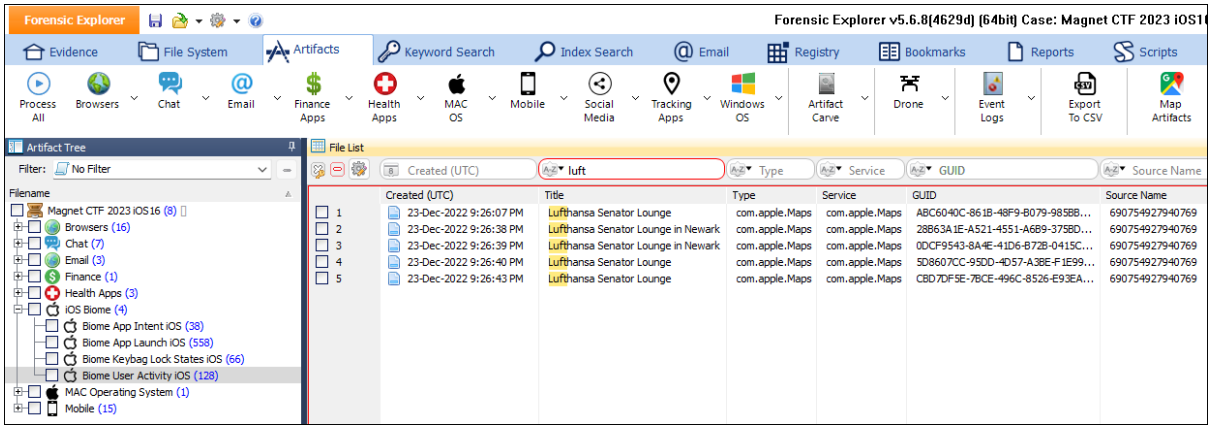


Figure 31: Figure 28: Artifacts > Search Artifact Results output



Artifacts > iOS Biome > Biome User Activity iOS was then examined.

Figure 32: Artifacts > Biome > Biome User Activity



QUESTION 11 - OUT OF THIS WORLD (25 POINTS)

Which terms and conditions site on Tik Tok is named after a space formation?

Q11. ANSWER

https://www.tiktok.com/falcon/forest/nebula/ad_legal

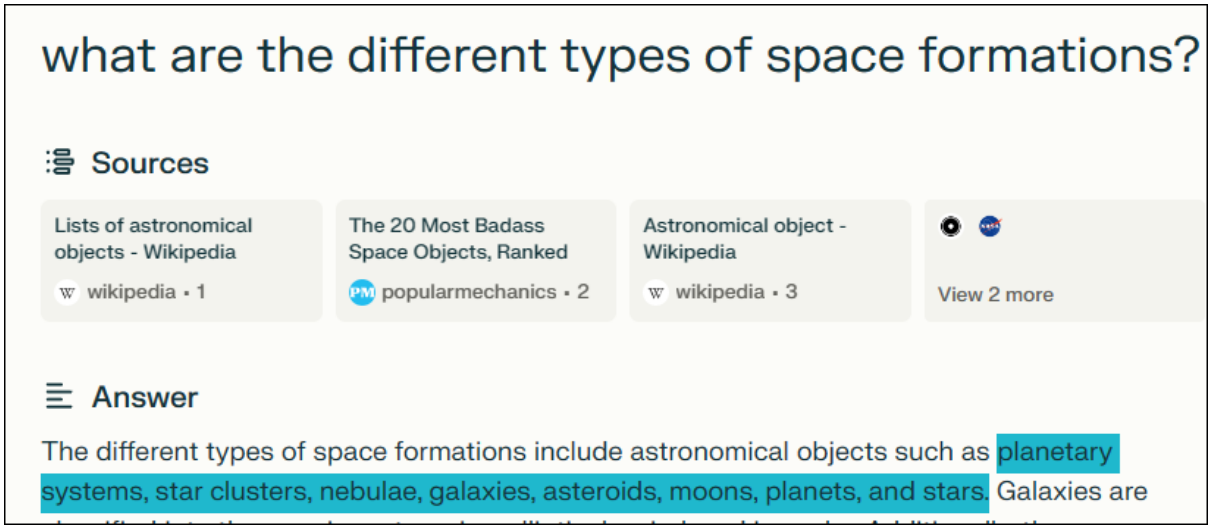
https://www.tiktok.com/falcon/forest/nebula/common_legal

Q11. FORENSIC EXPLORER METHODOLOGY

This question suggests that the answer will be in a TikTok URL.

