CELLEBRITE 2023

CAPTURE THE FLAG (CTF) FELIX IPHONE

| CTF Questions Only | 2 |
|---|----|
| About This CTF Challenge | 4 |
| Starting this challenge in Forensic Explorer | 5 |
| Question 1 - Voicemail - level 1 - (10 points) | 6 |
| Question 2 - Picture - level 1 (10 points) | 7 |
| Question 3 - Confirmation - level 1 (10 points) | 9 |
| Question 4 - Photo (10 points) | 11 |
| Question 5 - Location (10 points) | 12 |
| Question 6a - Size - Level1 (10 points) | 14 |
| Question 6b - Time - Level 2 (30 points) | 15 |
| Question 7 - Size - Level 2 (30 points) | 16 |
| Question 8 - Missing - Level 2 (30 points) | 17 |
| Question 9 - Wiped - Level 2 (30 points) | 19 |
| Question 10 - Cruise - Level 2 (30 points) | 20 |
| Question 11 - Data - Level 3 (50 points) | 23 |
| Question 12 - H is mean - Level 3 (100 points) | 24 |

CTF QUESTIONS ONLY

| 1. | Question 1 - Voicemail - level 1 - (10 points) <i>Please look at the following image: IMG_0026.HEIC. How many times do you see this</i> <i>picture on the device (including thumbnails)?</i> |
|----|--|
| 2. | Question 2 - Picture - level 1 (10 points) Felix confirmed receiving "everything." When Felix sent the confirmation, which account did he sent it from? |
| 3. | Question 3 - Confirmation - level 1 (10 points) <i>Felix confirmed receiving "everything." When Felix sent the confirmation, which</i> <i>account did he sent it from?</i> |
| 4. | Question 4 - Photo (10 points) <i>Private Photo Vault is an application that is installed on the phone. What is the passcode to the application?</i> |
| 5. | Question 5 - Location (10 points) Felix always had an interest in the USA. What application did he use to search an address in New Jersey USA? |
| 6. | Question 6a - Size - Level1 (10 points) What is the size (in bytes) of the ChatStorage.sqlite-wal file? (Answer with numeric digit(s) only) |
| 7. | Question 7 - Size - Level 2 (30 points) What is the date and time the -WAL file from Felix 06a committed to the main database? |

| 8. | Question 8 - Missing - Level 2 (30 points) When was the SIM card information on Felix's phone last updated? (Raw data, not converted) |
|-----|---|
| 9. | Question 9 - Wiped - Level 2 (30 points) The WhatsApp chat database appears to be missing some chat messages. Assuming the highest number is the last message, how many messages are missing? |
| 10. | Question 10 - Cruise - Level 2 (30 points) When was Felix's phone last wiped? [YYYY-MM-DD HH:MM:SS] |
| 11. | Question 11 - Data - Level 3 (50 points) Felix was researching / surveilling a ship as a possible target and downloaded a photo of it. What is the name of the cruise ship? |
| 12. | Question 12 - H is mean - Level 3 (100 points) Felix was referred information about pension reform. What is the SID associated with that artifact? |

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: CellebriteCTF23_Felix.zip

MD5: 996A913B1301AB011CA7DD8CA93A9400

OTHER ONLINE SOLUTIONS

The following other solutions can be found online:

- https://cellebrite.com/en/cellebrites-ctf-2023-recap-answers-for-felixs-iphone-device/
- https://www.stark4n6.com/2023/10/cellebrite-ctf-2023-felix.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 Cellebrite file: EXTRACTION_FFS.ufd
- 5. In the **Evidence Processor** window use the default options.

Figure 1: Evidence module > Add Image

| Evidence | |
|---------------|--|
| Add device | CTF 2023 - Cellebrite FELIX (1) |
| 👩 Add image 🗸 | Evidence Processor |
| Add file | Evidence Name: EXTRACTION_FFS.ufd |
| 🔁 Add folder | (DEFAULT) |
| | Tasks |
| Add group | Process in Parallel |
| 🏷 Add remote | Verify Device Hash Search for ISO Tracks (CD/DVD) |
| | - Search for MBRs |
| 🔀 Remove | Search for FileSystems |
| 🤌 Credentials | - Analysis - Analysis |
| | A Trippe |

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
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraint of the system

 Image: Constraint of the system
 Image: Constraity of the system

Figure 2: Artifacts > Process All

QUESTION 1 - VOICEMAIL - LEVEL 1 - (10 POINTS)

Felix received a voicemail from +1-416-435-5684. How many seconds in length was the voicemail message?

Q1. ANSWER

27 seconds.

Q1. FORENSIC EXPLORER METHODOLOGY

In the **Artifacts** module:

