Collaborative Testing Services, Inc
FORENSIC TESTING PROGRAM

P.O. Box 650820
Sterling, VA 20165-0820
e-mail: forensics@cts-interlab.com
Telephone: +1-571-434-1925
Web site: www.cts-forensics.com

Mobile Digital Evidence - iOS Analysis
Test No. 22-5551 Summary Report

Participants were provided with data yielded from an extraction of a smart phone. They were asked to analyze the sample and answer scenario based questions utilizing their own tools and methods. Data was returned from 71 participants and are compiled in the following tables:

	Page
Manufacturer's Information	2
Summary Comments	5
Table 1: Digital Evidence Responses	6
Table 2: Additional Comments	107

This report contains the data received from the participants in this test. Since these participants are located in many countries around the world, and it is their option how the samples are to be used (e.g., training exercise, known or blind proficiency testing, research and development of new techniques, etc.), the results compiled in the Summary Report are not intended to be an overview of the quality of work performed in the profession and cannot be interpreted as such. The Summary Comments are included for the benefit of participants to assist with maintaining or enhancing the quality of their results. These comments are not intended to reflect the general state of the art within the profession.

Participant results are reported using a randomly assigned "WebCode". This code maintains participant's anonymity, provides linking of the various report sections, and will change with every report.

Manufacturer's Information

The Mobile Digital Evidence – iOS Analysis test consisted of evidence data acquired from a smartphone. Participants were asked to examine the extracted data pertaining to a simulated scenario using their own software and methods.

SAMPLE PREPARATION:
A scripted scenario based upon a prison escape case was created to generate user data on the evidence iPhone device. The execution of the scripted crime took place between April 21, 2022 through June 25, 2022. An iPhone 6s smartphone was used to perform the activities and generate the intended artifacts.

The phone data was acquired via a file-system extraction of the smartphone using Cellebrite UFED version 7.50 software and compiled into two formats: a zip archive and a .dar archive. These files were uploaded to the CTS portal for participants to download. A MD5 checksum was calculated for the files to generate a unique hash value to allow participants to validate the successful download of the file.

SAMPLE VALIDATION/VERIFICATION:
The validation stage consisted of the examination of the phone data using various software including Cellebrite Physical Analyzer 7.55.2.2., Autopsy 4.19.3, DB Browser for SQLite Version 3.12.1, Powershell Version 5.1, HxD 2.4.0.0, and 7zip 19.00. Results from the predistribution laboratories were reviewed and certain questions were rephrased as necessary. Several forensic software tools were utilized during the validation of this test. CTS does not endorse any particular tools.

PLEASE NOTE: Questions marked with asterisks (**) did not show a clear consensus during preliminary review of the participants' responses. Further information and discussion will be available in the final summary report.

SCENARIO PROVIDED TO PARTICIPANTS

Casey Black escaped from prison and was re-captured several days later. Upon his arrest, this iPhone was discovered in his possession. Analysis is needed to determine if this phone contains information concerning details about the escape.

Manufacturer's Information, continued

Question	*Manufacturer's Expected Response*
1	Provide the SHA256 hash for the file(s) you used (FullFileSystem.1.dar, or Apple_iPhone 6s (A1633).zip, or both). *FullFileSystem.1.dar 7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659* *root.zip* *07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C*
2	On what date was this device reset (erasing all content and settings)? Provide date using the date picker. *2022-06-02*
3	Provide the Device Phone Number (MSISDN). *19842866876*
4	What type of extraction produced the provided dataset? *File system extraction or* *Full File System (checkm8) or* *Advanced Logical File System or* *iOS_Full_Filesystem*
5	What is the locale / language setting for this phone? *en-US and variations representing the same information*
6	Provide the AppleID associated with this phone. *therealvivianwhite@icloud.com*
7	What is the time zone setting for this phone? Provide response exactly as shown by the device. *America/New_York and variations representing the same information*
8	What is the Device Name for this phone? *Vivian's iPhone*
9	What is the SSID of the Wi-Fi access point with BSSID 70:f0:96:c7:1b:23? *ZurichAirport*
10	What is the device name for the (connected) device with MAC address A2:9D:FE:97:BE:53 ? *MONSTER WBA9-1008*
11	What (non-Apple) encrypted email app did the user install? *Proton Mail*
12	What email address was configured with the user-installed encrypted email app referenced in question 11? *caseyb_lack78@proton.me*
13	What is the email address of the party with whom the phone user corresponded with a subject line of "Traveling"? *passportcardzrus@proton.me*
14	What was the phone number of the call RECEIVED on 19 June 2022? *+13133082630*
15	Which contact did the user call on 6/21/2022 6:43:39 PM(UTC-4)? Provide the name of contact. *sissy*

Manufacturer's Information, continued

Question	*Manufacturer's Expected Response*
16	What is the CREATION date and time of the Note (taken with the notes App) titled "Greyhound station"? Provide your response in (UTC-4), using the date/time (24-hour) picker. *2022-06-25 11:57*
17	What event was scheduled to occur 6/24/2022 2:00:00 PM(UTC-4)? *Casey's Dr.'s Appointment*
18	To what location (place name) did the user navigate using the Apple Maps app with timestamp 6/24/2022 1:51:28 PM(UTC-4). *Coffeewood Correctional Center*
19	What did the phone user say they were going to do after they "got to the drs office"? *Find a way to take of[f] the tracker... Then a hotel.*
20	What did the user search in the Safari web browser, 6/24/2022 12:05:18 PM(UTC-4)? *remove ankle monitor*
21	According to the data for the Home Depot app, for what item did the user have a saved search? *bolt cutters*
22	Describe the type and content of the file with MD5 hash efa6da222aca7bbcc12fcf8c79414844. *Audio file of a ringing phone and variations representing the same information*
23	According to the voicemail message received on June 25, 2022, what does Casey owe the caller? *a hundred bucks ($100) and variations representing the same information*
24	Provide the GPS Position coordinates for IMG_0082.JPG in the format ##.##### (Indicate directionality as N or S), ##.##### (Indicate directionality as E or W). *43.50906 N, 16.47451 E*
25	With what application did the user receive an image of a New York birth certificate? *Telegram*
26	Who did the phone user communicate with using Signal Private Messenger? *frank grey*
27	Which contact has the phone number +44 1482 466581? Provide the name of contact. *Phil Lark*
28	Who sent the email with subject line "TALK TO ME"? Provide the email address. *mason12jake@gmail.com*
29	Provide a site visited in the DuckDuckGo browser. *www.amtrak.com and/or www.greyhound.com*
30**	Provide the path and filename, (i.e., /root/folder/subfolder…/filename.extension) for the file containing the (CASE SENSITIVE) term "Tytonidae" (capital T, without quotes). */private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG*
31**	What type of file is identified in Question 30 (the previous question)? *IMG_0100.JPG is a text file.*

Summary Comments

The purpose of this Mobile Digital Evidence (MDE) Test is to allow participants to evaluate their proficiency in analyzing digital artifacts using their own tools and methods. The participants were provided with a scripted scenario, the data extracted from a smart phone, and a series of questions related to the extracted data (See Manufacturer's Information for preparation details, test scenario, and test questions).

The participants were requested to analyze various digital artifacts including: phone and network settings, applications, communications, web browser history, and Geo-Location information.

A consensus was determined for each question based on the total number of participants returning results for that particular question. A total of 29 of the 31 questions reached a consensus response. Questions #30 and #31 are linked to each other and a consensus was not achieved by either. More details concerning the results received are discussed later in the report under their corresponding questions.

Please Note: Several forensic software tools were utilized during the validation of this test and may be referenced during the discussion of results. CTS does not endorse any particular tools.

Digital Evidence Responses

TABLE 1

Question 1 - Examination Questions

Question 1: Provide the SHA256 hash for the file(s) you used (FullFileSystem.1.dar, or Apple_iPhone 6s (A1633).zip, or both).

Manufacturer's Expected Response: FullFileSystem.1.dar
7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659
root.zip
07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C

WebCode	Response
2JFUWZ	07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
2YAJPB	07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
3329MU	93F4D17F19D195EE65DB2D060286A7CB9110ADD08948E85F5E2AF5C861994D4D
3R3DPY	pple_iPhone 6s (A1633).zip - SHA-256: 07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c, FullFileSystem.1.dar - SHA-256: 7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659
4FPB42	7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659
66P4MA	07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
6ERKDC	Apple_iPhone 6s (A1633).zip : 07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
6M83T7	7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659
6QMVJY	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
7CKLGB	Apple_iPhone 6s (A1633).ZIP hash: 7DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
7ND6X2	FullFileSystem.1.dar: 7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659 Apple_iPhone 6s (A1633).zip: 07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
7W8BQ3	07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C & 15ADA63CE4911794A0857D82F8D80BCC5E84DDAF3CEC1FAAC5051A7FF50903A9
7WQWJT	Apple_iPhone 6s (A1633).zip: 07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
8F34CZ	FullFileSystem.1.dar: 7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659 (From UFDR file)
8JDFPT	FullFileSystem.1.dar is 7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659; Apple_iPhone 6s (A1633).zip is 07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
8JXTWE	93F4D17F19D195EE65DB2D060286A7CB9110ADD08948E85F5E2AF5C861994D4D
8VQFKZ	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
9MCRLT	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
9VQVED	Apple_iPhone 6s (A1633).zip SHA256: 07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
AGMPY9	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c

TABLE 1

Question 1 - Examination Questions	
WebCode	**Response**
AKNRPA	Apple_iPhone 6s (1633).zip SHA256: 93F4D17F19D195EE65DB2D060286A7CB9110ADD08948E85F5E2AF5C861994D4D FullFileSystem.1.dar zip SHA256: 2E8C6D397C54A214CABD96926B8BE947F2FABBB23ED220A2098B19AAEA798240
BHAT4Y	93F4D17F19D195EE65DB2D060286A7CB9110ADD08948E85F5E2AF5C861994D4D
BNZ3DX	FullFileSystem.1.dar: 7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659 Apple_iPhone 6s (A1633).zip: 07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
C6EZRU	7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659
CERU9G	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
CKT9RX	e8ece265840375a3961c20fb4197a9ea
CZNJJA	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
DNUPM7	7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659
DQZW7Y	90C06CB7AEC849C8340E1D4AE86302D0B5CF06BB2D52AE0D56C463406C91F16E
DT3X7V	Apple_iPhone 6s (A1633).zip=07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
DYD4P9	93f4d17f19d195ee65db2d060286a7cb9110add08948e85f5e2af5c861994d4d
E7PH86	Apple_iPhone 6s (A1633).zip, SHA256 93F4D17F19D195EE65DB2D060286A7CB9110ADD08948E85F5E2AF5C861994D4D
FLWZEV	FullFileSystem.1.dar: 7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659 ,Apple_iPhone 6s (A1633).zip: 07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
G8C3KE	7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659
GPDMNU	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
GQPFJW	2e8c6d397c54a214cabd96926b8be947f2fabbb23ed220a2098b19aaea798240
GYF3AR	07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
HGFG4R	07DEFBE915A3D9034546C3FF8B78DBB220B91A6535DCD57901466B55CF1D7C
JCC299	FullFileSystem.1.dar = 7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659
JEJH6J	93f4d17f19d195ee65db2d060286a7cb9110add08948e85f5e2af5c861994d4d
JL3MGR	FullFileSystem.1.dar: 7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659
KVP67K	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
L6PWCQ	7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659
MFJPZ8	FullFileSystem.1.dar 7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659, Apple_iPhone 6s (A1633).zip 07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C

TABLE 1

Question 1 - Examination Questions	
WebCode	**Response**
MXKEER	07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
N634TR	FullFileSystem.1.dar:7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659 Apple_iPhone 6s (A1633).zip: 07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
NE7FKF	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
NEP2GC	Apple_iPhone 6s (A1633).zip: 07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
NP67AT	7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659; 07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
NT6H7T	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
NZNRBG	FullFileSystem.1.dar 7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659 Apple_iPhone 6s (A1633).zip: 07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
P77HBH	93f4d17f19d195ee65db2d060286a7cb9110add08948e85f5e2af5c861994d4d
P9Y9K3	07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
QLFNYL	07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C (zip); 7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659 (dar)
QM9E98	FullFileSystem.1.dar 7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659, Apple_iPhone 6s (A1633).zip 07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
R748U6	FullFileSystem.1.dar 7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659; Apple_iPhone 6s (A1633).zip 07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
T8BAT9	FullFileSystem.1.dar 7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659 Apple_iPhone 6s (A1633).zip 07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
T9LU2H	2E8C6D397C54A214CABD96926B8BE947F2FABBB23ED220A2098B19AAEA798240
TPPKJE	Apple_iPhone 6s A1633.zip - 07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C FullFileSystem.1.dar - 7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659
TYEAHM	07defbe915a3d9034546c3cff8678dbb220bb91a6535dcd57901
U7V8LZ	7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659
V7R6A2	Apple_iPhone 6s (A1633).zip SHA256 Hash - 07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
VDB8G4	Apple_iPhone 6s (A1633).zip SHA256 hash: 07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
VG9PVJ	7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659
VJEAGX	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c
VLPWFC	93f4d17f19d195ee65db2d060286a7cb9110add08948e85f5e2af5c861994d4d
VP3UPK	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c

TABLE 1

Question 1 - Examination Questions	
WebCode	**Response**
WVNBEF	7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659 (Dar) 07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c (Zip)
ZEAZKD	07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C
ZGVLBE	7c961a2736843eb8c728f0b724a8d14e3b53ad4e077743a67f900a1760bc4659
ZKXMCC	07defbe915a3d9034546c3cff8b78dbb220bb91a6535dcd57901466b55cf1d7c

Question 1: Provide the SHA256 hash for the file(s) you used (FullFileSystem.1.dar, or Apple_iPhone 6s (A1633).zip, or both).

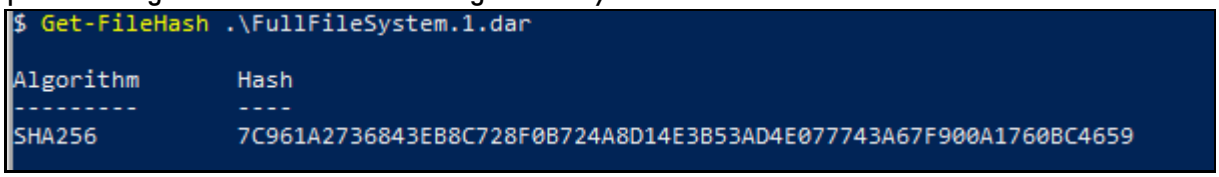
Consensus Result: FullFileSystem.1.dar
7C961A2736843EB8C728F0B724A8D14E3B53AD4E077743A67F900A1760BC4659 and/or
root.zip
07DEFBE915A3D9034546C3CFF8B78DBB220BB91A6535DCD57901466B55CF1D7C

Expected Response Explanation:

The question specifically asked for the SHA256 hash of one or both of the evidence files. File digests (hashes) can be calculated using any trusted hashing tool.

Expected Response Illustration:

powershell get-filehash cmdlet hashing FullFileSystem.1.dar



7zip checksum tool showing hash of Apple_iPhone 6s (A1633).zip

Other Responses:

Another 15% of participants reported the SHA256 hash for the zip files containing the examination material, and not the hash of the materials themselves as requested in this question. Eight of these participants reported "93f4d17f19d195ee65db2d060286a7cb9110add08948e85f5e2af5c861994d4d" for the 42551_iPhone6s.zip, the zip file (as downloaded from the portal) containing Apple_iPhone 6s (A1633).zip and Apple_iPhone 6s (A1633).zip.ufd. Two participants reported the SHA256 hash "2e8c6d397c54a214cabd96926b8be947f2fabbb23ed220a2098b19aaea798240" for the 22-5551_iPhone6s-dar.zip, the zip file (as downloaded from the portal) containing FullFileSystem.1.dar and Apple_iPhone 6s A1633 dar.ufd. And one participant reported both of these SHA256 hash values.

TABLE 1

Question 2 - Examination Questions

Question 2: On what date was this device reset (erasing all content and settings)? Provide date using the date picker.

Manufacturer's Expected Response: 2022-06-02

WebCode	Response
2JFUWZ	2022-06-02
2YAJPB	2022-06-02
3329MU	2022-06-02
3R3DPY	2022-06-02
4FPB42	2022-02-06
66P4MA	2022-06-02
6ERKDC	2022-06-02
6M83T7	2022-06-02
6QMVJY	2022-06-02
7CKLGB	2022-06-02
7ND6X2	2022-06-02
7W8BQ3	2022-06-02
7WQWJT	2022-06-02
8F34CZ	2022-06-02
8JDFPT	2022-06-02
8JXTWE	2022-06-02
8VQFKZ	2022-06-02
9MCRLT	2022-06-02
9VQVED	6/2/2022
AGMPY9	2022-06-02
AKNRPA	2022-06-02
BHAT4Y	2022-06-02
BNZ3DX	2022-06-02
C6EZRU	2022-06-02
CERU9G	2022-06-02
CKT9RX	2022-06-02
CZNJJA	2022-06-02
DNUPM7	2022-06-02
DQZW7Y	2022-06-02

TABLE 1

Question 2 - Examination Questions	
WebCode	**Response**
DT3X7V	2022-06-02
DYD4P9	2022-06-02
E7PH86	2022-06-02
FLWZEV	2022-06-02
G8C3KE	2022-06-02
GPDMNU	2022-06-02
GQPFJW	2022-06-02
GYF3AR	2022-06-02
HGFG4R	2022-06-02
JCC299	2022-06-02
JEJH6J	2022-06-02
JL3MGR	2022-06-02
KVP67K	2022-06-02
L6PWCQ	2022-06-02
MFJPZ8	2022-06-02
MXKEER	2022-06-02
N634TR	2022-06-02
NE7FKF	2022-06-02
NEP2GC	2022-06-02
NP67AT	2022-06-02
NT6H7T	2022-06-02
NZNRBG	2022-02-06
P77HBH	2022-06-02
P9Y9K3	2022-06-02
QLFNYL	2022-06-02
QM9E98	2022-06-02
R748U6	2022-06-02
T8BAT9	2022-06-02
T9LU2H	2022-06-06
TPPKJE	2022-06-02
TYEAHM	2022-06-02
U7V8LZ	2022-06-02

TABLE 1

Question 2 - Examination Questions	
WebCode	**Response**
V7R6A2	2022-06-02
VDB8G4	2022-06-02
VG9PVJ	2022-06-02
VJEAGX	2022-06-02
VLPWFC	2022-06-02
VP3UPK	2022-06-02
WVNBEF	2022-06-02
ZEAZKD	2022-06-02
ZGVLBE	2022-06-02
ZKXMCC	2022-06-02

Question 2: On what date was this device reset (erasing all content and settings)? Provide date using the date picker.

Consensus Result: 2022-06-02

Expected Response Explanation:

The creation/modification date of the .obliterated file at /private/var/root is a reliable means to establish when an iOS device was reset.

Expected Response Illustration:

.obliterated

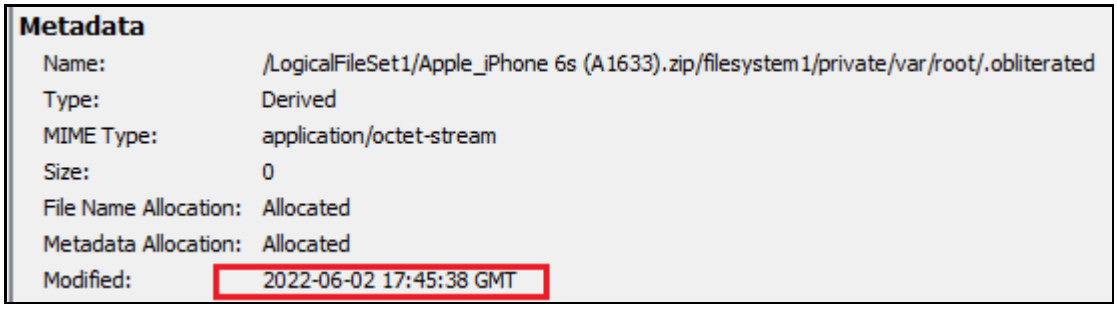


TABLE 1

Question 3 - Examination Questions

Question 3: Provide the Device Phone Number (MSISDN).

Manufacturer's Expected Response: 19842866876

WebCode	Response
2JFUWZ	19842866876
2YAJPB	19842866876
3329MU	19842866876
3R3DPY	19842866876
4FPB42	19842866876
66P4MA	19842866876
6ERKDC	+19842866876
6M83T7	19842866876
6QMVJY	1-984-286-6876
7CKLGB	19842866876
7ND6X2	19842866876
7W8BQ3	19842866876
7WQWJT	+19842866876
8F34CZ	19842866876
8JDFPT	19842866876
8JXTWE	1-984-286-6876
8VQFKZ	19842866876
9MCRLT	19842866876
9VQVED	984-286-6876
AGMPY9	19842866876
AKNRPA	19842866876
BHAT4Y	+19842866876
BNZ3DX	+19842866876
C6EZRU	19842866876
CERU9G	19842866876
CKT9RX	19842866876
CZNJJA	19842866876
DNUPM7	19842866876
DQZW7Y	+19842866876
DT3X7V	19842866876

TABLE 1

Question 3 - Examination Questions	
WebCode	**Response**
DYD4P9	19842866876
E7PH86	19842866876
FLWZEV	19842866876
G8C3KE	19842866876
GPDMNU	+19842866876
GQPFJW	1984286676
GYF3AR	19842866876
HGFG4R	19842866876
JCC299	19842866876
JEJH6J	9842866876
JL3MGR	+19842866876
KVP67K	19842866876
L6PWCQ	19842866876
MFJPZ8	19842866876
MXKEER	19842866876
N634TR	+19842866876
NE7FKF	19842866876
NEP2GC	19842866876
NP67AT	19842866876
NT6H7T	+19842866876
NZNRBG	+19842866876
P77HBH	19842866876
P9Y9K3	19842866876
QLFNYL	19842866876
QM9E98	19842866876
R748U6	1-984-286-6876
T8BAT9	19842866876
T9LU2H	19842866876
TPPKJE	+19842866876
TYEAHM	+19842866876
U7V8LZ	19842866876
V7R6A2	19842866876

TABLE 1

Question 3 - Examination Questions	
WebCode	**Response**
VDB8G4	+19842866876
VG9PVJ	19842866876
VJEAGX	+19842866876
VLPWFC	19842866876
VP3UPK	+19842866876
WVNBEF	19842866876
ZEAZKD	19842866876
ZGVLBE	+19842866876
ZKXMCC	+19842866876

Question 3: Provide the Device Phone Number (MSISDN).

Consensus Result: 19842866876

Expected Response Explanation:

Device info such as the phone number can be found in /private/var/wireless/Library/Preferences/com.apple.commcenter.plist

Expected Response Illustration:

com.apple.commcenter.plist

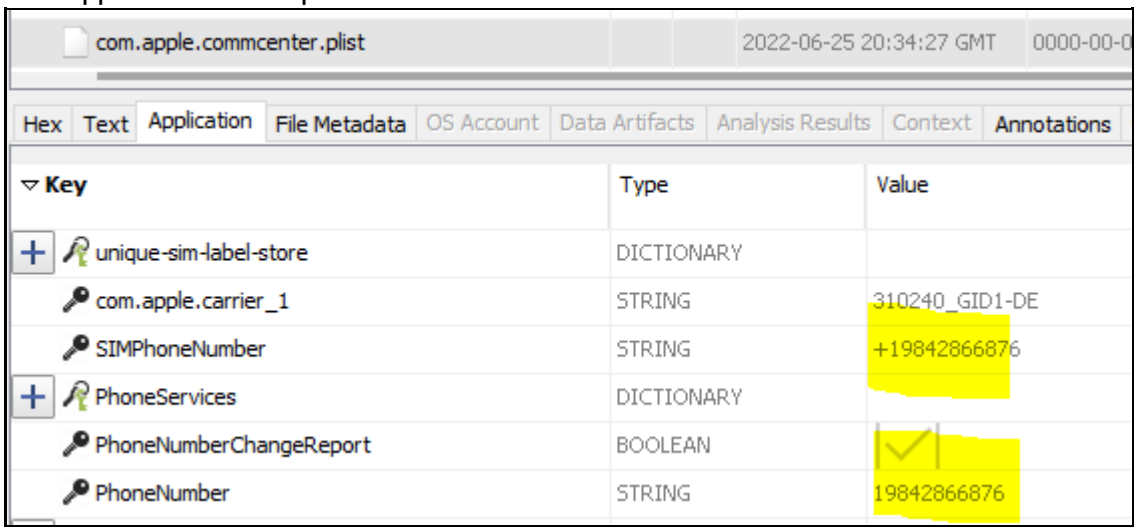


TABLE 1

Question 4 - Examination Questions

Question 4: What type of extraction produced the provided dataset?

