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

CTF Questions Only	2
About This CTF Challenge	4
Starting this challenge in Forensic Explorer	5
Question 1 - A few too many - (5 points)	6
Question 2 - Autofill me on the deets (5 points)	8
Question 3 - 1 fish 2 fish, red fish blue (5 points)	9
Question 4 - Q-uestion (5 points)	10
Question 5 - Chef boyardee 2.0 (10 points)	14
Question 6 - Staying stylish! (10 points)	16
Question 7 - Picking up steam (10 points)	17
Question 8 - Overlooking excellence (10 points)	19
Question 9 - You're going to crush this one! (10 points)	21
Question 10 - You are here (15 points)	22
Question 11 - Out of this world (25 points)	24
Question 12 - Which way? (25 points)	26
Question 13 - Boosting into a new era (25 points)	29
Question 14 - As a river runs (50 points)	31
Question 15 - Lo siento senor, its going to be a cold one (50 points)	33

# 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
5	Chef boyardee At which market was the user viewing Chef Pasquale tomato sauce? Staying stylish! What color shirt did the user choose to put their snapchat bitmoji in?	10
5 6 7	Chef boyardee At which market was the user viewing Chef Pasquale tomato sauce? Staying stylish! What color shirt did the user choose to put their snapchat bitmoji in? Picking up steam What server was the user interested in making?	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

Evidence	
	Magnet CTE 2023 (OS16 (1)
Add device	00008101-0010541A1130001E_files_full-001.zip (0)
📄 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.

Forensic Explorer	🖶 👌 🗸	🌼 🗕 🔞		
Evidence	File Syst	em 🚽	Artifacts	
Process Browsers ~	🜪 <sub>Chat</sub> ~	(0) Email	Finance Apps	He At
Artifact Tree			🕂 🛄 File	List
Filter: 🗾 No Filter		~	- 00	۱
Filename				
Magnet CTF 2023 iC Magnet CTF 2023 iC Chat (6) Chat (6) Chat (6) Magnet CTF 2023 iC Chat (6) Chat	DS16 (7) [] t iOS (1) System (1)			

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

Forensic Explorer 📙 🚵 👻 🛞				
合 Evidence 🗋 File System 🗚	rtifacts	P Keyword Search	${oldsymbol{ ho}}$ Index Searc	ch 🔘 Email
Process Browsers Chat Email F	inance Ha Apps A	ealth v MAC v pps OS	Mobile × Social Media	V Tracking Windows OS
Artifact Tree 4	🛄 File List			
Filter: 💭 No Filter 🗸 🚽	1 - Sector Secto	Timestamp	Account Desc	€Z▼ Username
Filename 🔺		Timestamp	Account Description	Username 🔺
Magnet CTF 2023 iOS16 (7)	1	21-Nov-2022 12:4	IDMS	blueisth3best@icloud.com
🗄 🗌 🎯 Browsers (16)	2	21-Nov-2022 12:4	Apple ID	blueisth3best@icloud.com
🕂 🗌 晃 Chat (6)	3	21-Nov-2022 12:4	Game Center	blueisth3best@icloud.com
🕀 🗌 🎯 Email (3)	4	21-Nov-2022 12:4	Messages	blueisth3best@icloud.com
🕀 🔄 S Finance (1)	5	21-Nov-2022 12:4	CloudKit	blueisth3best@icloud.com
🕀 🗌 🛟 Health Apps (3)	6	21-Nov-2022 12:4	iCloud	blueisth3best@icloud.com
🕀 🔜 🔹 MAC Operating System (1)	7	21-Nov-2022 12:4	IMAPMail	blueisth3best@icloud.com
□ □ □ □ Mobile (15)	8	21-Nov-2022 12:4	Device Locator	blueisth3best@icloud.com
Accounts Type iOS (32)	9	21-Nov-2022 12:4	Find My Friends	blueisth3best@icloud.com
Apple Maps Searches iOS (2)	10	21-Nov-2022 12:4	iTunes Store	blueisth3best@icloud.com
Application Permissions iOS (66)	11	21-Nov-2022 12:4	IDMS	blueisth3best@icloud.com

