



Mobile Digital Evidence - Android

Test No. 20-5550 Summary Report

Participants were provided with data yielded from a physical 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:

	<u>Page</u>
<u>Manufacturer's Information</u>	<u>2</u>
<u>Summary Comments</u>	<u>7</u>
<u>Table 1: Digital Evidence Responses</u>	<u>8</u>
<u>Table 2: Additional Comments</u>	<u>151</u>

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 – Android Analysis test consisted of evidence data acquired from a smart phone in the .BIN file format. Participants were asked to examine the extracted data pertaining to a simulated scenario utilizing their own software and methods.

SAMPLE PREPARATION:

A scripted scenario, based upon a case involving the unlawful use of payment card scanning devices and the trafficking of payment card information was created to generate user data on the evidence Android device. The execution of the scripted crime took place in December 2019. A Samsung Galaxy J2 smart phone was used to perform the activities and generate the intended artifacts.

The phone data was acquired through a physical extraction of the smart phone utilizing Cellebrite software. Following sample validation, the phone data was converted into a .BIN compressed file. This file was uploaded to the CTS portal for participants to download. MD5 and SHA-1 algorithms were run on the compressed zip file to generate unique hash values 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 utilizing various software to ensure the expected results could be achieved. Laboratories that conducted analysis during predistribution reported consistent results.

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

Over the previous several weeks, numerous parasitic magnetic card readers (commonly known as skimmers) have been discovered hidden within fuel pumps at several gas stations within the local area. Recently, a suspect, Allen Gonzales was caught tampering with a fuel pump and arrested by the local police department. In Gonzales' possession, the arresting officer discovered a parasitic Bluetooth credit card skimmer (similar to those recently discovered at other gas stations), and a Samsung Galaxy J2 (Android) smartphone. Police obtained a warrant authorizing the search of the smartphone for evidence relating to the unlawful use of payment card scanning devices and the trafficking of payment card information.

Manufacturer's Information, continued

<u>Question</u>	<u>Manufacturer's Expected Response</u>
1	<u>Provide the SHA256 Hash for the extraction blk0_mmcbk0.bin file.</u> D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
2	<u>What is the model name of this phone?</u> SM-J260T1
3	<u>What is the version of the Android operating system on this phone?</u> 8.1.0
4	<u>What is the set time zone for this phone? Report in the following format: Country/City</u> America/New_York
5	<u>What is the IMEI number associated with this phone?</u> 356212106714588
6	<u>Provide the Device Phone Number (MSISDN).</u> 15718351874
7	<u>What is the language/locale setting for this phone?</u> en_US
8	<u>Provide the primary Google account (email address) associated with this phone.</u> allengonzo79@gmail.com
9	<u>What is the name of the WiFi hotspot connected to by this phone on December 10, 2019?</u> FlyReagan
10	<u>What was the last date and time the phone was connected to the "Free LGA WiFi" hotspot? Provide your response in the time zone set for the device using the following format: MM/DD/YYYY, HH:MM AM/PM</u> 12/11/2019 10:47 AM
11	<u>What is the name of the paired bluetooth device with MAC Address 98:D3:31:FC:1B:64?</u> SKMR13
12	<u>What is the name of the (non-Gmail) email client installed by the user?</u> K-9 Mail
13	<u>What version is the (non-Gmail) email client installed by the user?</u> 5.6
14	<u>How many SMS messages were received from the phone number associated with the contact listed as "Francis Milligan"? Provide response using the numeric format.</u> 6

Manufacturer's Information, continued

<u>Question</u>	<u>Manufacturer's Expected Response</u>
15 <u>What is the account number for the device mobile service (cellular) provider?</u>	756887507
16 <u>How many unread SMS messages are on the phone? Provide response using the numeric format.</u>	8
17 <u>What communication service sent the 783514 verification code?</u>	Google Voice
18 <u>What contact (name) has the phone number "208-900-1987"?</u>	mom
19 <u>What was the duration of the call from Raymond Butner on 12/5/2019? Provide your response in the following format: HH:MM:SS</u>	00:00:27
20** <u>What was the date and time of the last outgoing call? Provide your response in the time zone set for the device using the following format: MM/DD/YYYY, HH:MM AM/PM</u>	12/15/2019 09:28 PM
21** <u>The last outgoing call was made to what phone number?</u>	**61*18056912815
22** <u>Provide the contact name belonging to the phone number reported in question #21?</u>	Allen Gonzales
23** <u>Provide the associated communication service to which the phone number in question #21 belongs?</u>	User's Google Voice Account
24 <u>What are the location coordinates for the photograph of the Christmas tree taken with the phone's camera? Provide your response using the following format: Latitude, Longitude (to 6 decimal places)</u>	38.888611, -77.005000
25 <u>According to the text in the file with MD5 hash 7a4860b10c8f6e73813b2d28f4b42893, what does the first amendment not cover?</u>	Burping
26 <u>What is the creation date and time (using time zone set for this device) of this file with MD5 hash 7a4860b10c8f6e73813b2d28f4b42893? Provide your response in the following format: MM/DD/YYYY, HH:MM AM/PM</u>	12/13/2019 12:20 PM
27 <u>What is the name of the saved parking location in the Google Maps app?</u>	Citgo

Manufacturer's Information, continued

<u>Question</u>	<u>Manufacturer's Expected Response</u>
28 <u>What is the name of the cryptocurrency related app installed on this phone?</u>	<i>BitPay</i>
29 <u>Within the app data for the installed cryptocurrency app (reported in question #28), what BTC address is indicated as last by the app?</u>	<i>1fjijkpUsooSWw3ATgXaB4uTEGzizonL9m</i>
30 <u>What was the amount (in USD) of the last transaction in the cryptocurrency app (reported in question #28)?</u>	<i>\$1</i>
31 <u>At what time (device local time) was the Starbucks app used to conduct a transaction at a Starbucks store on 12/15/2019? Provide your response in the following format: HH:MM AM/PM</u>	<i>02:33 PM</i>
32 <u>What was the transaction amount of the Starbucks transaction mentioned in question #31 (in USD, not counting tip)?</u>	<i>16.75</i>
33 <u>As recorded on the phone, at what Starbucks store was this transaction conducted (transaction from question #31)?</u>	<i>Fredericksburg, Warrenton Road</i>
34** <u>Provide the URL the user bookmarked for a dark web website.</u>	<i>http://apollon5e246vvhj.onion/login.php</i>
35 <u>What application did the user use to manage PGP keys?</u>	<i>OpenKeychain</i>
36 <u>Who's key (other than the user) did the user have stored in his PGP keychain? (provide email address)</u>	<i>francismilligan599@gmail.com</i>
37 <u>What application did the user utilize to access the bluetooth skimmers?</u>	<i>Serial Bluetooth Terminal</i>
38 <u>In what directory was the data downloaded from the bluetooth skimmers stored?</u>	<i>USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/</i>
39 <u>What did the user last search on Amazon?</u>	<i>Bluetooth Module</i>
120 <u>What was the date and time of the last outgoing call? Provide your response in the time zone set for the device using the following format: MM/DD/YYYY, HH:MM AM/PM (Subset 1)</u>	<i>12/15/2019 09:28 PM</i>

Manufacturer's Information, continued

<u>Question</u>	<u>Manufacturer's Expected Response</u>
121 <u>The last outgoing call was made to what phone number? (Subset 1)</u>	**61*18056912815
220 <u>What was the date and time of the last outgoing call? Provide your response in the time zone set for the device using the following format: MM/DD/YYYY, HH:MM AM/PM. (Subset 2)</u>	12/05/2019 06:35 AM
221 <u>The last outgoing call was made to what phone number? (Subset 2)</u>	1-703-940-7024
222 <u>Provide the contact name belonging to the phone number reported in question #21? (Subset 2)</u>	Raymond Butner

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 in the .BIN file format, 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: image details, phone and network settings, native and third-party applications, communications, web browser history, and Geo-Location information.

Of the 39 total questions, five questions did not reach a consensus response. Four of these five questions were linked together, therefore the answer reported for question #20 would affect the outcome for questions 21 – 23. Question #20 asked for the date and time of the last outgoing call and the following three questions related to this last outgoing call. Although a consensus was not achieved based on the total population, two distinct subsets of results were seen based on what the participant deemed to be the last outgoing call. These two subsets labeled as Subset 1 and Subset 2 were based on whether the participant recognized the date of 12/15/2019 or 12/5/2019 respectively as being associated with the last outgoing call. These subsets are shown in separate tables towards the end of the report. From additional comments provided by participants the main cause for these subsets of results was due to whether a call-forwarding call was to be considered an outgoing call.

Several participants raised concerns regarding the wording used in certain questions. The concern related to the idea that some questions may be interpreted in multiple ways. CTS recognizes this and is working on question development with the purpose of eliminating interpretation confusion.

We realize that the Digital Forensics field is increasing in complexity and there are generally not many clearly-defined answers. Similarly, for this test, participants should follow their laboratory's policies and procedures when evaluating the MDE proficiency test questions.

Please Note: Several forensic software tools were utilized during the validation of this test and may be referenced during the discussion of results. One tool used, Physical Analyzer 7.26 is referenced in the Expected Response Explanation section as "PA". CTS does not endorse any particular tools.

Digital Evidence Responses

TABLE 1

Question 1 - Acquisition / Device Information

Question 1: Provide the SHA256 Hash for the extraction blk0_mmcbk0.bin file.

Manufacturer's D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455

Expected Response:

WebCode	Response
2B66AE	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
2JDY68	SHA256: D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
3LWD98	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
3VNPE9	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
63XWWA	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
69MBU4	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
6EKPAN	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
6PRHA7	df59174cf8a96eb3fe82a9dc0e336b683c23fdff3f0b9b8f73f237b0462c6713
74MLQ2	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
77WBJY	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
7RU3AB	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
82DV2X	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
82VLFW	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
8CX7F4	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
8EN7R9	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
8K97CZ	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
8NC4K8	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
8NNHGL	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
9ANFQZ	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
9CUZL3	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
9XT88X	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
ABE2WW	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
AD6282	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
AEDEP3	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
B4AJ7X	N/A
BCMEEEX	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
BL9FU8	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
C2JJVT	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455

TABLE 1

Question 1 - Acquisition / Device Information	
WebCode	Response
C9ZCG4	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
CHMD3T	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
CKDDDX	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
CMH494	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
D7AC7Y	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
EBZ32N	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
EHJ79Q	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
EQURUZ	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
EYNXN2	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
F27G9V	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
GQ3JZL	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
H88C8U	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
HEPJ4T	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
JP4YCX	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
LWCVX9	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
MU3MGV	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
N9JXHH	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
NGD4BJ	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
NZ9WWG	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
PB49XM	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
PGULYB	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
PLMMZP	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
Q29PVJ	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
Q99RM3	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
QGJU94	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
RCRKJC	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
TF4QLP	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
TPBP6E	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
U899KL	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
UEREJE	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
UYQHMY	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455

TABLE 1

Question 1 - Acquisition / Device Information	
WebCode	Response
V9V7DB	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
VA6BPD	11f3c2cddd40ca21280a8a858f003fcc48902c55
W2UCV3	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
W4KC78	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
W4VZYW	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
WAMHLA	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
WTZ4AC	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
XBWQEF	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
XFRN2L	d384cb08e9a58937b4682a42bc03271367b41cba45fcb6da6d561635d4194455
YGFWDW	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
YK GK4G	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
ZVXNQ8	D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455

Question 1: Provide the SHA256 Hash for the extraction blk0_mmcbk0.bin file.

Consensus Result: D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455

Expected Response Explanation:

This hash value can be obtained by using a file compression utility (e.g. 7zip, Windows Explorer) to extract the sample image file from the provided ZIP folder, then using a checksum / hashing utility to calculate a SHA256 digest for the extracted blk0_mmcbk0.bin file.

Expected Response Illustration:

SHA256 Hash Value:

```
PS t:\> get-filehash -alg sha256 .\blk0_mmcbk0.bin

Algorithm      Hash
-----
SHA256         D384CB08E9A58937B4682A42BC03271367B41CBA45FCB6DA6D561635D4194455
```

TABLE 1

Question 2 - Acquisition / Device Information	
---	--

Question 2: What is the model name of this phone?

