# CELLEBRITE 2023

# CAPTURE THE FLAG (CTF) ABE IPHONE

CTF Questions Only	2
About This CTF Challenge	5
Starting this challenge in Forensic Explorer	6
Question 1 - iCloud - Level 1 (10 points)	7
Question 2 - Comm App - Level 1 (10 points)	8
Question 3 - Wallet - Level 1 (10 points)	9
Question 4 - iCloud Backup - Level 1 (10 points)	
Question 5 - Tracking - Level 1 (10 points)	11
Question 6 - Steps - Level 2 (30 points)	13
Question 7 - BlueTooth - Level 2 (30 points)	14
Question 8 - App Notification - Level 2 (30 points)	15
Question 9 - Parked - Level 2 (30 points)	17
Question 10 - About - Level 2 (30 points)	20
Question 11 - Permissions - Level 2 (30 points)	21
Question 12 - Email - Level 3 (50 points)	22
Question 13 - Search - Level 3 (50 points)	25
Question 14 - Navigation - Level 3 (50 points)	27
Question 15 - Crypto - Level 2 (30 points)	
Question 16 - Picture - Level 2 (30 points)	29
Question 17 - Location - Level 2 (30 points)	
Question 18 - BokerTov - Level 3 (100 points)	

# CTF QUESTIONS ONLY

1	iCloud - Level 1 <i>Abe used a unique email address for his iCloud account. What is that email address?</i>	10
2	Comm App - Level 1 Abe used different types of communication channels, through different applications. What communication application was used the most?	10
3	Wallet - Level 1 A payment card was used on Abe's device - Wallet. What are the last 4 digits of that card?	10
4	iCloud Backup - Level 1 Abe's phone was setup using iCloudBackup method. What is the Date & Time for that (UTC+0 time)?	10
5	Tracking - Level 1 Abe was suspicious about being tracked. After searching the rental vehicle he was using while in NJ, he found a device attached to his vehicle, what was the make/model (need to refine)?	10
6	Steps - Level 2 <i>Abe was not really active on 6/24/2023 local time. How many steps were recorded?</i>	30
7	BlueTooth - Level 2 <i>Abe pairs his iPhone with few different Bluetooth devices. How many unique Bluetooth connections were paired?</i>	30

8	App Notification - Level 2 <i>Abe got notified by Harold of a potential arrest, Abe then opened which app?</i>	30
9	Parked - Level 2 Abe went to a party at RAIN Event Space. What is the name of the street (just the street name) where he parked his vehicle?	30
10	About - Level 2 What was Abe Rudder's About bio on WhatsApp?	30
11	Permissions - Level 2 Abe is paranoid and not always giving access to everything. One of the apps Abe used on the iPhone received access to Photos however as an "Add Photos Only" permission. What is the name of the app (one word i.e.: Starbucks)?	30
12	Email - Level 3 Abe used a specific method to find/check/share locations via an app. In order to keep privacy up, Abe signed up with a different email address which keeps it isolated to that vendor. What is that email address?	50
13	Search - Level 3 Abe got suspicious when he had to deal with some shady people almost as if a crime was known to be committed and wanted to leave no traces. Abe wanted to create an anonymous email. Where did Abe search for that? (3 words)?	50
14	Navigation - Level 3 Abe was navigating while driving, on June 26, 2023. What was the destination address on the navigation?	50

15	Crypto - Level 2 Abe used MOB to send/receive crypto within Signal. Can you find the Recovery Phrase for Signal Mobile Coin wallet? What is it? (24 words)?	30
16	Picture - Level 2 Abe loves taking pictures and videos on the iPhone, the problem is when Abe is trying to look for a picture, he is having hard time finding it therefore he utilizes the Search within the Apple Photos app. If Abe would have looked for a picture of: Myself, Pawel, and Hat he would end up with one photo. Can you name that filename?	30
17	Location - Level 2 Abe went for some shady meeting on an island but tried to conceal as a vacation so he took a boat tour and tracked dolphins. He then decided to mark a location with "dolphins". What was the timestamp for that location? [HH:MM:SS] written in UTC time"?	30
18	BokerTov Within the last month before Abe got arrested (and his device was extracted), Abe used to wake up naturally however, there was one day the phone did. What was the day and (local) time? [YYYY-MM-DD HH:MM:SS] e.g: 2021-09-19 08:35:00?Within the last month before Abe got arrested (and his device was extracted), Abe used to wake up naturally however, there was one day the phone did. What was the day and (local) time? [YYYY-MM-DD HH:MM:SS] e.g: 2021-09-19 08:35:00?Within the last month before Abe got arrested (and his device was extracted), Abe used to wake up naturally however, there was one day the phone did. What was the day and (local) time? [YYYY-MM-DD HH:MM:SS] e.g: 2021-09-19 08:35:00?	100

# ABOUT THIS CTF CHALLENGE

This challenge was created by Cellebrite (see: https://cellebrite.com/en/cellebrite-capture-the-flag-september-2023/).

#### FORENSIC IMAGE SOURCE

Download (24gb): https://drive.google.com/file/d/1dn5IRU1Sa3A9NokW5v5HhJsiRud3tYHa/view

# OTHER ONLINE CELLEBRITE 2023 ABE SOLUTIONS

The following other solutions can be found online:

- https://cellebrite.com/en/cellebrites-ctf-2023-recap-answers-on-abes-iphone/
- https://www.stark4n6.com/2023/10/cellebrite-ctf-2023-abe.html
- https://forensafe.com/blogs/challenges/CellebriteCtfAbe.html

# OTHER FORENSIC EXPLORER CTF WALKTHROUGHS

Other Forensic Explorer Capture the Flag walkthroughs are located on this page: <u>https://getdataforensics.com/capture-the-flag/</u>

# 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 Cellebrite file: EXTRACTION\_FFS.ufd

In the Evidence Processor window use the default options.

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 1: Artifacts > Process All



# **QUESTION 1 - ICLOUD - LEVEL 1 (10 POINTS)**

Abe used a unique email address for his iCloud account. What is that email address?

#### Q1. ANSWER

aberudder@icloud.com

#### Q1. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer Artifacts module:

- 1. Select Mobile > Accounts Type iOS.
- 2. The iCloud account Username is listed as: aberudder@icloud.com.

#### 🔚 🚵 🗕 🎲 🗕 🔞 Artifacts A Keyword Search Evidence File System Index Search ( Email Regist $( \mathbf{b} )$ 6 ∢ О 9 풍 Email Process Browsers Chat Mobile MAC Windows Social Health Artifact Drone All OS OS Media Apps Carve Artifact Tree 🎹 File List Filter: 🗐 No Filter 82 8 I Timestamp Account Description Ar Username $\sim$ -Filename Account Description Timestamp Username 🔲 🧱 ABE Test (6) 🛛 1 03-Feb-2023 1:18:49 AM Tunes Store local 2 3 4 03-Feb-2023 1:18:52 AM iTunes Store (Sandbox) local 03-Feb-2023 1:26:23 AM IDMS aberudder@icloud.com 03-Feb-2023 1:26:23 AM Apple ID aberudder@icloud.com Health Apps (4) Health Apps (4) MAC Operating System (1) Mobile (13) 5 03-Feb-2023 1:26:30 AM aberudder@icloud.com Messages 03-Feb-2023 1:26:30 AM aberudder@icloud.com 6 Game Center 7 03-Feb-2023 1:26:30 AM CloudKit aberudder@icloud.com 8 03-Feb-2023 1:26:30 AM iCloud aberudder@icloud.com 🔲 🚯 Apple Maps Searches iOS (36) 9 03-Feb-2023 1:26:44 AM CalDAV -Application State iOS (217) IMAPMail aberudder@icloud.com 10 03-Feb-2023 1:26:44 AM Bluetooth Seen Devices iOS (1049) 11 📄 03-Feb-2023 1:26:44 AM IMAPNotes Cached Locations iOS (103391) 12 03-Feb-2023 1:26:44 AM CardDAV 13 03-Feb-2023 1:26:47 AM Device Locator aberudder@icloud.com Call History iOS (41) 14 aberudder@icloud.com 03-Feb-2023 1:26:47 AM Find My Friends Cell Tower Locations iOS (3314) 15 03-Feb-2023 1:26:48 AM aberudder@icloud.com iTunes Store 🔲 🍰 Contacts Details iOS (1146) 16 03-Feb-2023 1:28:34 AM Holiday Calendar Installed Applications iOS (217)

#### Figure 2: Artifacts > Mobile > Account Types iOS

F

# QUESTION 2 - COMM APP - LEVEL 1 (10 POINTS)

Abe used different types of communication channels, through different applications. What communication application was used the most?