1. Select Mobile > Voice Mail iOS.

Figure 3: Artifacts > Mobile > Voice Mail iOS

| Forensic Explorer 🚦 🚵 👻 🎯 | | | | | | |
|--|-----------------|--|---|---|--|----------------------------------|
| 合 Evidence 🛛 🎦 File System | Artifacts | P Keyword | d Search | ▶ Index Sear | ch 🔘 E | mail |
| Process All Browsers Chat Email | Finance Apps | Health Apps B | iOS MA iome O | AC Mobile | Social Media | Tracking Apps |
| Artifact Tree 4 | 🔜 File List | _ | Ve | | ~ | Ven |
| Filter: | | Date | <u>A-Z</u> ▼ | Token | Age Sender | Dur |
| Filename A Filename S CTF 2023 - Cellebrite FELIX (8) Browsers (9) Chat (7) Semail (2) Finance (0) Health Apps (3) Ction (2) Semail (2) Semail (2) Semail (2) MAC Operating System (1) Mobile (23) Mobile (23) Accounts Type iOS (34) Application Permissions iOS (127) Application Permissions iOS (127) Application Vage iOS (1998) Semail Bluetooth Devices iOS (1998) Semail Bluetooth Devices iOS (2) Bluetooth Devices iOS (2) Bluetooth Devices iOS (1001) Cached Locations iOS (7813) Calendar Items v4 iOS (60) Semail Calendar Items v4 iOS (60) Semail Calendar Items v4 iOS (10) Contacts Details iOS (10) Calendar Items v6 iOS (12) Contacts Details iOS (10) Calendar Items v6 iOS (10) Data Usage iOS (349) Semail Calendar Items v6 iOS (11) Photos.Sqlite iOS (11) Photos.Sqlite iOS (11) Photos.Sqlite iOS (13) | | Date 24-Feb-2023 12:3 20-Jun-2023 2:09 24-Feb-2023 12:3 20-Jun-2023 2:09 | Toker 8:12 PM <uni 8:12 PM <uni 8:12 PM <uni< td=""><td>n isys-VVM-33785 isys-VVM-33785 isys-VVM-33785</td><td>Sender +33787557682 +14164355684 +33787557682 +14164355684</td><td>Duration 21 27 21 27</td></uni<></uni </uni | n isys-VVM-33785 isys-VVM-33785 isys-VVM-33785 | Sender +33787557682 +14164355684 +33787557682 +14164355684 | Duration 21 27 21 27 |
| Significant Locations iOS (22) Significant Locations Visits iOS (28) SMS v4 iOS (57) Ov Voice Mail iOS (4) Wifi Locations iOS (1944) | | | | | | |

QUESTION 2 - PICTURE - LEVEL 1 (10 POINTS)

Please look at the following image: IMG_0026.HEIC. How many times do you see this picture on the device (including thumbnails)?

Q2. ANSWER

5 instances.

Q2. FORENSIC EXPLORER METHODOLOGY

Important: If HEIC files do not display in either Gallery View or display view, a HEIC drive is required. Install from: <u>https://www.copytrans.net/copytransheic/</u>.

To locate IMG_0026.HEIC files:

- 1. Branch plate [] the entire case.
- 2. In the File System > File List > Filename column filter, enter IMG_0026.HEIC.
- 3. This filter locates **four files**, plus **one folder**, of the same name.
- 4. Inside the IMG_0026.HEIC folder is an additional file called 5005.JPG.



A search was also run using the File Name Search button.

Figure 4: File System > File Name Search



Figure 5: File Name Search result

File/Folder Name

```
EXTRACTION_FFS.ufd\filesystem2\mobile\Library\Caches\com.apple.MobileSMS\Previews\Attachments\ff\15\D4797FAC-8067-4768-A
EXTRACTION_FFS.ufd\filesystem2\mobile\Library\SMS\Attachments\97\07\64E43269-C3B4-4FFD-8A14-41FFD406EDA1\IMG_0026.HEIC
EXTRACTION_FFS.ufd\filesystem2\mobile\Library\SMS\Attachments\ff\15\D4797FAC-8067-4768-A5E7-EE3D325E5711\IMG_0026.HEIC
EXTRACTION_FFS.ufd\filesystem2\mobile\Media\DCIM\100APPLE\IMG_0026.HEIC
EXTRACTION_FFS.ufd\filesystem2\mobile\Media\PhotoData\Thumbnails\V2\DCIM\100APPLE\IMG_0026.HEIC
```

Figure 6: IMG_0026.HEIC



QUESTION 3 - CONFIRMATION - LEVEL 1 (10 POINTS)

Felix confirmed receiving "everything." When Felix sent the confirmation, which account did he sent it from?

Q3. ANSWER

felix.davey@orange.fr

Q3. FORENSIC EXPLORER METHODOLOGY

In the **Artifacts** module:

1. Use the Search Artifact Results button to search for "I received everything".

Figure 7: Artifacts > Search Artifact Results



Figure 8: Artifacts > Search Artifact Results > output

| Search Artifacts Results | | | | | | | | | |
|--|------------------------------|---------------|--|--|--|--|--|--|--|
| Keyword Count: | | 1 | | | | | | | |
| Artifacts Bates ID | Module: RegEx Search Term | Folder | Match Text | | | | | | |
| 432545 | everything | Mail iOS | I receive everything Sent from my iPhone | | | | | | |
| Match Summ RegEx Terr | nary: n - J | Hits 1 | | | | | | | |
| Total Artifacts: Search Artifacts Results finished. | | 1 | | | | | | | |
| Search Art | tifacts Results finished. | | | | | | | | |

The search result identifies **Artifacts** > **Emil** > **Mail iOS** as a potential source:

Figure 9: Artifacts > Email > Mail iOS

| Forensic Explorer 🗟 🔹 🍥 🗸 🔞 | | | | | | | | | |
|---------------------------------------|--------------|---------------------------|------------------------|----------------------------------|-----------------------|--|--|--|--|
| 🔂 Evidence 🕅 File System | m 📌 | Artifacts 🖉 Keyv | word Search 👂 🔎 | Index Search | () Email | Registry Bookmarks | | | |
| Process All Browsers Chat V | @ Email ~ | Finance Apps Apps Apps | iOS Biome Biome | ↓ Mobile ↓ | Social Media | Vindows Artifact Carve | | | |
| 📕 Artifact Tree 🛛 🕂 | 🧰 File List | | | | | | | | |
| Filter: 🔄 No Filter 🗸 😑 | ig e 🔯 | Date Sent | Date Received | AZ▼ Sender | AZ▼ Subject | Summary | | | |
| Filename 🔺 | | Date Sent | Date Received | Sender | Subject | Summary | | | |
| 🛄 🚟 CTF 2023 - Cellebrite FELIX (8) 🛛 | 1 | 19-May-2023 2:11 | 19-May-2023 2:11:53 | noreply.intern | Mail Orange : Bienve | Le Mail Orange Bonjour, Avec le Mai | | | |
| 🕂 🗌 🎯 Browsers (9) | 2 | 02-Jun-2023 3:42: | 02-Jun-2023 3:42:35 PM | felix.davey@o | Confirmation | I receive everything Sent from my i. | | | |
| 🕂 🗌 架 Chat (7) | 3 | 02-Jun-2023 7:00: | 02-Jun-2023 7:00:00 PM | felix.davey@o Material | | | | | |
| - Email (2) | 4 | 02-Jun-2023 3:59: | 02-Jun-2023 3:59:48 PM | aberudder 77 | Confirmation | Ok, thanks for letting me know. | | | |
| — Mail Addresses iOS (6) | 5 | 14-Jun-2023 4:24: | 14-Jun-2023 4:24:42 PM | hello@what3w | Get started with the | Finding a what3words address View | | | |
| Mail iOS (8) | 6 | 14-Jun-2023 4:14: | 14-Jun-2023 4:14:31 PM | support@what | Please confirm your d | Please confirm your details Hello Feli | | | |
| Finance (0) | 7 | 22-Jun-2023 4:36: | 22-Jun-2023 4:36:56 PM | hello@what3w How what3words bega | | n Watch our CEO and Co-founder's T | | | |
| 🕀 🖸 🛟 Health Apps (3) | 8 | 30-Jun-2023 4:37: | 30-Jun-2023 4:37:03 PM | hello@what3w | Add a what3words wi | Quick access to your current what3 | | | |

As a follow-up search, In the **Keyword Search** module:

1. Add the keyword phrase "I received everything".

This search locates two files in the filesystem called **full.emlx**. These files can be displayed with the full email header.

| Forensic Explorer | 👌 = 🎲 = 🙆 | | | | | Forensic Exp |
|----------------------------------|-------------------------------------|---|--------------------------------------|------------------------------------|--|---|
| 合 Evidence | File System | Artifacts | 🔑 Keyword Search | ho Index Search | () Email | Registry |
| Add Add A Keyword Multiple Gr | Add Edit Youp Keyword K | Delete Impor Keyword Keywor | t Export Start ds Keywords Search | Keyword Keywords Count In Files | | |
| Keyword Management 4 | Keyword Tree Keyword Label | | Keyword Result List 🔋 Galler | y View 😨 Video View | | |
| Keyword Label | Keyword Res | ults (1) 😼 🖻 | 🐼 🐼 Filename | Hits | | (|
| Keywords (1) | | eive everyt | Filename | Hits Hit Te | ext | |
| - V Treceive everyuni | | 9- | full.emlx | 1 | _ | |
| | | ₽-E | - Difull.emlx | 1/1 .co 2 | m> <mark>I receive eve</mark> : | ythingSen |
| | | | - | 1/2 te: | <pre>> I receive ever 4)">I receive ever</pre> | <pre>rything.>.>.> rything .<</pre> |
| | | | Protected Index-v | val 10 | | |
| | | <u>+</u> + | hot. 16699150435 | 563 2 | | |
| | 0 of 2 Charland | EX | IRACTION_FFS.ufd\filesystem | n2\mobile\Library\Mail\N | NonpurgeableMessageD | ata\33\full.emlx |
| | 0 of 5 Checked | 5015 | USIDIE [L3 390 KD P3 390 KD] | | r Highlighted [ES 540 by | (les PS 540 byles) |
| | Subject: Confirma From: Felix Da | ation wey <felix.davey@< td=""><td>prange.fr></td><td></td><td></td><td></td></felix.davey@<> | prange.fr> | | | |
| | Sent Date: 02-Jun- | 2023 5:42:35 PM UT | C Received Date: | | | |
| | To: Abe Rud | dder <aberudder77< td=""><td>@gmail.com></td><td></td><td></td><td></td></aberudder77<> | @gmail.com> | | | |
| | 📄 Message 付 | Header | | | | |
| | 1 receive eve | rything | | | | |
| | Sent from my | iPhone | | | | |

Figure 10: Keyword Search > "I received everything"

QUESTION 4 - PHOTO (10 POINTS)

Private Photo Vault is an application that is installed on the phone. What is the passcode to the application?

Q4. ANSWER

2510.

Q4. FORENSIC EXPLORER METHODOLOGY

This answer is being updated. Check back soon.

QUESTION 5 - LOCATION (10 POINTS)

Felix always had an interest in the USA. What application did he use to search an address in New Jersey USA?

Q5. ANSWER

Apple Maps.