Manufacturer's Expected Response: File system extraction or
Full File System (checkm8) or
Advanced Logical File System or
iOS_Full_Filesystem

WebCode	Response
2JFUWZ	iOS_Full_Filesystem
2YAJPB	Full File System (checkm8)
3329MU	File System
3R3DPY	FFS / Full File System
4FPB42	File System
66P4MA	iOS_Full File system
6ERKDC	File System
6M83T7	File System
6QMVJY	file system extraction
7CKLGB	File System
7ND6X2	Full File System (checkm8)
7W8BQ3	File System
7WQWJT	File System
8F34CZ	File System
8JDFPT	Full File System (checkm8 exploit); ZIP obtained 6/25/22 at 1651 hours (UTC-4); DAR obtained 6/25/22 at 1709 hours (UTC-4)
8JXTWE	Cellebrite lists this extraction as a file system extraction. The file system itself is viewable, it is confirmed this is not a logical extraction and appears to be a file system extraction
8VQFKZ	File System
9MCRLT	File System
9VQVED	File System
AGMPY9	File system
AKNRPA	File System
BHAT4Y	File System
BNZ3DX	Full File System (FFS checkm8)
C6EZRU	Full File System
CERU9G	File System
CKT9RX	File System Extraction
CZNJJA	File System
DNUPM7	File System

TABLE 1

Question 4 - Examination Questions	
WebCode	**Response**
DQZW7Y	File System
DT3X7V	Full File System (checkm8)
DYD4P9	File System
E7PH86	File System
FLWZEV	File system
G8C3KE	File System
GPDMNU	File System
GQPFJW	File System
GYF3AR	Taken from UFD extraction File
HGFG4R	Full File System
JCC299	iOS_Full_Filesystem
JEJH6J	logical
JL3MGR	FILESYSTEM
KVP67K	File System
L6PWCQ	File System Extraction
MFJPZ8	Full File System
MXKEER	Full File System
N634TR	File system extractions
NE7FKF	File System
NEP2GC	iOS_Full_Filesystem
NP67AT	File System
NT6H7T	Full File System
NZNRBG	The two types of extractions
P77HBH	File System
P9Y9K3	File System
QLFNYL	Checkra1n beta 0.9.6 using Cellebrite
QM9E98	File System
R748U6	iOS Full Filesystem extraction using checkm8.
T8BAT9	Filesystem with Checkm8 exploit
T9LU2H	File System
TPPKJE	filesystem
TYEAHM	FILE SYSTEM

TABLE 1

Question 4 - Examination Questions	
WebCode	**Response**
U7V8LZ	File System
V7R6A2	File System
VDB8G4	iOS_Full_Filesystem
VG9PVJ	File System
VJEAGX	File System
VLPWFC	iOS_Full_Filesystem
VP3UPK	Full File System
WVNBEF	File System
ZEAZKD	ExtractionType=FileSystem
ZGVLBE	iOS Full Filesystem
ZKXMCC	File System

Question 4: What type of extraction produced the provided dataset?

Consensus Result: File System and variations representing similar information.

Expected Response Explanation:

This information is available in the provided Apple_iPhone 6s (A1633).ufd file.

Expected Response Illustration:

Apple_iPhone 6s (A1633).ufd

Apple_iPhone 6s (A1633).ufd

```
1  [DeviceInfo]
2  DeviceModel=N71AP
3
4  [Dumps]
5  FileDump=Apple_iPhone 6s (A1633).zip
6  Keychain=Apple_iPhone 6s (A1633).zip
7
8  [ExtractionStatus]
9  ExtractionStatus=Success
10
11 [FileDump]
12 ExtractionMethod=iOS_Full_Filesystem
13 Type=ZIP
14
15 [General]
16 ConnectionType=Cable No. 210
17 Date=25/06/2022 16:37:36 (-4)
18 Device=IPHONE
19 EndTime=25/06/2022 16:51:37 (-4)
20 ExtractionNameFromXML=Full File System    (checkm8)
```

TABLE 1

Question 5 - Examination Questions

Question 5: What is the locale / language setting for this phone?

Manufacturer's Expected Response: en-US and variations representing the same information

WebCode	Response
2JFUWZ	en-US
2YAJPB	English
3329MU	en_US
3R3DPY	en_US
4FPB42	en_us
66P4MA	en-US
6ERKDC	en_US
6M83T7	en-US
6QMVJY	en_US
7CKLGB	en_US(English US)
7ND6X2	en_US
7W8BQ3	Language = English > En_US
7WQWJT	en_US / en-US
8F34CZ	En_US
8JDFPT	en_US (United States/English)
8JXTWE	Locale= En_US Language= En-US US English Located within the GlobalPreferences.plist file
8VQFKZ	en-US
9MCRLT	En_US
9VQVED	en-US
AGMPY9	en_US
AKNRPA	en_US
BHAT4Y	en_US
BNZ3DX	en_US
C6EZRU	en-US
CERU9G	English (US)
CKT9RX	en_US
CZNJJA	en_US
DNUPM7	en_US
DQZW7Y	English-US
DT3X7V	en-US (English (US))

TABLE 1

Question 5 - Examination Questions	
WebCode	**Response**
DYD4P9	en_US
E7PH86	English US
FLWZEV	en_US
G8C3KE	en_US
GPDMNU	en_US
GQPFJW	English
GYF3AR	US/English
HGFG4R	American
JCC299	United States / English (US)
JEJH6J	en_US
JL3MGR	en_US
KVP67K	Locale = en_US / Language = en_US
L6PWCQ	English US
MFJPZ8	en-US (English US)
MXKEER	en-US
N634TR	En_US
NE7FKF	en_US
NEP2GC	en_US
NP67AT	en_US / en-US
NT6H7T	en_US
NZNRBG	en-US
P77HBH	en_US (US English)
P9Y9K3	English
QLFNYL	en_US
QM9E98	New York / English
R748U6	en-US
T8BAT9	en_US
T9LU2H	English - US
TPPKJE	en-US
TYEAHM	en_US
U7V8LZ	en-US
V7R6A2	NOT WITHIN LABORATORY'S SCOPE

TABLE 1

Question 5 - Examination Questions	
WebCode	**Response**
VDB8G4	en-US
VG9PVJ	en_US
VJEAGX	en-US
VLPWFC	en-US
VP3UPK	New_York (America)
WVNBEF	en-us
ZEAZKD	en_US
ZGVLBE	en_US
ZKXMCC	en_US

Question 5: What is the locale / language setting for this phone?

Consensus Result: en-US and variations representing the same information

Expected Response Explanation:

Language settings can be found in /private/var/mobile/Library/Preferences/.GlobalPreferences.plist

Expected Response Illustration:

.GlobalPreferences.plist

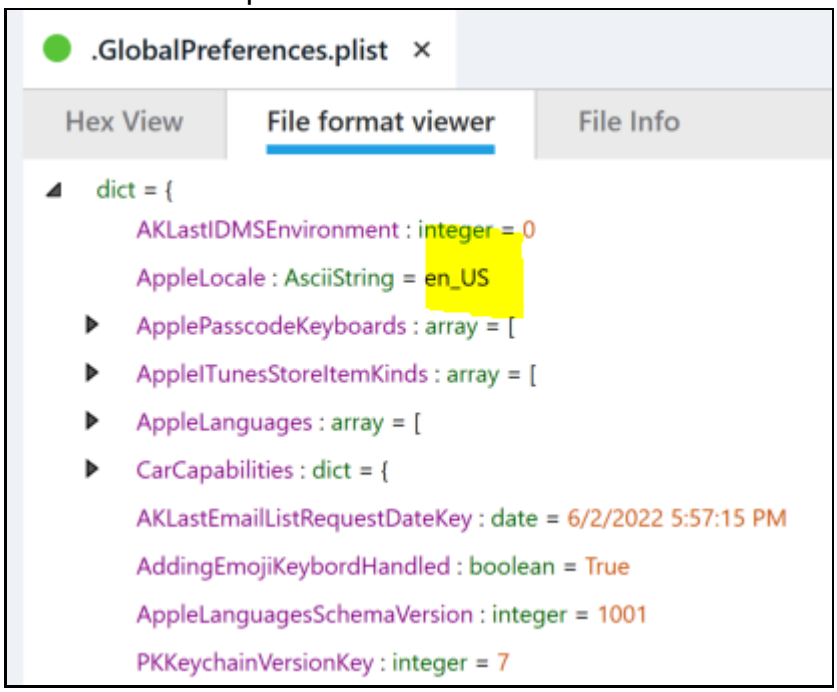


TABLE 1

Question 6 - Examination Questions

Question 6: Provide the AppleID associated with this phone.

Manufacturer's Expected Response: therealvivianwhite@icloud.com

WebCode	Response
2JFUWZ	therealvivianwhite@icloud.com
2YAJPB	therealvivianwhite@icloud.com
3329MU	therealvivianwhite@icloud.com
3R3DPY	therealvivianwhite@icloud.com
4FPB42	therealvivianwhite@icloud.com
66P4MA	therealvivianwhite@icloud.com
6ERKDC	therealvivianwhite@icloud.com
6M83T7	therealvivianwhite@icloud.com
6QMVJY	therealvivianwhite@icloud.com
7CKLGB	therealvivianwhite@icloud.com
7ND6X2	therealvivianwhite@icloud.com
7W8BQ3	therealvivianwhite@icloud.com
7WQWJT	therealvivianwhite@icloud.com
8F34CZ	therealvivianwhite@icloud.com
8JDFPT	therealvivianwhite@icloud.com
8JXTWE	therealvivianwhite@icloud.com
8VQFKZ	therealvivianwhite@icloud.com
9MCRLT	therealvivianwhite@icloud.com
9VQVED	therealvivianwhite@icloud.com
AGMPY9	therealvivianwhite@icloud.com
AKNRPA	therealvivianwhite@icloud.com
BHAT4Y	therealvivianwhite@icloud.com
BNZ3DX	therealvivianwhite@icloud.com
C6EZRU	therealvivianwhite@icloud.com
CERU9G	therealvivianwhite@icloud.com
CKT9RX	therealvivianwhite@icloud.com
CZNJJA	therealvivianwhite@icloud.com
DNUPM7	therealvivianwhite@icloud.com
DQZW7Y	therealvivianwhite@icloud.com
DT3X7V	therealvivianwhite@icloud.com

TABLE 1

Question 6 - Examination Questions	
WebCode	**Response**
DYD4P9	therealvivianwhite@icloud.com
E7PH86	therealvivianwhite@icloud.com
FLWZEV	therealvivianwhite@icloud.com
G8C3KE	therealvivianwhite@icloud.com
GPDMNU	therealvivianwhite@icloud.com
GQPFJW	therealvivianwhite@icloud.com
GYF3AR	therealvivianwhite@icloud.com
HGFG4R	therealvivianwhite@icloud.com
JCC299	therealvivianwhite@icloud.com
JEJH6J	therealvivianwhite@icloud.com
JL3MGR	therealvivianwhite@icloud.com
KVP67K	therealvivianwhite@icloud.com
L6PWCQ	therealvivianwhite@icloud.com
MFJPZ8	therealvivianwhite@icloud.com
MXKEER	therealvivianwhite@icloud.com
N634TR	therealvivianwhite@icloud.com
NE7FKF	therealvivianwhite@icloud.com
NEP2GC	therealvivianwhite@icloud.com
NP67AT	therealvivianwhite@icloud.com
NT6H7T	therealvivianwhite@icloud.com
NZNRBG	therealvivianwhite@icloud.com
P77HBH	therealvivianwhite@icloud.com
P9Y9K3	therealvivianwhite@icloud.com
QLFNYL	therealvivianwhite@icloud.com
QM9E98	therealvivianwhite@icloud.com
R748U6	therealvivianwhite@icloud.com
T8BAT9	therealvivianwhite@icloud.com
T9LU2H	therealvivianwhite@icloud.com
TPPKJE	therealvivianwhite@icloud.com
TYEAHM	therealvivianwhite@icloud.com
U7V8LZ	therealvivianwhite@icloud.com
V7R6A2	therealvivianwhite@icloud.com

TABLE 1

Question 6 - Examination Questions	
WebCode	**Response**
VDB8G4	therealvivianwhite@icloud.com
VG9PVJ	therealvivianwhite@icloud.com
VJEAGX	therealvivianwhite@icloud.com
VLPWFC	therealvivianwhite@icloud.com
VP3UPK	therealvivianwhite@icloud.com
WVNBEF	therealvivianwhite@icloud.com
ZEAZKD	therealvivianwhite@icloud.com
ZGVLBE	therealvivianwhite@icloud.com
ZKXMCC	therealvivianwhite@icloud.com

Question 6: Provide the AppleID associated with this phone.

Consensus Result: therealvivianwhite@icloud.com

Expected Response Explanation:

Account information is stored in the ZACCOUNT table of /private/var/mobile/Library/Accounts/Accounts3.sqlite

Expected Response Illustration:

Accounts3.sqlite

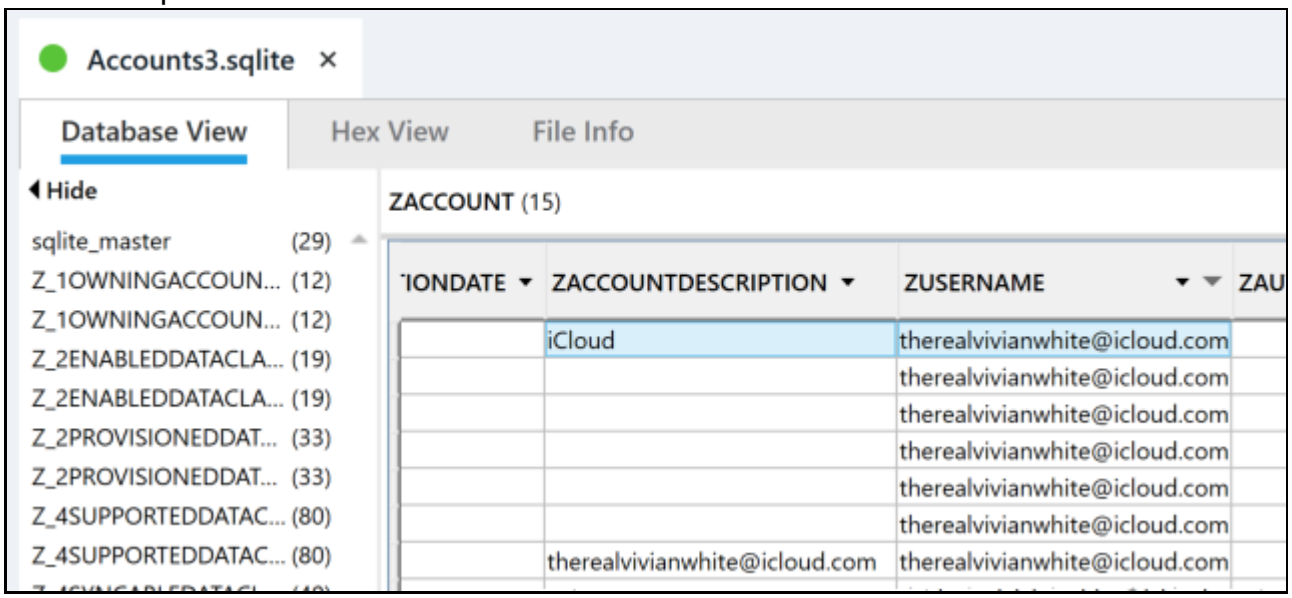


TABLE 1

Question 7 - Examination Questions

Question 7: What is the time zone setting for this phone? Provide response exactly as shown by the device.

Manufacturer's Expected Response: America/New_York and variations representing the same information

WebCode	Response
2JFUWZ	America/New_York
2YAJPB	(UTC-05:00) New_York (America)
3329MU	(UTC-05:00) New_York (America)
3R3DPY	(UTC -05:00) New_York(America)
4FPB42	-(UTC-05:00) New York (America)
66P4MA	(UTC-05:00) New_York (America)
6ERKDC	(UTC-05:00) New_York (America)
6M83T7	(UTC-05:00) New_York (America)
6QMVJY	(UTC -05:00) New_York (America)
7CKLGB	America/New_York
7ND6X2	America/New_York
7W8BQ3	Timezone = (UTC-05:00) New_York (America)
7WQWJT	(UTC-05:00) New_York (America)
8F34CZ	(UTC-05:00) New_York(America)
8JDFPT	(UTC-05:00) New_York (America)
8JXTWE	(UTC-05:00) New_York (America) This is recovered within the file: com.apple/Appstore.plist
8VQFKZ	(UTC -5:00) New_York (America)
9MCRLT	(UTC-05:00) New_York (America)
9VQVED	America/New_York
AGMPY9	America/New_York
AKNRPA	from Device Info: (UTC-05:00) New_York (America) from com.apple.AppStore.plist: America/New_York
BHAT4Y	(UTC-05:00) New_York (America)
BNZ3DX	America/New_York
C6EZRU	UTC-05:00 New_York (America)
CERU9G	(UTC-5:00) New_York (America)
CKT9RX	America/New_York
CZNJJA	America/New_York
DNUPM7	America/New_York
DQZW7Y	(UTC-05:00) New_York (America)

TABLE 1

Question 7 - Examination Questions	
WebCode	**Response**
DT3X7V	(UTC-05:00) New_York (America)
DYD4P9	(UTC-05:00) New_York (America)
E7PH86	(UTC-05:00) New_York (America)
FLWZEV	(UTC-05:00) New_York (America)
G8C3KE	America/New_York
GPDMNU	America/New_York
GQPFJW	(UTC-05:00) New _York (America)
GYF3AR	(UTC-05:00) New_York (America)
HGFG4R	(UTC-05:00) New_York (American)
JCC299	America/New_York
JEJH6J	America/New_York
JL3MGR	(UTC-05:00) New_York (America)
KVP67K	America/New_York
L6PWCQ	(UTC-05:00) New_York
MFJPZ8	(UTC-05:00) New_York (America)
MXKEER	(UTC-05:00) New_York (America)
N634TR	America/New_York
NE7FKF	(UTC-05:00) New_York (America)
NEP2GC	(UTC-05:00) New_York (America)
NP67AT	America/New_York
NT6H7T	America/New_York
NZNRBG	(UTC-05:00) New_York (America)
P77HBH	(UTC-05:00) New_York (America)
P9Y9K3	(UTC-05:00) New_York (America)
QLFNYL	America/New_York - Displayed in Cellebrite as (UTC-05:00) New_York (America)
QM9E98	(UTC-05:00) New_York (America)
R748U6	America/New_York
T8BAT9	America/New_York (UTC-05:00)
T9LU2H	(UTC-05:00) New_York (America)
TPPKJE	(UTC-05:00) New_York (America)
TYEAHM	(UTC -05:00) New_York (America)
U7V8LZ	America/New_York

TABLE 1

Question 7 - Examination Questions	
WebCode	**Response**
V7R6A2	(UTC -05:00) New_York (America)
VDB8G4	America/New_York
VG9PVJ	(UTC-05:00) New_York (America)
VJEAGX	(UTC -5:00) New_York (America)
VLPWFC	America/New_York
VP3UPK	(UTC-05:00) New_York
WVNBEF	(UTC-05:00) New_York (America)
ZEAZKD	America/New_York
ZGVLBE	(UTC-05:00) New_York (America)
ZKXMCC	America/New_York

Question 7: What is the time zone setting for this phone? Provide response exactly as shown by the device.

Consensus Result: (UTC -05:00) New_York (America) and variations representing the same information

Expected Response Explanation:

Time zone setting information is stored in /private/var/mobile/Library/Preferences/com.apple.AppStore.plist

Expected Response Illustration:

com.apple.AppStore.plist

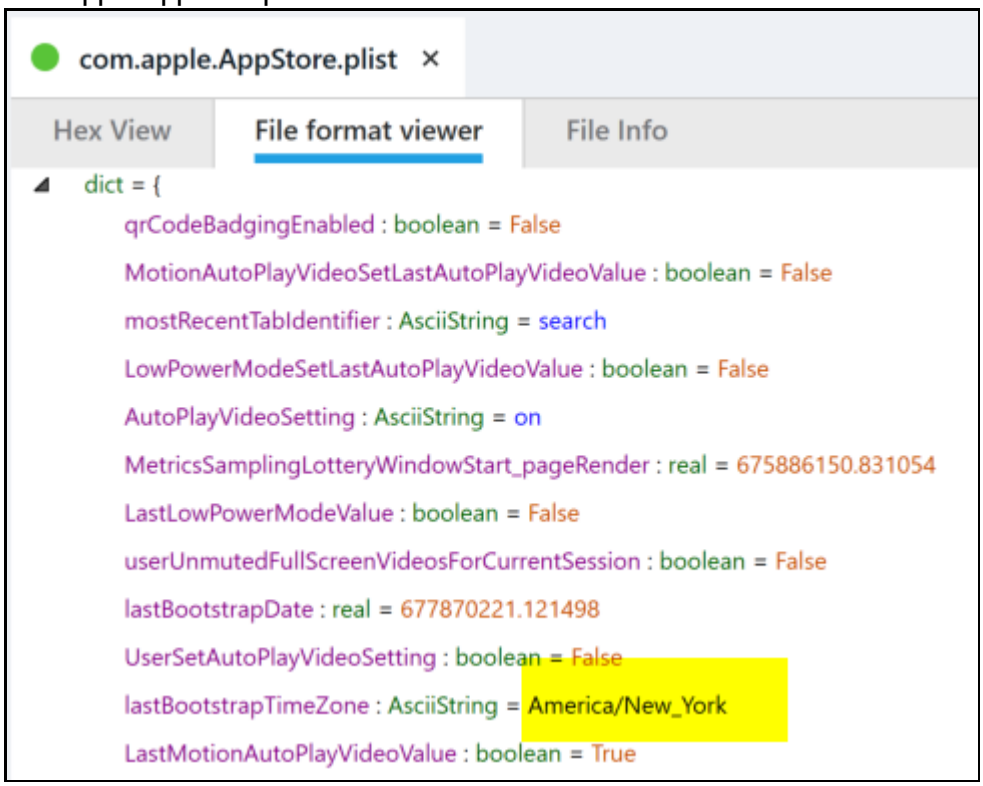


TABLE 1

Question 8 - Examination Questions

Question 8: What is the Device Name for this phone?

Manufacturer's Expected Response: Vivian's iPhone

WebCode	Response
2JFUWZ	Vivian's iPhone
2YAJPB	Vivian's iPhone
3329MU	Vivian's iPhone
3R3DPY	Vivian's iPhone
4FPB42	Vivian's iPhone
66P4MA	Vivian's iPhone
6ERKDC	Vivian's iPhone
6M83T7	Vivian's iPhone
6QMVJY	Vivian's iPhone
7CKLGB	Vivian's iPhone
7ND6X2	Vivian's iPhone
7W8BQ3	Vivian's iPhone
7WQWJT	Vivian's iPhone
8F34CZ	Vivian's iPhone
8JDFPT	Vivian's iPhone
8JXTWE	Vivian's iPhone Recovered within file: data.ark.plist
8VQFKZ	Vivian's iPhone
9MCRLT	Vivian's iPhone
9VQVED	Vivian's iPhone
AGMPY9	Vivian's iPhone
AKNRPA	Vivian's iPhone
BHAT4Y	Vivian's iPhone
BNZ3DX	Vivian's iPhone
C6EZRU	Vivian's iPhone
CERU9G	Vivian's iPhone
CKT9RX	Vivian's iPhone
CZNJJA	Vivian's iPhone
DNUPM7	Vivian's iPhone
DQZW7Y	Vivian's iPhone
DT3X7V	Vivian's iPhone

TABLE 1

Question 8 - Examination Questions	
WebCode	**Response**
DYD4P9	Vivian's iPhone
E7PH86	Vivian's iPhone
FLWZEV	Vivian's iPhone
G8C3KE	Vivian's iPhone
GPDMNU	Vivian's iPhone
GQPFJW	Vivian's iPhone
GYF3AR	Vivian's iPhone
HGFG4R	Vivian's iPhone
JCC299	Vivian's iPhone
JEJH6J	Vivian's iPhone
JL3MGR	Vivian's iPhone
KVP67K	Vivian's iPhone
L6PWCQ	Vivian's iPhone
MFJPZ8	Vivian's iPhone
MXKEER	Vivian's iPhone
N634TR	Vivian's iPhone
NE7FKF	Vivian's iPhone
NEP2GC	Vivian's iPhone
NP67AT	Vivian's iPhone
NT6H7T	Vivian's iPhone
NZNRBG	Vivian's iPhone
P77HBH	Vivian's iPhone
P9Y9K3	Vivian's iPhone
QLFNYL	Vivian's iPhone
QM9E98	Vivian's iPhone
R748U6	Vivian's iPhone
T8BAT9	Vivian's iPhone
T9LU2H	Vivian's iPhone
TPPKJE	Vivian's iPhone
TYEAHM	Vivian's iPhone
U7V8LZ	Vivian's iPhone
V7R6A2	Vivian's iPhone

TABLE 1

Question 8 - Examination Questions	
WebCode	**Response**
VDB8G4	Vivian's iPhone
VG9PVJ	Vivian's iPhone
VJEAGX	Vivian's iPhone
VLPWFC	Vivian's iPhone
VP3UPK	Vivian's iPhone
WVNBEF	Vivian's iPhone
ZEAZKD	Vivian's iPhone
ZGVLBE	Vivian's iPhone
ZKXMCC	Vivian's iPhone

Question 8: What is the Device Name for this phone?