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

Forensic Explorer 🚦 🚵 🗸 🎲 🗸	0						Forensic Exp
Tile System	A	Artifacts	P Keyword	Search	<b>P</b> Index Search	@ Emi	ail 🔠 Registry
Process Browsers - Chat - Emai	I *	\$ Finance Apps	Health Apps	IAC N DS	Nobile ~ Social ~	♥ Tracking Apps ~	Windows OS Artifact Carve
I Artifact Tree	џ	🛄 File List					
Filter: 🗾 No Filter	~ -	🛛 🖗 🖻 🔯	B Date Cre	ated	🐼 🕶 Origin URL		Username Value
Filename			Date Created		Origin URL	Userna	ame Value
Magnet CTF 2023 iOS 16 (7)		1	12-Dec-20	022 11:3	https://account.proton.m	e/login micha	elkborchardt@proton.me
E- Browsers (16)		2	28-Dec-2	022 5:00	https://mstdn.party/auth	/sign_up borch	nardtmichael78@gmail.com
Cloud Services (4)							
G @ Google Query (21)							
Chrome Autofill (9)							
Chrome Eavirons (40)							
Chrome History (21)							
Chrome Keyword Search Terms (7)							
Chrome Logins (2)							

### 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

Forensic Explorer 🚦 🚵 🔻 🎲 👻 📀			
合 Evidence 🛛 File System 🗚 A	rtifacts	P Keyword Search	Index Search 🛛 🔘 Email
Process Browsers Chat Email Fi	\$ inance H Apps	Health Apps OS MAC	<ul> <li>Social Media</li> <li>Media</li> &lt;</ul>
📕 Artifact Tree म	🧮 File List		
Filter: 🔄 No Filter 🗸 🚽	🖗 – 🔯	Date Created	🐼 Value
Filename 🔺		Date Created	Value
Magnet CTF 2023 iOS 16 (7)	1	12-Dec-2022 11:36:54 PM	michaelkborchardt@proton.me
E- Browsers (16)	2	28-Dec-2022 5:00:22 PM	borchardtmichael78@gmail.com
Cloud Services (4)	3	28-Dec-2022 4:21:42 PM	borchardtmichael78@gmail.com
G @ Google Query (21)	4	03-Jan-2023 1:01:09 AM	private-test
Chrome Autofill (9)	5	03-Jan-2023 1:08:20 AM	private
Chrome Bookmarks (6)	6	03-Jan-2023 1:05:11 AM	Testing
Chrome Favicons (40)	7	03-Jan-2023 12:54:31 AM	private testing
Chrome History (21)	8	03-Jan-2023 1:05:11 AM	Private
Chrome Keyword Search Terms (7)	9	05-Jan-2023 3:15:20 AM	tlouis@kurvalis.com
Chrome Logins (2)			

# 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 🚦 🚵 👻 🎯				
合 Evidence 🛛 🎦 File System	A	rtifacts	🔑 Keyword Search	🔎 Index Search
Process Browsers Chat Email	۲ Fi	\$ nance H Apps	ealth MAC N Apps OS	lobile × Social × Tr Media
📰 Artifact Tree	Ţ,	🌐 File List		
Filter: 🔄 No Filter 🗸 🗸		🖗 🖻 🔯	🐼 🕶 linkedin	Source Name
Filename			Application	Source Name
Magnet CTF 2023 iOS16 (7)		1	com.linkedin.LinkedIn	applicationState.db
Chat (6) Maccounts (0) Maccounts (0) Mobile (14) Mobile (14) Mobile (14) Accounts Type iOS (32) Application Permissions iOS (66) Application Variable iOS (192) Application Usage iOS (2456) Bluetooth Paired Low Energy Devices iO Bluetooth Seen Devices iOS (1001) Cached Locations iOS (14563) Calendar Items v4 iOS (129) Installed Applications iOS (192)	S (1)			