Q5. FORENSIC EXPLORER METHODOLOGY

Apple Maps is the usual suspect for navigation searches on an iPhone. In the **Keyword Search** module:

1. Search for the keyword **New Jersey**:

Figure 11: Keyword Search module

| E Keywor | d Result List 🔋 Gallery View | 🔋 Video V | iew | |
|-------------|------------------------------|-----------|---|-------------------|
| ig o 🔯 | Filename | 19 Hits | | Hit Offset (I |
| | Filename 🔺 | Hits | Hit Text | Hit Offset (File) |
| ₽- □ | MapsSync_0.0.1 | 12 | | |
| | | 1/12 | ateszzUnited StatesUS <mark>New Jersey</mark> ".NJ*.Bergen County2.Closte | 66945 |
| | | 2/12 | ted StatesUnited States <mark>New Jersey</mark> ".New Jersey*.Bergen County | 67127 |
| | | 3/12 | United StatesNew Jersey". <mark>New Jersey</mark> *.Bergen County2.ClosterB.G | 67139 |
| | | 4/12 | .)Address Â. {s:s}Closter, <mark>New Jersey</mark> {/s:s}2s`},ÅA". | 67452 |
| | | 5/12 | .)Address Â. {s:s}Closter, <mark>New Jersey</mark> {/s:s}2s`}ìÜÅA". | 538694 |
| | | 6/12 | ateszzUnited StatesUS <mark>New Jersey</mark> ".NJ*.Bergen County2.Closte | 539781 |
| | | 7/12 | ted StatesUnited States <mark>New Jersey</mark> ".New Jersey*.Bergen County | 539963 |
| | | 8/12 | United StatesNew Jersey". <mark>New Jersey</mark> *.Bergen County2.ClosterB.G | 539975 |
| | | 9/12 | ateszzUnited StatesUS <mark>New Jersey</mark> ".NJ*.Bergen County2.Closte | 546460 |
| | | 10/12 | ted StatesUnited States <mark>New Jersey</mark> ".New Jersey*.Bergen County | 546642 |
| | | 11/12 | United StatesNew Jersey". <mark>New Jersey</mark> *.Bergen County2.ClosterB.G | 546654 |
| | | 12/12 | .)Address Â. {s:s}Closter, <mark>New Jersey</mark> {/s:s}2s`},ÅA". | 546967 |
| ⊕- □ | MapsSync_0.0.1-wal | 4 | | |

The search result identifies MapsSync_0.0.1 (a known Apple Maps file) as a potential source.

In the Artifacts module:

1. Examine Mobile > Apple Maps Searches iOS.

This shows that the address **49 Colgate St, Closter, NJ 07624, United States**, was searched in Apple maps on 14 June 2023.

Figure 12: Artifacts > Mobile > apple Maps Searches iOS

| Forensic Explorer 🚦 🚵 👻 🎲 🗸 (| 0 | | |
|---|-----------------------|---|---------------|
| 合 Evidence 🛛 🎦 File System | Artifacts Reyword | Search 🔎 Index Search @ | En |
| Process Browsers Chat Emai | Finance Apps Apps Bio | j MAC Mobile Social MAC Mobile Mobile | ~ |
| 👖 Artifact Tree म | 🛄 File List | | |
| Filter: 🗾 No Filter 🗸 😑 | 🐉 🖻 🔯 🔳 Date Created | Map Item Storage BLOB | $\mathbb{D}($ |
| Filename 🔺 | Date Created | Map Item Storage BLOB | |
| CTF 2023 - Cellebrite FELIX (8) Browsers (9) Chat (7) Email (2) Health Apps (3) Group Biome (5) MAC Operating System (1) Mobile (23) Apple Maps Searches iOS (1) Apple Constant Style iOS (34) | 1 📄 14-Jun-2023 4:18: | 49 Colgate St, Closter, NJ 07624, United States | |

QUESTION 6A - SIZE - LEVEL1 (10 POINTS)

What is the size (in bytes) of the ChatStorage.sqlite-wal file? (Answer with numeric digit(s) only)

Q6A. ANSWER

0 bytes.

Q6A. FORENSIC EXPLORER METHODOLOGY

In the File System module:

- 1. Branch plate [] the entire case.
- 2. Enter ChatStorage.sqlite-wal in the Filename column filter.
- 3. Examine the Logical Size column.

Figure 13: File System > Filename column filter

| Forensic Explorer | 🔒 🗁 ד 🛞 ד 🌘 | 2) | | | | | | |
|---|--|-----------------------|-----------------|------------------|---------------------|-----------------------------|---------------|---------------------|
| Evidence | | Artifa | acts (| P Keyword Search | | ${oldsymbol{ ho}}$ Index Se | arch 🤇 | Email |
| Recover File Name Folders Search | File Carve Capy | Signature Analysis | Expand Files | Expand Video | Extract Metadata | Analysis Programs | C Triage ➤ | Quick ~ Registry |
| Folders Categories | | | | | | | ew 🅙 Catego | ry Graph |
| Filter: 🔄 No Filter | | <u>-</u> § | 3 🖻 🔯 | A₂▼ ChatSto | rage.sqlite-w | €xtensio | 1.9 | 1-9 |
| Filename | Filename | | Extension | Logical Size | Physical Size | | | |
| ▶ ■ ○ Cellebrite CTF F ⊕ - ● ■ ○ EXTRACTION | ELIX (1) [] N_FFS.ufd (8) [UTC (+00 | :00)] | 1 | ChatStor | age.sqlite-wal | sqlite-wal | 0 | 0 |

QUESTION 6B - TIME - LEVEL 2 (30 POINTS)

What is the date and time the -WAL file from Felix 06a committed to the main database?

Q6B. ANSWER

2023-07-01 05:49:55.