Consensus Result: Vivian's iPhone

Expected Response Explanation:

Device Name information is stored in /root/private/var/root/Library/Lockdown/data_ark.plist

Expected Response Illustration:

com.apple.AppStore.plist

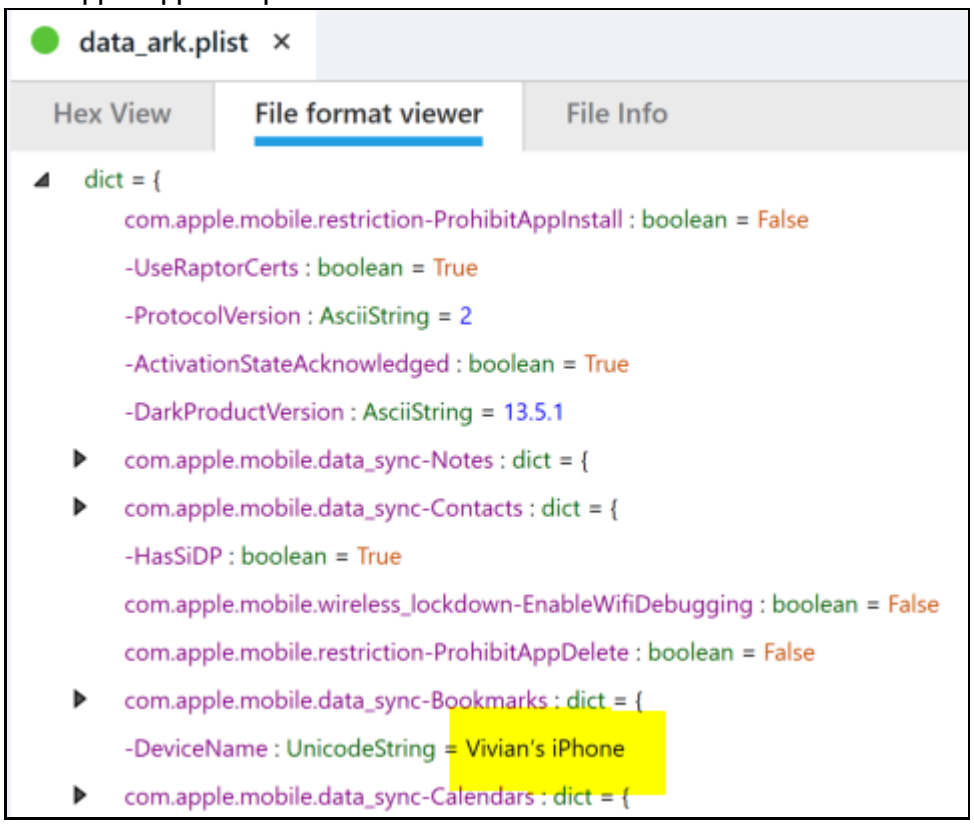


TABLE 1

Question 9 - Examination Questions

Question 9: What is the SSID of the Wi-Fi access point with BSSID 70:f0:96:c7:1b:23?

Manufacturer's Expected Response: ZurichAirport

WebCode	Response
2JFUWZ	ZurichAirport
2YAJPB	ZurichAirport
3329MU	ZurichAirport
3R3DPY	ZurichAirport
4FPB42	ZurichAirport
66P4MA	ZurichAirport
6ERKDC	ZurichAirport
6M83T7	ZurichAirport
6QMVJY	ZurichAirport
7CKLGB	ZurichAirport
7ND6X2	ZurichAirport
7W8BQ3	ZurichAirport
7WQWJT	ZurichAirport
8F34CZ	ZurichAirport
8JDFPT	ZurichAirport
8JXTWE	ZurichAirport
8VQFKZ	ZurichAirport
9MCRLT	ZurichAirport
9VQVED	ZurichAirport
AGMPY9	ZurichAirport
AKNRPA	ZurichAirport
BHAT4Y	ZurichAirport
BNZ3DX	ZurichAirport
C6EZRU	ZurichAirport
CERU9G	ZurichAirport
CKT9RX	ZurichAirport
CZNJJA	ZurichAirport
DNUPM7	ZurichAirport
DQZW7Y	ZurichAirport
DT3X7V	SSID: ZurichAirport

TABLE 1

Question 9 - Examination Questions	
WebCode	**Response**
DYD4P9	ZurichAirport
E7PH86	ZurichAirport
FLWZEV	ZurichAirport
G8C3KE	ZurichAirport
GPDMNU	ZurichAirport
GQPFJW	ZurichAirport
GYF3AR	ZurichAirport
HGFG4R	Zurich Airport
JCC299	ZurichAirport
JEJH6J	ZurichAirport
JL3MGR	ZurichAirport
KVP67K	ZurichAirport
L6PWCQ	ZurichAirport
MFJPZ8	ZurichAirport
MXKEER	ZurichAirport
N634TR	ZurichAirport
NE7FKF	ZurichAirport
NEP2GC	ZurichAirport
NP67AT	ZurichAirport
NT6H7T	ZurichAirport
NZNRBG	ZurichAirport
P77HBH	ZurichAirport
P9Y9K3	ZurichAirport
QLFNYL	ZurichAirport
QM9E98	ZurichAirport
R748U6	ZurichAirport
T8BAT9	ZurichAirport
T9LU2H	ZurichAirport
TPPKJE	ZurichAirport
TYEAHM	ZurichAirport
U7V8LZ	ZurichAirport
V7R6A2	NOT WITHIN LABORATORY'S SCOPE

TABLE 1

Question 9 - Examination Questions	
WebCode	**Response**
VDB8G4	ZurichAirport
VG9PVJ	ZurichAirport
VJEAGX	ZurichAirport
VLPWFC	ZurichAirport
VP3UPK	ZurichAirport
WVNBEF	ZurichAirport
ZEAZKD	ZurichAirport
ZGVLBE	ZurichAirport
ZKXMCC	ZurichAirport

Question 9: What is the SSID of the Wi-Fi access point with BSSID 70:f0:96:c7:1b:23?

Consensus Result: ZurichAirport

Expected Response Explanation:

Information about detected Wi-Fi access points is stored in /private/var/preferences/SystemConfiguration/com.apple.wifi.plist

Expected Response Illustration:

Autopsy view of com.apple.wifi.plist

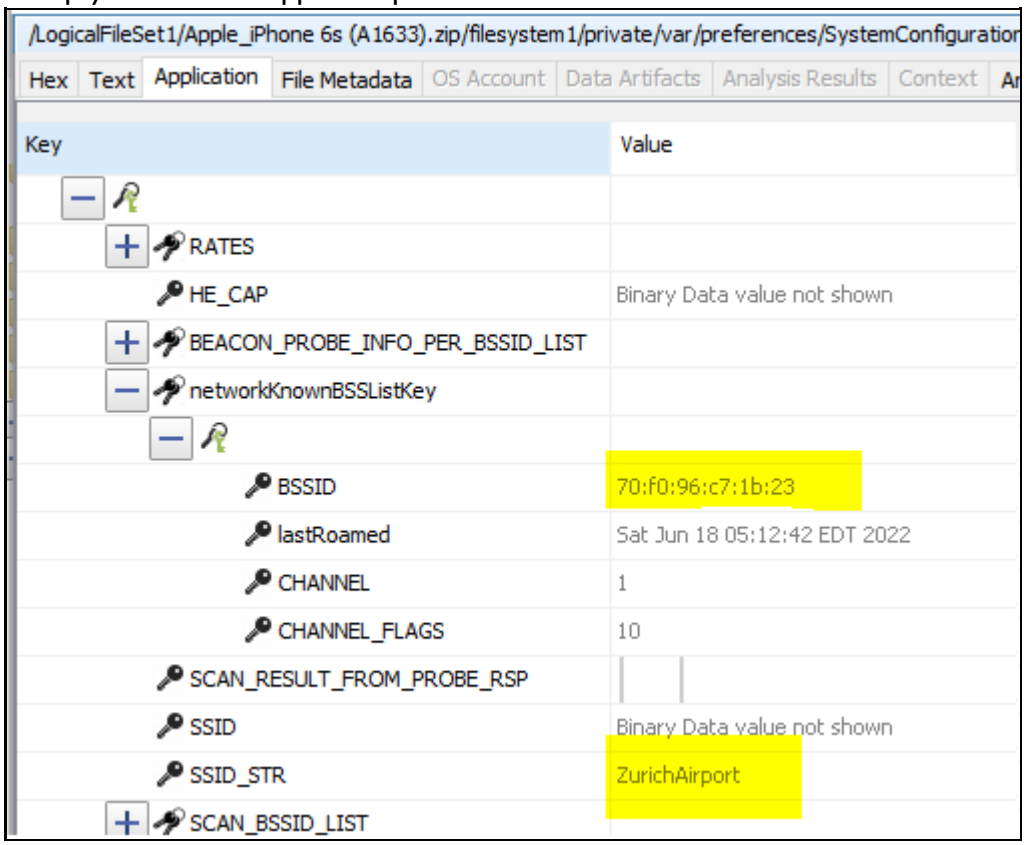


TABLE 1

Question 9 - Examination Questions

Cellebrite Wireless Networks table

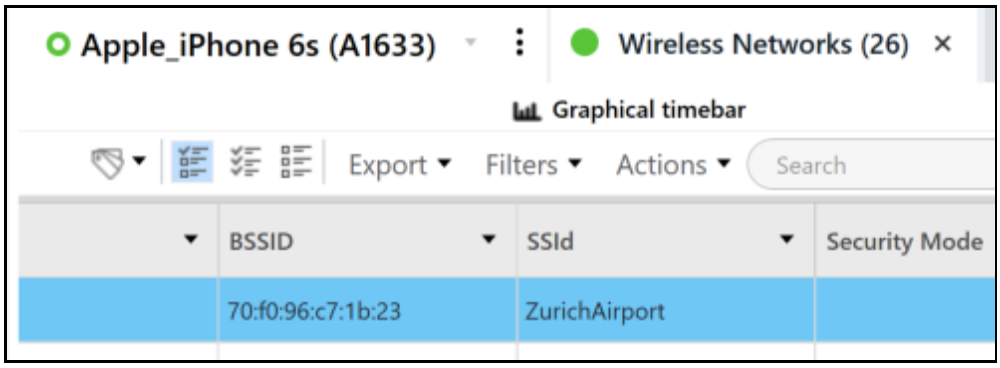


TABLE 1

Question 10 - Examination Questions

Question 10: What is the device name for the (connected) device with MAC address A2:9D:FE:97:BE:53 ?

Manufacturer's Expected Response: MONSTER WBA9-1008

WebCode	Response
2JFUWZ	MONSTER WBA9-1008
2YAJPB	MONSTER WBA9-1008
3329MU	MONSTER WBA9-1008
3R3DPY	MONSTER WBA9-1008
4FPB42	MONSTER WBA9-1008
66P4MA	MONSTER WBA9-1008
6ERKDC	MONSTER WBA9-1008
6M83T7	MONSTER WBA9-1008
6QMVJY	MONSTER WBA9-1008
7CKLGB	MONSTER WBA9-1008
7ND6X2	MONSTER WBA9-1008
7W8BQ3	MONSTER WBA9-1008
7WQWJT	MONSTER WBA9-1008
8F34CZ	MONSTER WBA9-1008
8JDFPT	MONSTER WBA9-1008
8JXTWE	MONSTER WBA9-1008
8VQFKZ	MONSTER WBA9-1008
9MCRLT	MONSTER WBA9-1008
9VQVED	MONSTER WBA9-1008
AGMPY9	MONSTER WBA9-1008
AKNRPA	MONSTER WBA9-1008
BHAT4Y	MONSTER WBA9-1008
BNZ3DX	MONSTER WBA9-1008
C6EZRU	MONSTER WBA9-1008
CERU9G	MONSTER WBA9-1008
CKT9RX	MONSTER WBA9-1008
CZNJJA	MONSTER WBA9-1008
DNUPM7	MONSTER WBA9-1008
DQZW7Y	MONSTER WBA9-1008

TABLE 1

Question 10 - Examination Questions	
WebCode	**Response**
DT3X7V	MONSTER WBA9-1008
DYD4P9	MONSTER WBA9-1008
E7PH86	MONSTER WBA9-1008
FLWZEV	MONSTER WBA9-1008
G8C3KE	MONSTER WBA9-1008
GPDMNU	MONSTER WBA9-1008
GQPFJW	Monster WBA9-1008
GYF3AR	MONSTER WBA9-1008
HGFG4R	Monster WBA9-1008
JCC299	MONSTER WBA9-1008
JEJH6J	MONSTER WBA9-1008
JL3MGR	MONSTER WBA9-1008
KVP67K	MONSTER WBA9-1008
L6PWCQ	MONSTER WBA9-1008
MFJPZ8	MONSTER WBA9-1008
MXKEER	MONSTER WBA9-1008
N634TR	MONSTER WBA9-1008
NE7FKF	Monster WBA9-1008
NEP2GC	MONSTER WBA9-1008
NP67AT	MONSTER WBA9-1008
NT6H7T	MONSTER WBA9-1008
NZNRBG	MONSTER WBA9-1008
P77HBH	MONSTER WBA9-1008
P9Y9K3	MONSTER WBA9-1008
QLFNYL	MONSTER WBA9-1008
QM9E98	MONSTER WBA9-1008
R748U6	MONSTER WBA9-1008
T8BAT9	MONSTER WBA9-1008
T9LU2H	MONSTER WBA9-1008
TPPKJE	MONSTER WBA9-1008
TYEAHM	MONSTER WBA9-1008
U7V8LZ	MONSTER WBA9-1008

TABLE 1

Question 10 - Examination Questions	
WebCode	**Response**
V7R6A2	NOT WITHIN LABORATORY'S SCOPE
VDB8G4	MONSTER WBA9-1008
VG9PVJ	MONSTER WBA9-1008
VJEAGX	MONSTER WBA9-1008
VLPWFC	MONSTER WBA9-1008
VP3UPK	MONSTER WBA9-1008
WVNBEF	MONSTER WBA9-1008
ZEAZKD	MONSTER WBA9-1008
ZGVLBE	MONSTER WBA9-1008
ZKXMCC	MONSTER WBA9-1008

Question 10: What is the device name for the (connected) device with MAC address A2:9D:FE:97:BE:53 ?

Consensus Result: MONSTER WBA9-1008

Expected Response Explanation:
A2:9D:FE:97:BE:53 corresponds with a paired Bluetooth device recorded in /root/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db

Expected Response Illustration:

Cellebrite Devices tab

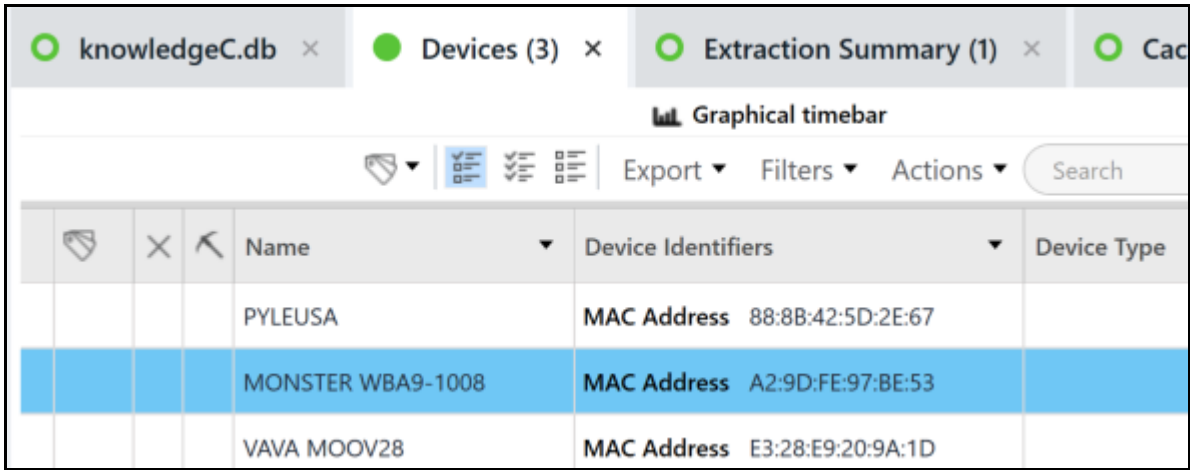


TABLE 1

Question 11 - Examination Questions

Question 11: What (non-Apple) encrypted email app did the user install?

Manufacturer's Expected Response: Proton Mail

WebCode	Response
2JFUWZ	ProtonMail
2YAJPB	ProtonMail
3329MU	Proton Mail - Encrypted Email
3R3DPY	Proton Mail - Encrypted Email - Version 4.0.0
4FPB42	caseyb_lack78@proton.me
66P4MA	protonmail
6ERKDC	Proton Mail
6M83T7	Proton Mail - Encrypted Email
6QMVJY	Proton Mail
7CKLGB	Proton Mail
7ND6X2	Proton Mail – Encrypted Email
7W8BQ3	Proton Mail - Encrypted Email
7WQWJT	Proton Mail – Encrypted Email
8F34CZ	Proton Mail – Encrypted Email
8JDFPT	Proton Mail
8JXTWE	ProtonMail
8VQFKZ	Proton Mail - Encrypted Email
9MCRLT	Proton Mail
9VQVED	Proton Mail - Encrypted Email
AGMPY9	Proton Mail
AKNRPA	Proton Mail - Encrypted Email
BHAT4Y	Proton Mail - Encrypted Email
BNZ3DX	Proton Mail – Encrypted Email
C6EZRU	Proton Mail
CERU9G	Proton Mail - Encrypted Email
CKT9RX	Protonmail
CZNJJA	Proton Mail - Encrypted Email
DNUPM7	ProtonMail
DQZW7Y	Proton Mail
DT3X7V	Proton Mail - Encrypted Email

TABLE 1

Question 11 - Examination Questions	
WebCode	**Response**
DYD4P9	Proton Mail - Encrypted Email
E7PH86	Proton Mail
FLWZEV	ProtonMail
G8C3KE	Proton Mail – Encrypted Email
GPDMNU	Proton Mail - Encrypted Email
GQPFJW	Proton Mail
GYF3AR	protonmail
HGFG4R	Proton Mail
JCC299	Proton Mail - Encrypted Email
JEJH6J	proton mail
JL3MGR	Proton Mail - Encrypted Email
KVP67K	ProtonMail
L6PWCQ	Proton Mail
MFJPZ8	Protonmail
MXKEER	Proton Mail
N634TR	Proton Mail - Encrypted Email
NE7FKF	Protomail
NEP2GC	Proton Mail – Encrypted Email
NP67AT	ProtonMail
NT6H7T	ProtonMail
NZNRBG	Proton mail
P77HBH	ProtonMail
P9Y9K3	Proton Mail
QLFNYL	Proton Mail
QM9E98	ProtonMail
R748U6	ProtonMail
T8BAT9	ProtonMail
T9LU2H	Proton Mail - Encrypted Email
TPPKJE	Proton Mail
TYEAHM	ProtonMail
U7V8LZ	Proton Mail - Encrypted Email
V7R6A2	NOT WITHIN LABORATORY'S SCOPE

TABLE 1

Question 11 - Examination Questions	
WebCode	**Response**
VDB8G4	Proton Mail - Encrypted Email
VG9PVJ	Proton Mail - Encrypted Email - ch.protonmail.protonmail
VJEAGX	Proton Mail
VLPWFC	Proton Mail
VP3UPK	Proton Mail - Encrypted Mail
WVNBEF	Proton Mail - Encrypted Email
ZEAZKD	ProtonMail
ZGVLBE	Proton Mail - Encrypted Email
ZKXMCC	Proton Mail - Encrypted Email

Question 11: What (non-Apple) encrypted email app did the user install?

Consensus Result: Proton Mail

Expected Response Explanation:

A review of installed applications for mail apps shows two non-Apple email apps, "Gmail - Email by Google" and "Proton Mail – Encrypted Email."

Expected Response Illustration:

Cellebrite Installed Applications table

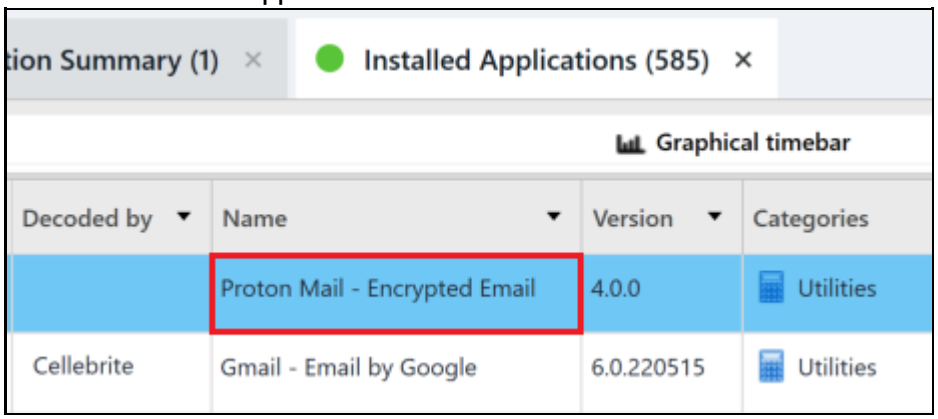


TABLE 1

Question 12 - Examination Questions

Question 12: What email address was configured with the user-installed encrypted email app referenced in question 11?

Manufacturer's Expected Response: caseyb_lack78@proton.me

WebCode	Response
2JFUWZ	caseyb_lack78@proton.me
2YAJPB	caseyb_lack78@proton.me
3329MU	caseyblack78@proton.me
3R3DPY	caseyb_lack78@proton.me
4FPB42	Proton Mail - Encrypted Email
66P4MA	passportcardzrus@proton.me
6ERKDC	caseyblack78@proton.me
6M83T7	caseyb_lack78@proton.me
6QMVJY	caseyb_lack78@proton.me
7CKLGB	caseyb_lack78@proton.me
7ND6X2	caseyb_lack78@proton.me
7W8BQ3	caseyb_lack78@proton.me
7WQWJT	caseyblack78@proton.me
8F34CZ	caseyb_lack78@proton.me
8JDFPT	caseyb_lack78@proton.me
8JXTWE	caseyb_lack78@proton.me
8VQFKZ	caseyb_lack78@proton.me
9MCRLT	Caseyb_lack78@proton.me
9VQVED	caseyb_lack78@proton.me
AGMPY9	caseyb_lack78@proton.me
AKNRPA	caseyb_lack78@proton.me
BHAT4Y	caseyb_lack78@proton.me
BNZ3DX	caseyb_lack78@proton.me
C6EZRU	caseyb_lack78@proton.me
CERU9G	caseyb_lack78@proton.me
CKT9RX	Not within laboratory's scope.
CZNJJA	caseyb_lack78@proton.me
DNUPM7	caseyb_lack78@proton.me
DQZW7Y	caseyb_lack78@proton.me

TABLE 1

Question 12 - Examination Questions	
WebCode	**Response**
DT3X7V	caseyb_lack78@proton.me
DYD4P9	caseyblack78@proton.me
E7PH86	caseyb_lack78@proton.me
FLWZEV	caseyb_lack78@proton.me
G8C3KE	caseyb_lack78@proton.me
GPDMNU	caseyb_lack78@proton.me
GQPFJW	caseyb_lack78@proton.me
GYF3AR	passportcardzrus@proton.me
HGFG4R	caseyb_lack78@proton.me
JCC299	caseyb_lack78@proton.me
JEJH6J	caseyb_lack78@proton.me
JL3MGR	caseyb_lack78@proton.me
KVP67K	caseyb_lack78@proton.me
L6PWCQ	caseyb_lack78@proton.me
MFJPZ8	caseyb_lack78@proton.me
MXKEER	caseyb_lack78@proton.me
N634TR	caseyb_lack78@proton.me
NE7FKF	caseyb_lack78@proton.me
NEP2GC	caseyb_lack78@proton.me
NP67AT	caseyb_lack78@proton.me
NT6H7T	caseyb_lack78@proton.me
NZNRBG	caseyb_lack78@proton.me
P77HBH	caseyb_lack78@proton.me
P9Y9K3	caseyb_lack78@proton.me
QLFNYL	caseyb_lack78@proton.me
QM9E98	caseyb_lack78@proton.me
R748U6	caseyb_lack78@proton.me
T8BAT9	Caseyb_lack78@proton.me
T9LU2H	caseyb_lack78@proton.me
TPPKJE	caseyblack78@proton.me
TYEAHM	caseyb_lack78@proton.me
U7V8LZ	caseyb_lack78@proton.me

TABLE 1

Question 12 - Examination Questions	
WebCode	**Response**
V7R6A2	NOT WITHIN LABORATORY'S SCOPE
VDB8G4	caseyb_lack78@proton.me
VG9PVJ	caseyb_lack78@proton.me
VJEAGX	passportcardzrus@proton.me
VLPWFC	caseyb_lack78@proton.me
VP3UPK	caseyb_lack78@proton.me
WVNBEF	caseyb_lack78@proton.me
ZEAZKD	caseyb_lack78@proton.me
ZGVLBE	caseyb_lack78@proton.me
ZKXMCC	caseyb_lack78@proton.me

Question 12: What email address was configured with the user-installed encrypted email app referenced in question 11?

Consensus Result: caseyb_lack78@proton.me. The email address caseyblack78@proton.me was also accepted. Further investigation, identified that dependent on how the answer was found, certain artifacts could have misled participants to the email address caseyblack78@proton.me.

Expected Response Explanation:

Proton Mail app data is stored in /private/var/mobile/Containers/Shared/AppGroup/84E1289D-4453-424E-8CC9-22F05D9D5B6E/ProtonMail.sqlite. The email address caseyblack78@proton.me is the recipient of all messages in the account.