A list of 'space formation' keywords was collected from Perplexity:

Figure 33: Perplexity



The keyword list used was:

- asteroid
- galax
- moon
- nebula
- planet
- star

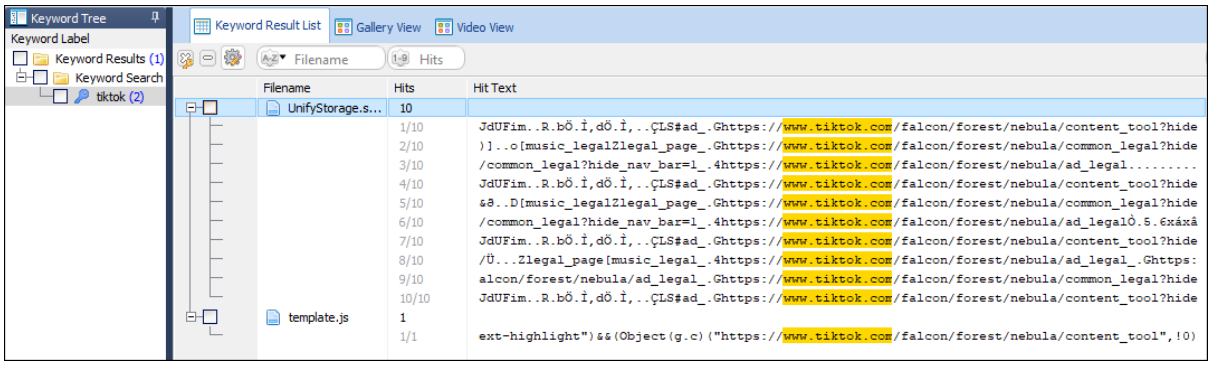
As a search of the Artifacts module did not return anything relevant.

The following RegEx search term was used in the **Keywords** module. This search term will locate **www.tiktok.com** within 5 words of any of the words in the keyword list:

\bwww\.tiktok\.com\b(?=(?:\W+\w+){0,5}\W+(asteroid|galax|moon|nebula|planet|star))

The search results identify **nebula** as a folder name in a **www.tiktok.com** URL relating to terms and conditions.

Figure 34: Keywords module search result



QUESTION 12 - WHICH WAY? (25 POINTS)

Which cardinal direction was the user turning when driving towards RHEINFAHRE?

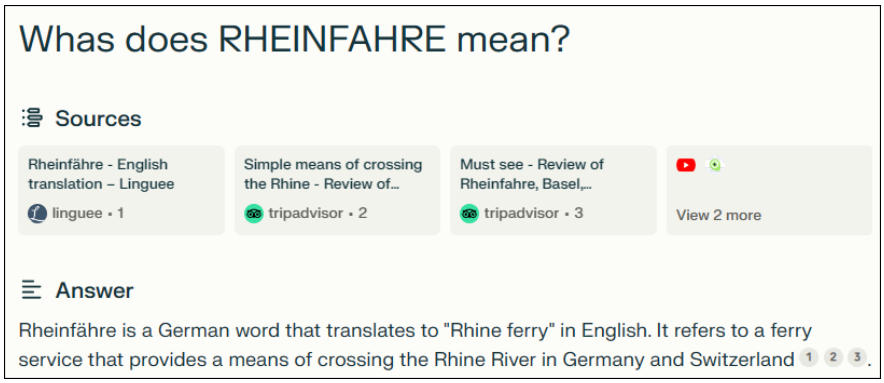
Q12. ANSWER

South.

Q12. FORENSIC EXPLORER METHODOLOGY

RHEINFAHRE is a German word that translates to “Rhine ferry”.