Q6B. FORENSIC EXPLORER METHODOLOGY

In the File System module:

- 1. Branch plate [] the entire case.
- 2. Enter ChatStorage.sqlite in the Filename column filter.
- 3. Examine the Logical Size column of the filtered results.

Figure 14: File System > Filename column filter



The **modified** date of **ChatStorage.sqlite** and **ChatStorage.sqlite-wal** files are the same. This is indicative of the commit from the -wal to the database.

QUESTION 7 - SIZE - LEVEL 2 (30 POINTS)

When was the SIM card information on Felix's phone last updated? (Raw data, not converted)

Q7. ANSWER

709888384.063589.

Q7. FORENSIC EXPLORER METHODOLOGY

| 📰 File List 🔋 Gallery View 🔋 Video View 🖨 Disk View 🅙 Category Graph | | | | | | | | | | | |
|--|------------------|----|-----------------|--------------------|--------------------|----------|--------------|--------|------------------|--------------|----------------|
| ig 🗆 🔯 | CellularUsage.db | | 8 | | Az▼ I | Extensio | 1-9 | 1.9 | | <u>A</u> -Z▼ | |
| | Filename | | Modif | ìed | Extens | sion | Logical Size | Physic | al Size | Path | |
| 1 | CellularUsage.db | | 01-J | ul-2023 7:13:04 AM | db | db 4 | | 45,05 | 56 | EXTRACTION | _FFS.ufd\files |
| EXTRACTION_FFS.ufd\filesystem2\wireless\Library\Databases\CellularUsage.db | | | | | | | | | | | |
| ✓ · Tables | | RO | VID * | SUBSCRIBER_ID | | SUBSCR | IBER_MDN | TAG | LAST_U | JPDATE_TIME | SLOT_ID |
| > ·_SqliteDatabaseProperties > ·bundle_info | | 1 | 893301222138136 | | 26250 +33785650921 | | 650921 | 1 | 709888384.063589 | | 1 |
| > ·bundle_uuid > ·sqlite_sequence > ·subscriber_info | | | | | | | | | | | |

QUESTION 8 - MISSING - LEVEL 2 (30 POINTS)

The WhatsApp chat database appears to be missing some chat messages. Assuming the highest number is the last message, how many messages are missing?

Q8. ANSWER

19 messages are missing.

Q8. FORENSIC EXPLORER METHODOLOGY

Artifacts > Chat > WhatsApp Chat iOS shows 10 messages:

Figure 15: WhatsApp Chat iOS

| Forensic Explorer 🚦 🚵 🕶 🎲 🕶 (| 0 | | | |
|---------------------------------|-------------------|---------------------------|------------------------|---|
| 合 Evidence 🛛 🛅 File System | Artifact | ts 🖉 Keyword Search | h 👂 🔎 Index Searc | h 🔘 Email |
| Process Browsers - Chat - Ema | I Finance Apps | Health Apps Biome | MAC Mobile | Social Media Media Trackin Apps |
| Artifact Tree 4 | 🧮 File List | | | |
| Filter: 🔄 No Filter 🗸 🖃 | i e 🖗 | Message Date | Sentdate | AZ Text |
| Filename 🔺 | | Message Date | Sentdate | Text |
| CTF 2023 - Cellebrite FELIX (8) | 1 | 01-Dec-2022 6:05:32 PM | | |
| 🗄 🗌 🎯 Browsers (9) | 2 | 01-Dec-2022 6:05:32 PM | 01-Dec-2022 6:05:32 PM | Hello how are you ? |
| 🖻 🛄 🕎 Chat (7) | 3 | 01-Dec-2022 6:05:43 PM | 01-Dec-2022 6:05:43 PM | Just sending a photo |
| - iMessage Attachments OSX (13) | 4 | 01-Dec-2022 6:06:00 PM | 01-Dec-2022 6:06:00 PM | |
| | 5 | 📄 31-Mar-2023 10:03:42 AM | | |
| 📃 🛃 Telegram T7 Chat iOS (50) | 6 | 19-May-2023 2:18:08 PM | | |
| Telegram User iOS (3) | 7 | 19-May-2023 2:18:08 PM | | |
| - WhatsApp Chat iOS (10) | 8 | 03-Jun-2023 1:37:43 PM | | |
| WhatsApp Contacts iOS (6) | 9 | 03-Jun-2023 1:37:43 PM | | |
| WhatsApp Preferences iOS (1) | 10 | 📄 01-Jul-2023 5:41:04 AM | 01-Jul-2023 5:41:04 AM | Try to retrieve my m |
| 🕀 🔣 Email (2) | | | | |
| | | | | |

The **Source Path** and **Source Name** columns show **ChatStorage.sqlite** to be the source. The **Location** column lists the primary SQL Table as **zwamessage**.

To examine the ChatStorage.sqlite, zwamessage table:

- 1. In the **File System** module, Branch plate [] the **entire case**.
- 2. Enter ChatStorage.sqlite in the Filename column filter.
- 3. In the **Display View**, locate the **ZWAMESSAGE** table.