#### Q2. ANSWER

Telegram (1038 messages).

#### Q2. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer **Artifacts module**:

- 1. Select Chat.
- 2. Telegram T7 Chat IOS has the most chat messages.

#### Figure 3: Artifacts > Chat > Telegram T7 Chat iOS

Forensic Explorer 🚦 🚵 👻 🛞 🗸 🕖					
合 Evidence 🗋 File System 🗚	rtifacts	P Keyword Search	Index Search	(C) Email	E Re
Process All Browsers Chat Email	Mobile 🗸	MAC V Windows V Social OS OS Media	~ thealth Apps	Artifact × Carve	र Drone
Artifact Tree	🔜 File List				
Filter: 🔄 No Filter 🗸 🖃	i o 🖗	Date	Chat ID	AZ N	/lessage ID
Filename 🔺		Date	Chat ID	Messag	je ID
ABE Test (6)		09-Jun-2022 6:14:17 PM	35467832743	12884	901888
+- Browsers (19)	2	01-Jul-2022 1:54:18 AM	35554392637	17179	869184
🕂 💭 💬 Chat (13)	3	24-Feb-2023 3:23:01 AM	777000	25769	803776
- 🔤 🔗 Facebook Messenger Chat iOS (24)	4	27-Aug-2022 1:53:39 PM	10179064274	43211	92970523
	5	17-Aug-2022 6:53:06 PM	10179064274	43175	71660102
- iMessage Attachments OSX (29)	6	17-Aug-2022 6:27:00 PM	10179064274	43134	55788032
iMessage Message OSX (206)	7	17-Aug-2022 10:22:53 AM	10179064274	43091	60820736
- Instagram Group Members Chat iOS (8)	8	10-Aug-2022 11:37:30 AM	10179064274	42992	62263296
- Instagram Direct Message Chat iOS (24)	9	09-Aug-2022 7:42:44 AM	10179064274	42949	67296000
SnapChat Message (arroyo.db) Android (198)	10	08-Aug-2022 10:26:09 AM	10179064274	42906	72328704
Telegram T7 Chat iOS (1308)	11	07-Aug-2022 10:37:28 PM	10179064274	42863	77361408
Telegram User iOS (198)	12	04-Aug-2022 9:31:42 PM	10179064274	42820	82394112
Tiktok Chat iOS (6)	13	04-Aug-2022 9:11:52 PM	10179064274	42777	87426816
Tinder Chat iOS (12)	14	01-Nov-2022 4:23:13 PM	10196367041	70952	85972992
WhatsApp Chat iOS (63)	15	01-Nov-2022 4:23:12 PM	10196367041	70923	83514624
WhatsApp Contacts iOS (582)	16	01-Nov-2022 3:27:27 PM	10196367041	70866	96038400
Email (3)	17	01-Nov-2022 2:29:22 PM	10196367041	70824	01071104
Health Apps (4)	18	01-Nov-2022 1:09:02 PM	10196367041	70781	06103808
H MAC Operating System (1)	19	01-Nov-2022 8:27:50 AM	10196367041	70738	11136512
	20	01-Nov-2022 1:31:07 AM	10196367041	70695	16169216

# QUESTION 3 - WALLET - LEVEL 1 (10 POINTS)

#### A payment card was used on Abe's device - Wallet. What are the last 4 digits of that card?

# Q3. ANSWER

# 7438.

# Q3. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer Artifacts module:

- 1. Select Finance > Apple Wallet.
- 2. The last 4 digits of the Credit Card Number are listed as 7438.

#### Figure 4: Artifacts > Finance > apple Wallet iOS

Forensic Explorer 🚦 🚵 👻 🎲	- 🕜			
合 Evidence 🛛 🎦 File System	Artifacts	Keyword Search	Index Search 🛛 🔘 E	mail 🔠 Re
Process Browsers Chat Chat	email ~ Mobile ~ MA OS	C Vindows Social OS Media	Finance Apps	× Artifact × Carve
Tree 4	🛄 File List			ļ
Filter: 💭 No Filter 🗸 😑	😼 🖻 🔯 🐼 Pass Type	e AZY Cor AZY Desc	rip 🐼 Credit Card Nı	🖉 🖲 Expiration Date
Filename A	Pass Type	Company Description	n Credit Card Number E	Expiration Date
ABE Test (7)	🗌 1 📄 paymentpa	ss.co Apple Inc. Apple Cas	h ***7438	2023-12
Chat (13)     Chat (14)     Chat (14)				

### QUESTION 4 - ICLOUD BACKUP - LEVEL 1 (10 POINTS)

Abe's phone was setup using iCloudBackup method. What is the Date & Time for that (UTC+0 time)?

#### Q4. ANSWER

20-Feb-2023 1:43:14 AM.

#### Q4. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer Artifacts module:

- 1. Select Mobile > Mobile Backup Restore Info iOS.
- 2. The Restore Date is listed as 20-Feb-2023 1:43:14 AM.

#### Figure 5: Artifacts > Mobile > Mobile Backup Restore Info iOS

-							
Forensic Explorer	🗟 🖻 🗝 🛞	- 🕜					
Evidence	File System	<b>-</b> /~ ^	rtifacts	P Keyword Search	🔎 Index Search	(C) Email	🔡 Reg
Process All	∽ 👷 ∽ Chat ∽	email ×	Mobile ~	MAC Windows OS OS	Social Kedia Kedia	Y Health Apps	rtifact ~ Carve
Artifact Tree		Д	🛄 File List				
Filter: 🗾 No Filter		× =	1 in	Restore Date	Backup Build'	₩ Was Cloud Res	Devi
Filename				Restore Date	Backup Build Version	Was Cloud Restore	Device Bui
🔲 🌉 ABE v2 (1) 🛛			1	20-Feb-2023 1:43:1	4 AM 20B101	True	20D67
🗀 📃 🚺 Mobile (1)							
Mobile Bac	kup Restore Info iOS	(1)					
_							

### QUESTION 5 - TRACKING - LEVEL 1 (10 POINTS)

Abe was suspicious about being tracked. After searching the rental vehicle he was using while in NJ, he found a device attached to his vehicle, what was the make/model (need to refine)?