Figure 35: Perplexity - RHEINFAHRE

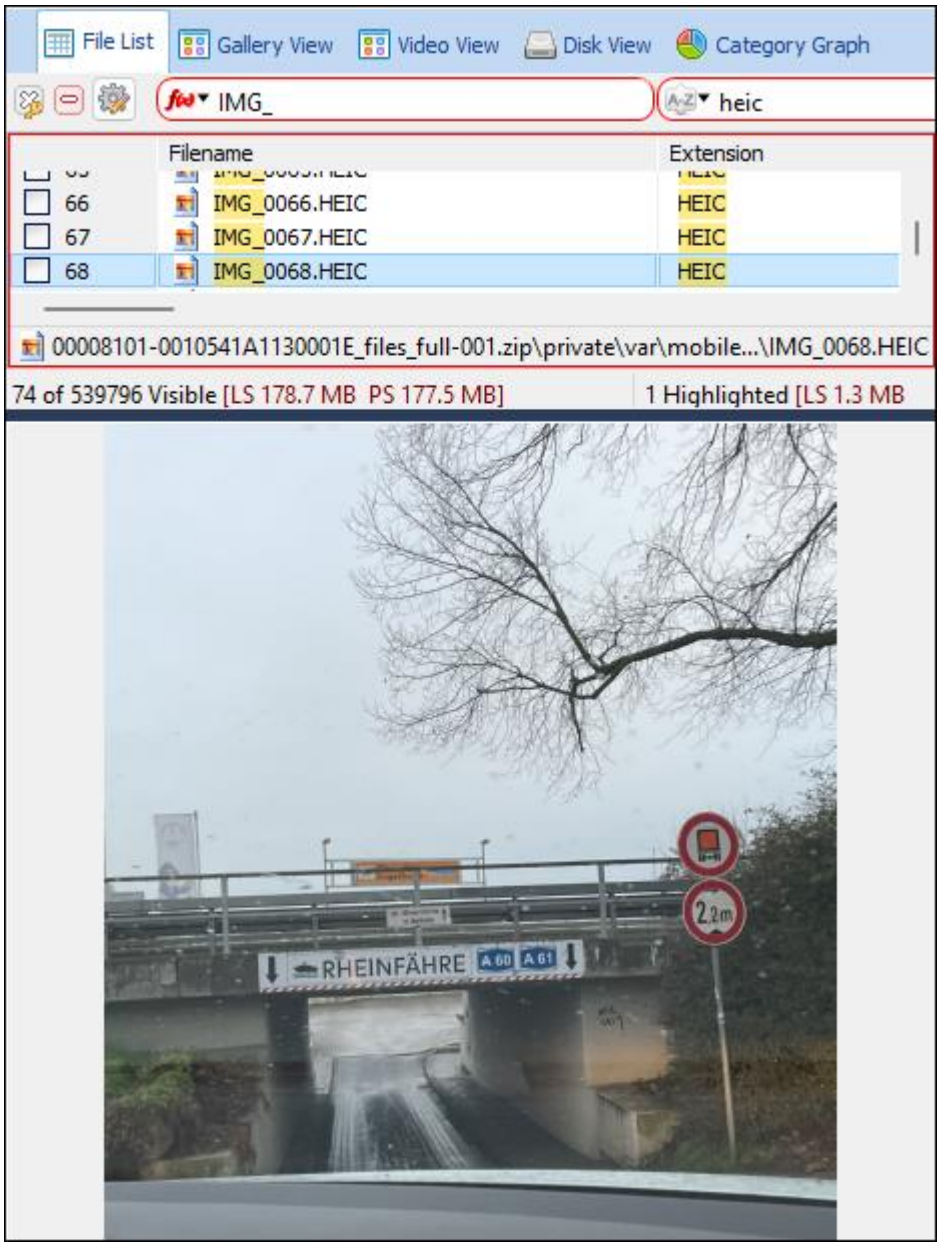


The **File System** > **Analysis Programs** > **GPS – Google Earth KML Create** script identifies **IMG_0068.HEIC** as a potential source.

Figure 36: File System > Analysis Programs > GPS - Google Earth KML Create

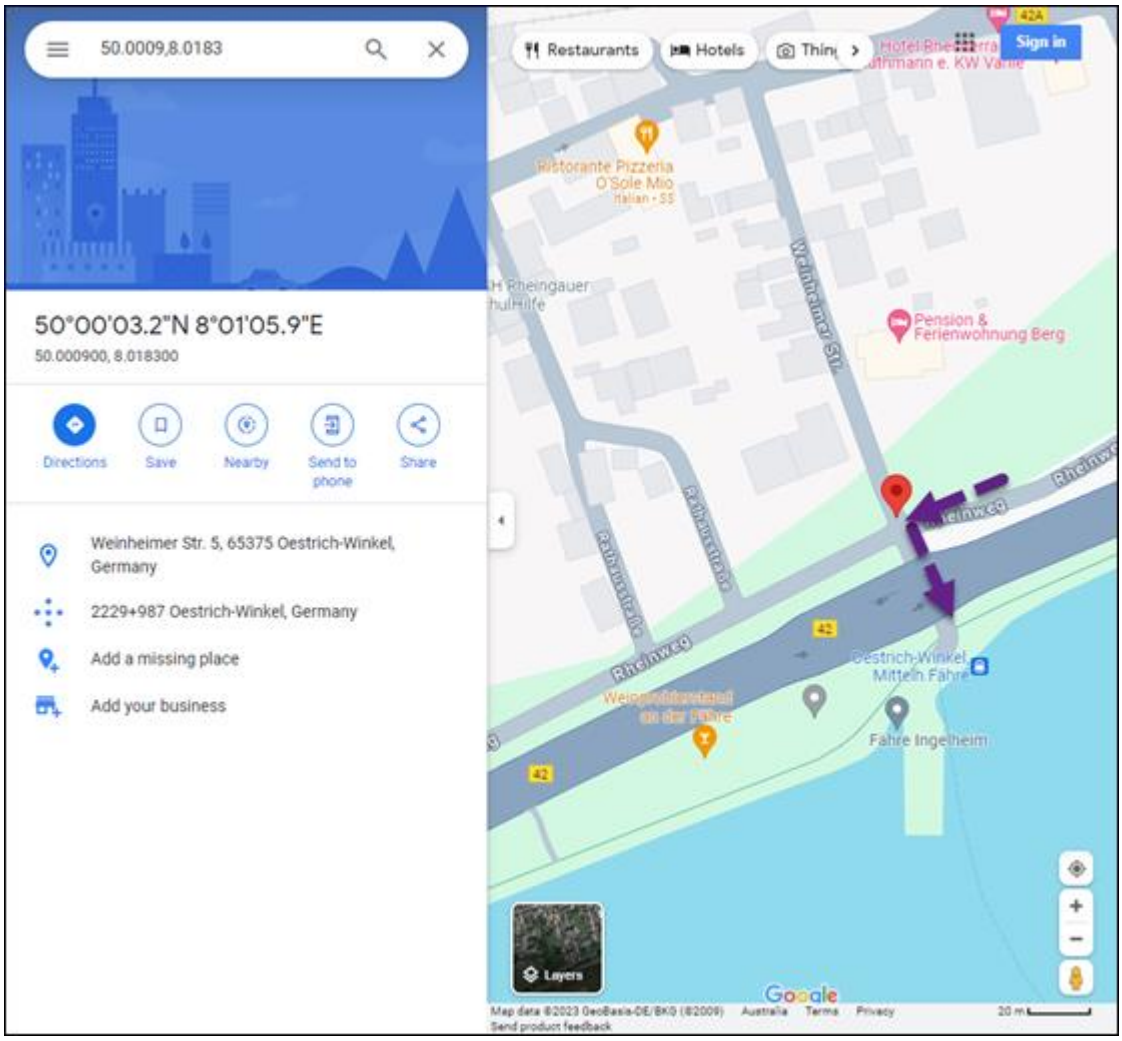
Examination of **IMG_0068.HEIC** (and its associated MOV file **IMG_0068.MOV**) show a **RHEINFAHRE** road sign.