Manufacturer's SM-J260T1

Expected Response:

WebCode	Response
2B66AE	SM-J260T1
2JDY68	SM-J260T1
3LWD98	SM-J260T1
3VNPE9	Samsung Galaxy J2 SM-J260T1
63XWWA	SM-J260T1
69MBU4	SM-J260T1
6EKPAN	Samsung GSM SM-J260T1 Galaxy J2
6PRHA7	SM-J260T1 Galaxy J2
74MLQ2	SM-J260T1 Galaxy J2
77WBJY	Galaxy J2
7RU3AB	Samsung Galaxy J2 Core (SM-J260T1)
82DV2X	SM-J260T1
82VLFW	SM-J260T1
8CX7F4	SM-J260T1
8EN7R9	SM-J260T1
8K97CZ	SM-J260T1
8NC4K8	SM-J260T1
8NNHGL	SM-J260T1
9ANFQZ	Samsung Galaxy J2 Core
9CUZL3	SM-J260T1 Galaxy J2
9XT88X	SM-J260T1
ABE2WW	SM-J260T1
AD6282	SM-J260T1
AEDEP3	SM-J260T1
B4AJ7X	SM-J260T1
BCMEEEX	SM-J260T1 Galaxy J2
BL9FU8	SM-J260T1
C2JJVT	SM-J260T1
C9ZCG4	MS-J260T1

TABLE 1

Question 2 - Acquisition / Device Information	
WebCode	Response
CHMD3T	SM-J260T1
CKDDDX	SM-J260T1 Galaxy J2
CMH494	SM-J260T1
D7AC7Y	SM-J260T1
EBZ32N	SM-J260T1
EHJ79Q	Galaxy J2
EQURUZ	SM-J260T1
EYNXN2	SM-J260T1
F27G9V	SM-J260T1
GQ3JZL	SM-J260T1
H88C8U	SM-J260T1
HEPJ4T	Samsung Galaxy J2 SM-J260T1
JP4YCX	SM-J260T1 Galaxy J2
LWCVX9	SM-J260T1 /Root/sec_efs/SVC
MU3MGV	SM-J260T1
N9JXHH	SM-J260T1
NGD4BJ	Samsung SM-J260T1 (Samsung Galaxy J2)
NZ9WWG	Galaxy J2
PB49XM	SM-J260T1
PGULYB	SM-J260T1
PLMMZP	SM-J260T1
Q29PVJ	SM-J260T1
Q99RM3	SM-J260T1 Galaxy J2
QGJU94	Galaxy J2
RCRKJC	SM-J260T1
TF4QLP	SM-J260T1
TPBP6E	SM-J260T1
U899KL	SM-J260T1
UEREJE	SM-J260T1
UYQHMY	SM-J260T1 Galaxy J2
V9V7DB	SM-J260T1
VA6BPD	Galaxy J2 SM-J260T1

TABLE 1

Question 2 - Acquisition / Device Information	
WebCode	Response
W2UCV3	SM-J260T1
W4KC78	Samsung Galaxy J2 (Model: SM-J260T1)
W4VZYW	SM-J260T1
WAMHLA	SM-J260T1
WTZ4AC	SM-J260T1
XBWQEF	SM-J260T1
XFRN2L	SM-J260T1
YGFDWD	SM-J260T1
YK GK4G	SM-J260T1
ZVXNQ8	SM-J260T1

Question 2: What is the model name of this phone?

Consensus Result: SM-J260T1

Expected Response Explanation:

The name of the phone model is contained at line 22 in /Root/build.prop and is auto parsed by PA.

Expected Response Illustration:

Model Name

```

21 ro.build.flavor=j2corepitentel-user
22 ro.product.model=SM-J260T1
23 ro.product.brand=samsung
    
```

Model Name

```

Current SIM Phone Number: 12718531874   simCard.dat: 0x112
Detected Phone Model: SM-J260T1         build.prop: 0x2C2
Detected Phone Vendor: samsung           build.prop: 0x2DD
    
```

TABLE 1

Question 3 - Acquisition / Device Information

Question 3: What is the version of the Android operating system on this phone?

Manufacturer's 8.1.0

Expected Response:

WebCode	Response
2B66AE	8.1.0
2JDY68	Android 8.1.0
3LWD98	8.1.0
3VNPE9	8.1.0
63XWWA	8.1.0
69MBU4	8.1.0
6EKPAN	Android 8.1.0
6PRHA7	8.1.0
74MLQ2	8.1.0
77WBJY	8.1.0
7RU3AB	8.1.0
82DV2X	8.1.0
82VLFW	8.1.0
8CX7F4	8.1.0
8EN7R9	8.1.0
8K97CZ	8.1.0
8NC4K8	8.1.0
8NNHGL	8.1.0
9ANFQZ	8.1.0
9CUZL3	Android 8.1.0
9XT88X	8.1.0
ABE2WW	8.1.0
AD6282	8.1.0
AEDEP3	8.1.0
B4AJ7X	N/A
BCMEEEX	8.1.0
BL9FU8	8.1.0
C2JJVT	8.1.0
C9ZCG4	8.1.0

TABLE 1

Question 3 - Acquisition / Device Information	
WebCode	Response
CHMD3T	8.1.0
CKDDDX	8.1.0
CMH494	8.1.0
D7AC7Y	8.1.0
EBZ32N	8.1.0
EHJ79Q	8.1.0
EQURUZ	8.1.0
EYNXN2	8.1.0
F27G9V	8.1.0
GQ3JZL	8.1.0
H88C8U	8.1.0
HEPJ4T	8.1.0
JP4YCX	8.1.0
LWCVX9	8.1.0 /Root/build.prop
MU3MGV	8.1.0
N9JXHH	8.1.0
NGD4BJ	8.1.0
NZ9WWG	8.1.0
PB49XM	8.1.0
PGULYB	8.1.0
PLMMZP	8.1.0
Q29PVJ	8.1.0
Q99RM3	8.1.0
QGJU94	8.1.0
RCRKJC	8.1.0
TF4QLP	8.1.0
TPBP6E	8.1.0
U899KL	8.1.0
UEREJE	8.1.0
UYQHMY	8.1.0
V9V7DB	8.1.0
VA6BPD	8.1.0

TABLE 1

Question 3 - Acquisition / Device Information	
WebCode	Response
W2UCV3	8.1.0
W4KC78	OS Version 8.1.0
W4VZYW	Android 8.1.0
WAMHLA	8.1.0
WTZ4AC	8.1.0
XBWQEF	8.1.0
XFRN2L	8.1.0
YGFDWD	8.1.0
YK GK4G	8.1.0
ZVXNQ8	8.1.0

Question 3: What is the version of the Android operating system on this phone?

Consensus Result: 8.1.0

Expected Response Explanation:

The Android OS version is contained at line 11 in /Root/build.prop and is auto parsed by PA.

Expected Response Illustration:

OS Version

```

10 ro.build.version.all_codenames=REL
11 ro.build.version.release=8.1.0
12 ro.build.version.security_patch=201
    
```

OS Version

```

Mock Locations allowed      False
OS Version                  8.1.0      build.prop : 0x132
SIM Change Operation        3         SimCard.dat : 0x150
    
```


TABLE 1

Question 4 - Acquisition / Device Information

Question 4: What is the set time zone for this phone? Report in the following format: Country/City

Manufacturer's America/New_York

Expected Response:

WebCode	Response
2B66AE	America/New_York
2JDY68	America/New_York
3LWD98	America/New York
3VNPE9	America / New York
63XWWA	America/New York
69MBU4	America/New York
6EKPAN	America/ New York
6PRHA7	New_York (America)
74MLQ2	America/New York
77WBJY	America/New York
7RU3AB	America/New_York
82DV2X	America/New_York
82VLFW	America/New York
8CX7F4	New_York (America)
8EN7R9	America/New_York
8K97CZ	America/New_York
8NC4K8	America/New_York
8NNHGL	America / New York (UTC-05:00)
9ANFQZ	America/New_York
9CUZL3	(UTC-05:00) (America) / New_York
9XT88X	America/New_York
ABE2WW	America/New York
AD6282	America New York (UTC-05:00)
AEDEP3	America/New_York
B4AJ7X	(UTC-05:00) New_York (America)
BCMEEX	America/New York
BL9FU8	America/New York
C2JJVT	America/New York
C9ZCG4	America/New York

TABLE 1

Question 4 - Acquisition / Device Information	
WebCode	Response
CHMD3T	America/New York
CKDDDX	America/New York
CMH494	America/New York
D7AC7Y	America/New_York
EBZ32N	(UTC-05:00) America/New York
EHJ79Q	America/New York
EQURUZ	America/New York
EYNXN2	America/New York
F27G9V	(UTC-05:00) New_York (America)
GQ3JZL	America / New_York
H88C8U	America/New York
HEPJ4T	USA/New York
JP4YCX	America/New York
LWCVX9	America / New_York /Root/property/persist.sys.timezone
MU3MGV	America/New_York
N9JXHH	America/New_York
NGD4BJ	America / New York
NZ9WWG	USA/New York
PB49XM	America/New_York
PGULYB	America/New York
PLMMZP	America/New York
Q29PVJ	America/New York
Q99RM3	(UTC-05:00) New_York (America)
QGJU94	USA/New York
RCRKJC	America/New York
TF4QLP	America/New York
TPBP6E	America/ New_York
U899KL	(UTC-05:00) New_York (America)
UEREJE	America/New_York
UYQHMY	America/New York
V9V7DB	America/New_York
VA6BPD	America/NY

TABLE 1

Question 4 - Acquisition / Device Information	
WebCode	Response
W2UCV3	America/New York
W4KC78	America / New York
W4VZYW	America/New_York
WAMHLA	America/New York
WTZ4AC	America/New York
XBWQEF	America/New_York
XFRN2L	America/New_York
YGFDWD	(UTC-05:00) New_York (America)
YK GK4G	(America), New_York
ZVXNQ8	America/New York

Question 4: What is the set time zone for this phone? Report in the following format: Country/City

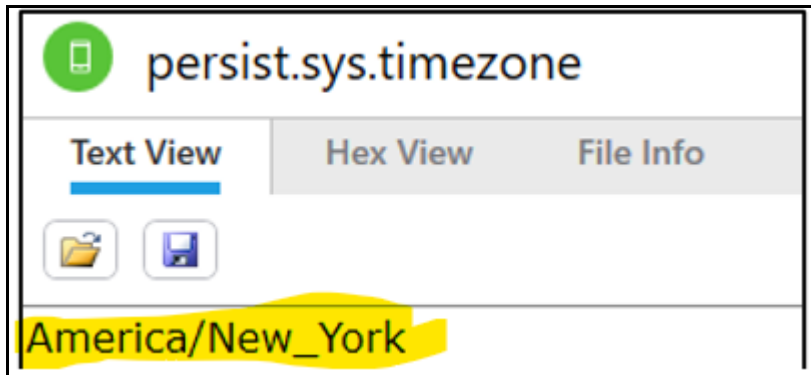
Consensus Result: America/New_York

Expected Response Explanation:

The set time zone for this phone is contained in /Root/property/persist.sys.timezone and is auto parsed by PA.

Expected Response Illustration:

Time Zone set for device



Time Zone set for device

SIM Change Operation	3	SimCard.oat : 0x150
Time Zone	(UTC-05:00) New_York (America)	persist.sys.timezone : 0x0
ICCID	8901260072996734294	com.android.phone.preferer

TABLE 1

Question 5 - Acquisition / Device Information

Question 5: What is the IMEI number associated with this phone?

Manufacturer's 356212106714588

Expected Response:

WebCode	Response
2B66AE	356212106714588
2JDY68	356212106714588
3LWD98	356212106714588
3VNPE9	SM2J260TZKATMK, which does not appear to be the IMEI as an IMEI is 15 digits and not alphanumeric. This was found in the following file path: EFS(ExtX)/Root/imei/prodcode.dat. If the question was asking for the IMSI, then the IMSI is 310260079673429
63XWWA	356212106714588
69MBU4	3527833548398814714
6EKPAN	356212106714588
6PRHA7	356212106714588
74MLQ2	356212106714588
77WBJY	356212106714588
7RU3AB	356212106714588
82DV2X	356212106714588
82VLFW	
8CX7F4	356212106714588
8EN7R9	356212106714588
8K97CZ	356212106714588
8NC4K8	356212106714588
8NNHGL	356212106714588
9ANFQZ	356212106714588
9CUZL3	356212106714588
9XT88X	356212106714588
ABE2WW	356212106714588
AD6282	
AEDEP3	356212106714588
B4AJ7X	N/A
BCMEEX	
BL9FU8	356212106714588
C2JJVT	356212106714588

TABLE 1

Question 5 - Acquisition / Device Information	
WebCode	Response
C9ZCG4	356212106714588
CHMD3T	356212106714588
CKDDDX	356212106714588
CMH494	356212106714588
D7AC7Y	356212106714588
EBZ32N	356212106714588
EHJ79Q	356212106714588
EQURUZ	356212106714588
EYNXN2	No Answer
F27G9V	356212106714588
GQ3JZL	35621210-671458-0
H88C8U	356212106714588
HEPJ4T	356212106714588
JP4YCX	310260079673429
LWCVX9	356212106714588 /Root/sec_efs/SVC
MU3MGV	356212106714588
N9JXHH	SM2J260TZKATMK
NGD4BJ	356212106714588
NZ9WWG	310260079673429
PB49XM	356212106714588
PGULYB	356212106714588
PLMMZP	356212106714588
Q29PVJ	356212106714588
Q99RM3	310260079673429 SM2J260TZKATMK
QGJU94	
RCRKJC	310260079673429
TF4QLP	This is beyond the scope of reporting
TPBP6E	not defined
U899KL	Not listed
UEREJE	SM2J260TZKATMK
UYQHMY	356212106714588
V9V7DB	356212106714588

TABLE 1

Question 5 - Acquisition / Device Information	
WebCode	Response
VA6BPD	356212106714588
W2UCV3	356212106714588
W4KC78	A traditional 15 digit decimal value IMEI was not located. The following value ASCII: SM2J260TZKATMK which is Hex: 534D324A323630545A4B41544D4B was located in the "prodcode.dat" file in the IMEI directory. The IMSI for this device was located and is: 310260079673429.
W4VZYW	356212106714588
WAMHLA	356212106714588
WTZ4AC	SM2J260TZKATMK
XBWQEF	356212106714588
XFRN2L	356212106714588
YGFDWD	356212106714588
YK GK4G	Neither Cellebrite nor Oxygen were able to recover an IMEI.
ZVXNQ8	356212106714588

Question 5: What is the IMEI number associated with this phone?