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

Forensic Explor	er 📙 🚵 🗸	🌼 <b>-</b> 🔞	)					
合 Evidence	File Sys	stem	Artifacts	5 <i>[</i> ]	Э Кеуи	ord Search	🔎 Ind	lex Search
Recover File Na Folders Searc	me File ~ h Carve	Shadow Copy	Signature Analysis	Expand Files	Expand Video	Extract Metadata	Analysis Programs	Triage
Folders Categories File List Signalery View Signalery View								
Filter: 🗾 No Filter				~		🖗 🖻 🔯 (	▲Z▼ linkedin	
Filename					▲		Filename	
		67879-C7BD	-4906-8865-EAE	0AA4E6236	5 (4)	✓ 1	🔚 LinkedIn.a	арр
	Ė-▶☑ 🚞	LinkedIn.app	(112)			2	📄 LinkedIn	
	🕂 🕀 🔄 ABIResources.bundle (26) 🛛 🗹 3 💼 🖬 linkedin_logo_dark.prg							
	🕂 🕒 🖳 AnalyticsResources.bundle (26) 🛛 🗹 4 📓 linkedin_logo_dark.png							
		🚞 ar.lproj (	3)			5	LinkedIn.	sinf
	<b>₽_₽</b>	Assets.b	undle (1)			6	LinkedIn.	supf

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.

		_											
Forensic	Explorer	🗟 🗟	- 🕸 - 🔇									Fore	ensic
合 Evide	ence	File S	System	Artifact	is 🖉	🔉 Keyı	vord	Search	${oldsymbol{ ho}}$ Index	Search	(C) Email	∎∎ F	Regist
Recover Folders	C File Name Search	File Carve	∑ Shadow Copy	Signature ~ Analysis	Expand Files	Expan Video	d ~	Extract Metadata	Analysis Programs	Triage ~	Quick Registry	File	
Folders	Categ	ories						🖩 File List	🔋 Gallery View	🔋 Video Viev	v 🔚 Disk View	🕙 Cate	gory G
Filter: 🗐 N	No Filter				`````	/ -	<b>B</b>	- 🔯	Az▼ Filename			AZ▼ Ext	A-Z-
Filename						Δ.			Filename			Extension	File
	Ē-		RE60DE7D-COA	E-4527-89C4-45	59C111EBC5	8 (4)		1	CodeSignat	ure			Fol
	. ⊨		411B7ABF-E85.	2-444A-8436-B3	5BF0B9A6CL	3 (4)		2	aBIResource	s.bundle			Fol
	- P-	P 🗖 🔁 🗧	1D867879-C7Bl	D-4906-8865-EA	E0AA 4E623	6 (4)		3	📔 AnalyticsRes	ources.bundle			Fol
		ė- 🖻 🗹 📴	LinkedIn.ap	p (112)				4	🚞 ar.lproj				Fol
		₽-₽-	🛯 🚞 ABIReso	urces.bundle (2	6)			5	📔 Assets.bund	e			Fol
		₽₽	🖌 📄 Analytic	Resources.bun	dle (26)			6	📔 CareersReso	urces.bundle			Fol
			🖌 📄 ar.lproj	(3)				7	📔 ChameleonRe	esources.bundle			Fol
		₽₽₽	🖊 🚞 Assets.t	oundle (1)				8	Conversation	sResources.bur	ndle		Fol
		₽₽₽	Careers	Resources.bund	le (26)			9	📄 cs.lproj				Fol
		<b>P</b>	🖞 📴 Chamele	onResources.bu	undie (2)	. 1		10	📄 da.lproj				Fol
		- +- <b>&gt;</b>	Convers	ationsResource	s.bundle (26		-						
			🛯 🚞 cs.lproj	(3)									
			🖞 🚞 da.lproj	(3)			4708	of 4708	/isible [LS 305.0 M	IB PS 116.1 MP	31 4	708 Highli	ahted
			🖞 🔚 de.lproj	(3)					121212 [25 56510 11				9