Cellebrite 2023 CTF - Felix iPhone

| 🏢 File List 😨 Gallery View 😨 Video View 🦲 Disk View 🅙 Category Graph | | | | | | |
|--|--------------|-------------|--------------|------------|-----------|-----|
| 🔯 🖻 👹 🐼 ChatStorage.sqlite 🕺 🐼 Ext | | | | | | |
| Filename | | Extension | File Signatu | re | | |
| 1 ChatStorage.sqlite | | sqlite | WhatsApp | iOS | | |
| 2 ChatStorage.sqlite-shm | | sqlite | Sqlite SHM | | | |
| 3 ChatStorage.sqlite-wal | | sqlite-wal | No size | | | |
| 4 ChatStorage.sqlite.enc | | enc Unknown | | | | |
| | | | | | | |
| EXTRACTION_FFS.ufd\filesystem2\mobile\Co | ntainers\Sha | ared∖AppGr | oup\5F021C | DF-1E49-45 | A3-A3EF-0 | 2BE |
| 4 of 432324 Visible [LS 408 KB PS 408 KB] | 1 | Highlighte | d [LS 344 KE | PS 344 KB | 1 | |
| V . Tables | | | | | | |
| > · ZWABLACKLISTITEM | Z_PK * | Z_ENT | Z_OPT | ZCHILD | ZCHILD | ZC |
| > ZWACHATPROPERTIES | 1 | 9 | 3 | 0 | 0 | 0 |
| > · ZWACHATPUSHCONFIG | 2 | 9 | 7 | 0 | 0 | 0 |
| > · ZWACHATSESSION | 3 | 9 | 7 | 0 | 0 | 0 |
| > · ZWAGROUPINFO | 4 | 9 | 11 | 0 | 0 | 0 |
| > · ZWAGROUPMEMBER | 10 | 9 | 2 | 0 | 0 | 0 |
| > · ZWAGROUPMEMBERSCHANGE | 11 | 9 | 2 | 0 | 0 | 0 |
| > · ZWAMEDIAITEM | 12 | 9 | 4 | 0 | 0 | 0 |
| ✓ ZWAMESSAGE | 20 | 9 | 2 | 0 | 0 | 0 |
| CREATE TABLE ZWAMESSAGE (Z_PK IN | 21 | 9 | 5 | 0 | 0 | 0 |
| > · ZWAMESSAGEDATAITEM | 29 | 9 | 5 | 0 | 0 | 0 |
| > · ZWAMESSAGEINFO | | | | | | |
| > · ZWAPROFILEPICTUREITEM | | | | | | |
| > · ZWAPROFILEPUSHNAME | | | | | | |
| > ZWAVCARDMENTION | | | | | | |
| > ZWAZ IPATMENT RANSACTION | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Figure 16: File System > ChatStorage.sqlite > Display View ZWAMESSAGE table

The **Z_PK** column shows **29** as the highest numbered message. Subtract the 10 visible messages and there are 19 missing items.

QUESTION 9 - WIPED - LEVEL 2 (30 POINTS)

When was Felix's phone last wiped? [YYYY-MM-DD HH:MM:SS]

Q9. ANSWER

2022-12-01 17:16:55.

Q9. FORENSIC EXPLORER METHODOLOGY

A common file that is used to identify an iOS device wipe is **root\.obliterated** (see:

<u>https://dfir.pubpub.org/pub/6i7d593n/release/1</u>). This is a zero-byte file created by the device upon booting after a wipe.

To search for **.obliterated**:

- 1. In the File System module, branch plate [] the **entire case**.
- 2. In the Filename column header, filter by obliterated.

The filter identified a .obliterated file with a created and modified date of 1 December 2022.

Figure 17: File System column filter

| 📰 File List 😨 Gallery View 😨 Video View 🖨 Disk View 🅙 Category Graph | | | | | | |
|--|--------------|-------------|------------------------|------------------------|--------------|---------------|
| 🥦 😑 🔯 | ebliterated | Extensio | 8 | 8 | 1.9 | <u>(19</u>) |
| | Filename 🔺 | Extension | Created | Modified | Logical Size | Physical Size |
| 1 | .obliterated | obliterated | 01-Dec-2022 5:16:55 PM | 01-Dec-2022 5:16:55 PM | 0 | 0 |
| | | | | | | |
| | | | | | | |
| EXTRACTION_FFS.ufd\filesystem2\root\.obliterated | | | | | | |
| | | | | | | |

QUESTION 10 - CRUISE - LEVEL 2 (30 POINTS)

Felix was researching / surveilling a ship as a possible target and downloaded a photo of it. What is the name of the cruise ship?

Q10. ANSWER

Q10. FORENSIC EXPLORER METHODOLOGY

A visual scan of File System > Gallery View was conducted:

- 3. In the File System module, branch plate [] the **entire case**.
- 4. Switch to Gallery View to examine the photos.

The following ship photos were located:



However the **Display View** resolution was too low to make our the ship name.

The highest resolution image was then exported from the Forensic Explorer case and uploaded to <u>https://tineye.com/</u> Reverse Image Search.

Figure 18: TinEye Reverse Image lookup



From the TinEye results the following picture was identified: <u>https://pixabay.com/photos/cruise-ship-dock-boats-yachts-6145828/</u> identifying the cruise ship as the **Crystal Serenity**.