#### Q5. ANSWER

Geotab go9 Ite or Geotab go9

#### Q5. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer Artifacts module:

1. Use the Search Artifact Results toolbar button to search for rental.

Figure 6: Search Artifact Results



2. Search activity indicates that the Safari Browser was used to research hertz rental.

#### Figure 7: Search Artifact Results output

Search Artifacts	s Results		- o ×
Keyword Count:		1	
Artifacts Modul Bates ID	.e: RegEx Search Term	Folder	Match Text
845205 845205 845326 845326 745545 745545 748674 788674 769772 774556 845436 854336	rental rental rental rental rental rental rental rental rental rental rental rental rental rental	<pre>@ Google Query @ Google Query @ Google Query Safari Bookmarks Safari Bookmarks Safari Tabs Safari Tabs URL Cache Generic Telegram T7 Chat iOS Mail iOS Mail iOS</pre>	<pre>hertz rental geotab go9 lte https://www.google.com/search?client=safari&amp;hl=en-us&amp;q=hertz hertz rental geotab go9 lte https://www.google.com/search?client=safari&amp;hl=en-us&amp;q=hertz hertz rental geotab go9 lte - Google Search https://www.google.com/search?client=safari&amp;hl=en-us&amp;q=hertz https://www.google.com/search?client=safari&amp;hl=en-us&amp;q=hertz https://www.google.com/search?client=safari&amp;hl=en-us&amp;q=hertz https://ajaxgeo.cattrawler.com/translations/Mobile.SmarthDoc Here are some of the stories weare covering from around th The latest on the Titanic-sub search, how car-rental compani A deadly new street drug, the most expensive U.S. rental mar</pre>
Match Summary: RegEx Term  rental		Hits  12	
Total Artifacts Search Artifact	: s Results finished.	8	
Search Artifact Time Taken: 00:	s Results finished. 02:36		
			Copy to Clipboard Save CSV and Close Close

Safari Tabs shows a search activity relating to **Geotab go9 Ite** and **Geotab go9**.

#### Figure 8: Artifacts > Browsers > Safari Tabs

Forensic Explorer 🚦 🚵 🔻 🎲 👻 🕖			Forensic Explo	rer v5.6.8(4655d) (64
合 Evidence 🗋 File System 🖌	Artifacts 🖉 Keyword Search	₽ Index Search	🛈 Email 🛛 🏦 Registry	E Bookmarks
Process Browsers Chat Email	Finance Apps Apps Biome	MAC V Mobile V Social OS Mobile V Mobile	I V Tracking V Windows V Apps OS	Artifact Carve Logs
Artifact Tree	7 File List			
Filter: 🗾 No Filter 🗸 🗸	- 🖗 🖻 🐲 🚱 🕶 hertz	AZT T AZ	🔻 hertz	
Filename	∧ Title	Type UR	۲L	
2023 CTF Cellebrite ABE (9) [         ● Browsers (19)         ● @ Bing Query (1)         ● @ Dating URL (43)         ● ① Dating URL (43)         ● ① Dating URL (43)         ● ① Chrome Bookmarks (3)         ● ○ Chrome Favicons (66)         ● ○ Chrome Heaver (45)         ● ○ Chrome Keyword Search Terms (6)         ● ○ Chrome Meaver (45)         ● ○ Chrome Meaver (41)         ● ○ Safari Bookmarks (89)         ● ○ Safari Cache (62)         ● ○ Safari Cache (52)         ● ○ Safari Recent Searches (20)         ● ○ Safari Recent Searches (20)         ● ○ Safari Recent Searches (20)         ● ○ Safari Recent Searches (20)	1	o9 lte - Google Search 0 ht	ttps://www.google.com/search?client=s	afari&h =en-us&q= <mark>hertz</mark> +ri

# QUESTION 6 - STEPS - LEVEL 2 (30 POINTS)

#### Abe was not really active on 6/24/2023 local time. How many steps were recorded?

#### Q6. ANSWER

#### 755.

# Q6. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer Artifacts module:

- 1. Select Health Apps > Apple Health Steps.
- 2. In the End Date column header, filter for 24 June 2023.

#### Figure 9: Artifacts > Health Apps > Apple Health Steps

Forensic Explorer					
合 Evidence 🛛 🗋 File System 🗚 A	rtifacts	P Keyword Search	<b>P</b> Index Search	(C) Email	🔡 Reg
Process All	Mobile ~	MAC Windows OS OS	Social × Finance × Media Apps	Health Apps	Artifact × Carve
📕 Artifact Tree 🛛 📮	🔠 File List				
Filter: 🔄 No Filter 🗸 😑	🖗 🖻 🔯	Start Date	3 24-jun-2023	🗐 Steps Taker	AZ Prov
Filename		Start Date	End Date 🔺	Steps Taken	Provenance
🔲 🧱 ABE v2 (7) 🛛	1	24-Jun-2023 1:00:27 AM	24-Jun-2023 1:02:34 AM	140	iPhone 10, 3
🗄 🗌 🌑 Browsers (19)	2	24-Jun-2023 1:30:22 AM	24-Jun-2023 1:31:00 AM	62	iPhone 10, 3
🕂 🗍 💬 Chat (13)	3	24-Jun-2023 4:17:00 PM	24-Jun-2023 4:21:34 PM	119	iPhone 10,3
🔁 💭 🌑 Email (3)	4	📄 24-Jun-2023 4:44:37 PM	24-Jun-2023 4:54:29 PM	95	iPhone 10,3
— M Gmail iOS (204)	5	📄 24-Jun-2023 4:54:42 PM	24-Jun-2023 4:58:56 PM	129	iPhone 10, 3
— Mail Addresses iOS (28)	6	24-Jun-2023 5:19:57 PM	24-Jun-2023 5:24:22 PM	65	iPhone 10,3
- Mail iOS (573)	7	24-Jun-2023 5:35:18 PM	24-Jun-2023 5:39:14 PM	36	iPhone 10, 3
E- S Finance (2)	8	24-Jun-2023 5:45:28 PM	24-Jun-2023 5:50:25 PM	29	iPhone 10, 3
E- Health Apps (4)	9	24-Jun-2023 5:57:48 PM	24-Jun-2023 6:06:44 PM	65	iPhone 10, 3
— 🥏 Apple Health Distance (3339)	10	24-Jun-2023 6:08:44 PM	24-Jun-2023 6:08:54 PM	21	iPhone 10, 3
Apple Health Flights Climbed (251)	11	24-Jun-2023 6:33:53 PM	24-Jun-2023 6:42:07 PM	108	iPhone 10, 3
Apple Health Steps (3337)	12	24-Jun-2023 6:45:18 PM	24-Jun-2023 6:52:17 PM	88	iPhone 10, 3
Apple Health User Height (1)					
🕀 🛄 📺 MAC Operating System (1)					

119	
95	
129	
65	
36	
29	
65	
21	
108	
88	
755	

Note that **local time is requested**, so the displayed UTC dates must be adjusted.

The sum of steps on **24 June 2023** is **755**.

# QUESTION 7 - BLUETOOTH - LEVEL 2 (30 POINTS)

Abe pairs his iPhone with few different Bluetooth devices. How many unique Bluetooth connections were paired?

#### Q7. ANSWER

10.

#### Q7. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer Artifacts module:

- Examine results for Mobile > Bluetooth Devices iOS and Bluetooth Paired Low Energy Devices iOS.
- 2. The sum of these devices is **10**.

Figure 10: Artifacts > Mobile > Bluetooth

Forensic Explorer 🚦 🚵 👻 🎯					
合 Evidence 📄 File System 🔥	Artifacts	P Keyword Search	🔎 Index Searc	h ()	Email 🔠 Re
Process Browsers Chat Email	Mobile ~	MAC OS OS	Social Social Media	Health Apps	↓ Artifact ↓ Carve
Artifact Tree	🛄 File List				
Filter: 🗾 No Filter 🗸 🚽	) 🖗 🗆 🖗	MAC Address	AZ▼ Device Na	• User Nam	▲Z▼ Default Name
Filename A		MAC Address	Device Name 🔺 Use	er Name	Default Name
ABE v2 (1)	1	18:62:E4:17:1B:F5			Handsfree
E- Mobile (3)	2	08:65:18:D4:87:46	AirPods Pro Bla	ah Blah Blah	Blah Blah Blah Blah Bla
Bluetooth Devices iOS (8)	3	30:74:67:AF:CA:6C	Ed's S21		Mobile Phone
Bluetooth Paired Low Energy Devices iOS (2)	4	EC:65:CC:98:AD:78	Ford Edge		
Bluetooth Seen Devices iOS (1049)	5	EC:65:CC:BC:9F:14	Ford Edge		
	6	48:7A:FF:79:78:B7	Kia		Handsfree
	7	CC:88:26:55:4A:16	Tesla Model 3		Handsfree
	8	28:F0:33:6F:97:BA			

# QUESTION 8 - APP NOTIFICATION - LEVEL 2 (30 POINTS)

#### Abe got notified by Harold of a potential arrest, Abe then opened which app?

# Q8. ANSWER

Signal.