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

🔡 Edit Keyword	
Search Type:	Regular Expression (PCRE) $\sim$
Keyword Label:	Websites - \bhttps?://\S+?\b
Search Term:	\bhttps?://\S+?\b
Case Sensitive:	0
Status:	Regex OK

### 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 13.

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

Figure 12: Keyword Search on checked items only

👹 Keywo	rd Search 12 Options	_		×			
Process Nar	ne:						
Search Link	edIn for websites						
Source							
Module:	FileSystem			$\sim$			
◯ Sea	rchable Items (539795 items, 17.81 GB)						
	Unallocated space						
O Che	Checked items (4709 items 305.0 MB)						
	Include Raw Devices, Partitions and Files						

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 v	Hit Text	Hit Offset (File)
84/180	nding_endorsementhttps://hangouts.google.com/start	65604400
85/180	com/start	65604448
86/180	fView:)profil	65642240
87/180	<pre>//user?screen_name=http://twitter.com/profil</pre>	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/	65643312
91/180	ewModel()https://www.linkedin.com/help/linked	65674528
92/180	trend	65679568

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

# 

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:



Ė− gps							
GPSInfo 1 (GPSLatitudeRef)	Ν	I N	AString				
- 🗊 GPSInfo 2 (GPSLatitude)	45 28 45.91	45 28 45.91	Double (3)				
- a GPSInfo 3 (GPSLongitudeRef)	W	/ W	AString				
- 🔢 GPSInfo 4 (GPSLongitude)	73 34 35.48	3 73 34 35.48	Double (3)				
- a GPSInfo 12 (GPSSpeedRef)	k	с к	AString				
- I GPSInfo 13 (GPSSpeed)	0.0	0 0	Double				
- a GPSInfo 16 (GPSImgDirectionRef)	1	гт	AString				
- 🗊 GPSInfo 17 (GPSImgDirection)	132.124984728161	1 132.124984728161	Double				
<ul> <li>— a GPSInfo 23 (GPSDestBearingRef)</li> </ul>	1	г т	AString				
- 🛒 GPSInfo 24 (GPSDestBearing)	132.124984728161	1 132.124984728161	Double				
GPSInfo 31	40	9 40	Double				
00008101-0010541A1130001E_files_full-001.zip\private\var\mobile\Media\DCIM\100APPLE\IMG_0034.HEIC							
🛗 Hex 🚍 Text 🚍 Info 🧾 Bookmark 🔐 Byte	e Plot 📑 Display 🚔 Filesys	stem Record 🗏 File Metadata	🚍 File Extent				

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

Forensic Explorer 🚦 🚵 👻 🍘					Forensic E
合 Evidence 📄 File System 📌	Artifacts	P Keyword Search	🔎 Index Sear	ch 🔘 Email	Registry
Process All Browsers × Chat × @	Finance Apps	Health Apps OS	Mobile × Social Media	Tracking Windo Apps OS	ws × Artifac Carve
Artifact Tree	🛄 File List				
Filter: 🔄 No Filter 🗸 🚽	) 🖗 🖻 🖗	Image: A state of the state		Image: SnapChat User Na	Source Na
Filename 🔺		SnapChat User ID		SnapChat User Name	Source Name
Magnet CTF 2023 iOS 16 (7)	1	044aebd1-8c6d-48d	9-976b-61574a1519bf	m_b227468	user.plist
Browsers (16)					
Chat (7)					
Goode Chat (5)					
- Slack Accounts (1)					
SnapChat Message (arroyo.db) Android (7)					
🗌 🤁 SnapChat User (1)					