Figure 37: IMG_0068.HEIC



Plotting the GPS co-ordinates indicates the direction of travel under the bridge toward the water is south.

Figure 38: Google Maps



QUESTION 13 - BOOSTING INTO A NEW ERA (25 POINTS)

The user was trying to learn German through an application, what promotion featuring a rocket was most commonly shown to the user?

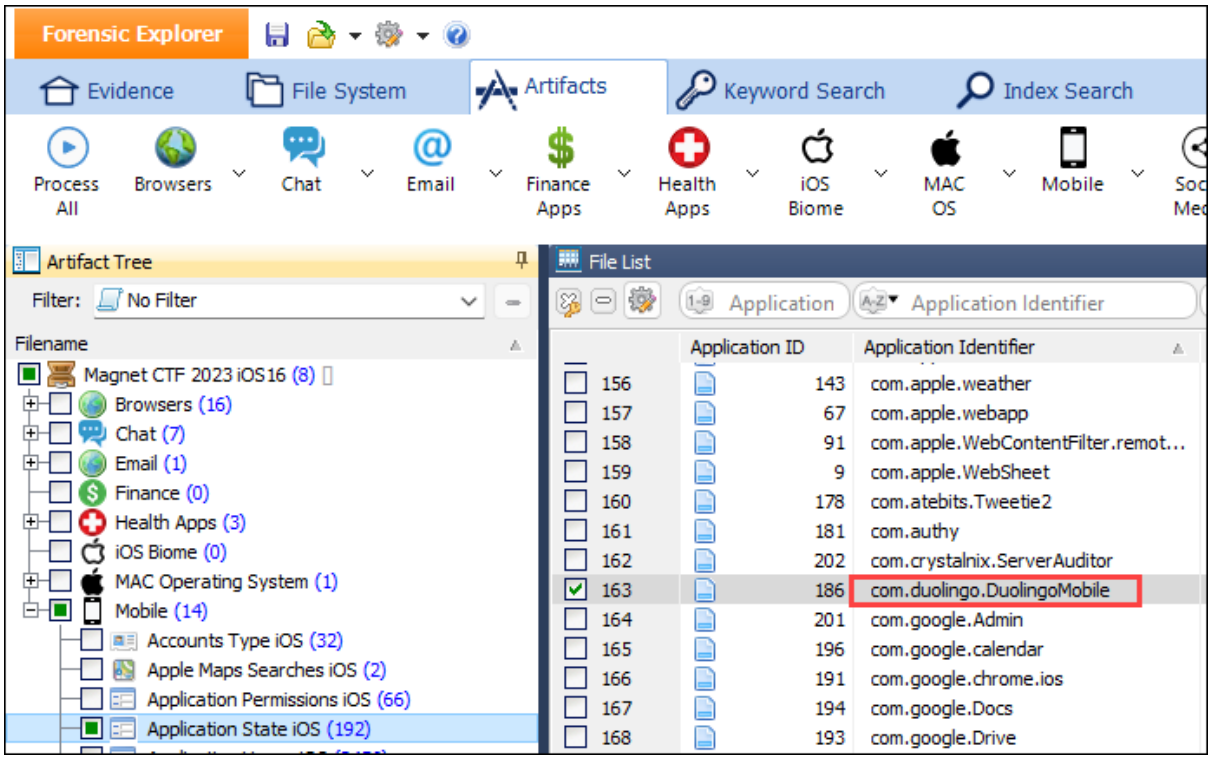
Q13. ANSWER

Super Duolingo

Q13. FORENSIC EXPLORER METHODOLOGY

A search of Artifacts > Application State iOS, for installed programs identified a language program called **com.duolingo.DuolingoMobile**.