Consensus Result: 356212106714588

Expected Response Explanation:

The IMEI number associated with this phone is contained in USERDATA (ExtX)/Root/data/com.samsung.android.mobileservice/shared_prefs/coreapps_pref.xml. PA does not automatically parse this information. It can be found (in PA) by opening blk0_mmcbk0.bin in Hex View from "Memory Images" and using the "Find" tool to search for "IMEI". Several entries contain the IMEI. This information can also be found by using a forensic tool which does full text searching and indexing (second example is Autopsy).

Expected Response Illustration:

IMEI Number

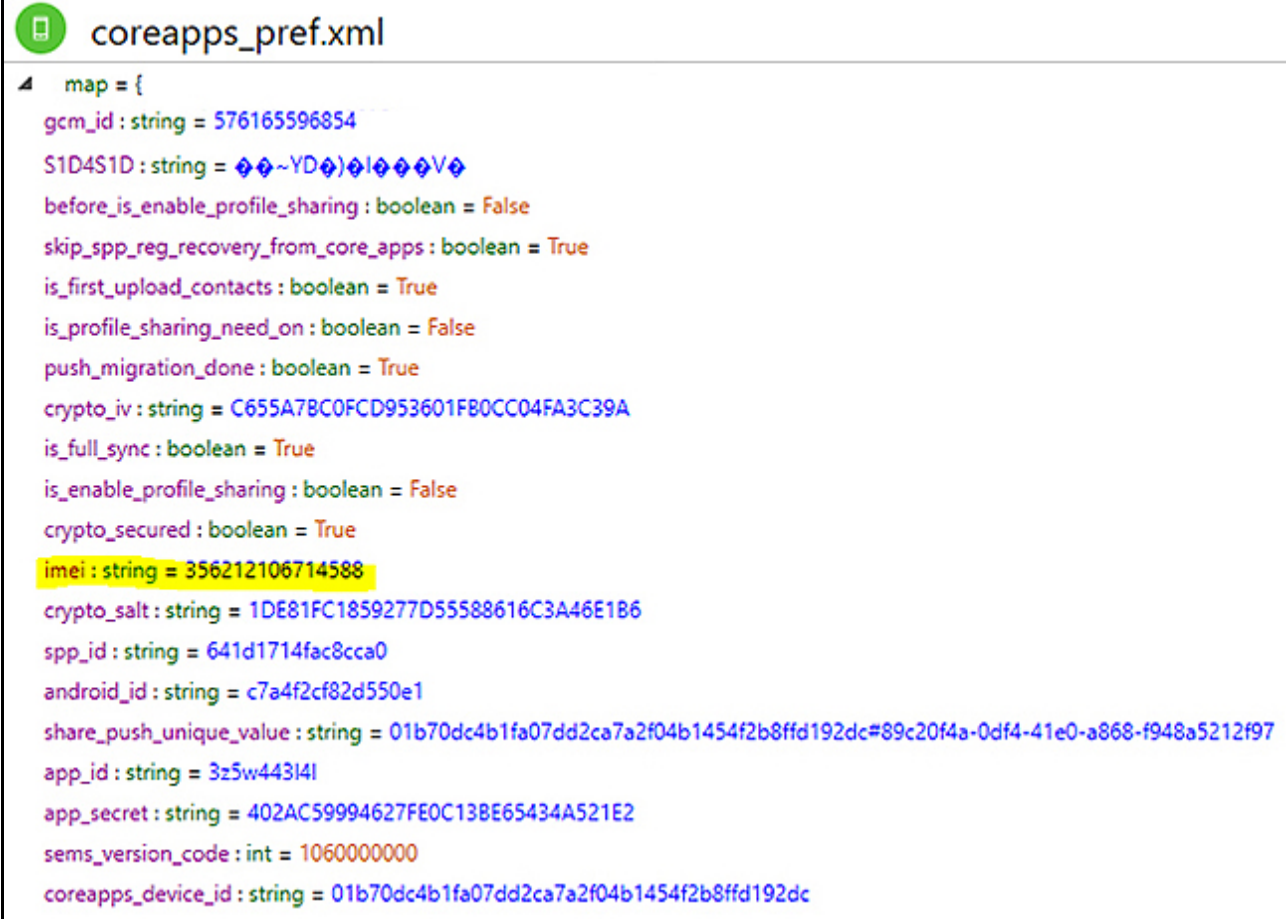
The screenshot shows a hex editor window titled "mmcbk0.bin". The main area displays hexadecimal data with corresponding ASCII values on the right. A search for "imei" has been performed, highlighting the following XML snippet in the ASCII view: `<string name="imei">356212106714588</string>`. Below the hex view, a table provides details for the search results:

Length	Value	Source	Mo
0x6	"imei"	/Root/data/com.samsung.android.mobileservice/shared_prefs/coreapps_pref.xml	

TABLE 1

Question 5 - Acquisition / Device Information

IMEI Number



```
coreapps_pref.xml
map = {
  gcm_id : string = 576165596854
  S1D4S1D : string = ~YD)lV
  before_is_enable_profile_sharing : boolean = False
  skip_spp_reg_recovery_from_core_apps : boolean = True
  is_first_upload_contacts : boolean = True
  is_profile_sharing_need_on : boolean = False
  push_migration_done : boolean = True
  crypto_iv : string = C655A7BC0FCD953601FB0CC04FA3C39A
  is_full_sync : boolean = True
  is_enable_profile_sharing : boolean = False
  crypto_secured : boolean = True
  imei : string = 356212106714588
  crypto_salt : string = 1DE81FC1859277D55588616C3A46E1B6
  spp_id : string = 641d1714fac8cca0
  android_id : string = c7a4f2cf82d550e1
  share_push_unique_value : string = 01b70dc4b1fa07dd2ca7a2f04b1454f2b8ffd192dc#89c20f4a-0df4-41e0-a868-f948a5212f97
  app_id : string = 3z5w44314l
  app_secret : string = 402AC59994627FE0C13BE65434A521E2
  sems_version_code : int = 1060000000
  coreapps_device_id : string = 01b70dc4b1fa07dd2ca7a2f04b1454f2b8ffd192dc
```

TABLE 1

Question 6 - Acquisition / Device Information	
---	--

Question 6: Provide the Device Phone Number (MSISDN).

Manufacturer's 15718351874

Expected Response:

WebCode	Response
2B66AE	15718351874
2JDY68	15718351874
3LWD98	15718351874
3VNPE9	1 (571) 835-1874
63XWWA	15718351874
69MBU4	1 571-835-1874
6EKPAN	15718351874
6PRHA7	1-571-835-1874
74MLQ2	15718351874
77WBJY	5718351874
7RU3AB	15718351874
82DV2X	15718351874
82VLFW	15718351874
8CX7F4	15718351874
8EN7R9	15718351874
8K97CZ	15718351874
8NC4K8	15718351874
8NNHGL	15718351874
9ANFQZ	15718351874
9CUZL3	15718351874
9XT88X	15718351874
ABE2WW	15718351874
AD6282	15718351874
AEDEP3	15718351874
B4AJ7X	15718351874
BCMEEEX	1 571 835 1874
BL9FU8	15718351874
C2JJVT	15718351874
C9ZCG4	15718351874

TABLE 1

Question 6 - Acquisition / Device Information	
WebCode	Response
CHMD3T	15718351874
CKDDDX	15718351874
CMH494	1-571-835-1874 or 571-835-1874 or 15718351874 or 5718351874
D7AC7Y	1-571-835-1874
EBZ32N	15718351874
EHJ79Q	15718351874
EQURUZ	15718351874
EYNXN2	15718351874
F27G9V	15718351874
GQ3JZL	15718351874
H88C8U	571-835-1874
HEPJ4T	15718351874
JP4YCX	1-571-835-1874
LWCVX9	15718351874
MU3MGV	15718351874
N9JXHH	1-571-835-1874
NGD4BJ	1 571-835-1874
NZ9WWG	5718351874
PB49XM	15718351874
PGULYB	15718351874
PLMMZP	1-571-835-1874
Q29PVJ	15718351874
Q99RM3	15718351874
QGJU94	15718351874
RCRKJC	15718351874
TF4QLP	15718351874
TPBP6E	not defined
U899KL	15718351874
UEREJE	1-571-835-1874
UYQHMY	15718351874
V9V7DB	15718351874
VA6BPD	15718351874

TABLE 1

Question 6 - Acquisition / Device Information	
WebCode	Response
W2UCV3	15718351874
W4KC78	15718351874
W4VZYW	15718351874
WAMHLA	15718351874
WTZ4AC	571 835 1874
XBWQEF	15718351874
XFRN2L	15718351874
YGFDWD	15718351874
YK GK4G	(1)571-835-1874
ZVXNQ8	15718351874

Question 6: Provide the Device Phone Number (MSISDN).

Consensus Result: 15718351874

Expected Response Explanation:

The MSISDN is contained in /Root/system/SimCard.dat and is auto parsed by PA.

Expected Response Illustration:

MSISDN

Current Sim Operator	310200	SimCard.dat : 0xb3
Current SIM Phone Number	15718351874	SimCard.dat : 0x115
Detected Phone Model	SM-J260T1	build.prop : 0x2C2

TABLE 1

Question 7 - Acquisition / Device Information	
---	--

Question 7: What is the language/locale setting for this phone?

Manufacturer's en_US

Expected Response:

WebCode	Response
2B66AE	en_US/ en_US
2JDY68	locale = en-US
3LWD98	en-US
3VNPE9	English_US
63XWWA	En_US
69MBU4	en_US
6EKPAN	en_US
6PRHA7	en_US
74MLQ2	en/US
77WBJY	en_US
7RU3AB	English/US
82DV2X	en_US
82VLFW	en-US
8CX7F4	en_US
8EN7R9	en_US
8K97CZ	en_US
8NC4K8	en_US
8NNHGL	en_US (English/United States)
9ANFQZ	en_US
9CUZL3	En_US
9XT88X	en_US
ABE2WW	en_US
AD6282	en-US
AEDEP3	en_US
B4AJ7X	N/A
BCMEEEX	en-US
BL9FU8	en_US
C2JJVT	en-US
C9ZCG4	en_US

TABLE 1

Question 7 - Acquisition / Device Information	
WebCode	Response
CHMD3T	en_US
CKDDDX	EN_US
CMH494	en_US or English
D7AC7Y	en_US
EBZ32N	en_US
EHJ79Q	en_US
EQURUZ	en - US
EYNXN2	en_us
F27G9V	en_US
GQ3JZL	en_US
H88C8U	en_US
HEPJ4T	en-US
JP4YCX	en_us
LWCVX9	en-US
MU3MGV	English/US
N9JXHH	en-US
NGD4BJ	English / US
NZ9WWG	En-US
PB49XM	en_US
PGULYB	en_US
PLMMZP	en_US
Q29PVJ	en_US
Q99RM3	En_US
QGJU94	English/US
RCRKJC	en_US
TF4QLP	en_US (English US)
TPBP6E	English - US
U899KL	us
UEREJE	en_us English
UYQHMY	English/US
V9V7DB	en-US
VA6BPD	en-US

TABLE 1

Question 7 - Acquisition / Device Information	
WebCode	Response
W2UCV3	en_US
W4KC78	English/ en_US
W4VZYW	en-US
WAMHLA	EN/US
WTZ4AC	English (en_us)
XBWQEF	en_US
XFRN2L	en-US
YGFDWD	English US
YK GK4G	en_US
ZVXNQ8	en/US

Question 7: What is the language/locale setting for this phone?

Consensus Result: en_US

Expected Response Explanation:

The language setting for this phone is located in /SYSTEM/Root/build.prop:0x4B1.

Expected Response Illustration:

Language Setting

```
ro.product.locale=en-US
```

TABLE 1

Question 8 - Acquisition / Device Information	
---	--

Question 8: Provide the primary Google account (email address) associated with this phone.