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 /	Artifacts Results		– – ×
Keyword Co	ount:	1	
Artifacts	Module:		
Bates ID	RegEx Search Term	Folder	Match Text
561739	server	@ Google Query	how to make a csgo server
561739	server	@ Google Query	https://www.google.com/search?q=how+
561740	server	@ Google Query	how to make a csgo server
561740	server	@ Google Query	https://www.google.com/search?q=how+
561741	server	@ Google Query	how to make a rust server
561741	server	@ Google Query	https://www.google.com/search?q=how+
561742	server	@ Google Query	how to make a rust server
561742	server	@ Google Query	https://www.google.com/search?q=how+
561748	server	@ Google Query	how to make a csgo server
5 61 7 4 0		A C1- C	······································
			Copy to Clipboard Save CSV and Close Close

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

### Figure 23: Artifacts > Google Query

Forensic Explorer 📑 🚵 🔻 🛞 👻				
合 Evidence 🛛 🗋 File System 🗚	Artifacts	P Keyword Search	🔎 Index Searc	h 🔘 Email
Process Browsers Chat Email	\$ Finance H Apps	ealth Apps OS	Mobile V Social Media	V Tracking Apps V Windows
Artifact Tree	🗜 🛄 File List			
Filter: 🗾 No Filter 🗸 🖉	B 🖗 🖻 🖗	QZ▼ URL		AZ▼ server
Filename 🔺		URL		Query
Magnet CTF 2023 iOS16 (7)		https://www.google.	com/search?g=how+t	how to make a csgo server
🕂 🗍 🍥 Browsers (16)	2	https://www.google	com/search?q=how+t	how to make a csgo server
- @ Cloud Services (4)	3	https://www.google.	com/search?q=how+t	how to make a rust server
- G @ Google Query (21)	4	https://www.google.	com/search?q=how+t	how to make a rust server
—— 📀 Chrome Autofill (9)	5	https://www.google.	com/search?q=how+t	how to make a csgo <mark>server</mark>
—— 📀 Chrome Bookmarks (6)	6	https://www.google.	com/search?q=how+t	how to make a rust server
Chrome Eavicons (40)			-	

#### 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

HEIC - iPhone 12
C - iPhone 12
IMG 0009 HEIC - iPhone 12
IPhone 12
Phone 12 IMG_0001.HEIC iPhone 12 IMG_0013.HEIC - iPhone 12
- iPhone 12
IMG_0011.HEIC - iPhone 12 IMG_0005.HEIC - iPhone 12
IMG_0007.HEIC - iPhone 12
IMG_0024.HEIC - iPhone 12



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.

Forensic Explorer 🚦 🚵 👻 🍘			
合 Evidence 🛛 🕅 File System 🚽	Artifacts	P Keyword Search	ndex Search
Process Browsers Chat Email	Finance Apps	Health Apps OS	Social Media
The Artifact Tree 🛛 🖓	🛄 File List		
Filter: 🔄 No Filter 🗸 😑	8 o 🐼	Appliction Name	19 Total Time (se
Filename 🔺		Appliction Name	Total Time (secs) 🔻
Magnet CTF 2023 iOS16 (7)	1	com.apple.Maps	3600
🗄 🗌 🍥 Browsers (16)	2	com.apple.Maps	3600
🕀 🛄 💬 Chat (7)	3	com.apple.Maps	875
🕀 🗌 🍥 Email (3)	4	com.apple.Maps	875
⊕ 🔇 Finance (1)	5	com.apple.AppStore	849
Health Apps (3)	6	com.apple.AppStore	849
H MAC Operating System (1)	7	com.apple.AppStore	762
	8	com.apple.AppStore	762
Accounts Type IOS (32)	9	com.hammerandchisel.discord	707
Apple Maps Searches IOS (2)	10	com.hammerandchisel.discord	707
Application Permissions IOS (66)	11	com.midasplayer.apps.candycrushsaga	577
Application Usage iOS (192)	12	com.midasplayer.apps.candycrushsaga	5//
Bluetooth Paired Low Energy Devices iOS		com.google.ios.youtube	562
Bluetooth Seen Devices iOS (1001)		com apple weather	502
Cached Locations iOS (14563)	15	com apple weather	513
Calendar Items v4 iOS (129)			454
Installed Applications iOS (192)	18	com.apple.Maps	454
Note Items iOS (4)	19	com.google.photos	424
Photos.Sqlite iOS (101)	20	com.google.photos	424
Screen Time Application Usage iOS (226)	21	com.apple.camera	423