Figure 39: Artifacts > Mobile > Application State iOS



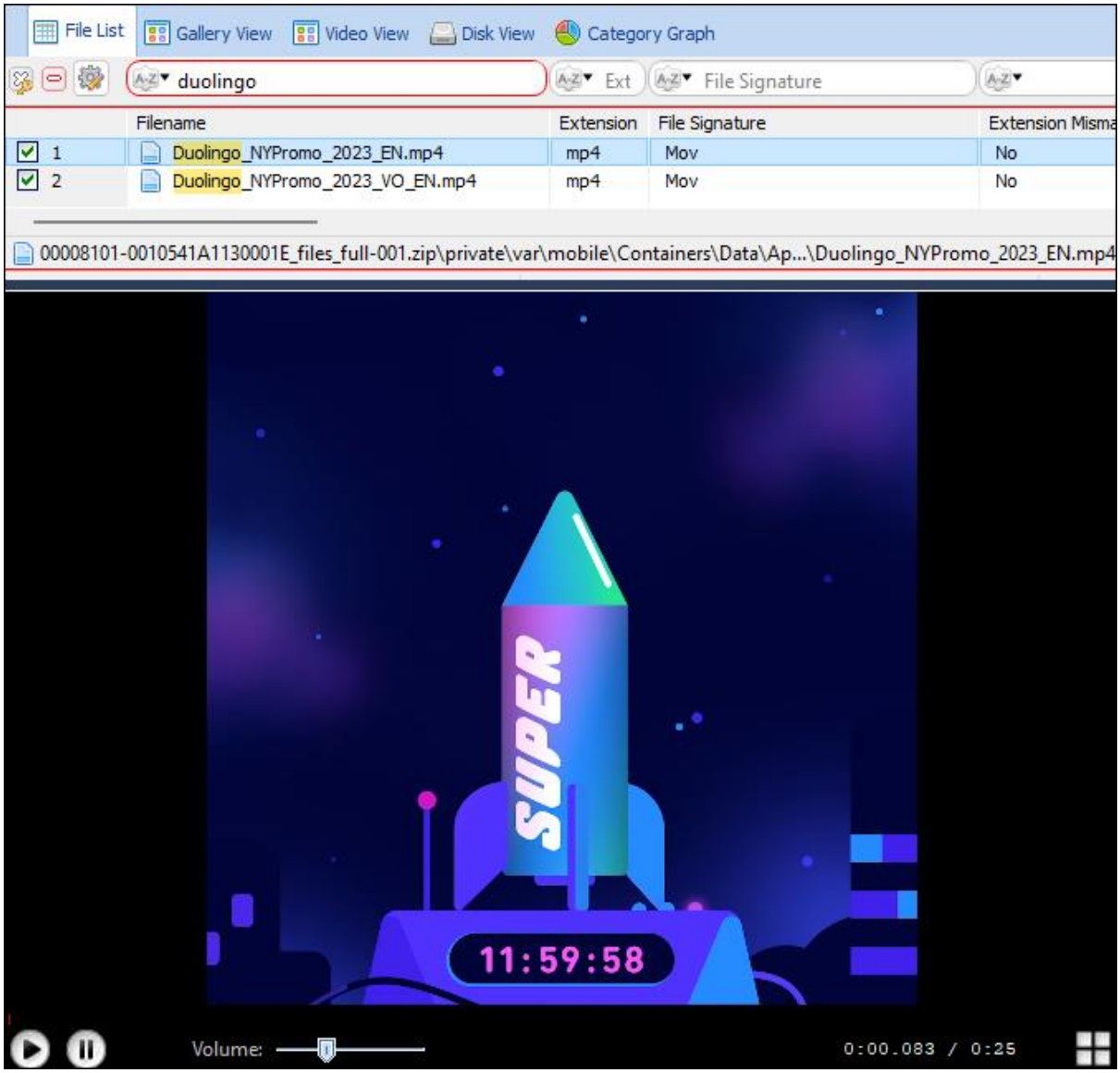
In the File System module:

1. In the File System module, branch plate [ ] the entire case.
2. In the Filename column, entry a column filter of **duolingo. Sixty-five** files were found.

A check of **Video** view identified a file called:

1. **Duolingo_NYPromo_2023_EN.mp4**
2. **Duolingo_NYPromo_2023_VO_EN.mp4**

Figure 40: Duolingo_NYPromo_2023_EN.mp4



QUESTION 14 - AS A RIVER RUNS (50 POINTS)

At which location did the user travel the most metres according to Apple? (City, Country)