# Q8. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer Artifacts module:

1. Use the **Search Artifact Results** toolbar button to search for **arrested**.

Figure 11: Artifacts > Search Artifact Results



#### 2. The search results show hits in **Biome User Notification Events**.

#### Figure 12: Search Artifact Results

Search Artifacts Result	ults		– 🗆 X
Keyword Count:		1	
Artifacts Module:			
Bates ID	RegEx Search Term	Folder	Match Text
772816	arrested	Telegram T7 Chat iOS	Ruling on Brittney Grinerâs Appeal Set for TuesdayA cour
773389	arrested	Telegram T7 Chat iOS	Here are some of the stories weâre covering from around th
773411	arrested	Telegram T7 Chat iOS	Here are some of the stories weâre covering from around th
773430	arrested	Telegram T7 Chat iOS	Here are some of the stories weâre covering from around th
773468	arrested	Telegram T7 Chat iOS	The chair of Ukraineâs Supreme Court was removed from his
773484	arrested	Telegram T7 Chat iOS	President Volodymyr Zelensky of Ukraine is set to appear in
773506	arrested	Telegram T7 Chat iOS	Here are some of the stories we're covering from around the
773529	arrested	Telegram T7 Chat iOS	Here are some of the stories we're covering from around the
774455	arrested	Telegram T7 Chat iOS	Here are some of the stories weâre covering from around th
774476	arrested	Telegram T7 Chat iOS	The U.S. on Monday designated Evan Gershkovich, the Wall Str
774479	arrested	Telegram T7 Chat iOS	The Airman Who Wanted to Give Gamers a Real Taste of WarFe
774618	arrested	Telegram T7 Chat iOS	Hundreds of thousands of people in southern Ukraine do not h
774662	arrested	Telegram T7 Chat iOS	Here are some of the stories we're covering from around the
774678	arrested	Telegram T7 Chat iOS	Here are some of the stories we're covering from around the
775033	arrested	Telegram T7 Chat iOS	180 people were arrested after protesters burned cars and bu
674977	arrested	Mail iOS	Disgraced crypto star arrested, haunting photos of the Dead
683923	arrested	Mail iOS	A notorious mafia boss arrested, the hidden cost of cheap TV
695857	arrested	Mail iOS	IRS hands over Trump's tax returns, why more seniors are get
820698	arrested	Mail iOS	U.S. journalist arrested in Russia, a tale of two housing ma
825995	arrested	Mail iOS	Here's what you need to know
826995	arrested	Mail iOS	Here's what you need to know
1044989	arrested	Biome User Notification Ev	7-year-old arrested for setting house on fire with parents a
1047669	arrested	Biome User Notification Ev	Here are some of the stories we're covering from around t
1047676	arrested	Biome User Notification Ev	Here are some of the stories we're covering from around t
1047845	arrested	Biome User Notification Ev	Here are some of the stories we're covering from around t
1048476	arrested	Biome User Notification Ev	Here are some of the stories we're covering from around t
1048818	arrested	Biome User Notification Ev	Here are some of the stories we're covering from around t
1049462	arrested	Biome User Notification Ev	Yo! Keep this. I may be getting arrested shortly
1049467	arrested	Biome User Notification Ev	Yo! Keep this. I may be getting arrested shortly
1049648	arrested	Biome User Notification Ev	B 180 people were arrested after protesters burned cars and
1049667	arrested	Biome User Notification Ev	B 180 people were arrested after protesters burned cars and
Match Summary:			
RegEx Term		Hits	
arrested		31	
Total Artifactor		21	
Count Artifacts:		31	
	sults finished.		
Search Artifacts Re	sults finished.		
Time Taken. 00:02:2			
			Copy to Clipboard Save CSV and Close Close

In the Forensic Explorer Artifacts module:

- 1. Select iOS Biome.
- 2. Use a **column filter** in the **Body** field for "I may be getting arrested shortly".
- 3. This identifies a Signal message from Harold.

Figure 13: iOS Biome > Biome User Notification Events iOS

Forensic Explorer 🚦 🚵 👻 🍘			Forensic Explorer v5.6.8(4655d)
合 Evidence 🛛 🔂 File System 🖌	Artifacts 🖉 Keyword Search	🔎 Index Search 🛛 🔘 Email	Registry E Bookmarks
Process Browsers Chat Email	Finance Health COS Apps Apps Biome	MAC V Mobile V Social V Tra OS Media A	cking     Windows     Artifact     Ex       pps     OS     Carve     Lot
Artifact Tree 🛛	🔜 File List		
Filter: 🖉 No Filter 🗸 🚽	🚱 🖻 😻 🔳 Timestamp	₩ Title ₩ Bundle ID	I may be getting arrested shortly
Filename       A	Imestamp         1       ⊇ 27-Jun-2023 11:58:04 PM         2       ⊇ 28-Jun-2023 12:00:45 AM	Title Bundle ID Harold org.whispersystems.signal Harold org.whispersystems.signal	Body Yo! Keep this. <u>I may be getting arrested shortly</u> . Yo! Keep this. <u>I may be getting arrested shortly</u> .

# The **Mobile > Application Usage iOS** records also show use of **Signal** at that time.

#### Figure 14: Artifacts > Application Usage iOS

Artifact Tree		📃 File List						
Filter: 🗾 No Filter	<	🖗 <b>-</b> 🖗	8 28-Jun-2023	▲ xRAW Creat	AZ▼ signal	AZ /app/	₩ Location	Source ►
Filename			Creation Date	▲ xRAW Creation D	Application Identifier	Stream N	Location	Source Name
🔲 🚟 ABE Walk-Through (8) 🛛			28-Jun-2023 12:04:19	AM 709603459.234884	org.whispersystems.signal	/app/usage	Table: zobject (row 13675)	knowledgeC.db
+ Browsers (19)		2	28-Jun-2023 12:05:26	AM 709603526.993078	org.whispersystems.signal	/app/usage	Table: zobject (row 13712)	knowledgeC.db
🕂 🗍 💬 Chat (14)		3	28-Jun-2023 9:08:11	PM 709679291.667014	org.whispersystems.signal	/app/usage	Table: zobject (row 13938)	knowledgeC.db
+ () Email (1)								
- S Finance (0)								
🕂 🗌 🛟 Health Apps (4)								
🕀 🔲 💣 MAC Operating System (1)								
- Mobile (20)								
Accounts Type iOS (16)								
Apple Maps Searches iOS (36)								
Application State iOS (217)								
Application Usage iOS (14156)								
Pluotooth Dovices iOE (2)								

# QUESTION 9 - PARKED - LEVEL 2 (30 POINTS)

Abe went to a party at RAIN Event Space. What is the name of the street (just the street name) where he parked his vehicle?

Q9. ANSWER

Water street.

#### Q9. FORENSIC EXPLORER METHODOLOGY

The first step is to locate the address of the RAIN Event Space. This is done using Google My Maps.

#### Figure 15: Google My Maps > RAIN Event Space

		×
RAIN Event Space		
Details from Google	Maps	1000
399 Water St, Teaned	ck, NJ 07666	учин
rain-event-space.bus	siness.site	fth Avenue Hairc
+1 201-817-8100		9
		*
47 ***** G	View in Google Ma	305
	, then in coogle inc	
2		
<ul> <li>Add to map</li> </ul>		Cedar
RAIN Event	t Space	- Ln
17/	0	N A
	V Pick	dé Licious, Inc

This question is likely to be answered using data from: **Artifacts > Mobile > Parked Car Locations**. Launch **Map Artifacts** from the toolbar button.