Manufacturer's allengonzo79@gmail.com

Expected Response:

WebCode	Response
2B66AE	allengonzo79@gmail.com
2JDY68	allengonzo79@gmail.com
3LWD98	allengonzo79@gmail.com
3VNPE9	allengonzo79@gmail.com
63XWWA	allengonzo79@gmail.com
69MBU4	allengonzo79@gmail.com
6EKPAN	allengonzo79@gmail.com
6PRHA7	allengonzo79@gmail.com
74MLQ2	allengonzo79@gmail.com
77WBJY	allengonzo79@gmail.com
7RU3AB	allengonzo79@gmail.com
82DV2X	allengonzo79@gmail.com
82VLFW	allengonzo79@gmail.com
8CX7F4	allengonzo79@gmail.com
8EN7R9	allengonzo79@gmail.com
8K97CZ	allengonzo79@gmail.com
8NC4K8	allengonzo79@gmail.com
8NNHGL	allengonzo79@gmail.com
9ANFQZ	allengonzo79@gmail.com
9CUZL3	allengonzo79@gmail.com
9XT88X	allengonzo79@gmail.com
ABE2WW	allengonzo79@gmail.com
AD6282	allengonzo79@gmail.com
AEDEP3	allengonzo79@gmail.com
B4AJ7X	allengonzo79@gmail.com
BCMEEX	allengonzo79@gmail.com
BL9FU8	allengonzo79@gmail.com
C2JJVT	allengonzo79@gmail.com
C9ZCG4	allengonzo79@gmail.com

TABLE 1

Question 8 - Acquisition / Device Information	
WebCode	Response
CHMD3T	allengonzo79@gmail.com
CKDDDX	allengonzo79@gmail.com
CMH494	allengonzo79@gmail.com
D7AC7Y	allengonzo79@gmail.com
EBZ32N	allengonzo79@gmail.com
EHJ79Q	allengonzo79@gmail.com
EQURUZ	allengonzo79@gmail.com
EYNXN2	allengonzo79@gmail.com
F27G9V	allengonzo79@gmail.com
GQ3JZL	allengonzo79@gmail.com
H88C8U	allengonzo79@gmail.com
HEPJ4T	allengonzo79@gmail.com
JP4YCX	ALLENGONZO79@GMAIL.COM
LWCVX9	allengonzo79@gmail.com
MU3MGV	allengonzo79@gmail.com
N9JXHH	allengonzo79@gmail.com
NGD4BJ	allengonzo79@gmail.com
NZ9WWG	allengonzo79@gmail.com
PB49XM	allengonzo79@gmail.com
PGULYB	allengonzo79@gmail.com
PLMMZP	allengonzo79@gmail.com
Q29PVJ	allengonzo79@gmail.com
Q99RM3	allengonzo79@gmail.com
QGJU94	allengonzo79@gmail.com
RCRKJC	allengonzo79@gmail.com
TF4QLP	allengonzo79@gmail.com
TPBP6E	allengonzo79@gmail.com
U899KL	allengonzo79@gmail.com
UEREJE	allengonzo79@gmail.com
UYQHMY	allengonzo79@gmail.com
V9V7DB	allengonzo79@gmail.com
VA6BPD	allengonzo79@gmail.com

TABLE 1

Question 8 - Acquisition / Device Information	
WebCode	Response
W2UCV3	allengonzo79@gmail.com
W4KC78	allengonzo79@gmail.com
W4VZYW	allengonzo79@gmail.com
WAMHLA	allengonzo79@gmail.com
WTZ4AC	allengonzo79@gmail.com
XBWQEF	allengonzo79@gmail.com
XFRN2L	allengonzo79@gmail.com
YGFDWD	allengonzo79@gmail.com
YK GK4G	allengonzo79@gmail.com
ZVXNQ8	allengonzo79@gmail.com

Question 8: Provide the primary Google account (email address) associated with this phone.

Consensus Result: allengonzo79@gmail.com

Expected Response Explanation:

The primary Google account associated with this phone is contained in USERDATA/Root/system_ce/0/accounts_ce.db:0x3F01.

Expected Response Illustration:

Primary Google Account

<input checked="" type="checkbox"/>	Allen Gonzales	allengonzo79@gmail.com	com.google	vNeEXjj8=
<input type="checkbox"/>		allengonzo79@gmail.com	com.google	Creation time:
<input type="checkbox"/>		allengonzo79@gmail.com	com.google	Service Type: com.google
<input type="checkbox"/>		allengonzo79@gmail.com	com.google	Server Address:
<input type="checkbox"/>	Allen Gonzales	allengonzo79@gmail.com	com.google	Source:
<input type="checkbox"/>				Extraction: Physical
<input checked="" type="checkbox"/>	Allen Gonzales	allengonzo79@gmail.com		Source file: USERDATA (ExtX)/Root/system_ce/0/accounts_ce.db : 0x3F01 (Table: accounts, 180224 bytes)
<input checked="" type="checkbox"/>	Allen Gonzales	allengonzo79		

TABLE 1

Question 9 - Acquisition / Device Information

Question 9: What is the name of the WiFi hotspot connected to by this phone on December 10, 2019?

Manufacturer's FlyReagan

Expected Response:

WebCode	Response
2B66AE	"FlyReagan"
2JDY68	FlyReagan
3LWD98	FlyReagan
3VNPE9	FlyReagan
63XWWA	FlyReagan
69MBU4	FlyReagan
6EKPAN	FlyReagan
6PRHA7	FlyReagan
74MLQ2	FlyReagan
77WBJY	FlyReagan
7RU3AB	FlyReagan
82DV2X	FlyReagan
82VLFW	FlyReagan
8CX7F4	FlyReagan
8EN7R9	FlyReagan
8K97CZ	FlyReagan
8NC4K8	FlyReagan
8NNHGL	FlyReagan
9ANFQZ	FlyReagan
9CUZL3	FlyReagan
9XT88X	FlyReagan
ABE2WW	FlyReagan
AD6282	FlyReagan
AEDEP3	FlyReagan
B4AJ7X	N/A
BCMEEEX	FlyReagan
BL9FU8	FlyReagan
C2JJVT	FlyReagan
C9ZCG4	FlyReagan

TABLE 1

Question 9 - Acquisition / Device Information	
WebCode	Response
CHMD3T	Fly Reagan
CKDDDX	FlyReagan
CMH494	FlyReagan
D7AC7Y	FlyReagan
EBZ32N	"FlyReagan"
EHJ79Q	"FlyReagan"
EQURUZ	FlyReagan
EYNXN2	No Answer
F27G9V	FlyReagan
GQ3JZL	FlyReagan
H88C8U	FlyReagan
HEPJ4T	FlyReagan
JP4YCX	FLY REAGAN
LWCVX9	FlyReagan USERDATA (ExtX)/Root/system/wifigeofence.db
MU3MGV	FlyReagan
N9JXHH	FlyReagan
NGD4BJ	FlyReagan
NZ9WWG	FlyReagan
PB49XM	FlyReagan
PGULYB	FlyReagan
PLMMZP	FlyReagan
Q29PVJ	FlyReagan
Q99RM3	FlyReagan
QGJU94	
RCRKJC	FlyReagan
TF4QLP	This is beyond the scope of reporting
TPBP6E	FlyReagan
U899KL	FlyReagan
UEREJE	FlyReagan
UYQHMY	"FlyReagan"
V9V7DB	FlyReagan
VA6BPD	FlyReagan

TABLE 1

Question 9 - Acquisition / Device Information	
WebCode	Response
W2UCV3	FlyReagan
W4KC78	FlyReagan
W4VZYW	FlyReagan
WAMHLA	FlyReagan
WTZ4AC	FlyReagan
XBWQEF	FlyReagan
XFRN2L	FlyReagan
YGFDWD	FlyReagan
YK GK4G	"FlyReagan"
ZVXNQ8	FlyReagan

Question 9: What is the name of the WiFi hotspot connected to by this phone on December 10, 2019?

Consensus Result: FlyReagan

Expected Response Explanation:

The name of the Wifi hotspot is contained in /USERDATA (ExtX)/Root/system/wifigeofence.db.

Expected Response Illustration:

Wifi Connections

wifigeofence.db						
Database View						
geofence_wifi (7)						
_id	location_id	network_id	config_key	bssid	time	
7	7	6	"_ Free LGA WiFi"NONE		12/11/2019 3:47:51 PM	
6	6	5	"FlyReagan"NONE		12/10/2019 8:38:26 PM	
5	5	4	"McDonalds Free WiFi"NONE		12/5/2019 6:27:47 PM	
4	4	3	"GSP-Public-WiFi"NONE		12/5/2019 2:54:34 PM	
3	3	2	"Fairfield_GUEST"NONE		12/5/2019 12:42:31 PM	
2	2	1	"Hilton Honors"NONE		12/5/2019 11:28:03 AM	
1	1	0	"FlyDulles"NONE		12/5/2019 5:01:15 PM	

TABLE 1

Question 10 - Acquisition / Device Information

Question 10: What was the last date and time the phone was connected to the "_Free LGA WiFi" hotspot? Provide your response in the time zone set for the device using the following format: MM/DD/YYYY, HH:MM AM/PM

Manufacturer's 12/11/2019 10:47 AM

Expected Response:

WebCode	Response
2B66AE	12/11/2019, 10:47 AM
2JDY68	12/11/2019 10:47 AM
3LWD98	12/11/2019 10:47 AM
3VNPE9	12/11/2019, 10:47 AM
63XWWA	11/12/2019 10:47 AM
69MBU4	12/11/2019 10:47 PM
6EKPAN	12/11/2019 10:47 AM
6PRHA7	12/11/2019 3:47 PM
74MLQ2	11.11.2019 10:47 AM
77WBJY	12/11/2019, 10:47 AM
7RU3AB	12/11/2019, 10:47 AM
82DV2X	12/11/2019, 10:47 AM
82VLFW	12/11/2019 10:47 AM
8CX7F4	12/11/2019 10:47 AM
8EN7R9	12/11/2019, 03:47 PM
8K97CZ	12/11/2019, 10:47 AM
8NC4K8	12/11/2019 10:47 AM
8NNHGL	12/11/2019, 10:47 AM
9ANFQZ	12/11/2019 10:47 AM
9CUZL3	12/11/2019, 10:47:51(UTC-5) AM
9XT88X	12/11/2019, 10:47 AM
ABE2WW	12/11/2019, 10:47 AM
AD6282	11/12/2019 10:47AM
AEDEP3	12/11/2019, 10:47 AM
B4AJ7X	N/A
BCMEEX	12/11/2019, 10:47 AM
BL9FU8	12/11/2019, 10:47 AM
C2JJVT	12/11/2019, 3:47 PM

TABLE 1

Question 10 - Acquisition / Device Information	
WebCode	Response
C9ZCG4	12/11/2019 10:47 AM
CHMD3T	12/11/2019 10:47 AM
CKDDDX	12/11/2019 10:47 AM
CMH494	12/11/2019 10:47 AM
D7AC7Y	12/11/2019 10:47 AM
EBZ32N	12/11/2019, 10:47 AM (UTC-5)
EHJ79Q	12/11/2019, 10:47 AM(UTC-5)
EQURUZ	12/11/2019 15:47 PM
EYNXN2	No Answer
F27G9V	12/11/2019, 10:47 AM
GQ3JZL	12/11/2019, 10:47 AM
H88C8U	12/11/2019, 10:47 AM
HEPJ4T	12/11/2019, 10:47 AM
JP4YCX	12/11/2019 10:47 AM
LWCVX9	12/11/2019, 10:47 AM misc\wifi\WifiConfigStore.xml
MU3MGV	12/11/2019, 10:47 AM
N9JXHH	12/11/2019, 10:47 AM
NGD4BJ	12/11/2019, 10:47 AM
NZ9WWG	12/11/2019, 10:47 AM
PB49XM	12/11/2019, 10:47 AM
PGULYB	12/11/2019, 10:47 AM
PLMMZP	12/11/2019, 10:47 AM
Q29PVJ	12/11/2019, 10:47 AM
Q99RM3	12/11/2019 10:47:46 pm
QGJU94	
RCRKJC	12/11/2019, 10:47 AM
TF4QLP	This is beyond the scope of reporting
TPBP6E	12/11/2019, 03:47 PM
U899KL	12/11/2019 10:47:51 AM(UTC-5)
UEREJE	12/11/2019 10:47 AM (-5 UTC)
UYQHMY	11/12/2019 15:47 PM
V9V7DB	12/11/2019, 10:47 AM

TABLE 1

Question 10 - Acquisition / Device Information	
WebCode	Response
VA6BPD	12/11/2019, 10:47 AM
W2UCV3	12/11/2019, 10:47 AM
W4KC78	12/11/2019, 10:47 AM
W4VZYW	12/11/2019, 10:47 AM
WAMHLA	12/11/2019 03:47 PM
WTZ4AC	12/11/2019 10:47 AM (-05:00 UTC)
XBWQEF	12/11/2019, 03:47 PM
XFRN2L	12/11/2019, 10:47 AM
YGFDDW	12/11/2019 15:47 PM
YK GK4G	12/11/2019 10:47 AM (UTC-5)
ZVXNQ8	12/11/2019, 10:47 AM

Question 10: What was the last date and time the phone was connected to the "_Free LGA WiFi" hotspot? Provide your response in the time zone set for the device using the following format: MM/DD/YYYY, HH:MM AM/PM

Consensus Result: 12/11/2019 10:47 AM and all formatting styles which represent the same information. In addition, the same date with the time 03:47 PM which represents the same time but in UTC+0 was also accepted. Seconds were not part of the time format requested, therefore reported seconds are not being evaluated.

Expected Response Explanation:

Information regarding the last date and time this phone was connected to a specific hotspot is contained in /USERDATA (ExtX)/Root/misc/wifi/WifiConfigStore.xml. The connection time is stored as GMT unix timestamp in milliseconds :1576079271184 and must be converted using a tool (e.g Cellebrite or excel).