Figure 19: https://pixabay.com/photos/cruise-ship-dock-boats-yachts-6145828/

Alternate Method

The word '**researching'** in the questions suggests web browser activity. A search of **Artifacts > Browsers > Safari History** identified browsing activity at the site:

https://www.pexels.com/photo/luxury-monaco-port-yachts-3586/

🖶 🚵 = 🎲 = 🥝 Forensic Explorer v5.6.8(4641d) (64bit) Case: Cellebrite CTF FE Artifacts Seyword Search **P** Index Search (C) Email 1 Evidence File System Registry E Bookmarks Reports Scripts 9 Ć 0 ► 6 @ 2 € • æ Chat Process All Browsers Email Map Artifac Artifact Carve Event Logs Export To CSV Artifact Tree 💷 File List 3 o 🕸 Filter: 🗐 No Filter Visit Date AZT URL URL Title Visit Date URI URL Title 274Way-2023 11:3... https://m.facebook.com/story.php?story_fbid=pfbid0xmdjdhtrxtljuVcFQc..
 05-Jun-2023 4:01:... https://www.google.fr/search?q=photos+monaco&ie=UTF-8&e=UTF-8... [FERMETURE DE ROUTE - RD2566] ▲ Du... - Mairie de Lucéram | Facebook 1 2 3 4 5 6 7 Browsers (9) photos monaco - Google Search photos monaco - Google Search 05-Jun-2023 4:01:... https://www.google.fr/search?g=photos+monaco&ie=UTE-8&oe=UTE-8... @ Google Query (9)
 Ø Safari Bookmarks (20)
 Ø Safari Cache (11) 05-Jun-2023 4:01:...
 05-Jun-2023 4:01:...
 05-Jun-2023 4:01:...
 05-Jun-2023 4:01:... https://www.google.fr/search?q=photos+ https://www.pexels.com/search/monaco/ photos monaco - Google Search Just a moment... onaco&ie=UTF-8&oe=UTF-8. https://www.pexels.com/search/monaco/?__cf_chl_rt_tk=85c7epxBLc32... Just a moment... Safari Caokies (20)
 Safari Recent Searches (1)
 Safari Recent Searches (1)
 Safari Tabs (20)
 URL Cache Generic (1820) 05-Jun-2023 4:01:.. https://www.pexels.com/search/monaco/ Just a moment. 05-Jun-2023 4:01:... 05-Jun-2023 4:01:... 05-Jun-2023 4:01:... https://www.pexels.com/search/monaco/?__cf_chl_tk=85c7epxBLc32N.0.. https://www.pexels.com/search/monaco/ Monaco Photos, Download The BEST Free Monaco Stock Photos & HD Images Monaco Photos, Download The BEST Free Monaco Stock Photos & HD Images 10 11 12 13 https://www.pexels.com/photo/luxury-monaco-port-yachts-3586/ Boat Lot on Calm Body of Water Beside Canal Houses . Free Stock Photo 05-Jun-2023 4:02:.. https://www.pexels.com/photo/luxury-monaco-port-yachts-3586/ 05-Jun-2023 4:02:... 05-Jun-2023 4:02:... https://www.pexels.com/search/monaco/ https://www.pexels.com/search/monaco/ - Chat (7) Monaco Photos, Download The BEST Free Monaco Stock Photos & HD Images Monaco Photos, Download The BEST Free Monaco Stock Photos & HD Images Email (2) 13 14 Mail Addresses iOS (6) 📄 05-Jun-2023 4:02:.. https://www.pexels.com/photo/apartment-apartments-architecture-ba Low Angle Photography of High-rise Buildings · Free Stock Photo

Figure 20: Artifacts > Browsers > Safari History

At https://www.pexels.com/photo/luxury-monaco-port-yachts-3586/ a high resolution version of the Crystal Serenity image was found.

https://www.pexels.com/photo/white-and-blue-cruise-ship-on-the-sea-7372476/

Figure 21: https://images.pexels.com/photos/7372476/pexels-photo-7372476.jpeg



A filename search for **pexels** located the following image in the **apple~CloudDocs\Downloads** folder:

Figure 22: File System > Filename column filter for 'pexels'

| III File List | 😨 Gallery View 😨 Video View 🚨 Disk View 🌒 Categ | ory Graph | |
|----------------|---|--------------------|----------------------------|
| 7 🖻 🖗 | exels | AZ Ext | en 🐼 File Signature |
| | Filename | Extension | n File Signature |
| 1 | pexels-helena-jankoviAlÂovAlÂi-kovAlÂiAlÂovAlÂi-7372 | 476.jpg jpg | Unknown |
| EXTRACTI | ON_FFS.ufd\filesystem2\mobile\Library\Mobile Document | s\com~apple~Clo | udDocs\Downloads\pexels-he |
| 1 of 432326 Vi | sible [LS 2.2 MB PS 2.2 MB] 1 Highlighte | d [LS 2.2 MB PS 2. | 2 MB] 1 |

This file has a jpg extension, but an unknown signature, and does not display in Forensic Explorer.

A HEX examination of the file shows that it has additional characters before the standard JPG header:

Figure 23: pexels-helena-.... file header

| <mark>ÿØÿà</mark> J |
|----------------------|
| FIFH.Hÿâ.XICC_PROFIL |
| EHLinomntrRGB XYZ |
| .ÎIacspMSFTIE |
| C sRGBöÖ |
| .Ó-HP |
| |
| .cprtP3desclwt |

A **right-click** > **open** with programs including Snagit and Irfan view, shows it to be the high-resolution Crystal Serenity picture.

QUESTION 11 - DATA - LEVEL 3 (50 POINTS)

Which process on Felix's phone used the most cellular data (network traffic INTO the device)?

Q11. ANSWER

CumulaltiveUsageTracker.

Q11. FORENSIC EXPLORER METHODOLOGY

In the Artifacts module:

- 1. Select Mobile > Data Usage iOS.
- 2. Double click on the Cellular Bytes In column header to sort by size.
- 3. The process with the most bytes is **CumulaltiveUsageTracker**.