Figure 16: Artifacts > Map Artifacts



#### Select **Parked Car Locations iOS** from the list of available artifacts:

#### Figure 17: Map Artifacts

Create Google Map .GPX	_		$\times$
About Select Artifacts			
Artifacts with GPS Coordinates	Current Resu	ts	
Apple Health Workout Latitude	0		
Apple Health Workout Longitude	0		
Apple Maps Searches iOS	36		
Cached Locations iOS	103391*		
Cell Tower Locations iOS	3314*		
Fitbit Event	0		
Garmin Connect Activities	0		
Garmin Connect Activity Details	0		
Google Maps Saved Places Android	0		
Parked Car Locations iOS	123		
Photos.Sqlite 14 iOS	0		
Significant Locations iOS	404		
Significant Locations Visits iOS	370		
SkySafe CSV	0		
Wifi Locations iOS	188918*		
Open Export Folder ? Sample < 2000*	Create GPX	Clos	e

Create a GPX file and import into Google My Maps (or similar).

#### Figure 18: Google My Maps import



# The map shows a data point on Walter St near the Rain Event Space.

#### Figure 19: Google My Maps



# QUESTION 10 - ABOUT - LEVEL 2 (30 POINTS)

What was Abe Rudder's About bio on WhatsApp?

# Q10. ANSWER

World peace.

# Q10. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer Artifacts module:

- 1. Select Chat > WhatsApp Preferences iOS.
- 2. Current Status is set to World Peace.

#### Figure 20: Artifacts > Chat > WhatsApp Preferences iOS

Forensic Explorer 🚦 🚵 👻 🍘 🗸 🥘					Forensic Ex	plorer v5.6
合 Evidence 🗋 File System 📌	Artifacts	P Keyword Search	🔎 Index Searc	h 🔘 Email	Registry	E Bookn
Process Browsers Chat Email	Mobile ~	MAC OS OS	Social Media	~ OHEALTH	Artifact Carve	✓ Event Logs
Artifact Tree	🛄 File List					
Filter: 💭 No Filter 🗸 🚽	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Whatsar Watsar	Vhatsapp ID	Curremt	Source Name	
Filename		Whatsapp U Whatsa	app ID	Current Status So	ource Name	
ABE Walkthrough (7) ABE Walkthrough (7)		AbeRudder 12065	937224@s.whatsapp.net	World peace 🔇	roup.net.whatsapp.WhatsApp	.shared.plist

# QUESTION 11 - PERMISSIONS - LEVEL 2 (30 POINTS)

Abe is paranoid and not always giving access to everything. One of the apps Abe used on the iPhone received access to Photos however as an "Add Photos Only" permission. What is the name of the app (one word i.e.: Starbucks)?

#### Q11. ANSWER

Chrome.

#### Q11. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer Artifacts module:

- 1. Select Mobile > Application Permissions iOS.
- 2. Apply a column filter in the **Application** and **Service** columns for **photos**.

A single entry for Chrome is associated with the **kTCCServicePhotosAdd** access permission. The **Auth Value** of **2** indicates that the application was granted permission (see https://www.rainforestga.com/blog/macos-tcc-db-deep-dive).

Figure 21: Artifacts > Mobile > Application Permissions iOS



# QUESTION 12 - EMAIL - LEVEL 3 (50 POINTS)

Abe used a specific method to find/check/share locations via an app. In order to keep privacy up, Abe signed up with a different email address which keeps it isolated to that vendor. What is that email address?

#### Q12. ANSWER

j9by422yjc@privaterelay.appleid.com

#### Q12. FORENSIC EXPLORER METHODOLOGY

There are several ways to approach this question. The biggest clues are **privacy** and **email address**.

To examine email addresses used on the iPhone:

- 1. In the Artifacts module, select **Email > Mail Addresses iOS**.
- 2. Of the 28-email address listed, the domain **privaterelay.appleid.com** stands out as a potential candidate.
- 3. One of the entries related to **priveaterelay** is **what3words**, and its Wikipedia entry indicates that it is geocode system used to share location information.



Figure 22: Artifacts > Mail Addresses > iOS

A broader search of all **Artifact module** results for email addressed can be done using the **Search Artifact Results** button.

1. Use the Quick Add menu option to add a regular expression for email addresses.

#### Figure 23: Artifacts module > Search Artifact Results > Quick Add > email regex

Search Artifacts Results		_		×
About Options				
Import Keywords	Enter or Add RegEx Keywords Here (one per line):	Save As	s TXT	
Clear Keywords	[a-zA-20-9.!#\$%&*+/=?^_`{ }~-]+@[a-zA-	20-9](?:[a-2	A-20- 4	
Email Addresses 🗸 🗸				
Quick Add> Child Protection - Basic Child Protection - Extensive Crypto Cyrrency				
Email Addresses Hacking/Security			_	

Artificial Intelligence websites, like Perplixity.com have made the creation and/or refinement of regular expression statements much simpler.

#### Figure 24: Perplexity



Save the search result to CSV and refine in Microsoft Excel (i.e. remove duplicates) to identify candidates.

#### Figure 25: Refine results in Microsoft Excel

73	no-reply_at_yelp_com_fg6y94j9wq_6dfd64e2@privaterelay.appleid.com
74	appleid@id.apple.com
75	hi_at_bumble_com_92544jy5m2_e9a6cbc1@privaterelay.appleid.com
76	hello_at_what3words_com_j9by422yjc_d024cb5a@privaterelay.appleid.com
77	j9by422yjc@privaterelay.appleid.com
78	applepaylater@insideapple.apple.com
79	Dear Abe Rudder
80	Security alert for aberudder77@gmail.com

**Artifacts > Application State iOS** and **Artifacts > Installed Applications iOS** can be used to confirm the presence of the what3words application on the iPhone.

Forensic Explorer     Image: Im	5 Keyword Search 6 Keyword Search 6 Keyword Search 6 Keyword Search 6 Social 6 Social 7	Index Search @ Email	Fa
Evidence The System Artifacts	5 Keyword Search C Keyword Search MAC Windows Social Media Social Media MAC Social Media	Index Search @ Email	Re
🕞 🚯 晃 📮 🗍	MAC Windows Social	\$ •	0
Process Browsers Chat Email Mobile All	03 03 Media	Apps Apps (	rtifact Carve
🔚 Artifact Tree 🛛 🕂 🧰 Fi	ile List		
Filter: 💭 No Filter 🗸 🗕 🤯 🖻	🖻 🎆 🐼 Application	Location	A-Z▼ S
Filename       A         B       ABE Walkthroujgh (7) ]         Browsers (19)         Chat (14)         Email (3)         Email (4)	Application 194 com.openai.chat 195 com.squareup.cash 197 com.starbucks.mystarbucks 198 com.target.Target 199 com.thelicapp.tile 201 com.thelicapp.tile 201 com.thyopagroup.picaboo 202 com.tripadvisor.LocalPicks 203 com.united.UnitedCustomerFac 204 com.uvnv.mintsim 205 com.waze.iphone 206 com.wather.TWC 207 com.wather.TWC 207 com.windytv.ios 208 com.windytv.ios 209 com.yelp.yelpiphone 210 com.thilaoapp.musically 211 net.whatsapp.WhatsApp 212 org.merlos.OpenGpxTracker 213 org.mozilla.ios.Firefox 214 org.toshi.distribution	<ul> <li>Location</li> <li>Table: application_identifier_tab (ro. Table: application_identifier_tab (ro.</li> </ul>	Source applica

Figure 26: Mobile > Application State and Installed Applications

#### QUESTION 13 - SEARCH - LEVEL 3 (50 POINTS)

Abe got suspicious when he had to deal with some shady people almost as if a crime was known to be committed and wanted to leave no traces. Abe wanted to create an anonymous email. Where did Abe search for that? (3 words)?