Expected Response Illustration:

WifiConfigStore

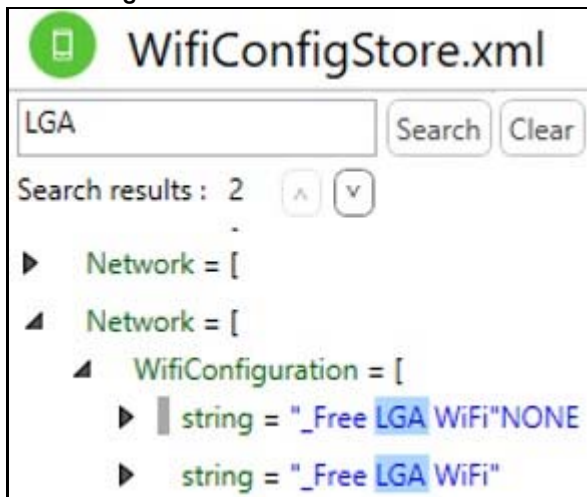


TABLE 1

Question 10 - Acquisition / Device Information

WifiConfigStore

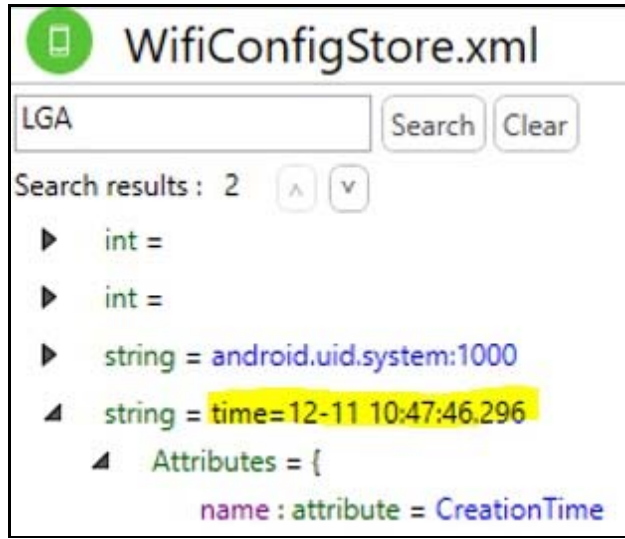


TABLE 1

Question 11 - Acquisition / Device Information

Question 11: What is the name of the paired bluetooth device with MAC Address 98:D3:31:FC:1B:64?

Manufacturer's SKMR13

Expected Response:

WebCode	Response
2B66AE	SKMR13
2JDY68	SKMR13
3LWD98	SKMR13
3VNPE9	SKMR13
63XWWA	SKMR13
69MBU4	SKMR13
6EKPAN	SKMR13
6PRHA7	SKMR13
74MLQ2	SKMR13
77WBJY	SKMR13
7RU3AB	SKMR13
82DV2X	SKMR13
82VLFW	SKMR13
8CX7F4	Serial Bluetooth Terminal
8EN7R9	SKMR13
8K97CZ	SKMR13
8NC4K8	SKMR13
8NNHGL	SKMR13
9ANFQZ	SKMR13
9CUZL3	SKMR13
9XT88X	SKMR13
ABE2WW	SKMR13
AD6282	SKMR13
AEDEP3	SKMR13
B4AJ7X	Galaxy J2
BCMEEEX	SKMR13
BL9FU8	SKMR13
C2JJVT	SKMR13
C9ZCG4	SKMR13

TABLE 1

Question 11 - Acquisition / Device Information	
WebCode	Response
CHMD3T	SKMR13
CKDDDX	SKMR13
CMH494	SKMR13
D7AC7Y	Serial Bluetooth Terminal
EBZ32N	SKMR13
EHJ79Q	SKMR13
EQURUZ	SKMR13
EYNXN2	SKMR13
F27G9V	SKMR13
GQ3JZL	SKMR13
H88C8U	SKMR13
HEPJ4T	SKMR13
JP4YCX	SKMR13
LWCVX9	SKMR13 misc\bluedroid\bt_config.conf
MU3MGV	SKMR13
N9JXHH	SKMR13
NGD4BJ	SKMR13
NZ9WWG	SKMR2
PB49XM	Serial Bluetooth Terminal
PGULYB	SKMR13
PLMMZP	SKMR13
Q29PVJ	SKMR13
Q99RM3	SKMR13
QGJU94	SKMR13
RCRKJC	SKMR13
TF4QLP	SKMR13
TPBP6E	SKMR13
U899KL	None located
UEREJE	SKMR13
UYQHMY	SKMR13
V9V7DB	SKMR13
VA6BPD	SKMR13

TABLE 1

Question 11 - Acquisition / Device Information	
WebCode	Response
W2UCV3	SKMR13
W4KC78	SKMR13
W4VZYW	SKMR13
WAMHLA	SKMR13
WTZ4AC	SKMR13
XBWQEF	SKMR13
XFRN2L	SKMR13
YGFDWD	SKMR13
YK GK4G	SKMR13
ZVXNQ8	SKMR13

Question 11: What is the name of the paired bluetooth device with MAC Address 98:D3:31:FC:1B:64?

Consensus Result: SKMR13

Expected Response Explanation:

Bluetooth pairing information is contained in /USERDATA (ExtX)/Root/user_de/0/com.android.bluetooth/databases/bonddevice.db and in USERDATA (ExtX)/Root/misc/bluedroid/bt_config.conf.

Expected Response Illustration:

Paired Bluetooth Device Name

bonddevice (7)								
event_id	address	name	cod	bond_state	appear	manu	date	link
7	98:D3:31:FC:1C:AC	SKMR4	7936	2	0		1576340080184	1
6	98:D3:71:FD:9A:B6	SKMR9	7936	2	0		1576339551775	1
5	98:D3:71:FD:9A:2A	SKMR5	7936	2	0		1576339119464	1
4	98:D3:31:FC:1B:64	SKMR13	7936	2	0		1576338559617	1
3	98:D3:11:FC:21:B8	SKMR2	7936	2	0		1576337874210	1
2	98:D3:11:FC:22:AE	SKMR1	7936	2	0		1576336224106	1
1	00:FA:21:05:6C:4D			101				

TABLE 1

Question 11 - Acquisition / Device Information

Paired Bluetooth Device Name

bt_config.conf		
Hex View	File Info	
000003c2	4c 69 6e 6b 4b 65 79 54 79 70 65 20 3d 20 30 0a 50 69 6e 4c 65 6e 67 74	LinkKeyType = 0.PinLength = 4.Link
000003e7	20 3d 20 61 65 30 66 61 33 35 31 61 39 36 64 35 66 66 35 64 64 30 37 63	= ae0fa351a96d5ff5dd07c2851e11fd1
0000040c	62 31 37 33 32 62 30 32 32 30 34 63 34 30 36 66 37 39 30 31 38 38 35 33	b1732b02204c406f790188535cba12.Rol
00000431	20 31 0a 4c 69 6e 6b 54 79 70 65 20 3d 20 31 0a 4d 61 6e 75 66 61 63 74	1.LinkType = 1.Manufacturer = 10.
00000456	56 65 72 20 3d 20 34 0a 4c 6d 70 53 75 62 56 65 72 20 3d 20 35 39 34 31	Ver = 4.LmpSubVer = 5941.Service =
0000047b	30 30 31 31 30 31 2d 30 30 30 30 2d 31 30 30 30 2d 38 30 30 30 2d 30 30	001101-0000-1000-8000-00805f9b34fb
00004a0	5b 39 38 3a 64 33 3a 33 31 3a 66 63 3a 31 62 3a 36 34 5d 0a 54 69 6d 65	[98:d3:31:fc:1b:64].Timestamp = 15'
00004c5	33 38 35 35 33 0a 44 65 76 43 6c 61 73 73 20 3d 20 37 39 33 36 0a 44 65	38553.DevClass = 7936.DevType = 1.
00004ea	72 54 79 70 65 20 3d 20 30 0a 4e 61 6d 65 20 3d 20 53 4b 4d 52 31 33 0a	rType = 0.Name = SKMR13.LinkKeyTyp
000050f	20 30 0a 50 69 6e 4c 65 6e 67 74 68 20 3d 20 34 0a 4c 69 6e 6b 4b 65 79	0.PinLength = 4.LinkKey = e3e888a

TABLE 1

Question 12 - Phone / Messaging

Question 12: What is the name of the (non-Gmail) email client installed by the user?

Manufacturer's K-9 Mail

Expected Response:

WebCode	Response
2B66AE	K-9 Mail
2JDY68	K-9 Mail
3LWD98	K-9 Mail
3VNPE9	K-9 Mail
63XWWA	K-9 Mail
69MBU4	Samsung email
6EKPAN	K-9 mail
6PRHA7	Samsung Email
74MLQ2	K-9 Mail
77WBJY	K-9 Mail
7RU3AB	K-9 Mail
82DV2X	K-9 Mail
82VLFW	K-9 Mail
8CX7F4	K-9 mail
8EN7R9	K-9 Mail
8K97CZ	K-9 Mail
8NC4K8	K-9 Mail
8NNHGL	K-9 Mail (com.fsck.k9)
9ANFQZ	K-9 Mail
9CUZL3	K-9
9XT88X	K-9 Mail
ABE2WW	K-9 Mail
AD6282	k-9 mail
AEDEP3	K-9 Mail
B4AJ7X	N/A
BCMEEEX	K-9 Mail
BL9FU8	K-9 Mail
C2JJVT	K-9 Mail
C9ZCG4	K9 Mail

TABLE 1

Question 12 - Phone / Messaging	
WebCode	Response
CHMD3T	K-9 Mail
CKDDDX	K-9 Mail
CMH494	K-9 Mail
D7AC7Y	K-9 Mail
EBZ32N	Samsung Email
EHJ79Q	Samsung Email
EQURUZ	K-9 Mail
EYNXN2	K9 Mail
F27G9V	K-9 Mail
GQ3JZL	K-9 Mail
H88C8U	K-9 Mail
HEPJ4T	K-9 Mail
JP4YCX	K9 MAIL
LWCVX9	K-9 Mail
MU3MGV	15718351874@s.whatsapp.net
N9JXHH	Samsung Email
NGD4BJ	K-9 Mail
NZ9WWG	K-9 Mail
PB49XM	K-9 Mail
PGULYB	K-9 Mail
PLMMZP	K-9 Mail
Q29PVJ	K-9 Mail
Q99RM3	K-9 Mail
QGJU94	K-9 Mail
RCRKJC	K-9 Mail
TF4QLP	Samsung Email
TPBP6E	K9-Mail
U899KL	Samsung Email
UEREJE	K-9 Mail com.fsck.k9
UYQHMY	K-9 Mail
V9V7DB	K-9 Mail
VA6BPD	K-9 Mail

TABLE 1

Question 12 - Phone / Messaging	
WebCode	Response
W2UCV3	K-9 Mail
W4KC78	K-9 mail
W4VZYW	K-9 Mail
WAMHLA	K-9 Mail
WTZ4AC	K-9 Mail (com.fsck.k9)
XBWQEF	K-9 Mail
XFRN2L	K-9 Mail
YGFDWD	K-9 Mail (com.fsck.k9)
YK GK4G	K9-Mail
ZVXNQ8	K-9 Mail

Question 12: What is the name of the (non-Gmail) email client installed by the user?

Consensus Result: K-9 Mail

Expected Response Explanation:

Information about installed applications is contained in /USERDATA (ExtX)/Root/data/com.android.vending/databases/localappstate.db. A review of this database for records related to email applications shows Gmail, Samsung Email, and K-9 Mail. The Samsung Email is installed by default.

Expected Response Illustration:

Email Applications

Decoded by	Name	Version	Descr	Identifier
	Samsung Email	6.1.01.0		com.samsung.android.ema..
Cellebrite	Gmail	2019.11.03....		com.google.android.gm
	K-9 Mail	5.600		com.fsck.k9
		8.9.9.21335...		Gmail2

Other Responses:

Seven participants reported "Samsung Email" which is installed by default not specifically by the user.

TABLE 1

Question 13 - Phone / Messaging

Question 13: What version is the (non-Gmail) email client installed by the user?