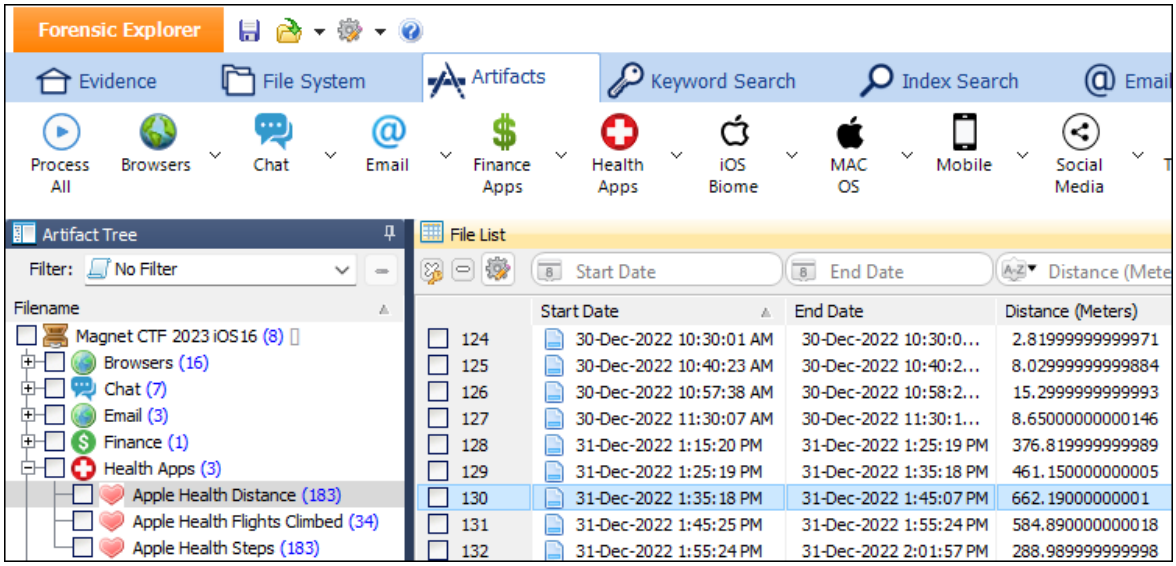
Q14. ANSWER

Eltville, Germany.

Q14. FORENSIC EXPLORER METHODOLOGY

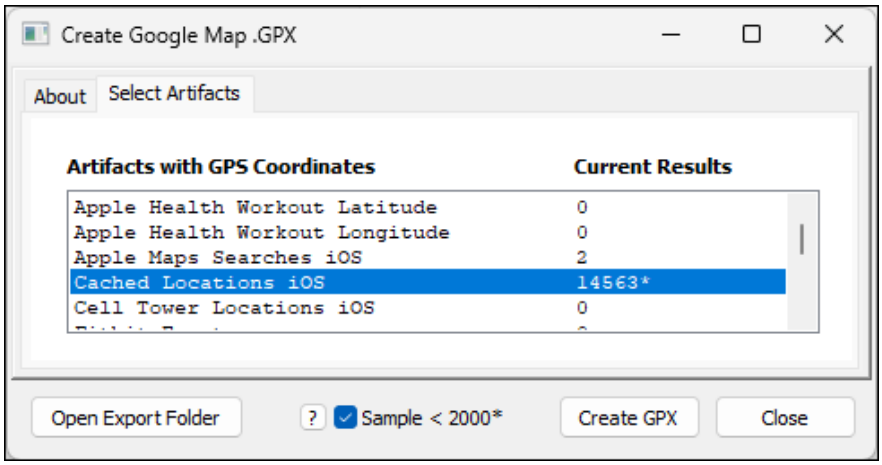
Apple records distance in the **Apple Health App**. The longest distance logged, 662 meters, was on **31 December 2022**.

Figure 41: Artifacts > Health Apps > Apple Health Distance



There is no GPS location information in the available Health App data. The **Artifacts > Map Artifacts button** if a fast method to determine what other common GPS data points are available. **Cached Locations** is a suitable candidate.

Figure 42: Artifacts > Map Artifacts



An examination of **Artifacts > Mobile > Cached Locations** shows that latitude and longitude information was collected at a similar time on 31 December 2022.