#### Q13. ANSWER

Duck Duck Go

#### Q13. FORENSIC EXPLORER METHODOLOGY

In the Forensic Explorer Keyword Search module:

- 1. Add the keyword anonymous email.
- 2. Run the keyword search across all FileSystem searchable items.

#### Figure 27: Keyword Search

👹 Keywo	👹 Keyword Search 2 Options - 🗆 🗙							
Process Nar	ne:							
Keyword S	earch 1							
Source								
Module:	FileSystem			$\sim$				
🔾 Sea	<ul> <li>Searchable Items (673875 items, 37.87 GB)</li> </ul>							
	Unallocated space							
Che	O Checked items (1 items 23 KB)							
	Include Raw Devices, Partitions and Files							
Advanced options:								
	Include file slack							

Keyword search hits are located that relate to the web browser **DuckDuckGo**. DuckDuckGo is considered good for anonymous browsing due to its strong privacy focus.

E Keywor	d Result List 🔋 Gallery View	🔋 Video	View		
i o 🖗	Interview Filename	19 H	File Si		🗐 Hit Offset (I
	Filename	Hits	File Signat	Hit Text	Hit Offset (File)
<b>+</b> -	Localizable.loctable	2	Plist (Binary)		
<b>₽-</b> □	27AF2E1C68777A7EC	4			
		1/4		title>how to create anonymous email at DuckDuckGo <td>11575</td>	11575
		2/4		tent="how to create anonymous email"> <link anonymous="" create="" email",rfq='0,rt="",ra="dd&lt;/th' how="" rel="preconn&lt;/td&gt;&lt;td&gt;12152&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;3/4&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;,rqd=" to=""/> <th>13362</th>	13362
		4/4		alue="how to create anonymous email"><input id="search_</td> <td>20652</td>	20652
₽-□	com.duckduckgo.mobil	1	Plist (Binary)		
		1/1		+how to create anonymous email at DuckDuckGoÓ)0	831
•	6B3F14B8E5F435C097	1			
±-	E5420DB330D033AA8	1			

#### Figure 28: Keyword Search results

Artifacts > Mobile > Application State iOS confirms that DuckDuckGo is installed:

```
Figure 29: Artifacts > Mobile > Application State iOS
```

Forensic Explorer 🚦 🚵 👻 🍘	
合 Evidence 🛛 🔂 File System 🗚	rtifacts 🖉 Keyword Search 👂 Index Search
Process Browsers Chat Email Fi	\$ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
Tree 4	🔜 File List
Filter: 💭 No Filter 🗸 🖃	🖗 🖻 🔯 😥 Application 🐼 🗸 duck
Filename A	Application ID Application Identifier
ABE (9) Chat (15) Chat (15) C	1 📄 250 com.duckduckgo.mobile.ios
Application State IOS (217)	

Figure 30: Artifacts > Browsers > DuckDuckgo

Forensic Explorer 🚦 🚵 👻 👹		
合 Evidence 🛛 🎦 File System	Artifacts P Keyword Search P Index Se	arch
Process Browsers Chat Ema	Finance Apps Apps Biome OS	le Sc M
Artifact Tree	📮 🥮 File List	
Filter: 🗾 No Filter	🗸 😑 🖗 🗑 🐼 🐼 Title 🛛 🐼 L 🐼 UU	ID
Filename	▲ Title URL UUID	
🔲 🚟 ABE (9) 🛛	1 📄 bookmarks_root bookmar	ks_root
Browsers (19)     Bing Query (1)     Dating URL (43)     PaceBook URLS (6)     G @ Google Query (88)     G Chrome Bookmarks (3)     Chrome Favicons (66)     G Chrome History (45)     Chrome Keyword Search Terms (6)     G Chromium Cache (1911)	2 📄 favorites_root favorites	s_root

# QUESTION 14 - NAVIGATION - LEVEL 3 (50 POINTS)

Abe was navigating while driving, on June 26, 2023. What was the destination address on the navigation?

Q14. ANSWER

284 Central Way, Kirkland

Q14. FORENSIC EXPLORER METHODOLOGY

This question is in progress. Check back soon.

# QUESTION 15 - CRYPTO - LEVEL 2 (30 POINTS)

Abe used MOB to send/receive crypto within Signal. Can you find the Recovery Phrase for Signal Mobile Coin wallet? What is it? (24 words)?

#### Q15. ANSWER

pet element blast mix trumpet usual leg aim office jaguar emerge fatigue tent volcano other unfair absent hope power annual banana speak initial gold

Q15. FORENSIC EXPLORER METHODOLOGY

This question is in progress. Check back soon.

# QUESTION 16 - PICTURE - LEVEL 2 (30 POINTS)

Abe loves taking pictures and videos on the iPhone, the problem is when Abe is trying to look for a picture, he is having hard time finding it therefore he utilizes the Search within the Apple Photos app. If Abe would have looked for a picture of: Myself, Pawel, and Hat he would end up with one photo. Can you name that filename?

#### Q16. ANSWER

IMG\_1100.HEIC

#### Q16. FORENSIC EXPLORER METHODOLOGY

The Photos.sqlite database on an iPhone contains a wealth of information about all the photos and videos stored on the device, including their metadata such as creation date, modified date, location data, and more. It also stores information about face recognition and the relationships between photos and the applications they were created with. The database can be challenging to work with due to its complex structure, but it provides valuable insights for forensic investigations.

In Forensic Explorer, to identify names attributed to iPhone photos:

- 1. Select Artifacts > Mobile > Photos.Sqlite Person iOS.
- 2. In the Display Name or Full Name columns, change the column filter to RegEx.
- 3. Filter the column by Myself | Pawel (Myself OR Pawel).
- 4. **Double-click** on the **File Name** column header to sort the filtered result by **File Name**.
- Search in the sorted File Name list for a file that contains both Myself and Powell. This identifies IMG\_1100.HEIC as a candidate.
- 6. Right-click and Copy cell to copy the Filename.
- In the File System module, branch plate [ > ] the entire case and paste the copied filename into the Filename column.
- 8. In the bottom window, change to the **Display View** to view the photo.

#### Figure 31: Artifacts > Photos.sqlite

Evidence       File System       Arttfacts       Keyword Search       Index Search       Index Search       Image	Forensic Explorer 🚦 🚵 🔻 🍘	0	
Image: Second	合 Evidence 🛛 🛅 File System	Artifacts P Keyword Search D Index Search	ch 🔘 Em
Artifact Tree       0       # File List         Filter:       No Filter       Image: State St	Process Browsers Chat Email	Finance Apps Health Apps Biome OS	✓ Social Media
Filter       Image: Second Secon	Artifact Tree 4	🛄 File List	
Filename       A       Date Created       File Name       Doplay Name         Image: CTF 2023 - Cellebrite - ABE (9)       Image: CTF 2023 - Cellebrite - ABE (7)       Image: CTF 2023 - Cellebrite - ABE (7)<	Filter: 🗾 No Filter 🛛 🗸 😑	🖗 🖻 🎯 📵 Date Created 🛛 🐼 🖬 File Name 🌘	<ul> <li>myself pawel</li> </ul>
Photos Solite Person iOS (150) 105 - st 150 Visible ILS 0 (b test DS 0 (b test) 2 (b test) 2 (b test d ILS 0 (b test DS	Filename       A         CTF 2023 - Cellebrite - ABE (9)       Browsers (19)         CTF 2023 - Cellebrite - ABE (9)       Filename         Chat (15)       Filename         Filename       Silename         Silename       <	Date Created         File Name         A         Dis           80         26-May-2023 ft.25.30 Min         IMG_0905.HEIC         Min           81         31-May-2023 ft.25.52 AM         IMG_0905.HEIC         Min           82         31-May-2023 ft.25.52 AM         IMG_0112.HEIC         Min           83         31-May-2023 ft.35:16 AM         IMG_0102.HEIC         Min           84         01-Jun-2023 ft.13:25 PM         IMG_1020.HEIC         Min           85         01-Jun-2023 ft.19:26 PM         IMG_1020.HEIC         Min           86         01-Jun-2023 ft.19:31 PM         IMG_1020.HEIC         Min           87         03-Jun-2023 ft.19:31 PM         IMG_1028.HEIC         Min           88         03-Jun-2023 12:11:49 AM         IMG_1053.HEIC         Min           89         05-Jun-2023 5:53:03 PM         IMG_1096.HEIC         Min           90         05-Jun-2023 5:53:03 PM         IMG_1098.HEIC         Min           91         05-Jun-2023 5:54:02 PM         IMG_1100.HEIC         Min           92         05-Jun-2023 12:50:07 AM         IMG_1121.HEIC         Min           93         05-Jun-2023 12:50:07 AM         IMG_1121.HEIC         Min           94         07-Jun-2023 12:50:07 AM	play Name ysen yself