Expected Response Illustration:

Cellebrite Analyzed Emails

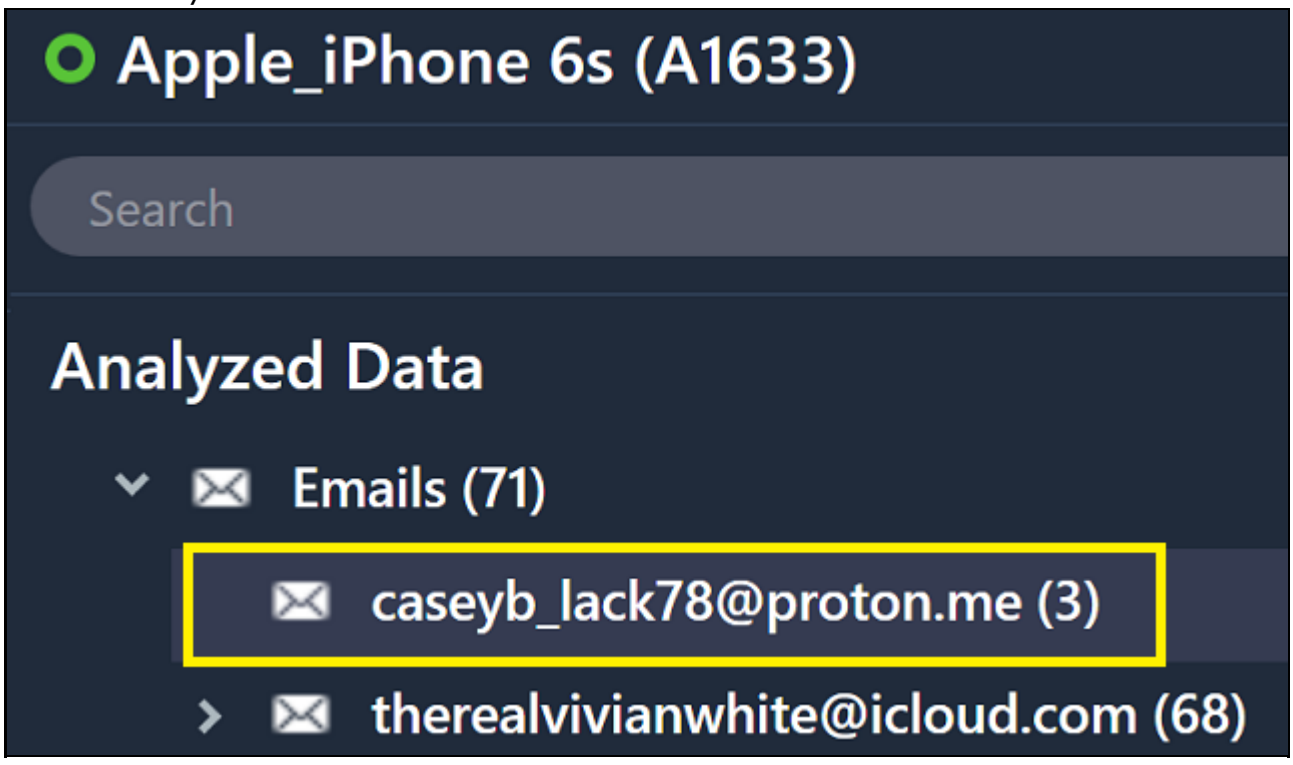


TABLE 1

Question 12 - Examination Questions

ProtonMail.sqlite

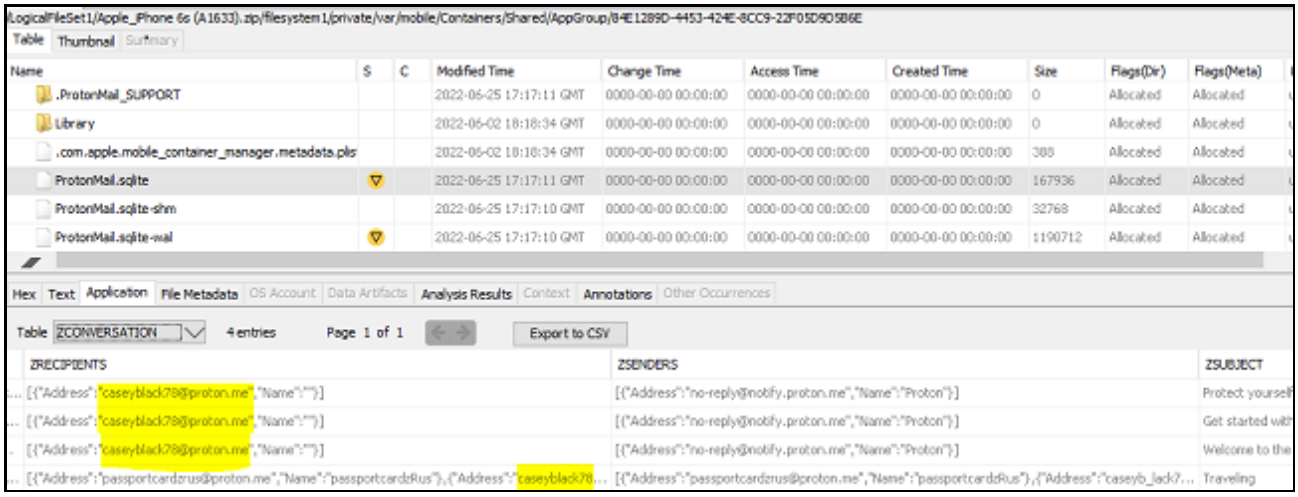


TABLE 1

Question 13 - Examination Questions

Question 13: What is the email address of the party with whom the phone user corresponded with a subject line of "Traveling"?

Manufacturer's Expected Response: passportcardzrus@proton.me

WebCode	Response
2JFUWZ	passportcardzrus@proton.me
2YAJPB	passportcardzrus@proton.me
3329MU	passportcardzRus@proton.me
3R3DPY	passportcardzrus@proton.me
4FPB42	passportcardzRus@proton.me
66P4MA	caseyb_lack78@proton.me
6ERKDC	no-reply@marketing.lyftmail.com
6M83T7	passportcardzRus@proton.me
6QMVJY	passportcardzrus@proton.me
7CKLGB	passportcardzrus@proton.me
7ND6X2	passportcardzrus@proton.me
7W8BQ3	passportcardzrus@proton.me
7WQWJT	passportcardzrus@proton.me
8F34CZ	passportcardzrus@proton.me
8JDFPT	passportcardzrus@proton.me
8JXTWE	passportcardzrus@proton.me
8VQFKZ	passportcardzrus@proton.me
9MCRLT	passportcardzrus@proton.me
9VQVED	passportcardzrus@proton.me
AGMPY9	passportcardzrus@proton.me
AKNRPA	passportcardzrus@proton.me
BHAT4Y	passportcardzRus@proton.me
BNZ3DX	passportcardzrus@proton.me
C6EZRU	passportcardzrus@proton.me
CERU9G	passportcardzus@proton.me
CKT9RX	Not within laboratory's scope.
CZNJJA	passportcardzrus@proton.me
DNUPM7	passportcardzrus@proton.me
DQZW7Y	passportcardzrus@proton.me

TABLE 1

Question 13 - Examination Questions	
WebCode	**Response**
DT3X7V	passportcardzrus@proton.me
DYD4P9	passportcardzrus@proton.me
E7PH86	passportcardzrus@proton.me
FLWZEV	passportcardzrus@proton.me
G8C3KE	passportcardzrus@proton.me
GPDMNU	passportcardzrus@proton.me
GQPFJW	passportcardzrus@proton.me
GYF3AR	sam.graylk@gmail.com
HGFG4R	passportcardzrus@proton.me
JCC299	passportcardzrus@proton.me
JEJH6J	
JL3MGR	passportcardzRus@proton.me
KVP67K	passportcardzrus@proton.me
L6PWCQ	passportcardzrus@proton.me
MFJPZ8	passportcardzrus@proton.me
MXKEER	passportcardzrus@proton.me
N634TR	passportcardzrus@proton.me
NE7FKF	passportcardzrus@proton.me
NEP2GC	passportcardzrus@proton.me
NP67AT	passportcardzrus@proton.me
NT6H7T	passportcardzrus@proton.me
NZNRBG	passportcardzRus@proton.me
P77HBH	passportcardzrus@proton.me
P9Y9K3	passportcardzrus@proton.me
QLFNYL	passportcardzrus@proton.me
QM9E98	passportcardzrus@proton.me
R748U6	passportcardzRus@proton.me
T8BAT9	passportcardzrus@proton.me
T9LU2H	passportcardzrus@proton.me
TPPKJE	passportcardzrus@proton.me
TYEAHM	passportcardzRus@proton.me
U7V8LZ	passportcardzRus@proton.me

TABLE 1

Question 13 - Examination Questions	
WebCode	**Response**
V7R6A2	NOT WITHIN LABORATORY'S SCOPE
VDB8G4	passportcardzrus@proton.me
VG9PVJ	passportcardzrus@proton.me
VJEAGX	caseyb_lack78@proton.me
VLPWFC	passportcardzrus@proton.me
VP3UPK	passportcardzrus@proton.me
WVNBEF	passportcardzRus@proton.me
ZEAZKD	passportcardzRus@proton.me
ZGVLBE	passportcardzrus@proton.me
ZKXMCC	passportcardzrus@proton.me

Question 13: What is the email address of the party with whom the phone user corresponded with a subject line of "Traveling"?

Consensus Result: passportcardzrus@proton.me

Expected Response Explanation:

Proton Mail app data is stored in /private/var/mobile/Containers/Shared/AppGroup/84E1289D-4453-424E-8CC9-22F05D9D5B6E/ProtonMail.sqlite in the ZCONVERSATION table. This table lists the email addresses and subject lines of all messages in the app. There is one message with subject "Traveling"

Expected Response Illustration:

ProtonMail.sqlite

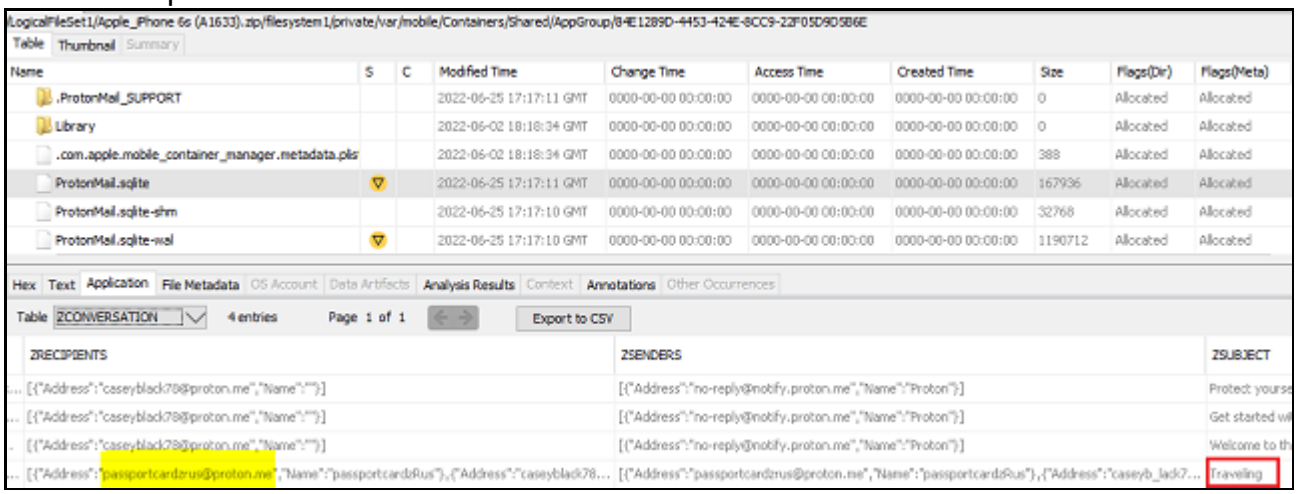


TABLE 1

Question 14 - Examination Questions

Question 14: What was the phone number of the call RECEIVED on 19 June 2022?

Manufacturer's Expected Response: +13133082630

WebCode	Response
2JFUWZ	+13133082630
2YAJPB	+1 (313) 308-2630
3329MU	+13133082630
3R3DPY	+1 (313) 308-2630
4FPB42	+13133082630
66P4MA	+13133082630
6ERKDC	+13133082630
6M83T7	+13133082630
6QMVJY	1-313-308-2630
7CKLGB	+13133082630
7ND6X2	+1 (313) 308-2630
7W8BQ3	+1 (313) 308-2630
7WQWJT	+13133082630
8F34CZ	+13133082630
8JDFPT	1 (313) 308-2630
8JXTWE	+1 (313) 308-2630
8VQFKZ	+13133082630
9MCRLT	+1 (313) 308-2630
9VQVED	1 (313) 308-2630
AGMPY9	+13133082630
AKNRPA	+13133082630
BHAT4Y	+1 (313) 308-2630
BNZ3DX	+1 (313) 308-2630
C6EZRU	+13133082630
CERU9G	+1 (313) 308-2630
CKT9RX	+13133082630
CZNJJA	13133082630
DNUPM7	+13133082630
DQZW7Y	+1 (313) 308-2630
DT3X7V	+1 (313) 308-2630

TABLE 1

Question 14 - Examination Questions	
WebCode	**Response**
DYD4P9	+13133082630
E7PH86	+3133082630
FLWZEV	13133082630
G8C3KE	13133082630
GPDMNU	+13133082630
GQPFJW	+1 (313) 308-2630
GYF3AR	+13133082630
HGFG4R	+13133082630
JCC299	+13133082630
JEJH6J	+3133082630
JL3MGR	+13133082630
KVP67K	+1 (313) 308-2630
L6PWCQ	+13133082630
MFJPZ8	13133082630
MXKEER	+1 (313) 308-2630
N634TR	13133082630
NE7FKF	13133082630
NEP2GC	+1 313 30 82 630
NP67AT	+13133082630
NT6H7T	+13133082630
NZNRBG	+13133082630
P77HBH	+13133082630
P9Y9K3	13133082630
QLFNYL	+1 (313) 308-2630
QM9E98	+1 (313) 308-2630
R748U6	1-313-308-2630
T8BAT9	+13133082630
T9LU2H	+13133082630
TPPKJE	+1 (313) 308-2630
TYEAHM	+13133082630
U7V8LZ	13133082630
V7R6A2	NOT WITHIN LABORATORY'S SCOPE

TABLE 1

Question 14 - Examination Questions	
WebCode	**Response**
VDB8G4	+13133082630
VG9PVJ	+1 (313) 308-2630
VJEAGX	+13133082630
VLPWFC	+1 (313) 308-2630
VP3UPK	+1 (313) 308-2630
WVNBEF	+13133082630
ZEAZKD	13133082630
ZGVLBE	+13133082630
ZKXMCC	+13133082630

Question 14: What was the phone number of the call RECEIVED on 19 June 2022?

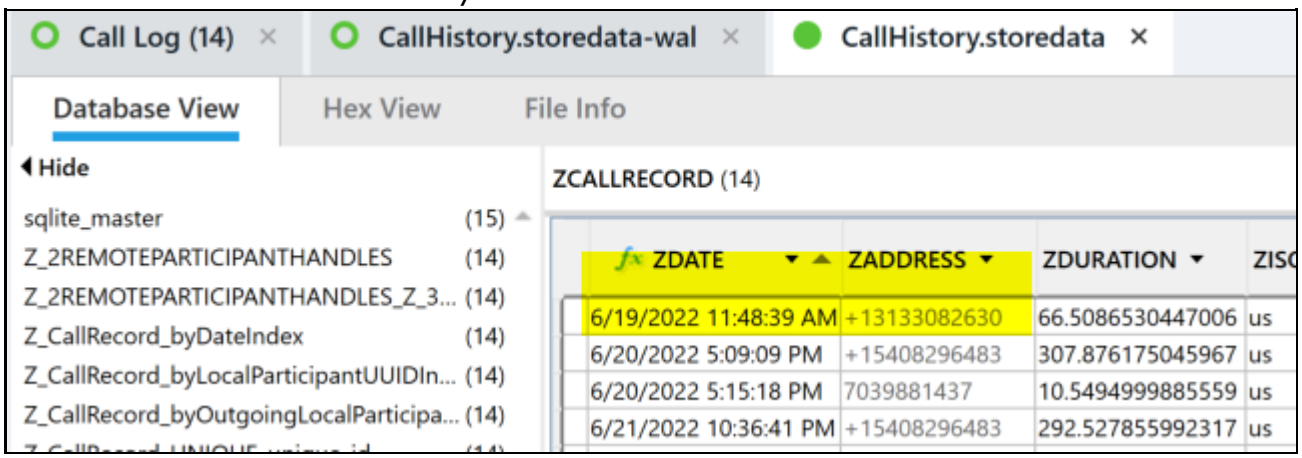
Consensus Result: +13133082630

Expected Response Explanation:

Call history information is stored in /private/var/mobile/Library/CallHistoryDB /CallHistory.storedata
Dialed and incoming numbers with associated timestamps are stored in the ZCALLRECORD table in the ZADDRESS and ZDATE fields, respectively.

Expected Response Illustration:

ZCALLRECORD Table from CallHistory.storedata



Cellebrite Call Log Table

TABLE 1

Question 15 - Examination Questions

Question 15: Which contact did the user call on 6/21/2022 6:43:39 PM(UTC-4)? Provide the name of contact.

Manufacturer's Expected Response: sissy

WebCode	Response
2JFUWZ	sissy
2YAJPB	sissy
3329MU	Sissy
3R3DPY	sissy
4FPB42	sissy
66P4MA	sissy
6ERKDC	5715497087 sissy
6M83T7	sissy
6QMVJY	sissy
7CKLGB	Contact number: 7039881437 Contact name: sissy
7ND6X2	sissy
7W8BQ3	5715497087, Sissy
7WQWJT	sissy
8F34CZ	sissy
8JDFPT	sissy
8JXTWE	sissy
8VQFKZ	Sissy
9MCRLT	sissy
9VQVED	sissy
AGMPY9	sissy
AKNRPA	sissy
BHAT4Y	sissy
BNZ3DX	sissy
C6EZRU	Sissy
CERU9G	sissy
CKT9RX	sissy
CZNJJA	sissy
DNUPM7	sissy
DQZW7Y	Sissy

TABLE 1

Question 15 - Examination Questions	
WebCode	**Response**
DT3X7V	sissy (number: 5715497087)
DYD4P9	sissy
E7PH86	sissy
FLWZEV	sissy
G8C3KE	sissy
GPDMNU	sissy
GQPFJW	sissy
GYF3AR	5715497087 sissy
HGFG4R	Sissy
JCC299	sissy
JEJH6J	sissy
JL3MGR	sissy
KVP67K	sissy
L6PWCQ	sissy
MFJPZ8	sissy
MXKEER	sissy
N634TR	sissy
NE7FKF	sissy
NEP2GC	sissy
NP67AT	sissy
NT6H7T	sissy
NZNRBG	sissy
P77HBH	sissy
P9Y9K3	sissy
QLFNYL	sissy - 5715497087
QM9E98	sissy
R748U6	sissy
T8BAT9	Sissy
T9LU2H	5715497087 sissy
TPPKJE	sissy
TYEAHM	sissy
U7V8LZ	sissy

TABLE 1

Question 15 - Examination Questions	
WebCode	**Response**
V7R6A2	NOT WITHIN LABORATORY'S SCOPE
VDB8G4	sissy
VG9PVJ	sissy
VJEAGX	sissy
VLPWFC	sissy
VP3UPK	sissy
WVNBEF	sissy
ZEAZKD	sissy
ZGVLBE	sissy
ZKXMCC	sissy

Question 15: Which contact did the user call on 6/21/2022 6:43:39 PM(UTC-4)? Provide the name of contact.

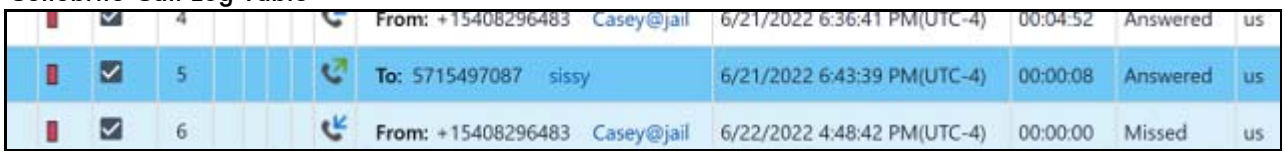
Consensus Result: sissy

Expected Response Explanation:

Call history information is stored in /private/var/mobile/Library/CallHistoryDB /CallHistory.storedata and the associated temp (shm, wal) files. Dialed (and incoming) numbers with associated timestamps are stored in the ZCALLRECORD table in the ZADDRESS and ZDATE fields, respectively. The call placed on 6/21/2022 6:43:39 PM(UTC-4) was to 5715497087. Address Book (Contact) information is stored in private/var/mobile/Library/AddressBook/AddressBook.sqlitedb. The contact associated with 5715497087 is “sissy.”

Expected Response Illustration:

Cellebrite Call Log Table



		4	From: +15408296483 Casey@jail	6/21/2022 6:36:41 PM(UTC-4)	00:04:52	Answered	us
		5	To: 5715497087 sissy	6/21/2022 6:43:39 PM(UTC-4)	00:00:08	Answered	us
		6	From: +15408296483 Casey@jail	6/22/2022 4:48:42 PM(UTC-4)	00:00:00	Missed	us

TABLE 1

Question 16 - Examination Questions

Question 16: What is the CREATION date and time of the Note (taken with the notes App) titled "Greyhound station"? Provide your response in (UTC-4), using the date/time (24-hour) picker.

Manufacturer's Expected Response: 2022-06-25 11:57

WebCode	Response
2JFUWZ	2022-06-25 11:57
2YAJPB	2022-06-25 11:57
3329MU	2022-06-25 11:57
3R3DPY	2022-06-25 11:57
4FPB42	2022-06-25 00:00
66P4MA	2022-06-25 11:57
6ERKDC	2022-06-25 11:57
6M83T7	2022-06-25 11:57
6QMVJY	2022-06-25 11:57
7CKLGB	2022-06-25 11:57
7ND6X2	2022-06-25 11:57
7W8BQ3	2022-06-25 11:57
7WQWJT	2022-06-25 11:57
8F34CZ	2022-06-25 11:57
8JDFPT	2022-06-25 11:57
8JXTWE	2022-06-25 11:57
8VQFKZ	2022-06-25 11:57
9MCRLT	2022-06-25 11:57
9VQVED	6/25/2022 11:57:43 AM (UTC-4)
AGMPY9	2022-06-25 11:57
AKNRPA	2022-06-25 11:57
BHAT4Y	2022-06-25 11:57
BNZ3DX	2022-06-25 11:57
C6EZRU	2022-06-25 11:57
CERU9G	2022-06-25 11:57
CKT9RX	2022-06-25 11:57
CZNJJA	2022-06-25 11:57
DNUPM7	2022-06-25 11:57
DQZW7Y	2022-06-25 11:57

TABLE 1

Question 16 - Examination Questions	
WebCode	**Response**
DT3X7V	2022-06-25 11:57
DYD4P9	2022-06-25 11:57
E7PH86	2022-06-25 11:57
FLWZEV	2022-06-02 01:56
G8C3KE	2022-06-25 11:57
GPDMNU	2022-06-25 11:57
GQPFJW	2022-06-25 01:57
GYF3AR	2022-06-25 11:57
HGFG4R	2022-06-25 11:57
JCC299	2022-06-25 11:57
JEJH6J	2022-06-25 11:57
JL3MGR	2022-06-25 11:57
KVP67K	2022-06-25 11:57
L6PWCQ	2022-06-25 11:57
MFJPZ8	2022-06-25 11:57
MXKEER	2022-06-25 11:57
N634TR	2022-06-25 11:57
NE7FKF	2022-06-25 11:57
NEP2GC	2022-06-25 11:57
NP67AT	2022-06-25 11:57
NT6H7T	2022-06-25 11:57
NZNRBG	2022-06-25 11:57
P77HBH	2022-06-25 11:57
P9Y9K3	2022-06-25 11:57
QLFNYL	2022-06-25 11:57
QM9E98	2022-06-25 11:57
R748U6	2022-06-25 11:57
T8BAT9	2022-06-25 11:57
T9LU2H	2022-06-25 11:57
TPPKJE	2022-06-25 11:57
TYEAHM	2022-06-25 11:57
U7V8LZ	2022-06-25 11:57

TABLE 1

Question 16 - Examination Questions	
WebCode	**Response**
V7R6A2	
VDB8G4	2022-06-25 11:57
VG9PVJ	2022-06-25 11:57
VJEAGX	2022-06-25 11:57
VLPWFC	2022-06-25 11:57
VP3UPK	2022-06-25 11:57
WVNBEF	2022-06-25 11:57
ZEAZKD	2022-06-25 11:57
ZGVLBE	2022-06-25 11:57
ZKXMCC	2022-06-25 11:57

Question 16: What is the CREATION date and time of the Note (taken with the notes App) titled "Greyhound station"? Provide your response in (UTC-4), using the date/time (24-hour) picker.

Consensus Result: 2022-06-25 11:57

Expected Response Explanation:

Data for the Apple notes app is stored in root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite. The ZICCLOUDSYNCINGOBJECT table contains the titles and creation dates of the notes.

Expected Response Illustration:

Cellebrite Notes Table

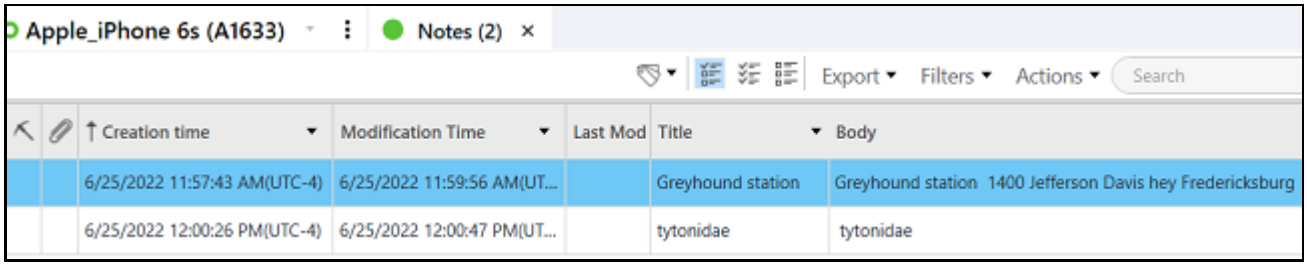


TABLE 1

Question 17 - Examination Questions

Question 17: What event was scheduled to occur 6/24/2022 2:00:00 PM(UTC-4)?