Figure 43: Artifacts > Mobile > Cached Locations

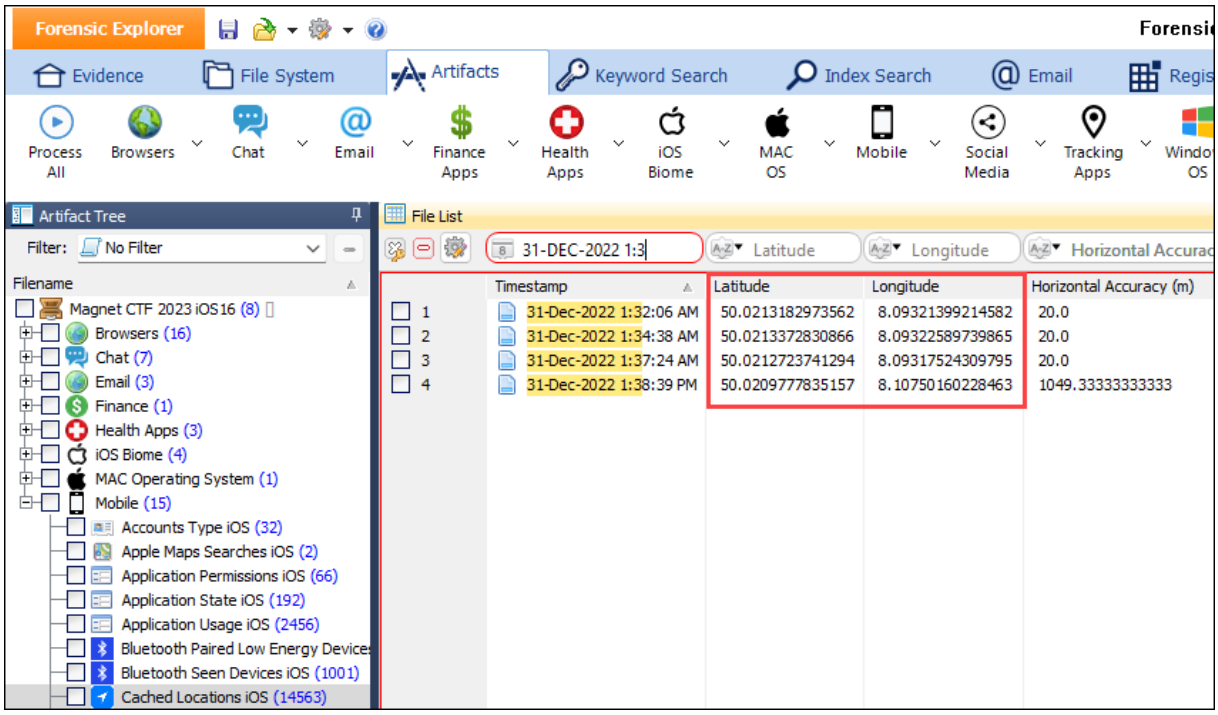
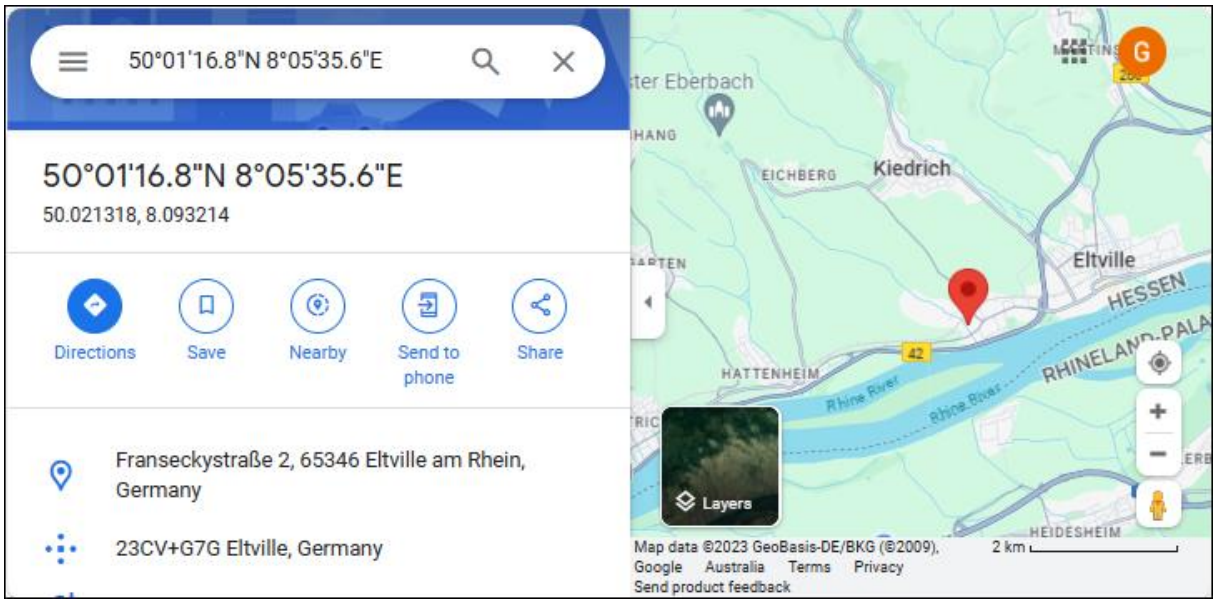


Figure 44: Google Maps coordinates



QUESTION 15 - LO SIENTO SENOR, ITS GOING TO BE A COLD ONE (50 POINTS)

What weather front was warned to the user by YouTube?