#### Figure 32: File System > column filter > Display View > IMG\_1100.HEIC

File List	Gallery View Stideo Vi	iew 🔚 Disk	View 🅙 Cate	gory Graph	1	1
0	MG_1100.HEIC	Ext	AZ▼ File Sig	Az▼ E	Gz File (	A-Z-
□ 1 □ 2	Filename TMG_1100.HEIC MG_1100.HEIC	Extension HEIC	File Signature HEIF Folder	Exte No	File Cate Graphics	Pat EX EX
EXTRACTI	ON_FFS.ufd\filesystem2\mob	ile\Media\DC	CIM\101APPLE\	IMG_1100	HEIC	
2 of 673874 Vi	sible [LS 1.2 MB PS 1.2 MB]		1 Highlight	ed [LS 1.2	MB PS 1.2 M	B]

#### Alternate Method – Custom SQLite Query

As the question asks for specific information that is drawn from sever different SQLite tables inside Photos.sqlite, a custom SQLite query is an effective method of locating the filename of interest. To perform a custom SQLite search:

- In the Forensic Explorer File System module, branch plate [▶] the entire case and use the column filter to locate the Photos.sqlite file and its associated -wal and -shm files.
- 2. Highlight the files, right-click and **Export > Files and folders**.

Figure 33: Open the raw Photos.sqlite database (and associtated -shm and -wal)

III File List	Sollery View	Video	View 🔚 Disk View 🅙 Cate	gory Grapł	i i				
Sg 🖸 🎆	PHOTOS.SQLITE			Az ▼ Ext	File Sig	AZ▼ E	File (	Main PhotoData	
	Filename			Extension File Signature Exte File Cate Path				Path	
1	Photos.sqlite			sqlite	SQLite	No	Database	EXTRACTION_FFS.ufd\filesystem2\mobile\Media\PhotoData\	
2	Photos.sqlite-shm			sqlite	Sqlite SHM	No	Database	EXTRACTION_FFS.ufd\filesystem2\mobile\Media\PhotoData\	
3	Photos.sqlite-wal		Add Bookmark	sqlite-w	al Sqlite WAL	No	Database	EXTRACTION_FFS.ufd\filesystem2\mobile\Media\PhotoData\	
			Classify						
			Flags						
EXTRACTION_FFS.utd(httesystems)			Open Open with	sqlite-w	al 5 MB PS 38.6 MB	Checked [LS 0 bytes PS 0 bytes] Pr			
			Export	Exp	Export Rows (TAB, CSV, HTML, XLSX)				
			Send to module	Folders and Files					

- 3. Use the shortcut folder at the top of Forensic Explorer to navigate to the **Exported** folder of the current case.
- 4. **Open Photos.sqlite** with a **3<sup>rd</sup> party application**, e.g. DB browser for SQLite.
- 5. The SQLite query suggested by STARK-4n6 is:

SELECT DISTINCT ZPERSON.ZFULLNAME AS FULL\_NAME, ZASSET.ZFILENAME AS FILENAME, ZASSET.ZDATECREATED + 978307200 AS DATECREATED FROM ZPERSON INNER JOIN ZDETECTEDFACE ON ZPERSON.Z\_PK=ZDETECTEDFACE.ZPERSON INNER JOIN ZASSET ON ZDETECTEDFACE.ZASSET=ZASSET.Z\_PK WHERE ZPERSON.ZFULLNAME LIKE "Pawel" ORDER BY ZASSET.ZDATECREATED DESC

#### Figure 34: DB Browser for SQLite (Query source: https://www.stark4n6.com/2023/10/cellebrite-ctf-2023-abe.html)

B Browser for SQLite - C:\Users\graha\Documents\Forensic Explorer v5\Cases\ABE Walk-Through\Exported\Photos.sqlite									
<u>F</u> ile I	<u>E</u> dit <u>V</u> iew <u>T</u> o	ols <u>H</u> elp							
( <b>a</b> o	pen Project 🛛 🤇	ave Project	😹 Attach Database 🛛 💥 Close Database						
Database Structure Browse Data Edit Pragmas Execute SQL Edit Database									
-				Mode: Text					
1 2 3 4	SQL 1 SELECT ZPE FROM ZPERS INNER JOIN	ERSON.ZFULLNAME, SON N ZDETECTEDFACE N ZASSET ON ZDET	ZPERSON.ZDISPLAYNAME, ZASSET.ZFILENAME ON ZPERSON.Z_PK=ZDETECTEDFACE.ZPERSON	1 Mysel					
5	WHERE ZPER ORDER BY 2	RSON.2FULLNAME L	IKE "myself" or ZPERSON.ZFULLNAME LIKE "pawel"	Type of data c 6 character(s)					
_				Remote					
	ZFULLNAME	ZDISPLAYNAME	ZFILENAME	Identity Sel					
89	Myself	Myself	IMG_1098.HEIC	DBHub.io					
90 Myself Myself IMG_1099.HEIC									
91	Pawel	Pawel	IMG_1100.HEIC						
92	Myself	Myself	IMG_1100.HEIC	Name					
93	Myself	Myself	IMG_1113.HEIC						

# QUESTION 17 - LOCATION - LEVEL 2 (30 POINTS)

Abe went for some shady meeting on an island but tried to conceal as a vacation so he took a boat tour and tracked dolphins. He then decided to mark a location with "dolphins". What was the timestamp for that location? [HH:MM:SS] written in UTC time"?

#### Q17. ANSWER

17:57:35.

#### Q17. FORENSIC EXPLORER METHODOLOGY

Figure 35: Artifacts > Search Artifact Results



#### Figure 36: Artifacts > Search Artifact Results > Dolphin

Search Artifacts	Results		-	
Keyword Count:		1		
Artifacts Module Bates ID	e: RegEx Search Term	Folder	Match Text	
678247	dolphins	Open GPX Tracker iOS	7:57:35 AM	dolphins
Match Summary: RegEx Term  dolphins		Hits  1		
Total Artifacts Search Artifacts	: 5 Results finished.	1		
Search Artifacts Time Taken: 00:0	s Results finished. 02:13			•
		Copy to Clipboard	Save CSV and Close	Close

In the **Artifacts** module, select **Tracking** > **Open GPX Tracker iOS** and examine the **Waypoint Name**. To confirm the **UTC time**:

- The Artifacts > Source Name column identifies open-gpx-tracker-session.sqlite as the source file. Right-click to copy the Source Name.
- 2. In the **File System** module, branch plate [▶] the **entire case**, and use the column filter to locate **open-gpx-tracker-session.sqlite**.
- In Display View, locate the ZCDWAYPOINT table, and for dolphins entry, copy the raw
   ZTIME integer value.
- 4. Enter this value into a time decoding program (e.g. DCode) to confirm that the time value is in **UTC**.