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"

	Search Artifacts Results		-		×
Abo	out Options				
	Import Keywords	Enter or Add RegEx Keywords Here (one per line):	Save As	атхт	
	Clear Keywords	lounge		4	•
	Quick Add> ~				

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

🔳 Search A	Artifacts Results			- 0	×
Keyword Co	ount:	1			
Artifacts	Module:				
Bates ID	RegEx Search Term	Folder	Match Text		
541643	lounge	Biome User Activity iOS	Lufthansa Senator Lounge		
541644	lounge	Biome User Activity iOS	Lufthansa Senator Lounge	in Newark	
541645	lounge	Biome User Activity iOS	Lufthansa Senator Lounge	in Newark	
541646	lounge	Biome User Activity iOS	Lufthansa Senator Lounge		
541647	lounge	Biome User Activity iOS	Lufthansa Senator Lounge		
Match Summ RegEx Tern 	hary: h	Hits  5			
Total Arti Search Art	.facts: ;ifacts Results finished.	5			
Search Art	ifacts Results finished.		-		
		Сору	to Clipboard Save CSV and Cl	ose Clo	se

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

Figure 32: Artifacts > Biome > Biome User Activity

Forensic Explorer 🚦 🚵 🕶 🎲 🕶 🔞			Forensic Explorer v5.	6.8(4629d) (64bit) Case: Magnet	CTF 2023 iOS1
合 Evidence 🛛 🗋 File System 🗚	Artifacts 🖉 Keyword Search	🔎 Index Search 🛛 🔘 Ema	il 🏦 Registry 📰 B	lookmarks 📄 Reports	Scripts
Process Browsers Y Chat Y Email Y	Finance Health Apps Apps OS	Mobile Social Tracking Media	Vindows OS Artifact Carve Dro	F Event Export Logs To CSV	Map Artifacts
🔚 Artifact Tree	🗜 🧮 File List				
Filter: 🍠 No Filter 🗸 🕒	- 😼 🖻 🔯 🔳 Created (UTC)	(Age▼ luft	₩ Type Service	🐼 • GUID	Source Name
Filename	Created (UTC)	Title	Type Service	GUID	Source Name
→ Magnet CTF 2023 IOS 16 (8) []           → @ Browsers (16)           → @ Brand (3)           → @ Brance (1)           → @ Brance (1)	1       ■ 32-bec-2022 92:63         2       ■ 32-bec-2022 92:63         3       ■ 32-bec-2022 92:63         4       ■ 23-bec-2022 92:26:4         5       ■ 23-bec-2022 92:26:4	<ul> <li>Mu Guffhansa Senator Lounge</li> <li>Mu Guffhansa Senator Lounge in Newark</li> <li>Mu Guffhansa Senator Lounge in Newark</li> <li>Mu Guffhansa Senator Lounge</li> <li>Mu Guffhansa Senator Lounge</li> <li>Mu Guffhansa Senator Lounge</li> </ul>	com.apple.Mags com.apple.Mags com.apple.Mags com.apple.Mags com.apple.Mags com.apple.Mags com.apple.Mags com.apple.Mags com.apple.Mags com.apple.Mags	ABCG040-661B-4879-0079-49588 28863A1E-A521-4551-A689-37580 00CF9343-844 = 105-64728-0415C 506070C-95D0-4057-A38E+1E99 CB070F9E-78CE-496C-8526-E93EA	690754927940769 690754927940769 690754927940769 690754927940769 690754927940769 690754927940769