Q15. ANSWER

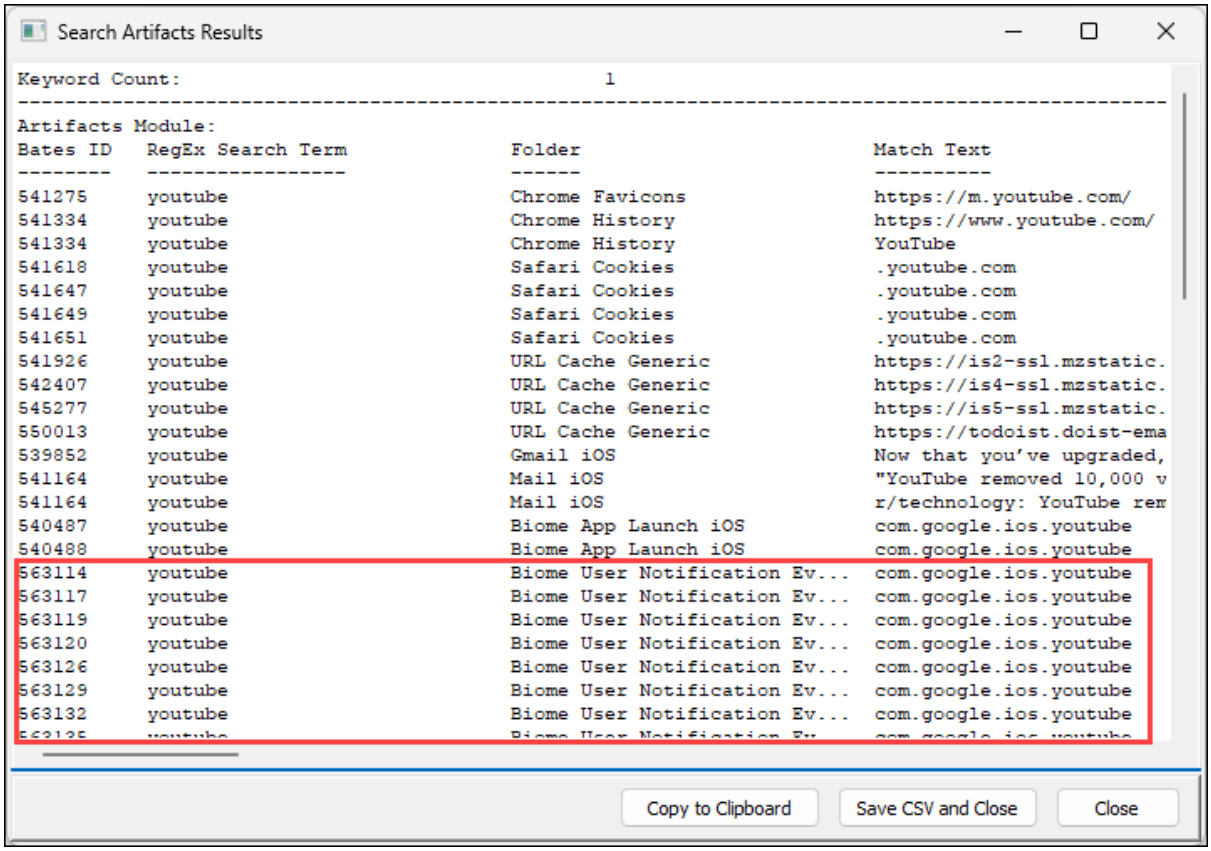
Artic front.

Q15. FORENSIC EXPLORER METHODOLOGY

The clues in the question are the use of Spanish and “YoutTube”.

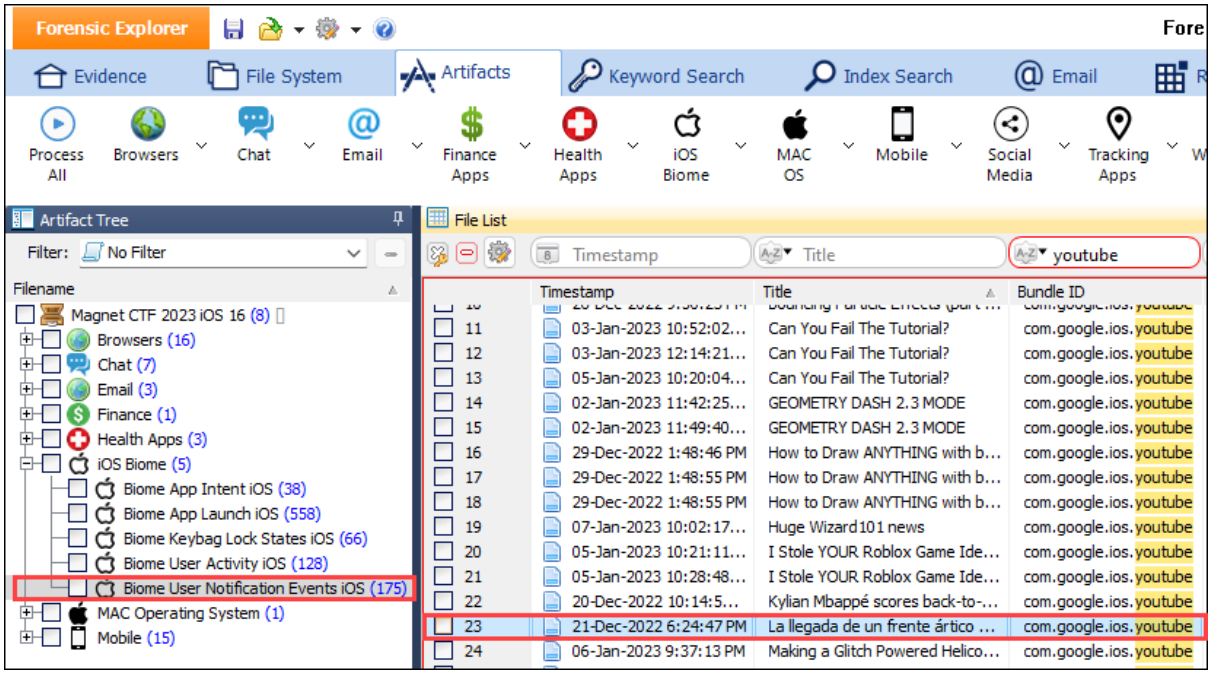
Artifacts module > Search Artifact Results > **youtube** produced the following result:

Figure 45: Search Artifact Results



A closer examination of Artifacts > **Biome user Notification Events** located the following entry with a Spanish title:

Figure 46: Artifacts > iOS Biome > Biome User Notification Events



The full Spanish text:

> *"La llegada de **un frente ártico** hará que el 80% de EEUU experimente sensaciones térmicas congelantes"*

Translated using Google is:

> *"The arrival of an **arctic front** will cause 80% of the US to experience freezing thermal sensations".*