Figure 24: Artifacts > Mobile > Data Usage iOS

| Forensic Explorer 🚦 🚵 👻 😨 Forensic Explorer | | | | | | | |
|--|---------------------------|-----------------------|------------------------------|---------------------|--|--|--|
| 合 Evidence 🗋 File System 🗚 | rtifacts | P Keyword Search | 🔎 Index Search | (Email | Registry | | |
| Process All Browsers × Chat × Chat Finail × F | \$ inance He Apps A | ealth × Ć × | MAC OS | Social Media | g ^v Windows ^v OS ^c arv | | |
| 🔚 Artifact Tree 🛛 🕂 | 🧮 File List | | | | | | |
| Filter: 🔄 No Filter 🗸 😑 | 🔯 🗆 🔯 | Cellular Bytes In | 😥 Cellular Byt 😥 Wifi | Byl 😥 Wifi Byte | Process Name | | |
| Filename A | | Cellular Bytes In 🛛 🔻 | Cellular Bytes Out Wifi Byte | s In Wifi Bytes Out | Process Name | | |
| Cellebrite CTF FELIX (8) | 1 | 479,085,390.0000 | 0.0000 0. | 0000 0.0000 | CumulativeUsageTracker | | |
| 🗄 🗌 🎯 Browsers (9) | 2 | 245,339,705.0000 | 0.0000 0. | 0000 0.0000 | _personalhotspot_/com.ap | | |
| 🕀 🛄 🕎 Chat (7) | 3 | 235,612,759.0000 | 0.0000 0. | 0000 0.0000 | _personalhotspot_/com.ap | | |
| ⊕ @ Email (2) | 4 | 29,715,745.0000 | 232,841.0000 0. | 0000 0.0000 | Telegram/ph.telegra.Telegr. | | |
| Finance (0) | 5 | 16,539,423.0000 | 12,450,473.0000 0. | 0000 0.0000 | mDNSResponder/com.appl | | |
| 🕀 🛄 🛟 Health Apps (3) | 6 | 15,855,496.0000 | 1,053,833.0000 0. | 0000 0.0000 | locationd/com.apple.datau | | |
| + OS Biome (5) | 7 | 15,252,750.0000 | 13,166,920.0000 0. | 0000 0.0000 | apsd/com.apple.datausage | | |
| 🕂 🔄 💣 MAC Operating System (1) | 8 | 12,160,012.0000 | 514,760.0000 0. | 0000 0.0000 | geod/com.apple.datausage. | | |
| E- Mobile (23) | 9 | 8,964,545.0000 | 857,235.0000 0. | 0000 0.0000 | itunescloudd/com.apple.da | | |
| Accounts Type iOS (34) | 10 | 7,128,554.0000 | 297,315.0000 0. | 0000 0.0000 | CommCenterMobileHelper/c. | | |
| Apple Maps Searches iOS (1) | 11 | 3,679,027.0000 | 174,680.0000 0. | 0000 0.0000 | mobileassetd/com.apple.da | | |
| Application Permissions iOS (127) | 12 | 2,883,646.0000 | 386,182.0000 0. | 0000 0.0000 | amsengagementd/com.appl. | | |
| Application State iOS (199) | 13 | 2,232,307.0000 | 19,081.0000 0. | 0000 0.0000 | coreidvd/com.apple.Passboo | | |
| Application Usage iOS (1998) | 14 | 1,780,972.0000 | 59,557.0000 0. | 0000 0.0000 | mobileassetd/com.apple.da | | |
| Bluetooth Devices iOS (2) | 15 | 1,678,432.0000 | 34,384.0000 0. | 0000 0.0000 | mobileassetd/com.apple.da | | |
| Bluetooth Paired Low Energy Devices iOS (2) | 16 | 1,484,222.0000 | 146,358.0000 0. | 0000 0.0000 | locationd/com.apple.datau | | |
| Bluetooth Seen Devices iOS (1001) | 17 | 1,474,531.0000 | 58,980.0000 0. | 0000 0.0000 | CommCenterMobileHelper/c. | | |
| Cached Locations iOS (7813) | 18 | 1,283,360.0000 | 117,513.0000 0. | 0000 0.0000 | com.apple.WebKit.Network | | |
| Calendar Items v4 iOS (60) | 19 | 1,283,026.0000 | 379,343.0000 0. | 0000 0.0000 | locationd/com.apple.datau | | |
| Call History iOS (12) | 20 | 1,242,659.0000 | 30,056,649.0000 0. | 0000 0.0000 | nsurlsessiond/com.apple.m | | |
| Cell Tower Locations iOS (986) | 21 | 1,221,062.0000 | 257,124.0000 0. | 0000 0.0000 | appstored/com.apple.data | | |
| Contacts Details iOS (10) | 22 | 1,120,219.0000 | 290,781.0000 0. | 0000 0.0000 | assistant_service/com.appl | | |
| Data Usage iOS (349) | 23 | 1,067,392.0000 | 1,485,015.0000 0. | 0000 0.0000 | assistant.assistantd/com.a | | |
| Installed Applications iOS (199) | 24 | 1.012.582.0000 | 194.469.0000 0. | 0000 0.0000 | nsurlsessiond/com.faceboo | | |

QUESTION 12 - H IS MEAN - LEVEL 3 (100 POINTS)

Felix was referred information about pension reform. What is the SID associated with that artifact?

Q12. ANSWER

c5141308-e98c-11ed-8f70-ea4e37ab9147

Q12. FORENSIC EXPLORER METHODOLOGY

This question is obscure. Please see the official Cellebrite solution on this page:

https://cellebrite.com/en/cellebrites-ctf-2023-recap-answers-for-felixs-iphone-device/