#### Figure 37: Artifacts > Tracking > Open GPX Tracker iOS

Forensic Explorer 🚦 🚵 🗸 🎲 🗸 🕡				For
合 Evidence 🗋 File System 🗚	Artifacts	P Keyword Search	🔎 Index Search	@ Email 🔡 Re
Process Browsers Chat Email F	\$ Finance H Apps A	ealth MAC Mob	ile <sup>×</sup> Social <sup>×</sup> W Media	indows <sup>×</sup> OS Carve
Artifact Tree 4	🛄 File List			
Filter: 💭 No Filter 🗸 🚽	8 o 🐯	I Timestamp	₩aypoint Nam	₩ Waypoint Description
Filename A		Timestamp 🛛	Waypoint Name	Waypoint Description
ABE Walk-Through (8)	1	29-Apr-2023 11:49:34 PM	4:49:34 PM	Apr 29, 2023 at 4:49:34 PM
Erowsers (19)	2	02-May-2023 11:20:15 PM	4:20:15 PM	May 2, 2023 at 4:20:15 PM
🕀 📃 🕎 Chat (14)	3	📄 26-May-2023 1:16:44 AM	6:16:44 PM	May 25, 2023 at 6:16:44 PM
🕀 📃 🎯 Email (1)	4	28-May-2023 11:01:57 PM	4:01:57 PM	May 28, 2023 at 4:01:57 PM
Finance (0)	5	28-May-2023 11:02:14 PM	4:02:14 PM	May 28, 2023 at 4:02:14 PM
🕀 🛄 😳 Health Apps (4)	6	📄 01-Jun-2023 9:57:20 PM	11:57:20 AM	Jun 1, 2023 at 11:57:20 AM
🕂 🔄 🌉 MAC Operating System (1)	7	02-Jun-2023 5:57:35 PM	7:57:35 AM dolphins	Jun 2, 2023 at 7:57:35 AM
EH Tracking (1)				
Open GPX Tracker iOS (7)				

#### Figure 38: open-gpx-tracker-session.sqlite

					Fo	rensic Ex	<plorer th="" √5<=""><th>.6.8(4559d) (6</th><th>i4bit) Case: A</th><th>BE Walk-Thro</th><th>ugh</th><th></th></plorer>	.6.8(4559d) (6	i4bit) Case: A	BE Walk-Thro	ugh	
ifacts 🖉 Keyword Sea	arch 🔎	Index Sear	rch	() Email	Re	gistry	EE Boo	okmarks	Reports	Script	s	
Expand Expand Expand Here	M ktract Analy tadata Progr	ysis 1 ams	Oriage ✓	Quick Registry	File	# Hash Files	# Hash Match	# Hash Set ~ Create	Virtual Live Boot	Cisco Clam Anti Virus	ر Tools ~	Quick ~ Reports
File List 😨 Gallery View	Stideo View	🔤 Disk View	🕘 Categ	gory Graph								
😼 🖻 😻 🐼 open-gpx-tr	acker-session			AZY Ext	√Z▼ File Sig	AZY E	AZ▼ File (	AZ Path				
Filename				Extension	File Signature	Exte	File Cate	Path				
1 open-gpx-trac	ker-session.sqlite			sglite	SQLite	No	Database	EXTRACTION FFS.ufd\filesystem2\mobile\Containers\Data\Application\A6655F				plication\A6655F24-1
2 open-gpx-trac	ker-session.solite-	shm		sglite	Sqlite SHM	No	Database	EXTRACTION	EXTRACTION FFS.ufd\filesvstem2\mobile\Containers\Data\Application\A6655F24			
3 open-gpx-trac	ker-session.solite-	wal		solite-wal	Solite WAL	No	Database	EXTRACTION FFS.ufd\filesvstem2\mobile\Containers\Data\Application\A6655F24-				plication\A6655F24-1
EXTRACTION_FFS.ufd\filesys	tem2\mobile\Cc	ontainers\Da	ta\Applicat	ion\A6655F2	4-1B16-4EC4	9DFA-2D5	5B562CB05\	Library\open-gp	x-tracker-sessio	n.sqlite		
3 of 673874 Visible [LS 1.6 MB P	5 1.6 MB]	1	1 Highlighte	ed [LS 1.5 ME	PS 1.5 MB]		(	Checked [LS 0 ]	oytes PS0 bytes	1	c	open-gpx-tracker-se
✓ Tables	7 PK *	Z ENT	Z OPT	ZWAYP.	ZELEVA	ZI ATIT	ZI ONG	ZTIME	ZDESC		71	IAME
> ZCDROOT				-	5.540	47.646	400.0	70 450 4074 007				
> ZCDTRACKPOINT		3	1		-5.545	47.040	-122.2	704504974.087	40 Apr 29, 701 Mar 2	2023 at 4:49:34 P	111 43 M 43	49:34 PM
<ul> <li>ZCDWAYPOINT</li> </ul>	B	3	1	1	3.1254	47.6/3	-122.2	/04/62415.601	781 May 2,	2023 at 4:20:15 P	M 4:	20:15 PM
···· CREATE TABLE ZCDW/	AYPOIN /	3	1	U	18.040	45.515	-122.6	/06/56604.19/	754 May 25,	2023 at 6:16:44	PM 6:	10:44 PM
> Z_METADATA	8	3	1	U	0.6652	47.676	-122.2	/0/00//17.739	188 May 28,	2023 at 4:01:57	PM 4:	01:57PM
> Z_MODELCACHE	9	3	1	1	5.2105	47.676	-122.2	/0/00/734.758	759 May 28,	2023 at 4:02:14	PM 4:	02:14 PM
> · Z_PRIMARYKEY	10	3	1	0	2.7629	21.329	-157.9	/07349440.617	/44 Jun 1, 2	023 at 11:57:20 /	AM 11	:57:20 AM
	11	3	2	0	1.3373	21.988	-159.7	707421455.0093	377 Jun 2, 2	023 at 7:57:35 Al	4 <mark>7:</mark>	57:35 AM dolphins

#### Figure 39: DCode (https://www.digital-detective.net/dcode/)

() DCode v5.5 –										
E Tr	File Tools Theme Help									
	Name	Timestamp	Value Input							
	→	2023-06-02 17:57:35.0090000 Z		Numeric						
	Apple Absolute Time	2023-06-03 03:57:35.0090000 +10:00	Format	Numeric •						
	Apple HFS (Local)	1926-06-01 17:57:35.0090000	Value	707421455.009377						
	Apple HFS+ (UTC)	1926-06-01 17:57:35.0090000 Z		Decode						
	Apple HFS+	1926-06-02 03:57:35.0090000 +10:00		L						

# QUESTION 18 - BOKERTOV - LEVEL 3 (100 POINTS)

Within the last month before Abe got arrested (and his device was extracted), Abe used to wake up naturally however, there was one day the phone did. What was the day and (local) time? [YYYY-MM-DD HH:MM:SS] e.g: 2021-09-19 08:35:00?

#### Q18. ANSWER

2023-06-16 06:00:00.

#### Q18. FORENSIC EXPLORER METHODOLOGY

Figure 40: Artifacts > Biome > User Notification Events iOS



#### Screen Snapshot:

There is a screenshot in the following path:

filesystem2\mobile\Containers\Data\Application\73B09176-74A6-4676-AE95-0769BC8603D3\Library\SplashBoard\Snapshots\sceneID\_com.apple.mobiletimerdefault\17FA1799-E1EF-42E8-A76F-91F7E63319E4@3x.ktx

Forensic Explorer does not currently view .ktx files. This feature is currently in development.