Manufacturer's Expected Response: Casey's Dr.'s Appointment

WebCode	Response
2JFUWZ	Casey's Dr.'s Appointment
2YAJPB	Casey's Dr.'s Appointment
3329MU	Casey's Dr.'s Appointment
3R3DPY	Casey's Dr.'s Appointment
4FPB42	Casey's Dr.'s Appointment
66P4MA	Casey's Dr.'s Appointment
6ERKDC	Casey's Dr.'s Appointment
6M83T7	Casey's Dr.'s Appointment
6QMVJY	Casey's Dr.'s Appointment
7CKLGB	Casey's Dr.'s Appointment
7ND6X2	Casey's Dr.'s Appointment
7W8BQ3	Casey's Dr.'s Appointment
7WQWJT	Casey's Dr.'s Appointment
8F34CZ	Casey's Dr.'s Appointment
8JDFPT	Casey's Dr.'s Appointment
8JXTWE	Casey's Dr.'s Appointment
8VQFKZ	Casey's Dr.'s Appointment
9MCRLT	Casey's Dr.'s Appointment
9VQVED	Casey's Dr.'s Appointment
AGMPY9	Casey's Dr.'s Appointment
AKNRPA	Casey's Dr.'s Appointment
BHAT4Y	Casey's Dr.'s Appointmen
BNZ3DX	Casey's Dr.'s Appointment
C6EZRU	Casey's Dr.'s Appointment
CERU9G	Casey's Dr.'s Appointment
CKT9RX	Casey's Dr.'s Appointment
CZNJJA	Casey's Dr.'s Appointment
DNUPM7	Casey's Dr.'s Appointment
DQZW7Y	Casey's Dr.'s Appointment
DT3X7V	Casey's Dr.'s Appointment

TABLE 1

Question 17 - Examination Questions	
WebCode	**Response**
DYD4P9	Casey's Dr.'s Appointment
E7PH86	Casey's Dr.'s Appointment
FLWZEV	Casey's Dr.'s Appointment
G8C3KE	Casey's Dr.'s Appointment
GPDMNU	Casey's Dr.'s Appointment
GQPFJW	Casey's Dr.'s Appointment
GYF3AR	Casey's Dr.'s Appointment
HGFG4R	Casey's Dr's Appointment
JCC299	Casey's Dr.'s Appointment
JEJH6J	Casey's Dr.'s Appointment
JL3MGR	Casey's Dr.'s Appointment
KVP67K	Casey's Dr.'s Appointment
L6PWCQ	Casey's Dr.'s Appointment
MFJPZ8	Casey's Dr.'s Appointment
MXKEER	Casey's Dr.'s Appointment
N634TR	Casey's Dr.'s Appointment
NE7FKF	Casey's Dr.'s Appointment
NEP2GC	Casey's Dr.'s Appointment
NP67AT	Casey's Dr.'s Appointment
NT6H7T	Casey's Dr.'s Appointment
NZNRBG	Casey's Dr.'s Appointment
P77HBH	Casey's Dr.'s Appointment
P9Y9K3	Casey's Dr.'s Appointment
QLFNYL	Casey's Dr.'s Appointment
QM9E98	Casey's Dr.'s Appointment
R748U6	Casey's Dr.'s Appointment
T8BAT9	Casey's Dr.'s Appointment
T9LU2H	Casey's Dr.'s Appointment
TPPKJE	Casey's Dr.'s Appointment
TYEAHM	Casey's Dr's Appointment
U7V8LZ	Casey's Dr.'s Appointment
V7R6A2	NOT WITHIN LABORATORY'S SCOPE

TABLE 1

Question 17 - Examination Questions	
WebCode	**Response**
VDB8G4	Casey's Dr.'s Appointment
VG9PVJ	Casey's Dr.'s Appointment
VJEAGX	Casey's Dr.'s Appointment
VLPWFC	Casey's Dr.'s Appointment
VP3UPK	Casey's Dr.'s Appointment
WVNBEF	Casey's Dr.'s Appointment
ZEAZKD	Casey's Dr.'s Appointment
ZGVLBE	Casey's Dr.'s Appointment
ZKXMCC	Casey's Dr.'s Appointment

Question 17: What event was scheduled to occur 6/24/2022 2:00:00 PM(UTC-4)?

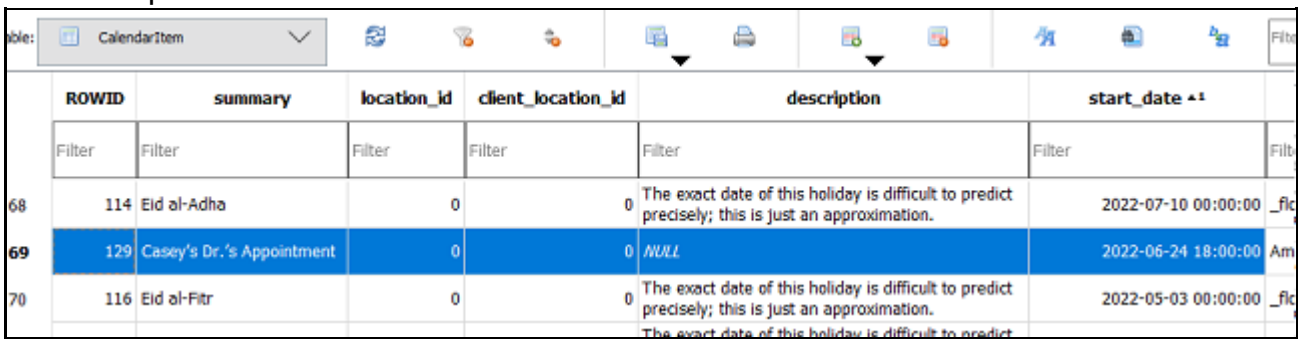
Consensus Result: Casey's Dr.'s Appointment

Expected Response Explanation:

Calendar entries are stored at /private/var/mobile/Library/Calendar/Calendar.sqlitedb and in the associated temp (shm, wal) files.

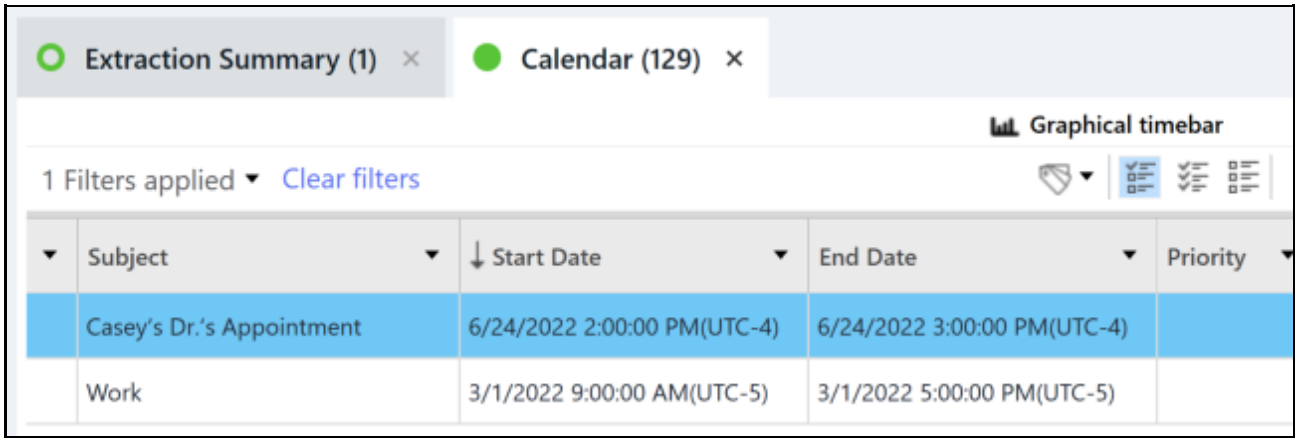
Expected Response Illustration:

Calendar.sqlitedb



	ROWID	summary	location_id	client_location_id	description	start_date
	Filter	Filter	Filter	Filter	Filter	Filter
68	114	Eid al-Adha	0	0	The exact date of this holiday is difficult to predict precisely; this is just an approximation.	2022-07-10 00:00:00
69	129	Casey's Dr.'s Appointment	0	0	*NULL*	2022-06-24 18:00:00
70	116	Eid al-Fitr	0	0	The exact date of this holiday is difficult to predict precisely; this is just an approximation.	2022-05-03 00:00:00

Cellebrite Calendar Table (Filtered)



Extraction Summary (1) | Calendar (129)

Graphical timebar

1 Filters applied | Clear filters

Subject	Start Date	End Date	Priority
Casey's Dr.'s Appointment	6/24/2022 2:00:00 PM(UTC-4)	6/24/2022 3:00:00 PM(UTC-4)	
Work	3/1/2022 9:00:00 AM(UTC-5)	3/1/2022 5:00:00 PM(UTC-5)	

TABLE 1

Question 18 - Examination Questions

Question 18: To what location (place name) did the user navigate using the Apple Maps app with timestamp 6/24/2022 1:51:28 PM(UTC-4).

Manufacturer's Expected Response: Coffeewood Correctional Center

WebCode	Response
2JFUWZ	Coffeewood Dr, Mitchells, VA 22729
2YAJPB	Coffeewood Correctional Center
3329MU	12352 Coffeewood Dr, Mitchells, VA 22729, United States
3R3DPY	Coffeewood Correctional Center
4FPB42	22373 Rapidan Rd, Mitchells, VA 22729, United States
66P4MA	Coffeewood Correctional Center
6ERKDC	Juvenile Justice Department
6M83T7	Coffeewood Correctional Center
6QMVJY	Coffeewood Correctional Center
7CKLGB	Coffeewood Correctional Center 12352 Drive, Culpeper County, VA22729, United States of America
7ND6X2	12352 Coffeewood Correctional Center, Mitchells, VA 22729, USA
7W8BQ3	Coffeewood Correctional Center
7WQWJT	Coffeewood Correctional Center
8F34CZ	Coffeewood Correctional Center
8JDFPT	Coffeewood Correctional Center
8JXTWE	Coffeewood Correctional Center at 12352 Coffeewood Dr, Mitchells, VA 22729
8VQFKZ	Coffeewood Correctional Center
9MCRLT	Coffeewood Correctional Center
9VQVED	Coffeewood Correctional Center
AGMPY9	Coffeewood Correctional Center
AKNRPA	Coffeewood Correctional Center
BHAT4Y	Coffeewood Correctional Center
BNZ3DX	Coffeewood Correctional Center 12352 Drive, Culpeper County, VA22729, United States of America
C6EZRU	Coffeewood Correctional Center
CERU9G	Coffeewood Correctional Center
CKT9RX	Coffeewood Correctional Center
CZNJJA	Coffeewood Correctional Center
DNUPM7	Coffeewood Correctional Center
DQZW7Y	Coffeewood Correctional Center

TABLE 1

Question 18 - Examination Questions	
WebCode	**Response**
DT3X7V	Coffeewood Correctional Center. (Address: Coffeewood Dr, 12352, Culpeper County, Mitchells, 22729, Virginia, United States. Position: (38.365130, -78.019218)
DYD4P9	Coffeewood Correctional Center
E7PH86	Coffeewood Correctional Center
FLWZEV	The Home Depot
G8C3KE	Coffeewood Correctional Center
GPDMNU	Coffeewood Correctional Center
GQPFJW	Winston, Virginia, USA
GYF3AR	Coffeewood Correctional Center
HGFG4R	Coffeewood Correctional Centre
JCC299	Coffeewood Correctional Center
JEJH6J	Coffeewood Correctional Center
JL3MGR	Coffeewood Correctional Center
KVP67K	Coffeewood Correctional Center
L6PWCQ	Coffeewood Correctional Center
MFJPZ8	Coffeewood Correctional Center
MXKEER	Coffeewood Correctional Center
N634TR	CoffeeWood Correctional Center
NE7FKF	Coffeewood Correctional Center
NEP2GC	Coffeewood Correctional Center
NP67AT	Coffeewood Correctional Center
NT6H7T	Coffeewood Correctional Center
NZNRBG	Coffeewood Correctional Center (12352 Coffeewood Dr, Mitchells, VA 22729, United States)
P77HBH	Coffeewood Correctional Center
P9Y9K3	Coffeewood Correctional Center
QLFNYL	Coffeewood Correctional Center
QM9E98	Coffeewood Correctional Center
R748U6	Coffeewood Correctional Center
T8BAT9	12352 Coffeewood Dr, Mitchells, VA 22729, United States
T9LU2H	12352 Coffeewood Dr, Mitchells, VA 22729 Coffeewood Correctional Center
TPPKJE	Coffeewood Correctional Center
TYEAHM	Coffeewood Correctional Center
U7V8LZ	Coffeewood Correctional Center

TABLE 1

Question 18 - Examination Questions	
WebCode	**Response**
V7R6A2	NOT WITHIN LABORATORY'S SCOPE
VDB8G4	12352 Coffeewood Dr, Mitchells, VA 22729, United States
VG9PVJ	Coffeewood Correctional Center
VJEAGX	Coffeewood Correctional Center
VLPWFC	Juvenile Justice Department (Coffeewood Dr, 12352, Culpeper County, Mitchells, 22729, Virginia, United States)
VP3UPK	Coffeewood Correctional Cente
WVNBEF	Coffeewood Correctional Center
ZEAZKD	12352 Coffeewood Dr, Mitchells, VA 22729, United States (Coffeewood Correctional Center)
ZGVLBE	Coffeewood Correctional Center
ZKXMCC	Coffeewood Correctional Center

Question 18: To what location (place name) did the user navigate using the Apple Maps app with timestamp 6/24/2022 1:51:28 PM(UTC-4).

Consensus Result: Coffeewood Correctional Center. Although the place name was requested in the question, the address was also accepted.

Expected Response Explanation:

Records for previous navigations are stored in /root/private/var/mobile/Containers/Data/Application/DEED16F6-1703-4830-B287-E865421DF4A8/Library/Maps/GeoHistory.mapsdata

Expected Response Illustration:

Cellebrite Apple Maps record table

#	Origin	Timestamp	Name	End tim	Position
1					(38.722558, -77.793593)
2		6/3/2022 11:38:00 AM(UTC-4)	The Christmas Shop		(35.897563, -75.667369)
3		6/21/2022 6:49:20 PM(UTC-4)			(38.365130, -78.019218)
4		6/24/2022 1:51:28 PM(UTC-4)	Coffeewood Correctional Center		(38.365130, -78.019218)
5		6/24/2022 1:56:17 PM(UTC-4)			(38.589523, -78.238642)
6		6/24/2022 2:12:20 PM(UTC-4)			(38.455653, -78.012534)
7		6/24/2022 2:12:22 PM(UTC-4)			(38.455653, -78.012534)
8		6/24/2022 2:47:25 PM(UTC-4)			(38.696420, -77.791482)
9		6/24/2022 2:47:27 PM(UTC-4)	The Home Depot		(38.696166, -77.791817)

TABLE 1

Question 19 - Examination Questions

Question 19: What did the phone user say they were going to do after they "got to the drs office"?

Manufacturer's Expected Response: Find a way to take of[f] the tracker... Then a hotel.

WebCode	Response
2JFUWZ	"Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?"
2YAJPB	"Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?"
3329MU	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
3R3DPY	"Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?"
4FPB42	Idk. Find a way to take of the tracker...
66P4MA	Find a way to take of the tracker
6ERKDC	"Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?"
6M83T7	Idk. Find a way to take of the tracker… Then a hotel. [emoji image]?
6QMVJY	Idk. Find away to take of the tracker... Then a hotel?
7CKLGB	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
7ND6X2	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
7W8BQ3	Idk. Find a way to take of the tracker...Then a hotel. [emoji image]?
7WQWJT	"Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?"
8F34CZ	Idk. Find a way to take of the tracker... Then a hotel?
8JDFPT	"Find a way to take of the tracker..."
8JXTWE	On 06/24/2022 at 2:14:56PM user stated: Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
8VQFKZ	idk. Find a way to take of the tracker...Then a hotel?
9MCRLT	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
9VQVED	"Idk. Find a way to take of the tracker...Then a hotel. (emoji)?"
AGMPY9	Find a way to take of the tracker...Then a hotel.
AKNRPA	"Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?"
BHAT4Y	Idk. Find a way to take of the tracker...Then a hotel. [emoji image]?
BNZ3DX	Idk. Find a way to take of the tracker...Then a hotel. [emoji image]?
C6EZRU	"idk. find a way to take off the tracker... then a hotel. (emoji)?"
CERU9G	Idk. Find a way to take of the tracker... Then a hotel?
CKT9RX	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
CZNJJA	Idk. Find a way to take of the tracker...Then a hotel. [emoji image]?
DNUPM7	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
DQZW7Y	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?

TABLE 1

Question 19 - Examination Questions	
WebCode	**Response**
DT3X7V	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
DYD4P9	Idk. Find a way to take of the tracker... Then a hotel. (emoji pictogram)?
E7PH86	Idk. Find a way to take of the tracker… Then a hotel
FLWZEV	19842866876
G8C3KE	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
GPDMNU	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
GQPFJW	"idk.Find a way to take of the tracker.... Then a hotel?"
GYF3AR	Find a way to take of the tracker, then a hotel.
HGFG4R	Idk. Find a way to take of the tracker...then a hotel?
JCC299	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
JEJH6J	Find a way to take off the tracker then find a hotel
JL3MGR	Idk. Find a way to take of the tracker...Then a hotel. ?
KVP67K	“Idk. Find a way to take of the tracker...Then a hotel. [emoji image]?”
L6PWCQ	"Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?"
MFJPZ8	"Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?"
MXKEER	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
N634TR	"Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?"
NE7FKF	Idk. Find a way to take of the tracker... Then a hotel.
NEP2GC	Idk. Find a way to take of the tracker… Then a hotel?
NP67AT	Idk. Find a way to take of the tracker...Then a hotel. [emoji image]?
NT6H7T	Find a way to take of the tracker... Then a hotel.
NZNRBG	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
P77HBH	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
P9Y9K3	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
QLFNYL	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
QM9E98	Idk. Find a way to take of the tracker....Then a hotel. ....?
R748U6	Find a way to take of the tracker...Then a hotel.
T8BAT9	Idk. Find a way to take of the tracker...Then a hotel. [emoji image]?
T9LU2H	Idk. Find a way to take of the tracker...Then a hotel. [emoji image]?
TPPKJE	Idk. Find a way to take of the tracker...Then a hotel. [emoji image]?
TYEAHM	idk. Find a way to take of the tracker...Then a hotel (emoji)
U7V8LZ	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?

TABLE 1

Question 19 - Examination Questions	
WebCode	**Response**
V7R6A2	NOT WITHIN LABORATORY'S SCOPE
VDB8G4	Find a way to take of the tracker... Then a hotel. [emoji image]?
VG9PVJ	“Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?”
VJEAGX	"Idk. Find a way to take of the tracker...Then a hotel."
VLPWFC	Idk. Find a way to take of the tracker...Then a hotel. [emoji image]?
VP3UPK	Idk. Find a way to take of the tracker… Then a hotel. [emoji image]?
WVNBEF	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
ZEAZKD	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
ZGVLBE	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?
ZKXMCC	Idk. Find a way to take of the tracker... Then a hotel. [emoji image]?

Question 19: What did the phone user say they were going to do after they “got to the drs office”?

Consensus Result: "Find a way to take of[f] the tracker... Then a hotel" and variations representing similar information.

Expected Response Explanation:

Searching the phone content for references to “got to the drs office” finds an SMS conversation in which the owner chats with sissy, saying she’ll “Find a way to take of the tracker... Then a hotel."

Expected Response Illustration:

Cellebrite Conversation View

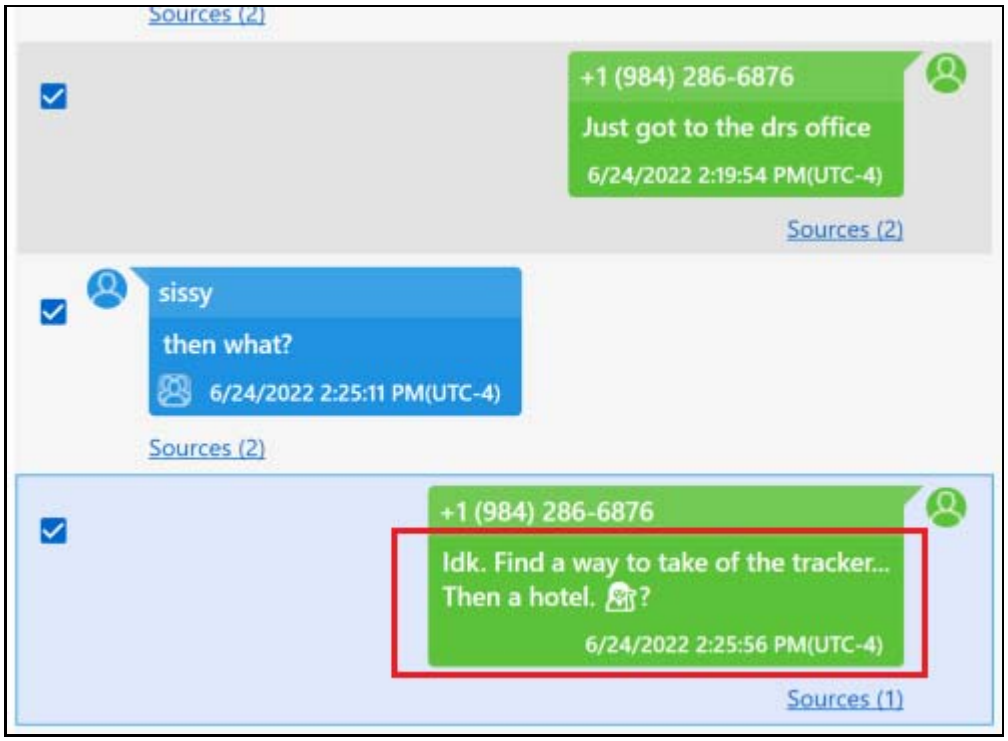


TABLE 1

Question 20 - Examination Questions

Question 20: What did the user search in the Safari web browser, 6/24/2022 12:05:18 PM(UTC-4)?

Manufacturer's Expected Response: remove ankle monitor

WebCode	Response
2JFUWZ	remove ankle monitor
2YAJPB	remove ankle monitor
3329MU	remove ankle monitor - Google Search
3R3DPY	remove ankle monitor
4FPB42	remove ankle monitor
66P4MA	remove ankle monitor
6ERKDC	remove ankle monitor
6M83T7	remove ankle monitor
6QMVJY	remove ankle monitor
7CKLGB	remove ankle monitor
7ND6X2	remove ankle monitor
7W8BQ3	remove ankle monitor
7WQWJT	remove ankle monitor
8F34CZ	remove ankle monitor-Google Search
8JDFPT	remove ankle monitor
8JXTWE	remove ankle monitor
8VQFKZ	Remove Ankle monitor
9MCRLT	remove ankle monitor
9VQVED	remove ankle monitor
AGMPY9	remove ankle monitor
AKNRPA	remove ankle monitor
BHAT4Y	remove ankle monitor
BNZ3DX	remove ankle monitor
C6EZRU	remove ankle monitor
CERU9G	remove ankle monitor
CKT9RX	remove ankle monitor
CZNJJA	remove ankle monitor
DNUPM7	remove ankle monitor
DQZW7Y	Remove Ankle Monitor
DT3X7V	remove ankle monitor

TABLE 1

Question 20 - Examination Questions	
WebCode	**Response**
DYD4P9	remove ankle monitor
E7PH86	remove ankle monitor
FLWZEV	remove ankle monitor
G8C3KE	remove ankle monitor
GPDMNU	remove ankle monitor
GQPFJW	remove ankle monitor
GYF3AR	remove ankle monitor
HGFG4R	Remove ankle monitor
JCC299	remove ankle monitor
JEJH6J	remove ankle monitor
JL3MGR	remove ankle monitor
KVP67K	remove ankle monitor
L6PWCQ	remove ankle monitor
MFJPZ8	"remove ankle monitor"
MXKEER	remove ankle monitor
N634TR	remove ankle monitor
NE7FKF	remove ankle monitor
NEP2GC	Remove ankle monitor
NP67AT	remove ankle monitor
NT6H7T	remove ankle monitor
NZNRBG	remove ankle monitor
P77HBH	remove ankle monitor
P9Y9K3	remove ankle monitor
QLFNYL	remove ankle monitor
QM9E98	remove ankle monitor
R748U6	remove ankle monitor
T8BAT9	Remote ankle monitor
T9LU2H	remove ankle monitor
TPPKJE	remove ankle monitor
TYEAHM	remove ankle monitor
U7V8LZ	remove ankle monitor
V7R6A2	NOT WITHIN LABORATORY'S SCOPE

TABLE 1

Question 20 - Examination Questions	
WebCode	**Response**
VDB8G4	remove ankle monitor
VG9PVJ	remove ankle monitor
VJEAGX	remove ankle monitor
VLPWFC	remove ankle monitor
VP3UPK	remove ankle monitor
WVNBEF	remove ankle monitor
ZEAZKD	remove ankle monitor - Google Search
ZGVLBE	remove ankle monitor - Google Search
ZKXMCC	remove ankle monitor

Question 20: What did the user search in the Safari web browser, 6/24/2022 12:05:18 PM(UTC-4)?

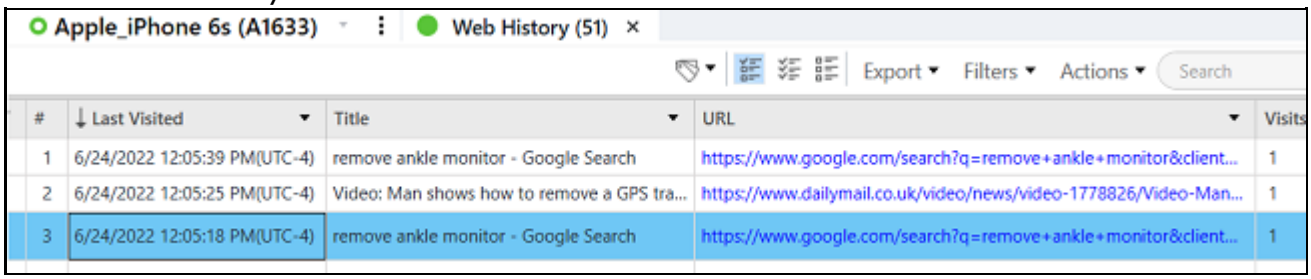
Consensus Result: remove ankle monitor

Expected Response Explanation:

A review of the browser history for the Safari web browser finds records of web searches for "remove ankle monitor" on 6/24/2022 12:05:18 PM(UTC-4).