Manufacturer's 5.6

Expected Response:

WebCode	Response
2B66AE	5.600
2JDY68	Version 5.600
3LWD98	5.600
3VNPE9	5.600
63XWWA	5.600
69MBU4	6.1.01.0
6EKPAN	5.600
6PRHA7	6.1.01.0
74MLQ2	5.600
77WBJY	5.600
7RU3AB	5.600 (26000)
82DV2X	5.600
82VLFW	5.600
8CX7F4	5.600
8EN7R9	5.600
8K97CZ	5.600
8NC4K8	5.600
8NNHGL	5.600
9ANFQZ	5.600
9CUZL3	6.0.02.10
9XT88X	5.600
ABE2WW	5.600
AD6282	5.600
AEDEP3	5.600
B4AJ7X	N/A
BCMEEEX	5.600
BL9FU8	5.600
C2JJVT	5.600
C9ZCG4	5.600

TABLE 1

Question 13 - Phone / Messaging	
WebCode	Response
CHMD3T	5.600
CKDDDX	5.600
CMH494	5.600
D7AC7Y	5.600
EBZ32N	6.0.02.10
EHJ79Q	6.0.02.10
EQURUZ	5.600
EYNXN2	26000
F27G9V	K-9 Mail_Version 5.600
GQ3JZL	5.600
H88C8U	5.600
HEPJ4T	5.600
JP4YCX	5.600
LWCVX9	5.600
MU3MGV	2.19.341
N9JXHH	6.1.01.0
NGD4BJ	5.600
NZ9WWG	6.0.02.10
PB49XM	5.600
PGULYB	5.600
PLMMZP	5.600
Q29PVJ	5.600
Q99RM3	5.600
QGJU94	5.600
RCRKJC	5.600
TF4QLP	6.1.01.0
TPBP6E	5.600
U899KL	6.0.02.10
UEREJE	5.600
UYQHMY	5.600
V9V7DB	5.600
VA6BPD	5.600

TABLE 1

Question 13 - Phone / Messaging	
WebCode	Response
W2UCV3	5.600
W4KC78	5.600
W4VZYW	5.600 (android:versionName)
WAMHLA	5.600
WTZ4AC	version 5.600
XBWQEF	5.600
XFRN2L	5600
YGFDWD	5.600
YK GK4G	5.600
ZVXNQ8	5.600

Question 13: What version is the (non-Gmail) email client installed by the user?

Consensus Result: 5.6

Expected Response Explanation:

Information about installed applications is contained in the following database:
 /USERDATA (ExtX)/Root/data/com.android.vending/databases/localappstate.db

Expected Response Illustration:

Email Applications

Decoded by	Name	Version	Description	Identifier	App
	Samsung Email	6.1.01.0		com.samsung.android.ema...	
Cellebrite	Gmail	2019.11.03...		com.google.android.gm	
	K-9 Mail	5.600		com.fsck.k9	
		8.9.9.21335...		Gmail2	

TABLE 1

Question 14 - Phone / Messaging

Question 14: How many SMS messages were received from the phone number associated with the contact listed as "Francis Milligan"? Provide response using the numeric format.

Manufacturer's 6

Expected Response:

WebCode	Response
2B66AE	6
2JDY68	6
3LWD98	6
3VNPE9	6 unique SMS messages. The forensic tool used displayed quadruplicate of the SMS messages observed, totaling to 24 SMS messages. The total 24 SMS messages include the 6 unique SMS messages.
63XWWA	6
69MBU4	6
6EKPAN	6
6PRHA7	6
74MLQ2	6
77WBJY	6
7RU3AB	6
82DV2X	6
82VLFW	6
8CX7F4	6
8EN7R9	6
8K97CZ	6
8NC4K8	6
8NNHGL	6
9ANFQZ	6
9CUZL3	6
9XT88X	6
ABE2WW	6
AD6282	18
AEDEP3	6
B4AJ7X	24
BCMEEEX	6
BL9FU8	6
C2JJVT	6

TABLE 1

Question 14 - Phone / Messaging	
WebCode	Response
C9ZCG4	6
CHMD3T	6
CKDDDX	6
CMH494	6
D7AC7Y	6
EBZ32N	6
EHJ79Q	6
EQURUZ	6
EYNXN2	18
F27G9V	6
GQ3JZL	6
H88C8U	6
HEPJ4T	6
JP4YCX	6
LWCVX9	18
MU3MGV	6
N9JXHH	6
NGD4BJ	6
NZ9WWG	6
PB49XM	6
PGULYB	6
PLMMZP	6
Q29PVJ	6
Q99RM3	6
QGJU94	6
RCRKJC	6
TF4QLP	6
TPBP6E	6
U899KL	6
UEREJE	6
UYQHMY	6
V9V7DB	6

TABLE 1

Question 14 - Phone / Messaging	
WebCode	Response
VA6BPD	18
W2UCV3	6
W4KC78	6 are unique
W4VZYW	6 (Six)
WAMHLA	6
WTZ4AC	6
XBWQEF	6
XFRN2L	6
YGFDDW	6 (18 in total but there are two sets of duplicate messages)
YK GK4G	6
ZVXNQ8	6

Question 14: How many SMS messages were received from the phone number associated with the contact listed as "Francis Milligan"? Provide response using the numeric format.

Consensus Result: 6

Expected Response Explanation:

Contacts are stored in /Root/data/com.samsung.android.providers.contacts/databases/contacts2.db; the number associated with Francis Milligan is (720) 686-5455. The SMS messages are contained in the following database: /USERDATA (ExtX)/Root/user_de/0/com.android.providers.telephony/databases/mmssms.db. By filtering the SMS table using "7206865455", six results are shown. PA automates this process.

Expected Response Illustration:

SMS Messages

mmssms.db		
sms (31)		
_id	thread_id	address
23	10	+17206865455
25	10	+17206865455
32	10	+17206865455
29	10	+17206865455
27	10	+17206865455
20	10	+17206865455
15	7	+17039407024

TABLE 1

Question 14 - Phone / Messaging

SMS Messages

SMS Messages (137)					
Clear filters					
Export Filters Actions milligan					
Timestamp	Delivered	Read	Folder	Parties	
12/15/2019 8:54:21 PM(UTC-5)			Inbox	From: +17206865455 Francis Milligan	
12/12/2019 8:13:13 PM(UTC-5)			Inbox	From: +17206865455 Francis Milligan	
12/12/2019 8:11:58 PM(UTC-5)			Inbox	From: +17206865455 Francis Milligan	
12/12/2019 8:10:41 PM(UTC-5)			Inbox	From: +17206865455 Francis Milligan	
12/12/2019 8:08:01 PM(UTC-5)			Inbox	From: +17206865455 Francis Milligan	
12/12/2019 8:06:03 PM(UTC-5)			Inbox	From: +17206865455 Francis Milligan	

TABLE 1

Question 15 - Phone / Messaging

Question 15: What is the account number for the device mobile service (cellular) provider?

Manufacturer's 756887507

Expected Response:

WebCode	Response
2B66AE	Acct756887507
2JDY68	756887507
3LWD98	756887507
3VNPE9	756887507
63XWWA	Acct756887507
69MBU4	Acct756887507
6EKPAN	310260
6PRHA7	756887507
74MLQ2	310260
77WBJY	756887507
7RU3AB	310260079673429
82DV2X	756887507
82VLFW	756887507
8CX7F4	756887507
8EN7R9	756887507
8K97CZ	756887507
8NC4K8	756887507
8NNHGL	310260
9ANFQZ	756887507
9CUZL3	756887507
9XT88X	756887507
ABE2WW	756887507
AD6282	756887507
AEDEP3	756887507
B4AJ7X	N/A
BCMEEEX	756887507
BL9FU8	756887507
C2JJVT	756887507
C9ZCG4	756887507

TABLE 1

Question 15 - Phone / Messaging	
WebCode	Response
CHMD3T	756887507
CKDDDX	756887507
CMH494	756887507
D7AC7Y	756887501
EBZ32N	756887507
EHJ79Q	756887507
EQURUZ	756887507
EYNXN2	756887507
F27G9V	15718351874
GQ3JZL	756887507
H88C8U	756887507
HEPJ4T	756887507
JP4YCX	T-MOBILE 756887507
LWCVX9	756887507
MU3MGV	756887507
N9JXHH	756887507
NGD4BJ	+14054720056
NZ9WWG	7206865455
PB49XM	756887507
PGULYB	756887507
PLMMZP	756887507
Q29PVJ	756887507
Q99RM3	3100260
QGJU94	
RCRKJC	756887507
TF4QLP	756887507
TPBP6E	+15718351874
U899KL	756887507
UREJE	756887507
UYQHMY	756887507
V9V7DB	756887507
VA6BPD	756887507

TABLE 1

Question 15 - Phone / Messaging	
WebCode	Response
W2UCV3	756887507
W4KC78	756887507
W4VZYW	756887507
WAMHLA	756887507
WTZ4AC	Account: 756887507 (Metro by T-Mobile)
XBWQEF	756887507
XFRN2L	756887507
YGFDWD	756887507
YK GK4G	756887507
ZVXNQ8	756887507

Question 15: What is the account number for the device mobile service (cellular) provider?

Consensus Result: 756887507

Expected Response Explanation:

The mobile service account number is found within the body of a SMS message. A review of the SMS messages finds a message from "611" containing the text "Please pay \$110.00 by 12/20/19 for Acct756887507 to avoid service interruption. Metro by T-Mobile...".

Expected Response Illustration:

SMS Messages

SMS Messages (137)				
Parties	Body	Status	SMSC	All timestamps
From: 611	Please pay \$110.00 by 12/20/19 for Acct756887507 to avoid service interruption. Metro by T-Mobile Terms&...	Unre	+14054720056	Network

TABLE 1

Question 16 - Phone / Messaging

Question 16: How many unread SMS messages are on the phone? Provide response using the numeric format.

Manufacturer's 8

Expected Response:

WebCode	Response
2B66AE	8
2JDY68	8
3LWD98	8
3VNPE9	8 unique unread SMS messages. The forensic tool used displayed triplicates of the unread SMS messages observed, totaling to 24 unread SMS messages. The total 24 unread SMS messages include the 8 unique unread SMS messages.
63XWWA	8
69MBU4	8
6EKPAN	8
6PRHA7	8
74MLQ2	12
77WBJY	8
7RU3AB	8
82DV2X	8
82VLFW	8
8CX7F4	8
8EN7R9	8
8K97CZ	8
8NC4K8	8
8NNHGL	8
9ANFQZ	8
9CUZL3	8
9XT88X	8
ABE2WW	8
AD6282	16
AEDEP3	8
B4AJ7X	8
BCMEEEX	8
BL9FU8	8

TABLE 1

Question 16 - Phone / Messaging	
WebCode	Response
C2JJVT	8
C9ZCG4	8
CHMD3T	8
CKDDDX	8
CMH494	8
D7AC7Y	8
EBZ32N	8
EHJ79Q	8
EQURUZ	8
EYNXN2	24
F27G9V	8
GQ3JZL	8
H88C8U	8
HEPJ4T	8
JP4YCX	8
LWCVX9	16
MU3MGV	8
N9JXHH	8
NGD4BJ	8
NZ9WWG	8
PB49XM	8
PGULYB	8
PLMMZP	8
Q29PVJ	8
Q99RM3	48
QGJU94	8
RCRKJC	8, but they were each duplicated for a total of 24.
TF4QLP	8
TPBP6E	8
U899KL	8
UEREJE	8
UYQHMY	8

TABLE 1

Question 16 - Phone / Messaging	
WebCode	Response
V9V7DB	8
VA6BPD	16
W2UCV3	8
W4KC78	8 are unique
W4VZYW	8 (Eight)
WAMHLA	8
WTZ4AC	8
XBWQEF	8
XFRN2L	8
YGFDDW	8 (16 in total but one set of duplicate messages)
YK GK4G	8
ZVXNQ8	8

Question 16: How many unread SMS messages are on the phone? Provide response using the numeric format.

Consensus Result: 8

Expected Response Explanation:

The quantity of unread SMS messages can be found in the following database: (ExtX)/Root/user_de/0/com.android.providers.telephony/databases/mmssms.db. This database contains eight (8) records with the "read" flag unset. PA parses this and shows it in the SMS Messages tab.

Expected Response Illustration:

SMS Messages

_id	thread_id	address	pers	date	date_sent	protocol	read	status
37	11	+15105014284		1576463668078	1576463668000	0	0	-1
34	3	22000		1576462612359	1576462610000	0	0	-1
31	2	611		1576253796785	1576253734000	0	0	-1
16	6	+15415265577		1576036289045	1576036289000	0	0	-1
14	8	2962		1576010304254	1576010239000	0	0	-1
38	11	+15105014284		1576463740977	1576463742000	0	0	-1
17	6	+15415265577		1576036363758	1576036364000	0	0	-1
36	11	+15105014284		1576463546840	1576463548000	0	0	-1
9	4	244444		1575396490594	0		1	-1
7	2	611		1574359949202	1574359946000	0	1	-1

TABLE 1

Question 16 - Phone / Messaging

SMS Messages

SMS Messages (137)					
Folder	Parties	Body	Status	SMSC	
Inbox	From: +1510501	15105014284 Depositing new message To accept press one to send a voicemail press two.. Click here: 13608...	Unread	+14054720056	
Inbox	From: +1510501	15105014284 Depositing new message One to send a voicemail press two.. Click here: 13608424004 to listen...	Unread	+14054720056	
Inbox	From: +1510501	15105014284 Depositing new message To send a voicemail press two.. Click here: 13608424003 to listen to f...	Unread	+14054720056	
Inbox	From: 22000	<#> 783514 is your Google Voice verification code. Don't share it with anyone else. https://goo.gl/UErgF7 o...	Unread	+14054720056	
Inbox	From: 611	Please pay \$110.00 by 12/20/19 for Acct756887507 to avoid service interruption. Metro by T-Mobile Terms&...	Unread	+14054720056	
Inbox	From: +1541526	<#> Your WhatsApp code: 378-117 You can also tap on this link to verify your phone: v.whatsapp.com/3781...	Unread	+14054720056	
Inbox	From: +1541526	<#> Your WhatsApp code: 804-093 You can also tap on this link to verify your phone: v.whatsapp.com/8040...	Unread	+14054720056	
Inbox	From: 2962	Check out our Top 5 Ways to Metro for pro tips on managing your Metro life digitally! https://metro-tmo.co...	Unread	+14054720056	

TABLE 1

Question 17 - Phone / Messaging

Question 17: What communication service sent the 783514 verification code?