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

Keyword Tree 4	Expword Result List E Gallery View E Video View					
Keyword Results (1)	i o 🖗	Filename	19 Hits			
E Keyword Search		Filename	Hits	Hit Text		
		UnifyStorage.s	10			
			1/10	JdUFimR.bÖ.İ,dÖ.İ,ÇLS‡adGhttps://www.tiktok.com/falcon/forest/nebula/content_tool?hide		
			2/10	)]o[music_legalZlegal_pageGhttps:// <mark>www.tiktok.com</mark> /falcon/forest/nebula/common_legal?hide		
			3/10	/common_legal?hide_nav_bar=l4https:// <mark>www.tiktok.com</mark> /falcon/forest/nebula/ad_legal		
			4/10	JdUFimR.bÖ.İ,dÖ.İ,ÇLS‡adGhttps:// <mark>www.tiktok.com</mark> /falcon/forest/nebula/content_tool?hide		
			5/10	&8D[music_legal2legal_pageGhttps://www.tiktok.com/falcon/forest/nebula/common_legal?hide		
			6/10	/common_legal?hide_nav_bar=l4https:// <mark>www.tiktok.com</mark> /falcon/forest/nebula/ad_legalÒ.5.6xáxâ		
			7/10	JdUFimR.bÖ.İ,dÖ.İ,ÇLS‡adGhttps:// <mark>www.tiktok.com</mark> /falcon/forest/nebula/content_tool?hide		
			8/10	/ÜZlegal_page[music_legal4https:// <mark>www.tiktok.com</mark> /falcon/forest/nebula/ad_legalGhttps:		
			9/10	alcon/forest/nebula/ad_legalGhttps:// <mark>www.tiktok.com</mark> /falcon/forest/nebula/common_legal?hide		
			10/10	JdUFimR.bÖ.İ,dÖ.İ,ÇLS#adGhttps://www.tiktok.com/falcon/forest/nebula/content_tool?hide		
	<u>⊖-</u> ⊡	📄 template.js	1			
			1/1	ext-highlight")&&(Object(g.c)("https://www.tiktok.com/falcon/forest/nebula/content_tool",!0)		

# 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

Whas does F	RHEINFAHRE	mean?	
음 Sources			
Rheinfähre - English translation – Linguee	Simple means of crossing the Rhine - Review of	Must see - Review of Rheinfahre, Basel,	
(1) linguee • 1	tripadvisor • 2	📾 tripadvisor • 3	View 2 more
Rheinfähre is a German service that provides a	word that translates to means of crossing the F	"Rhine ferry" in English. I Rhine River in Germany a	t refers to a ferry nd Switzerland 1 2 3.

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

	IMG_0068.H	IEIC
	JPEG EXIF DATA	
The state of	Date/Time:	
	Make:	Apple
	Model:	iPhone 12
	Software:	16.1.1
	Latitude:	50.000855555556
	Longitude:	8.0183333333334
	FORENSIC EXPLO	RER
IMG_0068.	FEXCase Folder	: 00008101-0010541A1130001E_files_full-
erstand an der Fähre	001.zip\privat	e\var\mobile\Media\DCIM\100APPLE\
	Filename:	IMG 0068.HEIC
	Logical Size:	1388703
- man and the for the form	Deleted File:	No
The second report of the second	Bookmarked:	No
A B B	Flags:	No Flags
- Entre		
Fähre Ingelheim	Created:	02-Jan-2023 3:07:04 PM
Fähre Ingelheim	Created: Modified:	02-Jan-2023 3:07:04 PM 02-Jan-2023 2:57:04 PM

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

≡ 50.0009,8.0183 Q X	Thing > Hotels @ Thing > Hotel Binesterna Sign in
Mar.	Historante Pizzeria O'Sole Mio Italian - 55
50°00'03.2"N 8°01'05.9"E	hullHilfe Pension & Ferienwohnung Berg
Orections     Image: Save     Image: Second to phone     Image: Smare       Owenheimer Str. 5, 65375 Oestrich-Winkel.	
Germany	
Add a missing place	estich Winkel
Add your business	Weingendeltzweinell et der Labre Patre Ingelneim
	Australia Terms Privecy 20 m