Expected Response Illustration:

Cellebrite Web History Table



Safari History.db

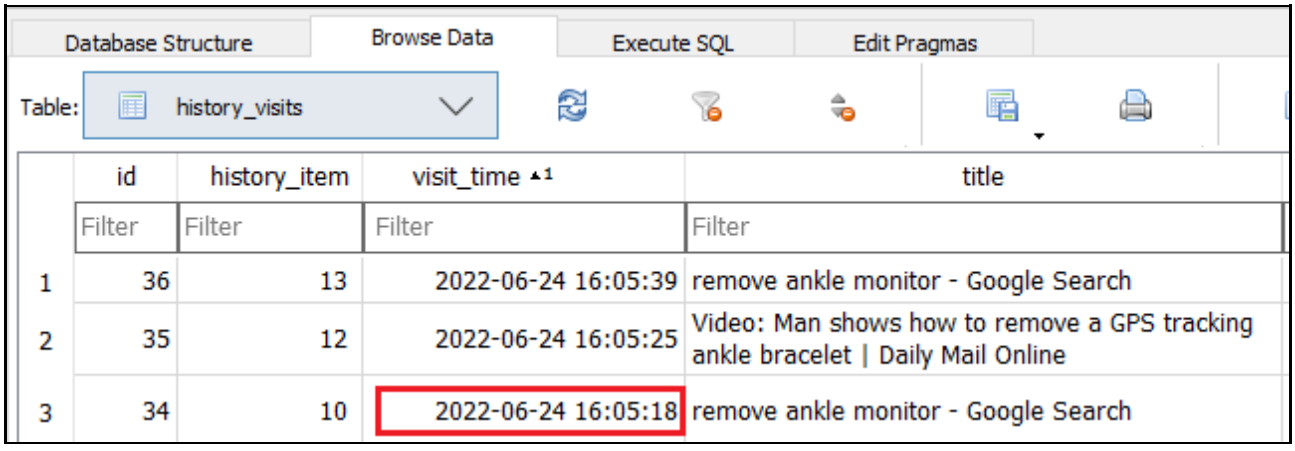


TABLE 1

Question 21 - Examination Questions

Question 21: According to the data for the Home Depot app, for what item did the user have a saved search?

Manufacturer's Expected Response: bolt cutters

WebCode	Response
2JFUWZ	bolt cutters
2YAJPB	bolt cutters0
3329MU	bolt
3R3DPY	bolt cutters
4FPB42	Old Car Horn.m4r – Audio file
66P4MA	bolt cutters
6ERKDC	soldering
6M83T7	Alwington Blvd, 267, Fauquier County, Warrenton, 20186, Virginia, United States
6QMVJY	bolt cutters
7CKLGB	Bolt Cutters
7ND6X2	Bolt Cutters
7W8BQ3	com.thehomedepot.homedepot – "bolt"
7WQWJT	bolt cutters
8F34CZ	Bolt Cutters
8JDFPT	bolt cutters
8JXTWE	bolt cutters Recovered within the HomeDepot application associated database THDConsumer.sqlite
8VQFKZ	Bolt cutters
9MCRLT	Bolt cutters
9VQVED	bolt cutters
AGMPY9	bolt cutters
AKNRPA	bolt cutters
BHAT4Y	Pliers (tongs)
BNZ3DX	Bolt Cutters
C6EZRU	bolt cutters
CERU9G	bolt cutters
CKT9RX	Bolt Cutters
CZNJJA	bolt cutters
DNUPM7	bolt cutters
DQZW7Y	Bolt cuters

TABLE 1

Question 21 - Examination Questions	
WebCode	**Response**
DT3X7V	bolt cutters
DYD4P9	bolt cutters
E7PH86	bolt cutters
FLWZEV	The bolt cutter
G8C3KE	bolt cutters
GPDMNU	bolt cutters
GQPFJW	Bolt Cutters
GYF3AR	cart activity
HGFG4R	Boltcutters
JCC299	bolt cutters
JEJH6J	bolt cutters
JL3MGR	bolt cutters
KVP67K	bolt cutters
L6PWCQ	Bolt cutters
MFJPZ8	bolt cutters
MXKEER	bolt cutters
N634TR	bolt cutters
NE7FKF	bolt cutters
NEP2GC	Bolt cutters
NP67AT	bolt cutters
NT6H7T	bolt cutters
NZNRBG	bolt cutters
P77HBH	bolt cutters
P9Y9K3	bolt cutters
QLFNYL	bolt cutters0
QM9E98	Alwington Blvd, 267, Fauquier County, Warrenton, 20186, Virginia, United States
R748U6	bolt cutters
T8BAT9	Bolt Cutters
T9LU2H	Bolt cutters (saved in the cart)
TPPKJE	bolt cutters
TYEAHM	bolt cutters
U7V8LZ	bolt cutters

TABLE 1

Question 21 - Examination Questions	
WebCode	**Response**
V7R6A2	NOT WITHIN LABORATORY'S SCOPEV
VDB8G4	Bolt Cutters
VG9PVJ	bolt cutters
VJEAGX	bolt%20
VLPWFC	bolt-cutter
VP3UPK	bolt cutters
WVNBEF	bolt cutters
ZEAZKD	bolt cutters
ZGVLBE	Bolt Cutters
ZKXMCC	bolt cutters

Question 21: According to the data for the Home Depot app, for what item did the user have a saved search?

Consensus Result: bolt cutters

Expected Response Explanation:

User data for the Home Depot application is stored in /private/var/mobile/Containers/Data/Application/A9904EAF-BF51-459E-90F9-FAAA37926FC4/Library/Preferences/. Contained within this directory in com.thehomedepot.homedepot.plist are saved searches.

Expected Response Illustration:

com.thehomedepot.homedepot.plist

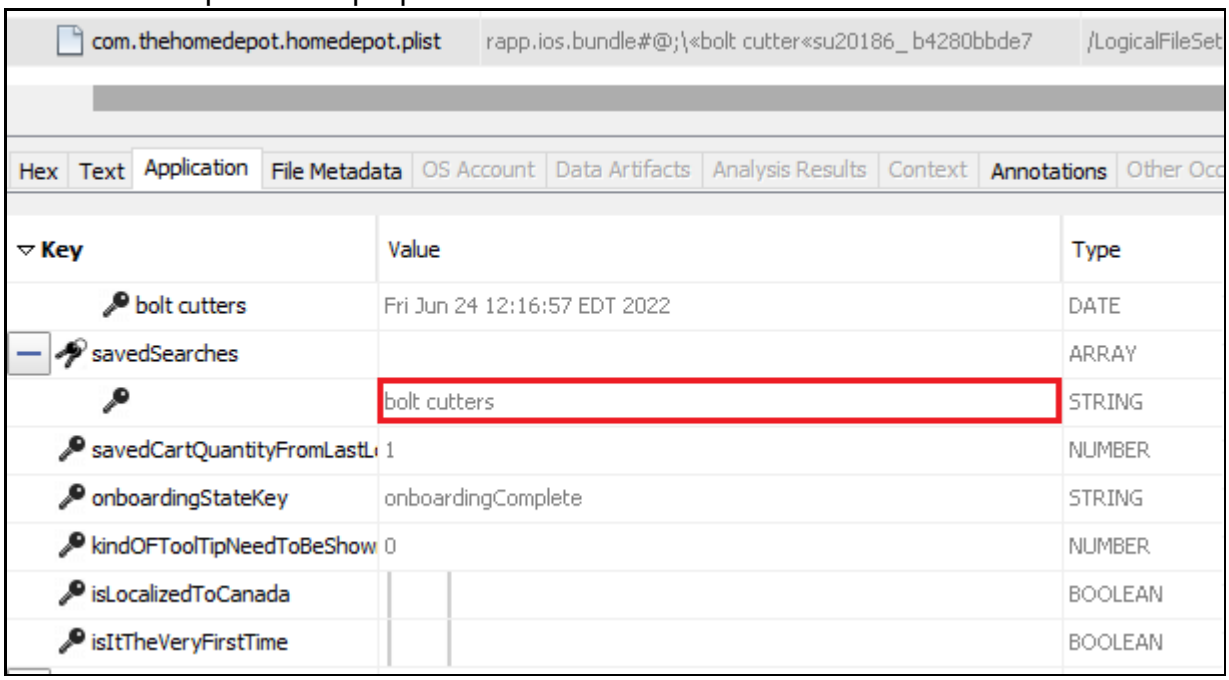


TABLE 1

Question 21 - Examination Questions

com.thehomedepot.homedepot.plist

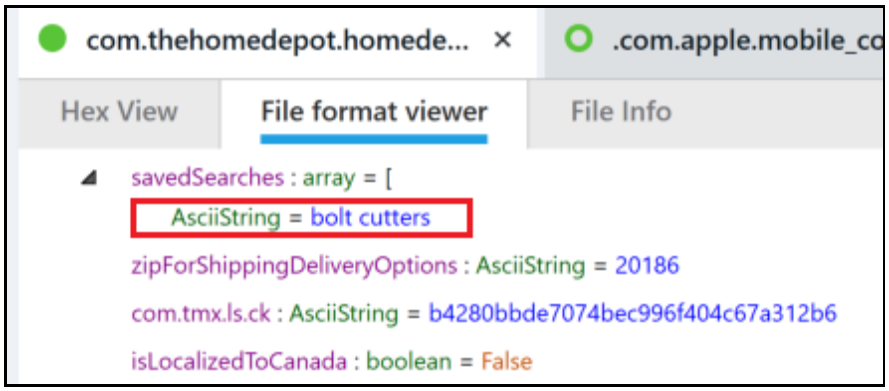


TABLE 1

Question 22 - Examination Questions

Question 22: Describe the type and content of the file with MD5 hash efa6da222aca7bbcc12fcf8c79414844.

Manufacturer's Expected Response: Audio file of a ringing phone and variations representing the same information

WebCode	Response
2JFUWZ	an old phone rings
2YAJPB	It is a .m4r audio file of a phone ringing.
3329MU	This is an audio file which contains the sound of a telephone ringer.
3R3DPY	ISO Media, Apple iTunes ALAC/AAC-LC (.M4A) Audio, the sound is an old phone ringing two times and the audio is 11 seconds long.
4FPB42	ringtone named “Old Phone.m4r”
66P4MA	audio, Ringtones
6ERKDC	Type : Audio, Content : Old Phone.m4r (Ringtone)
6M83T7	Old Phone.m4r
6QMVJY	audio file of phone ringing
7CKLGB	The file is named Old Phone.m4r, this is an audio file which appears to be a ringtone for the iPhone.
7ND6X2	Phone ringing
7W8BQ3	Phone Ringtone – named ‘Old Phone.m4r’ – 11 seconds
7WQWJT	The file type is an audio file (.m4r). It sounds like a ringing phone.
8F34CZ	An M4r file type with the file name old phone. Its is a ringtone.
8JDFPT	M4R audio file (a ringtone)
8JXTWE	This file is a M4A audio file, renamed to the file extension M4R. It is a ringtone file with the file name Old Phone.m4r and contains an audio clip of a classic telephone ringing
8VQFKZ	Audio - Ringtone Old Phone.m4r - an M4r file is associated with iPhone ringtone files and that an analogue type phone can be heard ringing when played
9MCRLT	The Old Phone.m4r file is a ringtone that sounds like an old telephone ringing.
9VQVED	The file that goes with the provided hash was an audio file titled, "Old Phone.m4r". When played back, it sounds like a phone ringing.
AGMPY9	Audio file of a phone ringing, “old phone.m4r”
AKNRPA	audio file titled Old Phone.m4r that plays the sound of a telephone ringing twice
BHAT4Y	Audio file, Phone Ringtone
BNZ3DX	This is an audio file which would appear to be a ringtone for this iPhone. The file is titled "Old Phone.m4r"
C6EZRU	an audio file of an old ring tone
CERU9G	Ringtone of an old phone ringing 2 times, file type is m4r.
CKT9RX	Not within laboratory's scope.
CZNJJA	Audio file: Old Phone.m4r. Content is audio of a phone ringing.

TABLE 1

Question 22 - Examination Questions	
WebCode	**Response**
DNUPM7	.m4r audio file of a old phone ringtone
DQZW7Y	Old Phone.m4r Ringtone
DT3X7V	Type: Ringtone. Audio Content: 'Old Phone' Ring Ring. 00:11 Second Long m4r file
DYD4P9	Type=Audio with file extension labeled = Old Phone.m4r | Content = heard a telephone ring.
E7PH86	It's an .m4r audio file ring tone sounding like the bells of an old telephone.
FLWZEV	This file is audio file. File name is Old phone.m4r.
G8C3KE	The file is a M4R format audio file of an old ringtone
GPDMNU	Old Phone.m4r- Audio File - Ringtone
GQPFJW	"Old Phone.m4r" file with retro style ringtone
GYF3AR	Audio File(M4A type) (its saved location is /Library/Ringtones) (its name is Old Phone.m4r)
HGFG4R	Audio file
JCC299	M4A (MPEG-4 [MP4]) audio file containing audio recording of classic (old) telephone ringer
JEJH6J	.m4r file; audio file that sounds like an old telephone
JL3MGR	Type: Sound Content: Ringtone
KVP67K	Type: Audio Name: Old Phone.m4r Ringtones/Old Phone.m4r
L6PWCQ	The file is ".m4r" and consists of audio for a ringtone
MFJPZ8	The name of the file is 'Old Phone.m4r'. It is an audio file containing the sound of a phone ringing. It is used as a ringtone.
MXKEER	The file is "Old Phone.m4r" and it is a ringtone and its sounds are of a telephone ringing twice
N634TR	File type: m4r Content: Ringtone
NE7FKF	Ringtone audio file of a phone ringing
NEP2GC	Type: Sound file [Old Phone.m4r]. It's a phone ring.
NP67AT	M4R iPhone ringtone file containing M4A audio of a phone ringing
NT6H7T	.m4r audio file (iPhone ringtone file), contains the sound of a telephone ringing twice
NZNRBG	Old ringtone (old Phone.m4r)
P77HBH	Ringtone Old Phone.m4r
P9Y9K3	Audio two telephone rings
QLFNYL	Ringtone named "Old Phone.m4r" - This sound is that of a regular phone call ring
QM9E98	Old Phone.m4r is a ring tone of the old telephone ring sound.
R748U6	Old Phone.m4r audio file. It's an audio file that sounds like an old telephone ringing.
T8BAT9	Audio file : ring tone of old phone
T9LU2H	Old Phone.m4r: an audio file of an old phone ringing
TPPKJE	Audio file named Old Phone.m4r. Contained the sound of a phone ringing/ring tone.

TABLE 1

Question 22 - Examination Questions	
WebCode	**Response**
TYEAHM	Audio file Old Phone.m4r
U7V8LZ	It is an audio file of the old phone ringtone. File name: Old Phone.m4r
V7R6A2	NOT WITHIN LABORATORY'S SCOPE
VDB8G4	.m4r Audio File "Old Phone.m4r" a ring tone in the style of a traditional ringing bell.
VG9PVJ	Old Phone.m4r - iPhone ringtone file – this is a ringtone file that can be set on the device.
VJEAGX	.m4r file - content is the sound of a phone ringing
VLPWFC	File name: Old Phone.m4r Type: sound Content: phone ring
VP3UPK	Old Phone.m4r - It is an audio file of a telephone ring sound clip
WVNBEF	Audio file .m4r named "Old Phone" found within the ringtones folder. Sounds like a phone ringing.
ZEAZKD	A ringtone file. ftyp (hex: 66 74 79 70) at offset 4, which defines QuickTime Container File Type. File sub-type is M4A_ (hex: 4D 34 41 20) which points to M4A file type. the content of the file is an old phone ringing sound file.
ZGVLBE	Audio File - Old Phone.m4r
ZKXMCC	Old Phone.m4r - Audio File - Ringtone

Question 22: Describe the type and content of the file with MD5 hash efa6da222aca7bbcc12fcf8c79414844.

Consensus Result: Audio file of a ringing phone and variations representing the same information

Expected Response Explanation:

Searching the data for a file with the noted MD5 hash discovers /root/Library/Ringtones/Old Phone.m4r, an audio file of a ringing phone .

Expected Response Illustration:

Old Phone.m4r

TABLE 1

Question 23 - Examination Questions

Question 23: According to the voicemail message received on June 25, 2022, what does Casey owe the caller?

Manufacturer's Expected Response: a hundred bucks ($100) and variations representing the same information

WebCode	Response
2JFUWZ	100$
2YAJPB	100 bucks
3329MU	100 bucks
3R3DPY	According to the voicemail, Casey owes the caller 100 bucks.
4FPB42	15094528541
66P4MA	100bucks
6ERKDC	100 bucks / USD100
6M83T7	a hundred bucks
6QMVJY	$100
7CKLGB	Casey owes Bev “100 bucks”
7ND6X2	$100
7W8BQ3	£100 bucks
7WQWJT	“100 bucks”
8F34CZ	$100
8JDFPT	"A hundred bucks"
8JXTWE	Casey owes the caller “one hundred bucks”
8VQFKZ	100 bucks
9MCRLT	100 bucks
9VQVED	According to the voicemail, Casey owes the caller a hundred bucks ($100).
AGMPY9	$100
AKNRPA	$100
BHAT4Y	100 USD
BNZ3DX	Casey owes Bev “$100 bucks”
C6EZRU	"100 bucks"
CERU9G	100 bucks
CKT9RX	100 bucks
CZNJJA	$100
DNUPM7	$100
DQZW7Y	efa6da222aca7bbcc12fcf8c79414844

TABLE 1

Question 23 - Examination Questions	
WebCode	**Response**
DT3X7V	100 bucks
DYD4P9	100 bucks
E7PH86	100 bucks
FLWZEV	100 USD
G8C3KE	100 bucks
GPDMNU	One Hundred Bucks
GQPFJW	"$100 bucks"
GYF3AR	100 bucks(dollars)
HGFG4R	100 bucks
JCC299	one hundred bucks
JEJH6J	$100
JL3MGR	a hundred bucks
KVP67K	$100 Bucks
L6PWCQ	$100.00
MFJPZ8	$100
MXKEER	100 bucks
N634TR	100 bucks
NE7FKF	One Hundred Bucks
NEP2GC	One hundred bucks
NP67AT	a hundred bucks
NT6H7T	$100 (a hundred bucks)
NZNRBG	One hundred bucks
P77HBH	100 bucks
P9Y9K3	100 bucks
QLFNYL	"100 bucks"
QM9E98	$100
R748U6	Casey owes the caller 100 bucks.
T8BAT9	$100 bucks
T9LU2H	Casey owes the called $100.00
TPPKJE	100 bucks
TYEAHM	A Hundred Bucks
U7V8LZ	100 bucks

TABLE 1

Question 23 - Examination Questions	
WebCode	**Response**
V7R6A2	NOT WITHIN LABORATORY'S SCOPE
VDB8G4	100 Bucks
VG9PVJ	100 bucks
VJEAGX	100 bucks
VLPWFC	100 bucks
VP3UPK	$100 "hundred bucks"
WVNBEF	"100 bucks"
ZEAZKD	100 bucks
ZGVLBE	100 Bucks
ZKXMCC	One Hundred Bucks

Question 23: According to the voicemail message received on June 25, 2022, what does Casey owe the caller?

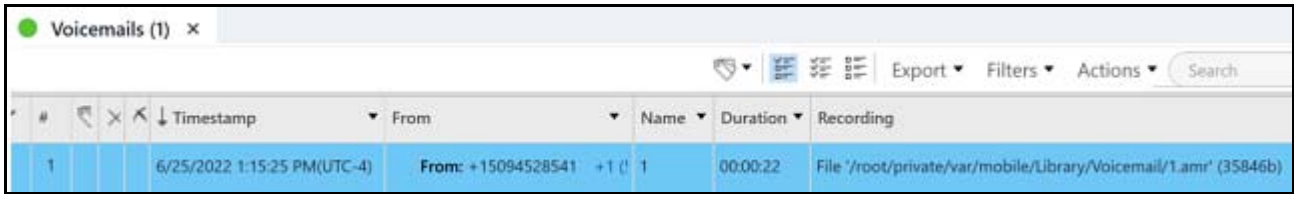
Consensus Result: a hundred bucks ($100) and variations representing the same information

Expected Response Explanation:

Voicemails are stored in /private/var/mobile/Library/Voicemail/. Reviewing the created dates of the files, or /private/var/mobile/Library/Voicemail/voicemail.db shows one message received on June 25th, 1.amr. The content can be heard by playing the amr file with any compatible media player.

Expected Response Illustration:

Cellebrite Voicemail Table



1.amr (1.transcript)

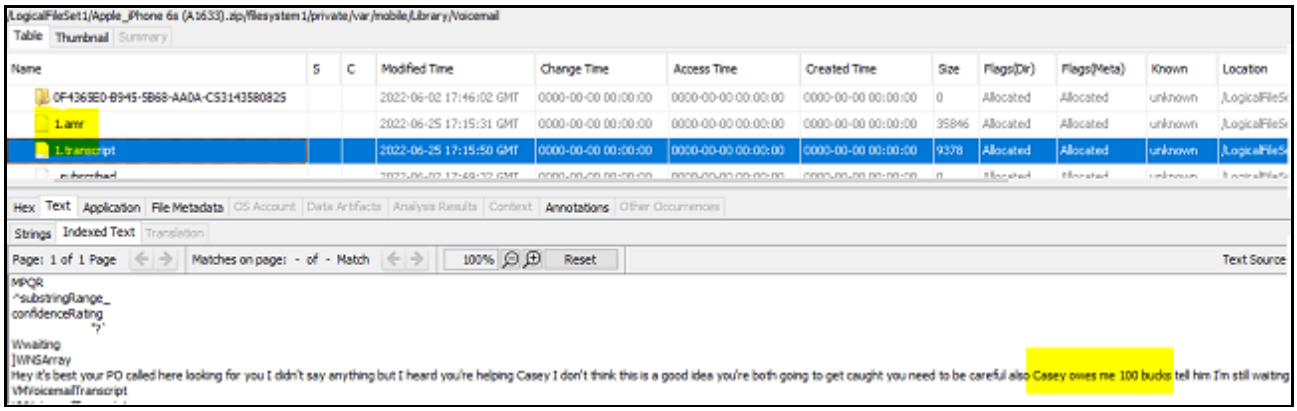


TABLE 1

Question 24 - Examination Questions

Question 24: Provide the GPS Position coordinates for IMG_0082.JPG in the format ##.##### (Indicate directionality as N or S), ##.##### (Indicate directionality as E or W).

Manufacturer's Expected Response: 43.50906 N, 16.47451 E

WebCode	Response
2JFUWZ	(43.509063 N, 16.474516 E)
2YAJPB	43.50906 N, 16.47451 E
3329MU	43.509063 N, 16.474516 E
3R3DPY	N 43.509063, E 16.474516
4FPB42	(43.509063, 16.474516) - Kroz Smrdečac 41, 21000 Split, Croatia
66P4MA	43.5090N, 16.4745E
6ERKDC	43.509063, 16.474516
6M83T7	43.509063 N, 16.474516 E
6QMVJY	43.509063 N, 16.474516 E
7CKLGB	43.509063 North 16.474516 East
7ND6X2	N43.509063, E16.474516
7W8BQ3	43.509063 / 16.474516
7WQWJT	43.50906 N / 16.47451 E
8F34CZ	N43.509063, E16.474516
8JDFPT	N 43.509063, E 16.474516
8JXTWE	(43.50906 N, 16.47451 E)
8VQFKZ	43.509063 N / 16.474516 E
9MCRLT	43.50906 (N), 16.47451 (E)
9VQVED	43.50906 N, 16.47451 E
AGMPY9	43.50906 N, 16.47452 E
AKNRPA	43.509063 N, 16.474516 E
BHAT4Y	43.509063, 16.474516
BNZ3DX	N43.509063, E16.474516
C6EZRU	N 43.509063 E 16.474516
CERU9G	N 43.509063, S 16.474516
CKT9RX	43.5091 N, 16.4745 E
CZNJJA	43.509063 N, 16.474516 E
DNUPM7	43.50906 N, 16.47452 E
DQZW7Y	(43.509063 N, 16.474516 E)

TABLE 1

Question 24 - Examination Questions	
WebCode	**Response**
DT3X7V	Lat/ Lon: 43.509063 N / 16.474516 E (In the format ##.#####: 43.50906 N / 16.47457 E)
DYD4P9	43.50906 (N), 16.47451 (E)
E7PH86	(43.50906 N) (16.47451 E)
FLWZEV	N 43.509064, E 16.474517
G8C3KE	43.509063 N, 16.474516 E
GPDMNU	43.509063 (N) , 16.474516 (E)
GQPFJW	43.509063 N 16.474516 E
GYF3AR	43.509063 N / 16.474516 E
HGFG4R	43.509063, 16.474516
JCC299	N 43.50906 E 16.47452
JEJH6J	43.303263 N, 16.282826 E
JL3MGR	43.509063 N / 16.474516 E
KVP67K	43.5090 N / 16.4745 E
L6PWCQ	43.509063 N, 16.474516 E
MFJPZ8	43.509063 N, 16.474516 E
MXKEER	43.509063 (N), 16.474516 (E)
N634TR	N:43.509063 E:16.474516
NE7FKF	(43.509063 N, 16.474516 E)
NEP2GC	43.509063 N / 16.474516 E
NP67AT	43.50906 N, 16.47451 E
NT6H7T	43.50906 N, 16.47451 E
NZNRBG	43.509063 N 16.474516 E
P77HBH	(43.509063, 16.474516)
P9Y9K3	43.50906 N, 16.47452 E
QLFNYL	43.50906 N, 16.47451 E
QM9E98	32.63 N, 28.26 E
R748U6	43.50906 N, 16.47451 E
T8BAT9	N (Lat): 43.50906333 E (Long): 16.47451667
T9LU2H	43.509063 North, 16.474516 East
TPPKJE	(43.509063, 16.474516)
TYEAHM	N43,30,32.63 E16,28,28.26
U7V8LZ	43.509063 N, 16.474516 E

TABLE 1

Question 24 - Examination Questions	
WebCode	**Response**
V7R6A2	NOT WITHIN LABORATORY'S SCOPE
VDB8G4	43.509063 N / 16.474516 E
VG9PVJ	43.509063N, 16.474516E
VJEAGX	43.509063 N, 16.474516 E
VLPWFC	N 43.509063, E 16.474516
VP3UPK	43.509063N, 16.474516E
WVNBEF	43.509063N, 16.474516E
ZEAZKD	43.5091 N, 16.4745 E
ZGVLBE	43.509063, 16.474516
ZKXMCC	43.509063 (N) , 16.474516 (E)

Question 24: Provide the GPS Position coordinates for IMG_0082.JPG in the format ##.##### (Indicate directionality as N or S), ##.##### (Indicate directionality as E or W).