Manufacturer's Google Voice

Expected Response:

WebCode	Response
2B66AE	Google Voice
2JDY68	Google Voice
3LWD98	Google Voice
3VNPE9	Google Voice
63XWWA	Google Voice
69MBU4	Google Voice
6EKPAN	Google Voice
6PRHA7	Google Voice
74MLQ2	Google Voice
77WBJY	Google Voice
7RU3AB	Google Voice
82DV2X	Google Voice
82VLFW	Google Voice
8CX7F4	Google Voice
8EN7R9	Google Voice
8K97CZ	Google Voice
8NC4K8	Google Voice
8NNHGL	22000 - Google Voice
9ANFQZ	Google Voice
9CUZL3	Google Voice verification code
9XT88X	Google Voice
ABE2WW	Google Voice
AD6282	Google voice
AEDEP3	Google Voice
B4AJ7X	Google Voice
BCMEEEX	Google Voice
BL9FU8	Google Voice
C2JJVT	Google Voice
C9ZCG4	Google Voice

TABLE 1

Question 17 - Phone / Messaging	
WebCode	Response
CHMD3T	Google Voice
CKDDDX	Google Voice
CMH494	Google Voice
D7AC7Y	Google Voice
EBZ32N	Google Voice
EHJ79Q	Google Voice
EQURUZ	Google Voice
EYNXN2	Google Voice via Android System Messages
F27G9V	Google Voice
GQ3JZL	Google Voice
H88C8U	Google Voice
HEPJ4T	Google Voice
JP4YCX	GOOGLE VOICE
LWCVX9	Google Voice
MU3MGV	Google Voice
N9JXHH	Google Voice
NGD4BJ	Google Voice
NZ9WWG	Google Voice
PB49XM	Google Voice
PGULYB	SMS
PLMMZP	22000 Google Voice
Q29PVJ	Google Voice
Q99RM3	Google Voice
QGJU94	Google Voice
RCRKJC	Google Voice
TF4QLP	Google Voice
TPBP6E	Google Voice verification
U899KL	Google Voice
UEREJE	Google Voice com.google.android.apps.googlevoice
UYQHMY	Google Voice (SMS)
V9V7DB	Google Voice
VA6BPD	Google Voice

TABLE 1

Question 17 - Phone / Messaging	
WebCode	Response
W2UCV3	SMS
W4KC78	Google Voice
W4VZYW	Google Voice verification code
WAMHLA	Google voice
WTZ4AC	Google Voice
XBWQEF	Google Voice
XFRN2L	Google Voice
YGFDWD	Google Voice
YK GK4G	Google Voice
ZVXNQ8	Google Voice

Question 17: What communication service sent the 783514 verification code?

Consensus Result: Google Voice

Expected Response Explanation:

Searching for 783514 finds one message, "783514 is your Google Voice verification code. Don't share it with anyone else".

Expected Response Illustration:

Message

Hex	Text	Application	Message	File Metadata	Context	Results	Annotations	Other Occurrences	
Strings		Indexed Text	Translation						
Matches on page: 1 of 1		Match	← →	Page: 1 of 1		Page	← →	100%	Res
<pre> Message Type : Android Message Date/Time : 2019-12-15 21:16:52 EST Read : Unread Direction : Incoming From Phone Number : 22000 To Phone Number : 93c5bb2c-7c12-4039-9b88-f1c76c0b6236 Text : <#> 783514 is your Google Voice verification code. Don't share it with anyone else. https://goo.gl/UErgF7owBEk0tbefD Thread ID : 2647f9c2-de01-45f1-b624-252c213b1609-3 </pre>									

TABLE 1

Question 18 - Phone / Messaging

Question 18: What contact (name) has the phone number "208-900-1987"?

Manufacturer's mom

Expected Response:

WebCode	Response
2B66AE	mom
2JDY68	mom
3LWD98	mom
3VNPE9	mom
63XWWA	mom
69MBU4	mom
6EKPAN	mom
6PRHA7	mom
74MLQ2	mom
77WBJY	Mom
7RU3AB	mom
82DV2X	mom
82VLFW	mom
8CX7F4	mom
8EN7R9	mom
8K97CZ	mom
8NC4K8	mom
8NNHGL	mom
9ANFQZ	mom
9CUZL3	Mom
9XT88X	mom
ABE2WW	mom
AD6282	Mom
AEDEP3	mom
B4AJ7X	mom
BCMEEEX	mom
BL9FU8	mom
C2JJVT	mom
C9ZCG4	Mom

TABLE 1

Question 18 - Phone / Messaging	
WebCode	Response
CHMD3T	mom
CKDDDX	Mom
CMH494	mom
D7AC7Y	Mom
EBZ32N	mom
EHJ79Q	mom
EQURUZ	mom
EYNXN2	mom
F27G9V	mom
GQ3JZL	mom
H88C8U	mom
HEPJ4T	mom
JP4YCX	MOM
LWCVX9	mom
MU3MGV	mom
N9JXHH	mom
NGD4BJ	Mom
NZ9WWG	Mom
PB49XM	mom
PGULYB	mom
PLMMZP	mom
Q29PVJ	Mom
Q99RM3	mom
QGJU94	mom
RCRKJC	mom
TF4QLP	mom
TPBP6E	mom
U899KL	mom
UEREJE	mom
UYQHMY	Mom
V9V7DB	mom
VA6BPD	mom

TABLE 1

Question 18 - Phone / Messaging	
WebCode	Response
W2UCV3	mom
W4KC78	mom
W4VZYW	mom
WAMHLA	mom
WTZ4AC	mom
XBWQEF	Mom
XFRN2L	mom
YGFDWD	mom
YK GK4G	mom
ZVXNQ8	mom

Question 18: What contact (name) has the phone number "208-900-1987"?

Consensus Result: mom

Expected Response Explanation:

Contacts are stored in /Root/data/com.samsung.android.providers.contacts/databases/contacts2.db, the contact name associated with this number is "mom".

Expected Response Illustration:

Contacts

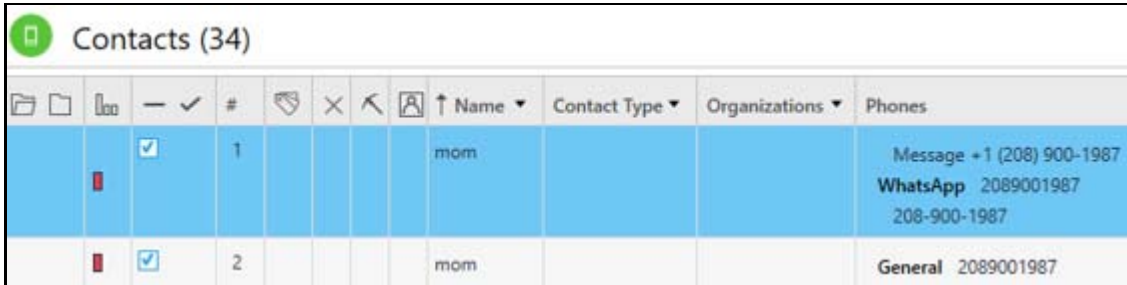


TABLE 1

Question 19 - Phone / Messaging

Question 19: What was the duration of the call from Raymond Butner on 12/5/2019? Provide your response in the following format: HH:MM:SS

Manufacturer's 00:00:27

Expected Response:

WebCode	Response
2B66AE	00:00:27
2JDY68	00:00:27
3LWD98	00:00:27
3VNPE9	00:00:27
63XWWA	00:00:27
69MBU4	00:00:27
6EKPAN	00:00:27
6PRHA7	00:00:27
74MLQ2	00.00.27
77WBJY	00:00:27
7RU3AB	00:00:27
82DV2X	00:00:27
82VLFW	00:00:27
8CX7F4	00:00:27
8EN7R9	00:00:27
8K97CZ	00:00:27
8NC4K8	00:00:27
8NNHGL	00:00:27
9ANFQZ	00:00:27
9CUZL3	00:00:27
9XT88X	00:00:27
ABE2WW	00:00:27
AD6282	00:00:27
AEDEP3	00:00:27
B4AJ7X	00:00:27
BCMEEEX	00:00:27
BL9FU8	00:00:27
C2JJVT	00:00:27

TABLE 1

Question 19 - Phone / Messaging	
WebCode	Response
C9ZCG4	00:00:27
CHMD3T	00:00:27
CKDDDX	00:00:27
CMH494	00:00:27
D7AC7Y	00:00:27
EBZ32N	00:00:27
EHJ79Q	00:00:27
EQURUZ	00:00:27
EYNXN2	00:00:27
F27G9V	00:00:27
GQ3JZL	00:00:27
H88C8U	00:00:27
HEPJ4T	00:00:27
JP4YCX	00:00:27
LWCVX9	00:00:27
MU3MGV	00:00:27
N9JXHH	00:00:27
NGD4BJ	00:00:27
NZ9WWG	00:00:27
PB49XM	00:00:27
PGULYB	00:00:27
PLMMZP	00:00:27
Q29PVJ	00:00:27
Q99RM3	00:00:27
QGJU94	00:00:27
RCRKJC	00:00:27
TF4QLP	00:00:27
TPBP6E	00:00:27
U899KL	00:00:27
UEREJE	00:00:27
UYQHMY	00:00:27
V9V7DB	00:00:27

TABLE 1

Question 19 - Phone / Messaging	
WebCode	Response
VA6BPD	00:00:27
W2UCV3	00:00:27
W4KC78	00:00:27
W4VZYW	00:00:27
WAMHLA	00:00:27
WTZ4AC	00:00:27
XBWQEF	00:00:27
XFRN2L	00:00:27
YGFDWD	00:00:27
YK GK4G	00:00:27
ZVXNQ8	00:00:27

Question 19: What was the duration of the call from Raymond Butner on 12/5/2019? Provide your response in the following format: HH:MM:SS

Consensus Result: 0:00:27

Expected Response Explanation:

The call log information is contained in /Root/data/com.samsung.android.providers.contacts/databases/calllog.db-wal.

Expected Response Illustration:

Call Log

Parties	Timestamp	Duration	Status
To: 5713130786	11/21/2019 10:19:38 AM(UTC-5)		Unknown
From: +17039407024 Raymond Butner	12/5/2019 6:32:30 AM(UTC-5)	00:00:27	Unknown
To: +17039407024 Raymond Butner	12/5/2019 6:35:03 AM(UTC-5)		Unknown
From: -1	12/15/2019 9:20:22 PM(UTC-5)		Rejected

TABLE 1

Question 20 - Phone / Messaging	
---------------------------------	--

Question 20: What was the date and time of the last outgoing call? Provide your response in the time zone set for the device using the following format: MM/DD/YYYY, HH:MM AM/PM

Manufacturer's 12/15/2019 09:28 PM

Expected Response:

WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
2B66AE	12/05/2019, 06:35 AM	
2JDY68	12/15/2019 9:28 PM	
3LWD98	12/15/2019 09:28 PM	
3VNPE9	12/15/2019, 09:28 PM was the last dialed outgoing call made to **61*18056912815, which appears to be a call forwarding service number. If the last call was made to a person or contact, it would be 12/05/2019, 06:35 AM.	
63XWWA	12/15/2019, 21:28 PM	
69MBU4	12/15/2019, 09:28 PM	
6EKPAN	12/15/2019 09:28 pm	
6PRHA7	12/15/2019, 06:35:03 AM	
74MLQ2	12/15/2019 09:28 PM	
77WBJY	12/05/2019, 06:35 AM	
7RU3AB	12/15/2019, 09:28 PM	
82DV2X	12/15/2019, 09:28 PM	
82VLFW	12/05/2019, 06:35 AM	
8CX7F4	12/05/2019, 6:35:03 AM	
8EN7R9	12/15/2019, 08:55 PM	
8K97CZ	12/15/2019, 09:28 PM	
8NC4K8	12/15/2019 8:55:26 PM	
8NNHGL	12/05/2019, 06:35 AM	
9ANFQZ	12/5/2019 6:35 AM	
9CUZL3	12/05/2019, 06:35:03 AM (UTC -5)	
9XT88X	12/15/2019, 09:28 PM	
ABE2WW	12/15/2019, 09:28 PM	
AD6282	12/15/2019 21:28 PM	
AEDEP3	12/05/2019, 06:35:03 AM	
B4AJ7X	12/15/2019 9:35:13 PM	
BCMEEEX	12/05/2019, 06:35 AM	
BL9FU8	12/15/2020 09:28 PM	