# 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

File List 😨 Gallery View 😨 Video View 🛄 Disk Vie	ew 🕘 Catego	ry Graph	
🖗 🖻 🎆 🙌 duolingo	€ Ext	File Signature	AZ▼
Filename	Extension	File Signature	Extension Mism
✓ 1 Duolingo_NYPromo_2023_EN.mp4	mp4	Mov	No
2 Duolingo_NYPromo_2023_VO_EN.mp4	mp4	Mov	No
			•
	: 59:58		
Volume:		0:	00.083 / 0:25

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

📑 Create Google Map .GPX	-		×
About Select Artifacts			
Artifacts with GPS Coordinates	Current Resu	ts	
Apple Health Workout Latitude	0		
Apple Health Workout Longitude	0		1.1
Apple Maps Searches iOS	2		· .
Cached Locations iOS	14563*		
Cell Tower Locations iOS	0		
	-	_	
Open Export Folder ? Sample < 2000*	Create GPX	Clos	æ

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

Forensic Explorer 🛛 🔒 褬 🗸 🚳					Forensi
Tile System	Artifacts	P Keyword Sear	rch 🔎 Index	K Search	Email Regis
Process Browsers Chat Chat Email	Finance Apps	Health Apps Biome	~ 🧯 мас м	Mobile ~ Social Media	V Tracking V Windo Apps OS
📰 Artifact Tree म	🛄 File List				
Filter: 🖉 No Filter 🗸 😑	8 <b>-</b> 🖗 🔳	31-DEC-2022 1:3	Az▼ Latitude	▲Z▼ Longitude	Horizontal Accurac
Filename         A           Magnet CTF 2023 iOS 16 (8)                     Image: Strain S	Tim 1	estamp         A           31-Dec-2022         1:32:06 AM           31-Dec-2022         1:34:38 AM           31-Dec-2022         1:37:24 AM           31-Dec-2022         1:38:39 PM	Latitude 50.0213182973562 50.0213372830866 50.0212723741294 50.0209777835157	Longitude 8.09321399214582 8.09322589739865 8.09317524309795 8.10750160228463	Horizontal Accuracy (m) 20.0 20.0 20.0 1049.33333333333333

#### 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

🔳 Search A	Artifacts Results	– 🗆 X	
Keyword Co	ount:		
Artifacts			
Bates ID	RegEx Search Term	Folder	Match Text
541275	youtube	Chrome Favicons	https://m.youtube.com/
541334	youtube	Chrome History	https://www.youtube.com/
541334	youtube	Chrome History	YouTube
541618	youtube	Safari Cookies	.youtube.com
541647	youtube	Safari Cookies	.youtube.com
541649	youtube	Safari Cookies	.youtube.com
541651	youtube	Safari Cookies	.youtube.com
541926	youtube	URL Cache Generic	https://is2-ssl.mzstatic.
542407	youtube	URL Cache Generic	https://is4-ssl.mzstatic.
545277	youtube	URL Cache Generic	https://is5-ssl.mzstatic.
550013	youtube	URL Cache Generic	https://todoist.doist-ema
539852	youtube	Gmail iOS	Now that you've upgraded,
541164	youtube	Mail iOS	"YouTube removed 10,000 v
541164	youtube	Mail iOS	r/technology: YouTube rem
540487	youtube	Biome App Launch iOS	com.google.ios.youtube
540488	youtube	Biome App Launch iOS	com.google.ios.youtube
563114	youtube	Biome User Notification Ev	com.google.ios.youtube
563117	youtube	Biome User Notification Ev	com.google.ios.youtube
563119	youtube	Biome User Notification Ev	com.google.ios.youtube
563120	youtube	Biome User Notification Ev	com.google.ios.youtube
563126	youtube	Biome User Notification Ev	com.google.ios.youtube
563129	youtube	Biome User Notification Ev	com.google.ios.youtube
563132	youtube	Biome User Notification Ev	com.google.ios.youtube
669196	wowtube	Biomo Hoor Motification Fu	com geogle ios voutube
		Copy to Clipboard	Save CSV and Close Close

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".