Consensus Result: 43.50906 N, 16.47451 E and variations representing the same information

Expected Response Explanation:

When enabled, GPS Position (fix) information is embedded as EXIF data in photographs taken with the iPhone. This data can be extracted and parsed with any reliable tool.

Expected Response Illustration:

exiftool parse of EXIF data from IMG_0082

```
> .\exiftool.exe -c '%.6f' -GPSPosition .\IMG_0082.JPG
GPS Position                    : 43.509064 N, 16.474517 E
```

Cellebrite view of IMG_0082

TABLE 1

Question 24 - Examination Questions

Name:	IMG_0082.JPG
Type:	Images
Size (bytes):	1633197
Path:	DarArchive/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0082.JPG
Created:	6/10/2022 4:30:54 AM(UTC-4)
Accessed:	6/10/2022 4:30:55 AM(UTC-4)
Modified:	6/10/2022 4:30:55 AM(UTC-4)
Changed:	6/10/2022 4:31:03 AM(UTC-4)
Deleted:	
Extraction:	File System
MD5:	4f49adc52c5a283c6ead6ff8935cbe5e
Source file:	IMG_0082.JPG

Metadata

Camera Make:	Apple
Camera Model:	iPhone 6s
Capture Time:	6/10/2022 10:30:55 AM
Pixel resolution:	4032x3024
Resolution:	72x72 (Unit: Inch)
Orientation:	Horizontal (normal)
Lat/Lon:	43.509063 / 16.474516

Map

Position:	(43.509063, 16.474516)
Address:	
Map Address:	

Cellebrite info pane for the photo

IMG_0082.JPG ×

Hex View | Image view | File Info

Find:

General	
User ID	501
Group ID	501
File size	1633197 Bytes
Chunks	1
iOS classifications	plant : 33.07%, outdo...
Offsets	
Data offset	0x0
Date & Time	
Creation time	6/10/2022 4:30:54 A...
Modify time	6/10/2022 4:30:55 A...
Last access time	6/10/2022 4:30:55 A...
Deleted time	
Change time	6/10/2022 4:31:03 A...
EXIF	
GPSLatitudeRef	N
GPSLatitude	43, 30, 32.63
GPSLongitudeRef	E
GPSLongitude	16, 28, 28.26
GPSAltitudeRef	0
GPSAltitude	67.303832969772515

TABLE 1

Question 25 - Examination Questions

Question 25: With what application did the user receive an image of a New York birth certificate?

Manufacturer's Expected Response: Telegram

WebCode	Response
2JFUWZ	Telegram
2YAJPB	Telegram
3329MU	Telegram
3R3DPY	Telegram
4FPB42	Telegram
66P4MA	Telegram Messenger
6ERKDC	Telegram
6M83T7	telegram
6QMVJY	Telegram
7CKLGB	Telegram
7ND6X2	Telegram
7W8BQ3	Telegram
7WQWJT	Telegram
8F34CZ	Telegram
8JDFPT	Telegram
8JXTWE	Application: Telegram , from user: 10250010690
8VQFKZ	Telegram
9MCRLT	Telegram
9VQVED	Telegram Messenger
AGMPY9	Telegram
AKNRPA	Telegram
BHAT4Y	Telegram app
BNZ3DX	Telegram
C6EZRU	Telegram
CERU9G	Telegram
CKT9RX	Telegram
CZNJJA	Telegram
DNUPM7	Telegram
DQZW7Y	Telegram
DT3X7V	Telegram

TABLE 1

Question 25 - Examination Questions	
WebCode	**Response**
DYD4P9	Telegram
E7PH86	Telegram
FLWZEV	Telegram
G8C3KE	Telegram
GPDMNU	Telegram
GQPFJW	Telegram
GYF3AR	Telegram
HGFG4R	Telegram
JCC299	Telegram
JEJH6J	Telegram
JL3MGR	Telegram
KVP67K	Telegram
L6PWCQ	Telegram
MFJPZ8	Telegram
MXKEER	Telegram
N634TR	Telegram
NE7FKF	Telegram
NEP2GC	Telegram
NP67AT	Telegram Messenger
NT6H7T	Telegram
NZNRBG	telegram
P77HBH	Telegram
P9Y9K3	Telegram
QLFNYL	Telegram messaging app
QM9E98	Telegram
R748U6	Telegram
T8BAT9	Telegram
T9LU2H	Telegram Messenger
TPPKJE	telegram
TYEAHM	Telegram
U7V8LZ	Telegram
V7R6A2	NOT WITHIN LABORATORY'S SCOPE

TABLE 1

Question 25 - Examination Questions	
WebCode	**Response**
VDB8G4	Telegram
VG9PVJ	Telegram
VJEAGX	Telegram
VLPWFC	Telegram Messenger
VP3UPK	Telegram
WVNBEF	Telegram
ZEAZKD	Telegram
ZGVLBE	Telegram
ZKXMCC	Telegram

Question 25: With what application did the user receive an image of a New York birth certificate?

Consensus Result: Telegram

Expected Response Explanation:

Reviewing the images on the phone, discovers one image of a (redacted) NY birth certificate, telegram-cloud-photo-size-1-5019349728911010616-y_partial, in /root/private/var/mobile/Containers/Shared/AppGroup/ECD179FF-45F8-4C69-BBDC-E5E9F4DEF40C/telegram-data/account-2292819133321558358/postbox/media/

TABLE 1

Question 25 - Examination Questions

Expected Response Illustration:

telegram-cloud-photo-size-1-5019349728911010616-y_partial

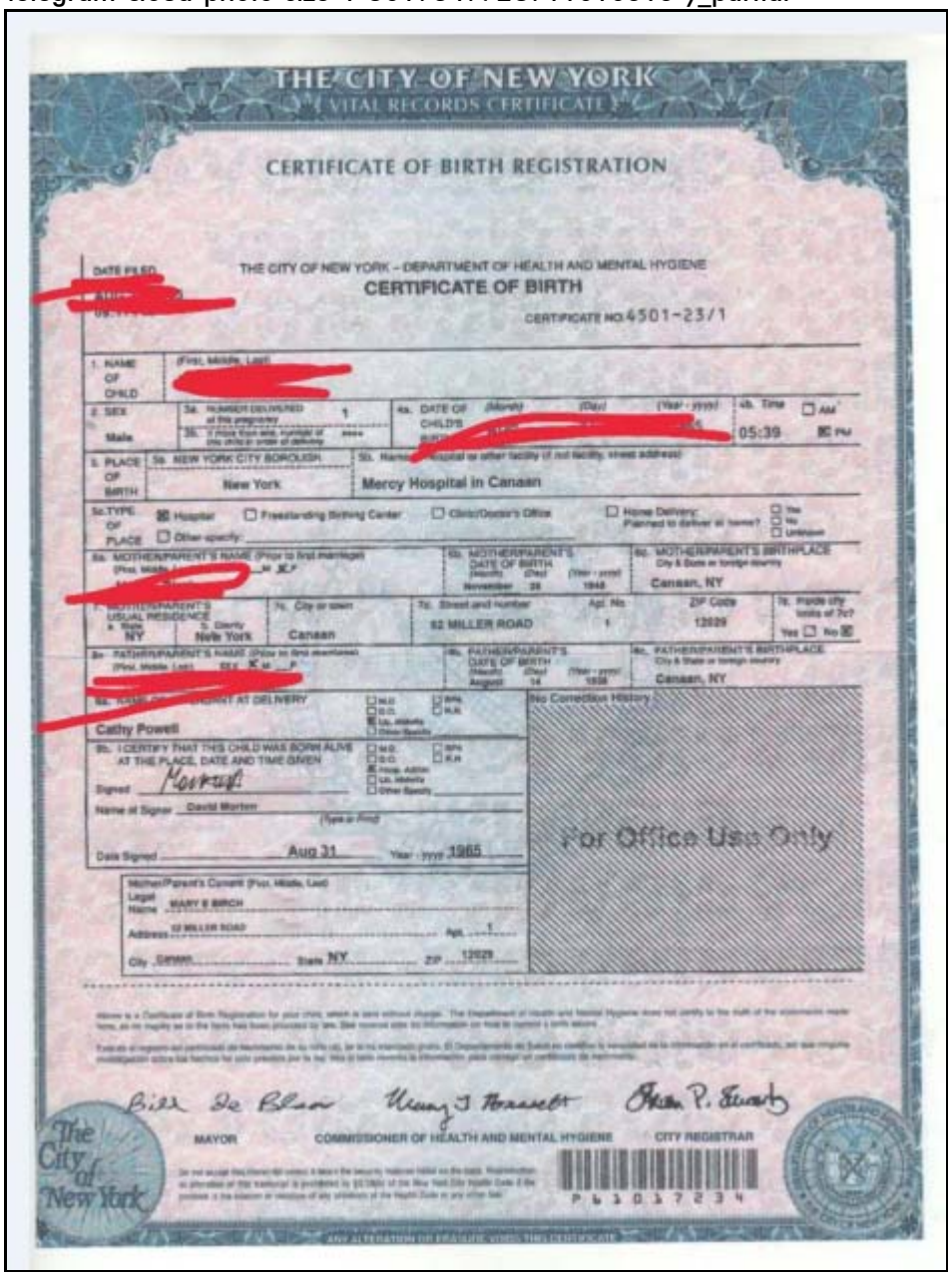


TABLE 1

Question 26 - Examination Questions

Question 26: Who did the phone user communicate with using Signal Private Messenger?

Manufacturer's Expected Response: frank grey

WebCode	Response
2JFUWZ	frank grey +15713077268
2YAJPB	frank grey
3329MU	Frank
3R3DPY	frank grey
4FPB42	frank grey
66P4MA	frank grey
6ERKDC	frank +15713077268
6M83T7	frank grey
6QMVJY	frank grey
7CKLGB	Name: Frank Grey Number:15713077268
7ND6X2	frank grey
7W8BQ3	Frank Grey, +15713077268
7WQWJT	frank grey
8F34CZ	+15713077268 Frank grey
8JDFPT	Frank Grey
8JXTWE	frank grey
8VQFKZ	Frank Grey
9MCRLT	Frank Grey
9VQVED	Frank Grey
AGMPY9	frank grey
AKNRPA	frank grey
BHAT4Y	frank grey
BNZ3DX	Name: Frank Grey , Number:15713077268
C6EZRU	frank grey
CERU9G	frank
CKT9RX	frank grey
CZNJJA	frank grey
DNUPM7	frank grey
DQZW7Y	frank gray
DT3X7V	frank grey (+15713077268)

TABLE 1

Question 26 - Examination Questions	
WebCode	**Response**
DYD4P9	frank
E7PH86	frank grey
FLWZEV	Vivian
G8C3KE	frank grey
GPDMNU	frank grey, +15713077268
GQPFJW	frank grey
GYF3AR	Frank Grey
HGFG4R	Frank Grey
JCC299	frank grey
JEJH6J	frank grey
JL3MGR	frank grey
KVP67K	frank grey
L6PWCQ	frank grey
MFJPZ8	Frank Grey
MXKEER	frank grey
N634TR	Frank Grey +15713077268
NE7FKF	Frank Grey
NEP2GC	Frank Grey
NP67AT	frank grey
NT6H7T	frank grey
NZNRBG	frank grey +15713077268
P77HBH	frank grey
P9Y9K3	frank grey
QLFNYL	+15713077268 - frank grey
QM9E98	frank grey
R748U6	frank grey
T8BAT9	Frank Gray +15713077268
T9LU2H	frank grey
TPPKJE	sissy
TYEAHM	Frank Grey +15713077268
U7V8LZ	frank grey 15713077268
V7R6A2	NOT WITHIN LABORATORY'S SCOPE

TABLE 1

Question 26 - Examination Questions	
WebCode	**Response**
VDB8G4	frank +15713077268
VG9PVJ	+15713077268 frank grey
VJEAGX	frank grey
VLPWFC	frank grey
VP3UPK	Frank grey (+15713077268)
WVNBEF	frank grey
ZEAZKD	Frank Grey
ZGVLBE	frank grey
ZKXMCC	frank grey, +15713077268

Question 26: Who did the phone user communicate with using Signal Private Messenger?

Consensus Result: frank grey

Expected Response Explanation:

Using a forensic tool that supports decryption of Signal app data, the messages can be read. There is only one Signal conversation on the phone.

Expected Response Illustration:

/root/private/var/mobile/Containers/Shared/AppGroup/F9080574-5F7F-405D-84D3-578DED3B697E/grdb/signal.sqlite [decrypted]

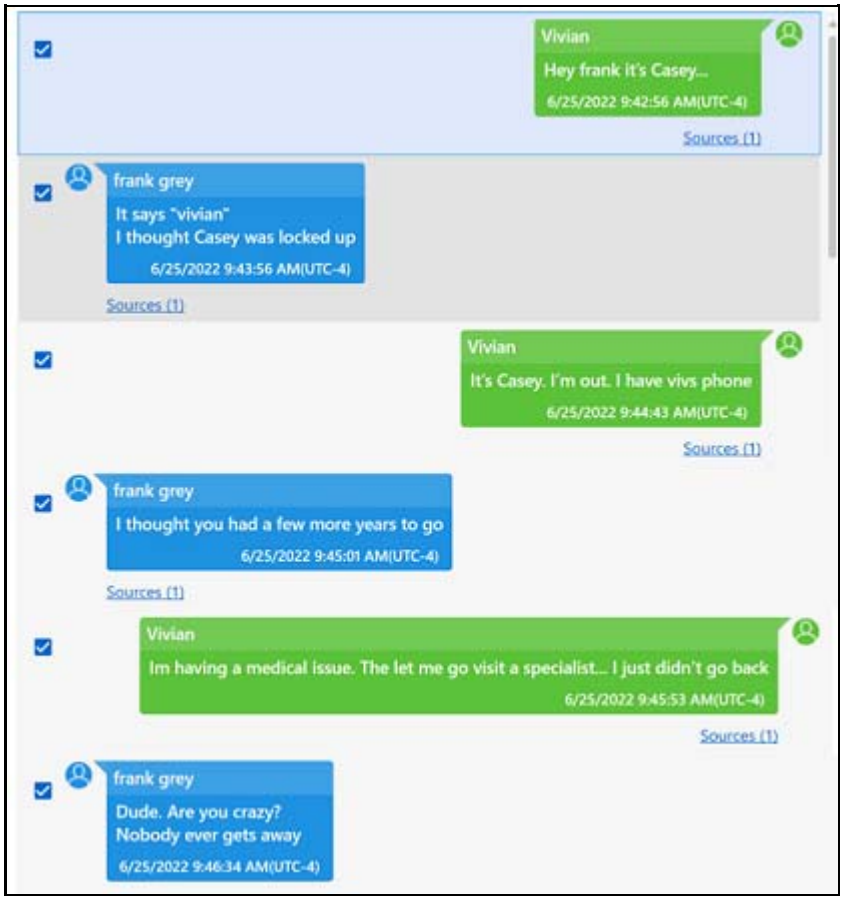


TABLE 1

Question 27 - Examination Questions

Question 27: Which contact has the phone number +44 1482 466581? Provide the name of contact.

Manufacturer's Expected Response: Phil Lark

WebCode	Response
2JFUWZ	Phil Lark
2YAJPB	Phil Lark
3329MU	Phil Lark
3R3DPY	Phil Lark
4FPB42	Phil Lark
66P4MA	Phil Lark
6ERKDC	Phil Lark
6M83T7	Phil Lark
6QMVJY	Phil Lark
7CKLGB	Phil Lark
7ND6X2	Phil Lark
7W8BQ3	Phil Lark, +44 1482 466581
7WQWJT	Phil Lark
8F34CZ	Phil Lark
8JDFPT	Phil Lark
8JXTWE	Phil Lark
8VQFKZ	Phil Lark
9MCRLT	Phil Lark
9VQVED	Phil Lark
AGMPY9	Phil Lark
AKNRPA	Phil Lark
BHAT4Y	Name: +44 1482 466581
BNZ3DX	Phil Lark
C6EZRU	Phil Lark
CERU9G	Phil Lark
CKT9RX	Phil Lark
CZNJJA	Phil Lark
DNUPM7	Phil Lark
DQZW7Y	Phil Lark
DT3X7V	Phil Lark

TABLE 1

Question 27 - Examination Questions	
WebCode	**Response**
DYD4P9	Phil Lark
E7PH86	Phil Lark
FLWZEV	Phil Lark
G8C3KE	Phil Lark
GPDMNU	Phil Lark
GQPFJW	Phil Lark
GYF3AR	LarkPhil
HGFG4R	Phil Larkin
JCC299	Phil Lark
JEJH6J	Phil Lark
JL3MGR	Phil Lark
KVP67K	Phil Lark
L6PWCQ	Phil Lark
MFJPZ8	Phil Lark
MXKEER	Phil Lark
N634TR	Phil Lark
NE7FKF	Phil Lark
NEP2GC	Phil Lark
NP67AT	Phil Lark
NT6H7T	Phil Lark
NZNRBG	Phil Lark
P77HBH	Phil Lark
P9Y9K3	+44 1482 466581
QLFNYL	Phil Lark
QM9E98	Phil Lark
R748U6	Phil Lark
T8BAT9	Phil Lark
T9LU2H	Phil Lark
TPPKJE	Phil Lark
TYEAHM	Phil Lark
U7V8LZ	Phil Lark
V7R6A2	NOT WITHIN LABORATORY'S SCOPE

TABLE 1

Question 27 - Examination Questions	
WebCode	**Response**
VDB8G4	Phil Lark
VG9PVJ	Phil Lark
VJEAGX	Phil Lark
VLPWFC	Phil Lark
VP3UPK	Phil Lark
WVNBEF	Phil Lark
ZEAZKD	Phil Lark
ZGVLBE	Phil Lark
ZKXMCC	Phil Lark

Question 27: Which contact has the phone number +44 1482 466581? Provide the name of contact.

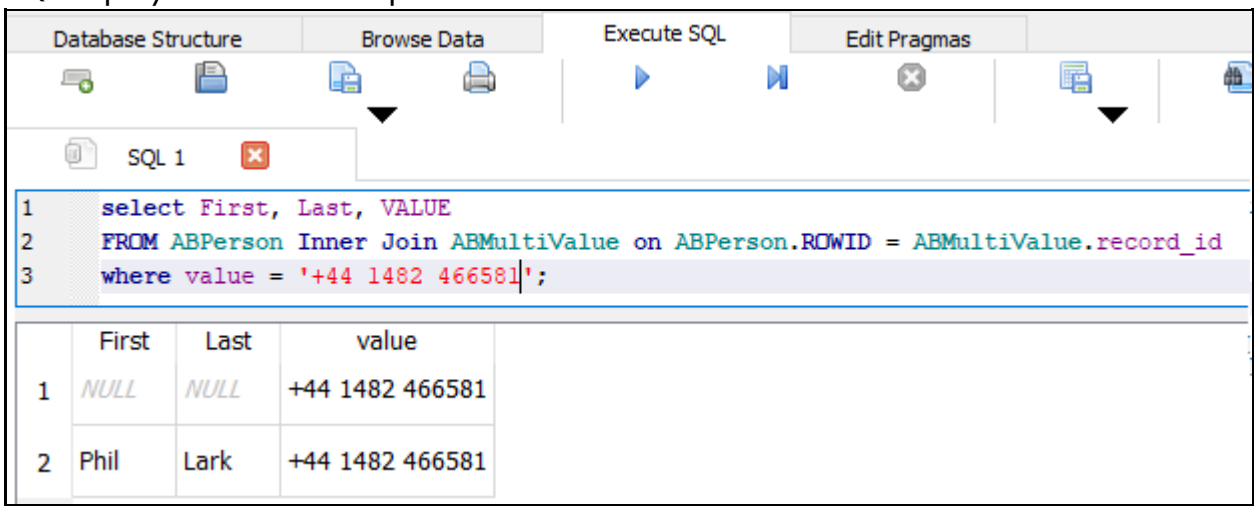
Consensus Result: Phil Lark

Expected Response Explanation:

Phone numbers for contacts are stored in /private/var/mobile/Library/AddressBook/AddressBook.sqlitedb and in the associated temp (shm, wal) files. Contact names are in the ABPerson table and phone numbers are stored in the ABMultiValue table. Joining these tables by the ROWID and record_id fields (respectively) associates the names with their phone numbers.

Expected Response Illustration:

SQLite query of AddressBook.sqlitedb



Cellebrite Contact table

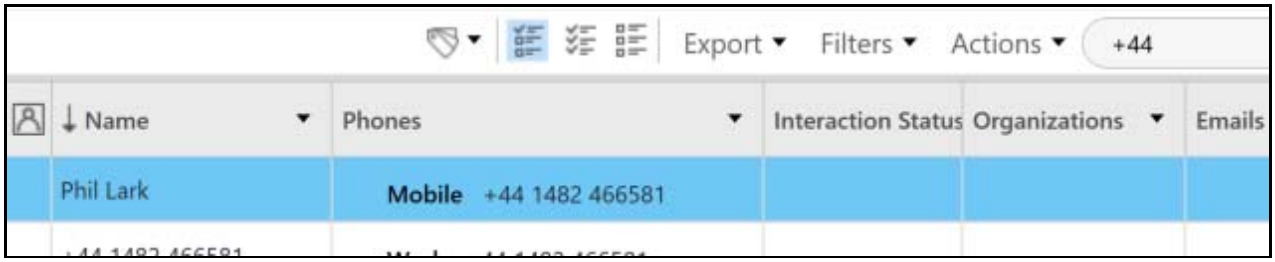


TABLE 1

Question 28 - Examination Questions

Question 28: Who sent the email with subject line "TALK TO ME"? Provide the email address.

Manufacturer's Expected Response: mason12jake@gmail.com

WebCode	Response
2JFUWZ	mason12jake@gmail.com
2YAJPB	mason12jake@gmail.com
3329MU	mason12jake@gmail.com
3R3DPY	mason12jake@gmail.com
4FPB42	28-mason12jake@gmail.com
66P4MA	mason12jake@gmail.com
6ERKDC	mason12jake@gmail.com
6M83T7	mason12jake@gmail.com
6QMVJY	mason12jake@gmail.com
7CKLGB	mason12jake@gmail.com
7ND6X2	mason12jake@gmail.com - Mason Jake
7W8BQ3	Mason Jake, mason12jake@gmail.com
7WQWJT	mason12jake@gmail.com
8F34CZ	mason12jake@gmail.com
8JDFPT	Mason Jake; mason12jake@gmail.com
8JXTWE	mason12jake@gmail.com
8VQFKZ	mason12jake@gmail.com
9MCRLT	mason12jake@gmail.com
9VQVED	mason12jake@gmail.com (Mason Jake)
AGMPY9	mason12jake@gmail.com
AKNRPA	mason12jake@gmail.com
BHAT4Y	mason12jake@gmail.com
BNZ3DX	mason12jake@gmail.com
C6EZRU	mason12jake@gmail.com
CERU9G	Mason Jake
CKT9RX	mason12jake@gmail.com
CZNJJA	mason12jake@gmail.com
DNUPM7	mason12jake@gmail.com
DQZW7Y	mason12jake@gmail.com
DT3X7V	mason12jake@gmail.com

TABLE 1

Question 28 - Examination Questions	
WebCode	**Response**
DYD4P9	mason12jake@gmail.com
E7PH86	mason12jake@gmail.com
FLWZEV	mason12jake@gmail.com
G8C3KE	mason12jake@gmail.com
GPDMNU	mason12jake@gmail.com
GQPFJW	mason12jake@gmail.com
GYF3AR	mason12jake@gmail.com
HGFG4R	mason12jake@gmai.com
JCC299	mason12jake@gmail.com
JEJH6J	mason12jake@gmail.com
JL3MGR	mason12jake@gmail.com
KVP67K	mason12jake@gmail.com
L6PWCQ	mason12jake@gmail.com
MFJPZ8	mason12jake@gmail.com
MXKEER	mason12jake@gmail.com
N634TR	Mason Jake: mason12jake@gmail.com
NE7FKF	mason12jake@gmail.com
NEP2GC	mason12jake@gmail.com
NP67AT	mason12jake@gmail.com
NT6H7T	mason12jake@gmail.com
NZNRBG	mason12jake@gmail.com
P77HBH	mason12jake@gmail.com
P9Y9K3	mason12jake@gmail.com
QLFNYL	mason12jake@gmail.com
QM9E98	mason12jake@gmail.com
R748U6	mason12jake@gmail.com
T8BAT9	mason12jake@gmail.com
T9LU2H	mason12jake@gmail.com Mason Jake
TPPKJE	mason12jake@gmail.com
TYEAHM	mason12jake@gmail.com
U7V8LZ	mason12jake@gmail.com
V7R6A2	NOT WITHIN LABORATORY'S SCOPE

TABLE 1

Question 28 - Examination Questions	
WebCode	**Response**
VDB8G4	Mason Jake: mason12jake@gmail.com
VG9PVJ	mason12jake@gmail.com
VJEAGX	mason12jake@gmail.com
VLPWFC	mason12jake@gmail.com
VP3UPK	mason12jake@gmail.com
WVNBEF	mason12jake@gmail.com
ZEAZKD	mason12jake@gmail.com
ZGVLBE	mason12jake@gmail.com
ZKXMCC	mason12jake@gmail.com

Question 28: Who sent the email with subject line "TALK TO ME"? Provide the email address.

Consensus Result: mason12jake@gmail.com

Expected Response Explanation:

Email details are stored in /filesystem1/private/var/mobile/Library/Mail/Envelope Index (database).

Expected Response Illustration:

Cellebrite Emails Table

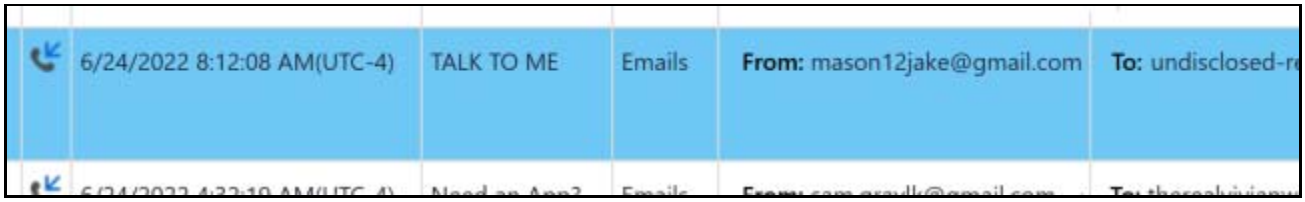


TABLE 1

Question 29 - Examination Questions

Question 29: Provide a site visited in the DuckDuckGo browser.

Manufacturer's Expected Response: www.amtrak.com and/or www.greyhound.com

WebCode	Response
2JFUWZ	www.greyhound.com; www.antrak.com; duckduckgo.com; bing.com
2YAJPB	https://www.greyhound.com/en/info/session-timeout
3329MU	https://www.greyhound.com
3R3DPY	https://www.greyhound.com/en/info/session-timeout
4FPB42	www.greyhound.com - www.amtrak.com
66P4MA	www.amtrak.com, www.greyhound.com
6ERKDC	https://www.greyhound.com/en/info/session-timeout
6M83T7	www.greyhound.com, www.amtrak.com
6QMVJY	www.greyhound.com
7CKLGB	www.greyhound.com
7ND6X2	www.greyhound.com
7W8BQ3	http://www.amtrak.com/favicon.ico
7WQWJT	https://www.greyhound.com/en/info/session-timeout
8F34CZ	https://www.amtrak.com/favico.ico
8JDFPT	https://www.amtrak.com
8JXTWE	http://www.amtrak.com/favicon.ico Recovered from the cache.db for the DuckDuckGo application, visited on 06/25/2022
8VQFKZ	https://www.greyhound.com/en/info/session-timeout
9MCRLT	https://www.greyhound.com/en/info/session-timeout
9VQVED	www.amtrak.com
AGMPY9	www.greyhound.com
AKNRPA	https://www.greyhound.com/en/info/session-timeout
BHAT4Y	www.greyhound.com
BNZ3DX	www.greyhound.com
C6EZRU	www.greyhound.com
CERU9G	content.amtrak.com
CKT9RX	https://www.greyhound.com/en/info/session-timeout
CZNJJA	https://www.greyhound.com/en/info/session-timeout
DNUPM7	https://www.greyhound.com/en/info/session-timeout
DQZW7Y	www.greyhound.com

TABLE 1

Question 29 - Examination Questions	
WebCode	**Response**
DT3X7V	https://www.amtrak.com/apple-touch-icon.png OR https://duckduckgo.com/ac/?q=greyhou&is_nav=1
DYD4P9	https://www.greyhound.com/en/info/session-timeout
E7PH86	greyhound.com
FLWZEV	ProtonMail
G8C3KE	www.greyhound.com
GPDMNU	www.amtrak.com
GQPFJW	amtrak.com
GYF3AR	Greyhound (https://www.greyhound.com/en/info/session-timeout)
HGFG4R	www.greyhound.com
JCC299	www.greyhound.com
JEJH6J	https://duckduckgo.com/email/start
JL3MGR	content.amtrak.com
KVP67K	www.amtrak.com
L6PWCQ	content.amtrak.com
MFJPZ8	www.amtrak.com
MXKEER	https://www.greyhound.com/en/info/session-timeout
N634TR	www.amtrak.com
NE7FKF	www.amtrak.com
NEP2GC	www.amtrak.com
NP67AT	www.greyhound.com
NT6H7T	www.greyhound.com
NZNRBG	www.amtrak.com
P77HBH	https_www.amtrak.com
P9Y9K3	https://www.greyhound.com/en/info/session-timeout
QLFNYL	https://www.greyhound.com/en/info/session-timeout
QM9E98	amtrak
R748U6	https://www.greyhound.com
T8BAT9	https://www.greyhound.com
T9LU2H	DarArchive/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
TPPKJE	www.greyhound.com
TYEAHM	www.amtrak.com
U7V8LZ	www.greyhound.com

TABLE 1

Question 29 - Examination Questions	
WebCode	**Response**
V7R6A2	NOT WITHIN LABORATORY'S SCOPE
VDB8G4	www.greyhound.com
VG9PVJ	chinaqking.com https://www.greyhound.com/en/info/session-timeout
VJEAGX	https://www.greyhound.com
VLPWFC	www.amtrak.com, www.greyhound.com
VP3UPK	www.greyhound.com
WVNBEF	http://www.amtrak.com
ZEAZKD	https://www.greyhound.com
ZGVLBE	https://www.greyhound.com/en/info/session-timeout
ZKXMCC	www.amtrak.com

Question 29: Provide a site visited in the DuckDuckGo browser.

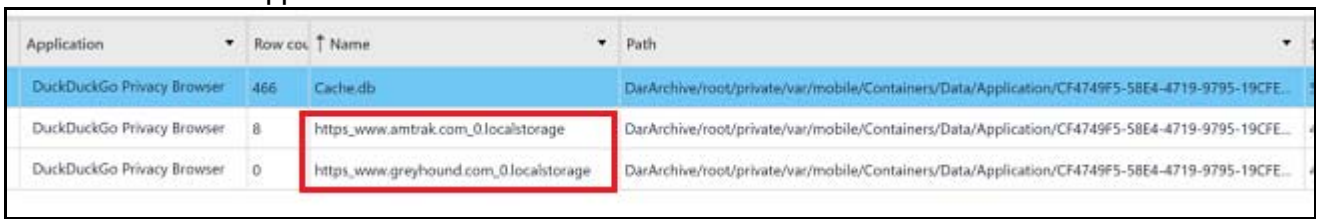
Consensus Result: www.amtrak.com and/or www.greyhound.com

Expected Response Explanation:

Limited DuckDuckGo browser history data is stored in DarArchive/root/private/var/mobile/Containers/Data/Application/CF4749F5-58E4-4719-9795-19CFEEF4EFB2/Library/. A review of these files discovers records of visits to the above sites.

Expected Response Illustration:

DuckDuckGo files snippets



Application	Row co	Name	Path
DuckDuckGo Privacy Browser	466	Cache.db	DarArchive/root/private/var/mobile/Containers/Data/Application/CF4749F5-58E4-4719-9795-19CFE...
DuckDuckGo Privacy Browser	8	https_www.amtrak.com_0.localstorage	DarArchive/root/private/var/mobile/Containers/Data/Application/CF4749F5-58E4-4719-9795-19CFE...
DuckDuckGo Privacy Browser	0	https_www.greyhound.com_0.localstorage	DarArchive/root/private/var/mobile/Containers/Data/Application/CF4749F5-58E4-4719-9795-19CFE...

TABLE 1

Question 30 - Examination Questions

Question 30: Provide the path and filename, (i.e., /root/folder/subfolder…/filename.extension) for the file containing the (CASE SENSITIVE) term "Tytonidae" (capital T, without quotes).

Manufacturer's Expected Response: /private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG

WebCode	Response ** Inconsistencies not highlighted; No consensus achieved **
2JFUWZ	root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
2YAJPB	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
3329MU	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
3R3DPY	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
4FPB42	/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE7C81B1E959C9/NoteStore.sqlite-wal
66P4MA	/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG, IMG_0100.JPG
6ERKDC	/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite-wal
6M83T7	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
6QMVJY	root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
7CKLGB	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
7ND6X2	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
7W8BQ3	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
7WQWJT	Apple_iPhone 6s (A1633).zip/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
8F34CZ	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
8JDFPT	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
8JXTWE	Apple_iPhone 6s (A1633).zip/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
8VQFKZ	Apple_iPhone 6s (A1633).zip/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite.wal - \private\var\mobile\library\keyboard\en-dynamic.;m\dynamic-lexicon.dat - Neither AXIOM nor Cellebrite PA have managed to find the Capitalised version.
9MCRLT	Apple_iPhone 62 (A1633).zip\filesystem1\private\var\mobile\Containers\Shared\AppGroup\0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9\NoteStore.sqlite
9VQVED	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
AGMPY9	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
AKNRPA	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
BHAT4Y	/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite-wal
BNZ3DX	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG
C6EZRU	root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite-wal

TABLE 1

Question 30 - Examination Questions		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
CERU9G	/root/private/var/mobile/Media/DCIM/100Apple/IMG_100.JPG	
CKT9RX	\private\var\mobile\Containers\Shared\AppGroup\0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9\NoteStore.sqlite	
CZNJJA	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
DNUPM7	root\private\var\mobile\Media\DCIM\100APPLE\IMG_0100.JPG	
DQZW7Y	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
DT3X7V	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
DYD4P9	Path: Apple_iPhone 6s (A1633).zip/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG Filename: IMG_0100.JPG	
E7PH86	42551_iPhone6s.zip\42551_iPhone6s\Apple_iPhone 6s (A1633).zip\filesystem1\private\var\mobile\Media\DCIM\100APPLE\IMG_0100.JPG	
FLWZEV	/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite-wal	
G8C3KE	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
GPDMNU	Apple_iPhone 6s (A1633).zip/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
GQPFJW	root/private/var/mobile/Containers/Shared/AppGroup/NoteStore.sqlite-wal	
GYF3AR	Path: Apple_iPhone 6s (A1633).zip/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite-wal : 0x20E770 , File name:	
HGFG4R		
JCC299	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
JEJH6J	not found	
JL3MGR	/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite-wal	
KVP67K	/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite-wal	
L6PWCQ	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
MFJPZ8	Apple_iPhone 6s (A1633).zip/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
MXKEER	Apple_iPhone 6s (A1633).zip/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
N634TR	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
NE7FKF	Apple_iPhone 6s (A1633).zip/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
NEP2GC	/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
NP67AT	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
NT6H7T	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
NZNRBG	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
P77HBH	/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite-wal	

TABLE 1

Question 30 - Examination Questions		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
P9Y9K3	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
QLFNYL	/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
QM9E98	Apple_iPhone 6s (A1633).zip/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite-wal	
R748U6	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
T8BAT9	Apple_iPhone 6s (A1633).zip\filesystem1\private\var\mobile\Containers\Shared\AppGroup\0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9\NoteStore.sqlite-wal	
T9LU2H	/root/private/var/mpobile/Media/DCIM/100APPLE/IMG_0100.JPG	
TPPKJE	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
TYEAHM	Path - Apple_iPhone 6s (A1663).zip/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.aqlite-wal Filename - tytonidae	
U7V8LZ	DarArchive/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
V7R6A2	NOT WITHIN LABORATORY'S SCOPE	
VDB8G4	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
VG9PVJ	DarArchive/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
VJEAGX	/root/private/var/mobile/Media/DCIM/100APPLE/IMG_100.JPG	
VLPWFC	/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite-wal	
VP3UPK	/root/private/var/mobile/Containers/Shared/AppGroup/0E40D9D4-BCA7-41A5-8DBE-7C81B1E959C9/NoteStore.sqlite-wal	
WVNBEF	DarArchive/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	
ZEAZKD	Apple_iPhone 6s (A1633).zip\filesystem1\private\var\mobile\Media\DCIM\100APPLE\IMG_0100.JPG	
ZGVLBE	FullFileSystem.1.dar\private\var\mobile\Media\DCIM\100APPLE\IMG_0100.JPG	
ZKXMCC	Apple_iPhone 6s (A1633).zip/root/private/var/mobile/Media/DCIM/100APPLE/IMG_0100.JPG	

Question 30: Provide the path and filename, (i.e., /root/folder/subfolder…/filename.extension) for the file containing the (CASE SENSITIVE) term "Tytonidae" (capital T, without quotes).

Consensus Result: While a majority of participants reported the expected response, a consensus was not achieved for this question. Eighteen participants reported a different path and filename that included the word "tytonidae" with the lowercase "T."

TABLE 1

Question 30 - Examination Questions

Expected Response Explanation:

Conducting a keyword search will discover this keyword in the listed file. Using a method such as an "Advanced Search" and selecting "Search file contents" in Cellebrite, or a live search in Axiom, configuring the tool (e.g. making sure to index all text when searching in Axiom), will find this file. This term also exists (beginning with a lowercase T) in a Note and in several system files.

Expected Response Illustration:

IMG_0100.JPG

TABLE 1

Question 31 - Examination Questions

Question 31: What type of file is identified in Question 30 (the previous question)?

Manufacturer's Expected Response: IMG_0100.JPG is a text file.

WebCode	Response ** Inconsistencies not highlighted; No consensus achieved **
2JFUWZ	txt
2YAJPB	Extension is a .jpg (Picture) but the hex appears to be a text file.
3329MU	Image
3R3DPY	Unicode text, UTF-8 text, with very long lines (977)
4FPB42	notes
66P4MA	text(txt)
6ERKDC	Apple Notes
6M83T7	JPG
6QMVJY	image
7CKLGB	Text Document
7ND6X2	The original file type is showing as a '.jpg'. However, opening the file as '.txt' displays the content of the file.
7W8BQ3	.JPG fil named 'IMG_0100.JPG'
7WQWJT	Plain text
8F34CZ	A jpg file. (which is really a document not an image)
8JDFPT	JPG image
8JXTWE	A text file with the file extension JPG. The file is not a JPG and does not contain the JPG header FF D8 FF
8VQFKZ	NoteStore.sqlite.wal
9MCRLT	Apple Note
9VQVED	The file located in #30 was identified as a JPG image file; however, an image/picture was not visible, and the file header of the file did not contain a JPG image header (hex: FF D8) or footer (hex: FF D9). The file appeared to be a text file that contained typed text "Tytonidae".
AGMPY9	.txt
AKNRPA	picture
BHAT4Y	Database SQLite – WAL file
BNZ3DX	The original file in the path is named as being a '.jpg' file. It has been obfuscated. However, reviewing file data(in Hex) opening the file as '.txt' file instead actually shows the content.
C6EZRU	A note file synced to the cloud
CERU9G	JPG
CKT9RX	sqlite / Apple Note entry
CZNJJA	plist
DNUPM7	Text file

TABLE 1

Question 31 - Examination Questions		
WebCode	**Response**	** Inconsistencies not highlighted; No consensus achieved **
DQZW7Y	a JPG	
DT3X7V	Text file (Lorem ipsum - dummy text)	
DYD4P9	JPEG = Joint Photographic Experts Group	
E7PH86	42551_iPhone6s.zip\42551_iPhone6s\Apple_iPhone 6s (A1633).zip\filesystem1\private\var\mobile\Media\DCIM\100APPLE\IMG_0100.JPG .jpg is identified as a jpeg image file but is actually some type of text file.	
FLWZEV	sqlite	
G8C3KE	The file has a JPG extension but does not appear to be an image file.	
GPDMNU	The extension shows its .JPG however the file type is UTF-8 Unicode text file	
GQPFJW	“Apple Notes” (sqlite-wal)	
GYF3AR	.sqlite-wal	
HGFG4R	Note	
JCC299	Plain text. The file extension is .JPG, corresponding to a JPEG picture file; however, the file content is not consistent with a JPEG, as it contains plain, mostly lorem ipsum, text.	
JEJH6J	not found	
JL3MGR	database .sqlite(wal)	
KVP67K	SQLite database file	
L6PWCQ	.JPG image file	
MFJPZ8	It has a .jpg extension but the data appears to be a text file.	
MXKEER	A jpg image	
N634TR	Plaintext file	
NE7FKF	JPG	
NEP2GC	Image File “JPG”	
NP67AT	The file has a .JPG extension, but the file content has no header and appears to be text	
NT6H7T	text file	
NZNRBG	Text file with image extension (JPG).	
P77HBH	Note	
P9Y9K3	JPG	
QLFNYL	This text is located in a file identified as jpg image file, but the header information is not consistent with a .jpg image file. It is more like a text file, but there is no identifiable header/footer.	
QM9E98	NoteStore.wal is a write ahead log for atomic commit and rollback sqlite.	
R748U6	It is actually a plain text file	
T8BAT9	SQLite database write-ahead-log file	
T9LU2H	.JPG	

TABLE 1

Question 31 - Examination Questions	
WebCode	**Response** ** Inconsistencies not highlighted; No consensus achieved **
TPPKJE	File extension suggests .jpg, but it's a text file.
TYEAHM	Note File
U7V8LZ	File with a .jpg file extension that does not appear to be an image. Contains text.
V7R6A2	NOT WITHIN LABORATORY'S SCOPE
VDB8G4	It has an Image file extension but the file does not contain picture information; it is a text file with '.jpg' extension.
VG9PVJ	JPG – Image file
VJEAGX	.JPG extension but missing the JPG header - possibly a txt file
VLPWFC	Notes
VP3UPK	SQLITE file (database)
WVNBEF	TXT
ZEAZKD	it appears to be a plain text file rendering of a Lorem Ipsum generator page. TrID was used to attempt to decode the file signature and it came back as null and suggested that it was possibly a plain text. The text contains data that is in related to the a standard Lorem Ipsum passage that can be generated on Lipsum.com
ZGVLBE	.JPG
ZKXMCC	The extension shows its .JPG however the file type is UTF-8 Unicode text file

Question 31: What type of file is identified in Question 30 (the previous question)?

Consensus Result: A consensus was not achieved for this question. All 18 participants who reported the file containing the word "tytonidae" with the lowercase "T" in question 30 analyzed that file when responding to this question and not the intended file. Of the 50 participants that reported the expected file in question 30, only 31 participants reported the expected response for this question.

Expected Response Explanation:

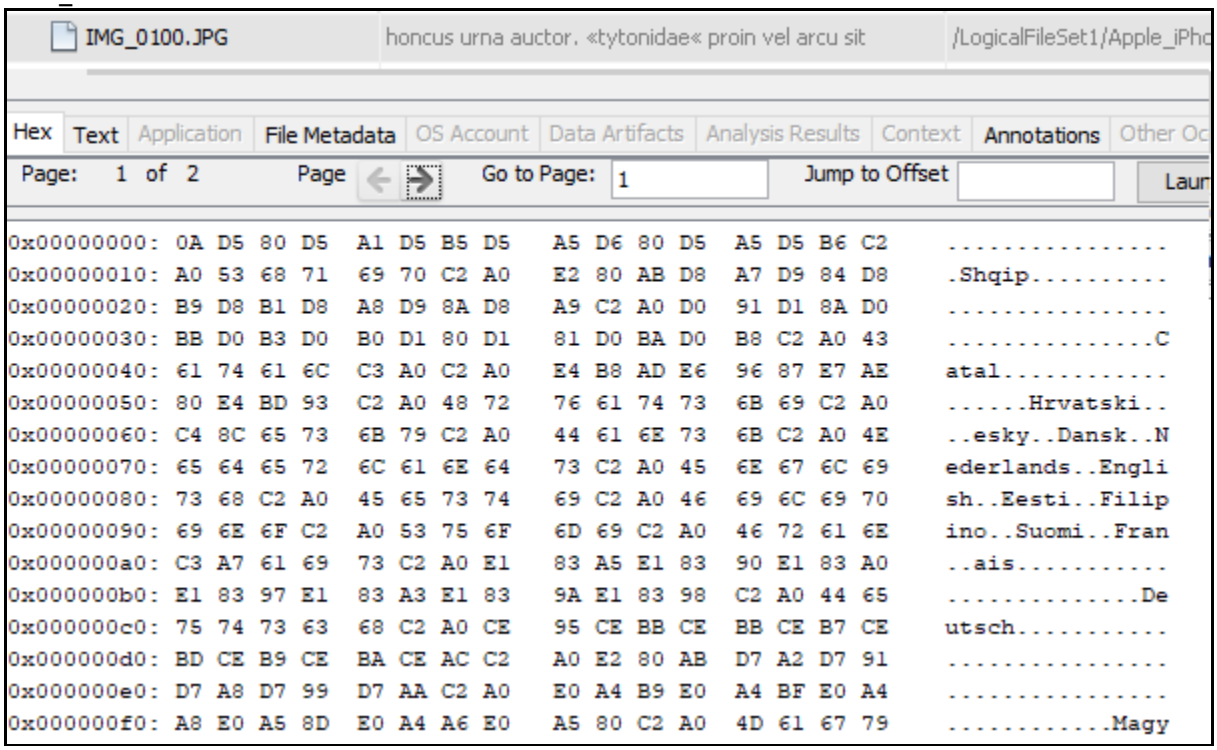
IMG_0100.JPG is considered an "Aliased file" as it has an extension (.jpg) which differs from its true type or content (text). An actual JPG image file would begin with the file header for a JPG (FF D8 FF) and contain image data. IMG_0100.JPG contains only text.

TABLE 1

Question 31 - Examination Questions

Expected Response Illustration:

IMG_0100.JPG



Additional Comments

TABLE 2

WebCode	Additional Comments
2JFUWZ	29. Websites visited: www.greyhound.com; www.antrak.com; duckduckgo.com; bing.com - probably reservation systems (data from /root/private/var/mobile/Containers/Data/Application/CF4749F5-58E4-4719-9795-19CFEEF4EFB2/Library/WebKit/WebsiteData/LocalStorage/, cookies, snapshots in /root/private/var/mobile/Containers/Data/Application/CF4749F5-58E4-4719-9795-19CFEEF4EFB2/Library/SplashBoard/Snapshots/sceneID/com.duckduckgo.mobile.ios-default/ and blobs in /root/private/var/mobile/Containers/Data/Application/CF4749F5-58E4-4719-9795-19CFEEF4EFB2) but there are also traces of accessing other domains like google.com, gstatic.com (Google services like captcha and JS scripts). Additionally there were requests (queries) to the duckduckgo.com with search keywords (/root/private/var/mobile/Containers/Data/Application/CF4749F5-58E4-4719-9795-19CFEEF4EFB2/Library/Caches/com.duckduckgo.mobile.ios/Cache.db)
66P4MA	thanks
6M83T7	This test was solved by 12 expert personnel. [List of Names]
8JXTWE	Can you provide support for uploading a PDF of the question and answers along with filling out the exam questions as it is now? It would be helpful to have a backup of the answers which were reviewed prior to submitting within the online form fields, that is submitted in parallel. Our forensic systems are not online and this is being submitted with another internet only PC. This, so we can avoid pasting errors and typos.
C6EZRU	Could not identify a file that contained the word "Tytonidae" where the T was capitalized
CKT9RX	Number 12: I did not locate any specific email associated with the protonmail setup. Curious as to where to find that. Number 13: I index searched "Traveling" as well as "Travelling" (in case of misspelling) and was unable to locate any email or other communication at all with this term. There was only a Telegram message about Mexico that appeared unrelated. Number 22: I hashed all image files as part of Axiom's process. There were no hits for this MD5 at all. Not even partial hits. The file must be something other than a photo. Curious how to do this. Number 30: The term "Tytonidae" was not located with a capital T at all. I index searched it. There was only an entry in the sqlite database under Notes section with the lowercase version.
DYD4P9	Unable to find selected data sets on an outdated Cellebrite Physical Analyzer version.
KVP67K	Question 7: (UTC-05:00) New_York (America). Question 29: www.greyhound.com. Questions 30 and 31. I conducted a search for the word Tytonidae with a capital T in both Physical Analyzer and AXIOM. Neither program located a match for the word with a capital T. Both did find one instance of the word with a lower-case t. I provided the file path of the data with the lower-case t. This I believe could be interrupted as a database-wal file or a Note file.
P9Y9K3	The audio questions (22 and 23) formatting were unclear. Whether to round the GPS coordinates in question 24 was unclear.
R748U6	For question 16, the full answer is 6/25/2022 11:57:43 UTC-4. However, the submitted time was truncated to follow CTS formatting requirements.
V7R6A2	Question #16 was left blanked because it is not within the laboratory's scope.
VLPWFC	Question Nr. 30: If we strictly follow the question there is no file containing the term “Tytonidae”, however there is one file contains “tytonidae”. Consider that there is no point of question 31 without a valid result of question 30.

-End of Report-
(Appendix may follow)