TABLE 1

Question 20 - Phone / Messaging	
WebCode	Response
C2JJVT	12/15/2019, 9:28 PM
C9ZCG4	12/15/2019 09:28 PM
CHMD3T	12/15/2019 9:28 PM
CKDDDX	12/15/2019 21:28 PM
CMH494	12/15/2019 09:35 PM
D7AC7Y	12/5/2019 6:35 AM
EBZ32N	12/15/2019, 09:28 PM(UTC-5)
EHJ79Q	12/15/2019 9:28:53 PM(UTC-5)
EQURUZ	12/15/2019 2128 PM
EYNXN2	12/15/2019 09:28 PM
F27G9V	12/15/2019, 09:28 PM
GQ3JZL	12/15/2019, 09:28 PM
H88C8U	12/15/2019,09:28 AM
HEPJ4T	12/05/2019, 06:35 AM
JP4YCX	12/15/2019 09:28 pm
LWCVX9	12/15/2019, 09:28 PM
MU3MGV	12/15/2019, 09:28 PM
N9JXHH	12/05/2019, 06:35 AM
NGD4BJ	12/15/2019, 09:28 PM
NZ9WWG	12/15/2019, 09:28 PM
PB49XM	12/05/2019, 06:35 AM
PGULYB	12/5/2019, 6:35:03 AM
PLMMZP	12/05/19, 6:35 AM
Q29PVJ	12/15/2019, 09:28 PM
Q99RM3	12.15.2019 09:28 pm
QGJU94	12/15/2019, 21:28 PM
RCRKJC	12/15/2019, 09:28 PM
TF4QLP	12/15/2019, 09:28 PM (technically last call but this is a call forward) 12/15/2019, 08:55 PM (last true call)
TPBP6E	12/15/2019 9:28:53 PM(UTC-5)
U899KL	12/15/2019 9:28 PM
UEREJE	12/15/2019 09:28 PM

TABLE 1

Question 20 - Phone / Messaging	
WebCode	Response
UYQHMY	16/12/2019 02:28 AM
V9V7DB	12/15/2019, 09:28 PM
VA6BPD	12/15/2019, 09:28 PM
W2UCV3	12/05/2019, 06:53 AM
W4KC78	12/05/2019, 06:35 AM is the date and time of the last outgoing call made to a contact. (This time stamp corresponds to the outgoing call made to "+17039407024" "Raymond Butner") Note: 12/15/2019, 09:28 PM is the date and time of the last outgoing call parsed by both CelleBrite and XRY (which corresponds to the outgoing call to "***61*18056912815") - **61 is a T-mobile/ Metro PCS Short Code to "Turn on forwarding if no reply (CF NRY) to a number (unanswered calls ring to alternate number)".
W4VZYW	12/15/2019 09:28 PM
WAMHLA	12/15/2019 9:28 PM
WTZ4AC	12/15/2019, 9:28 PM (UTC-5)
XBWQEF	12/05/2019, 06:35 AM
XFRN2L	12/05/2019 06:35 AM
YGFDWD	12/15/2019, 21:28:53 PM
YK GK4G	12/5/2019 06:35(UTC-5)
ZVXNQ8	12/15/2019, 09:28 PM

Question 20: What was the date and time of the last outgoing call? Provide your response in the time zone set for the device using the following format: MM/DD/YYYY, HH:MM AM/PM

Consensus Result: The objective of this question was to identify the last number dialed as context for the following three questions. A consensus was not achieved for this question which affected the full series of questions 20-23. However, two distinct subsets of responses were received for this question and the additional questions in the series which achieved a consensus within the subsets are presented at the end of the report. Questions labeled #120 and #220 relate to this specific question and cover the two subsets.

Expected Response Explanation:

The last outgoing call date and time can be found in the Call log located in /Root/data/com.samsung.android.providers.contacts/databases/calllog.db-wal

Expected Response Illustration:

Call Log

#	Parties	Timestamp	Duration	Status
1	To: 5713130786	11/21/2019 10:19:38 AM(UTC-5)		Unknown
2	From: +17039407024 Raymond Butner	12/5/2019 6:32:30 AM(UTC-5)	00:00:27	Unknown
3	To: +17039407024 Raymond Butner	12/5/2019 6:35:03 AM(UTC-5)		Unknown
4	From: -1	12/15/2019 9:20:22 PM(UTC-5)		Rejected
5	To: ***61*18056912815	12/15/2019 9:28:53 PM(UTC-5)		Unknown
6	From: Unknown	12/15/2019 9:31:58 PM(UTC-5)		Rejected

TABLE 1

Question 21 - Phone / Messaging

Question 21: The last outgoing call was made to what phone number?

Manufacturer's **61*18056912815Expected Response:

WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
2B66AE	+17039407024	
2JDY68	**61*18056912815	
3LWD98	**61*18056912815	
3VNPE9	1 (805) 691-2815, however, it is listed with the prefix number "***61*". The entire number dialed out is "***61*18056912815". The "***61*" number appears to be a call forwarding service and is going to a Google Voice number. If the last call was made to a person or contact, it would be the phone number 1 (703) 940-7024.	
63XWWA	**61*18056912815	
69MBU4	+17039407024	
6EKPAN	**61*18056912815	
6PRHA7	703-940-7024	
74MLQ2	+17039407024	
77WBJY	17039407024	
7RU3AB	+17039407024	
82DV2X	7206865455	
82VLFW	+17039407024	
8CX7F4	17039407024	
8EN7R9	7206865455	
8K97CZ	**61*18056912815	
8NC4K8	7206865455	
8NNHGL	17039407024	
9ANFQZ	+17039407024	
9CUZL3	+17039407024	
9XT88X	**61*18056912815	
ABE2WW	**61*18056912815	
AD6282	**61*18056912815	
AEDEP3	17039407024	
B4AJ7X	**61*18056912815	
BCMEEX	1 703 940 7024	
BL9FU8	**61*18056912815	

TABLE 1

Question 21 - Phone / Messaging		
WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
C2JJVT	**61*18056912815	
C9ZCG4	**61*18056912815	
CHMD3T	**61*18056912815	
CKDDDX	**61*18056912815	
CMH494	1-510-501-4284 or 510-501-4284 or 15105014284 or 5105014284	
D7AC7Y	1-703-940-7024	
EBZ32N	**61*18056912815	
EHJ79Q	**61*18056912815	
EQURUZ	**61*18056912815	
EYNXN2	**61*18056912815	
F27G9V	**61*18056912815	
GQ3JZL	**61*18056912815	
H88C8U	**61*18056912815	
HEPJ4T	+17039407024	
JP4YCX	**61*18056912815	
LWCVX9	**61*18056912815	
MU3MGV	7206865455	
N9JXHH	1-703-940-7024	
NGD4BJ	+6118056912815	
NZ9WWG	**61*18056912815	
PB49XM	17039407024	
PGULYB	17039407024	
PLMMZP	+17039407024	
Q29PVJ	**61*18056912815	**61* entry is a call forwarding service. The last call to an individual was made to 17039407024.
Q99RM3	**61*18056912815	
QGJU94	**61*18056912815	
RCRKJC	**61*18056912815	
TF4QLP	**61*18056912815 (this is a forwarded call) 720-686-5455 (last true call)	
TPBP6E	18056912815	
U899KL	**61*18056912815	
UEREJE	**61*18056912815 (1-805-691-2815)	

TABLE 1

Question 21 - Phone / Messaging		
WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
UYQHMY	**61*18056912815	
V9V7DB	**61*18056912815	
VA6BPD	The last outgoing call on the phone was **61*18056912815. The last outgoing call in the calllog.db was 7206865455	
W2UCV3	+17039407024	
W4KC78	17039407024	
W4VZYW	**61*18056912815	
WAMHLA	**61*18056912815	
WTZ4AC	**61*18056912815	
XBWQEF	17039407024	
XFRN2L	+17039407024	
YGFDWD	**61*18056912815	
YKGK4G	+17039407024	
ZVXNQ8	**61*18056912815	

Question 21: The last outgoing call was made to what phone number?

Consensus Result: The objective of this question was to identify the last number dialed as context for a group of questions. A consensus was not achieved for question #20 which affected the full series of questions 20-23. A consensus was also not achieved for this question. However, two distinct subsets of responses were received for this question and the additional questions in the series which achieved a consensus within the subsets are presented at the end of the report. Questions labeled #121 and #221 relate to this specific question and cover the two subsets.

Expected Response Explanation:

The last outgoing call can be found in the Call log located in /Root/data/com.samsung.android.providers.contacts/databases/calllog.db-wal.

TABLE 1

Question 21 - Phone / Messaging

Expected Response Illustration:

Call Log

Call Log (8)							
	<input type="checkbox"/>	#		Parties	↑ Timestamp	Duration	Status
	<input checked="" type="checkbox"/>	1		To: 5713130786	11/21/2019 10:19:38 AM(UTC...		Unknown
	<input checked="" type="checkbox"/>	2		From: +17039407024 Raymond Butner	12/5/2019 6:32:30 AM(UTC-5)	00:00:27	Unknown
	<input checked="" type="checkbox"/>	3		To: +17039407024 Raymond Butner	12/5/2019 6:35:03 AM(UTC-5)		Unknown
	<input checked="" type="checkbox"/>	4		From: -1	12/15/2019 9:20:22 PM(UTC-5)		Rejected
	<input checked="" type="checkbox"/>	5		To: **61*18056912815	12/15/2019 9:28:53 PM(UTC-5)		Unknown
	<input checked="" type="checkbox"/>	6		From: Unknown	12/15/2019 9:31:58 PM(UTC-5)		Rejected
	<input checked="" type="checkbox"/>	7		From: Unknown	12/15/2019 9:33:57 PM(UTC-5)		Rejected
	<input checked="" type="checkbox"/>	8		From: -1	12/15/2019 9:35:13 PM(UTC-5)		Rejected

TABLE 1

Question 22 - Phone / Messaging

Question 22: Provide the contact name belonging to the phone number reported in question #21?

Manufacturer's Allen Gonzales

Expected Response:

WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
2B66AE	Raymond Butner	
2JDY68	Allen Gonzales	
3LWD98	Allen Gonzales	
3VNPE9	The phone number from question 21 needed clarification. CTS was contacted and could not clarify the question being asked. The "***61**" prefix number appears to be a call forwarding service for Metro PCS mobile phone service provider. Therefore, the name of the contact may be associated with a Google Voice voicemail account and the name of the contact is Google Voice. However, if the call forward service number is not considered a dialed out call, then I am putting contact name as Raymond Butner with the dialed out number of 1 (703) 940-7024 made on 12/05/2019, 06:35 AM (UTC-5)	
63XWWA	Unknown	
69MBU4	Raymond Butner	
6EKPAN	Unknown	
6PRHA7	Raymond Butner	
74MLQ2	Raymond Butner	
77WBJY	Raymond Butner	
7RU3AB	Raymond Butner	
82DV2X	Francis Milligan	
82VLFW	Raymond Butner	
8CX7F4	Raymond Butner	
8EN7R9	Francis Milligan	
8K97CZ	Allen Gonzales	
8NC4K8	Francis Milligan	
8NNHGL	Raymond Butner	
9ANFQZ	Raymond Butner	
9CUZL3	Raymond Butner	
9XT88X	Allen Gonzales	
ABE2WW	Allen Gonzales	
AD6282	611 Customer Care	
AEDEP3	Raymond Butner	
B4AJ7X	No name was attached to the phone number.	
BCMEEX	Raymond Butner	

TABLE 1

Question 22 - Phone / Messaging		
WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
BL9FU8	None reported.	
C2JJVT	Unknown Unknown	
C9ZCG4	T-Mobile	
CHMD3T	Call forwarding	
CKDDDX	Unknown	
CMH494	IRS	
D7AC7Y	Raymond Butner	
EBZ32N	The contact name associated with the phone number 8056912815 is unknown.	
EHJ79Q	The phone number in #21 is a google voice number that had calls forwarded to it from this suspect device. It appears that you are asking for the contact name for the owner of the device but the question is not clear on this.	
EQURUZ	No name in report	
EYNXN2	Not Listed	
F27G9V	Francis Milligan	
GQ3JZL	Customer Care	
H88C8U	Allen Gonzales	
HEPJ4T	Raymond Butner	
JP4YCX	NO CONTACT STORED WITH SAID NUMBER.	
LWCVX9	No name	
MU3MGV	Francis Milligan	
N9JXHH	Raymond Butner	
NGD4BJ	It is not listed.	
NZ9WWG		
PB49XM	Raymond Butner	
PGULYB	Raymond Butner	
PLMMZP	Raymond Butner	
Q29PVJ	The contact name for the number **61*18056912815 is unknown. The contact name for the number 17039407024 is Raymond Butner	
Q99RM3	Francis Milligan	
QGJU94		
RCRKJC	No Contact Name	
TF4QLP	Francis Milligan	
TPBP6E	Not saved	

TABLE 1

Question 22 - Phone / Messaging		
WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
U899KL	Not located	
UEREJE	**61* is a call forwarding or call diversion feature of some telephone systems which redirects a telephone call to another destination, which may be a phone number. The 1-805-691-2815 has a phone account address of 1-571-835-1874, who is Allen Gonzales. Allen Gonzales	
UYQHMY	None	
V9V7DB	Allen Gonzales	
VA6BPD	**61*18056912815 doesn't not appear to be in the contacts. 7206865455 belongs to Francis Milligan	
W2UCV3	Raymond Butner	
W4KC78	Raymond Butner	
W4VZYW	None (Don't exist in the contact)	
WAMHLA	Raymond Butner	
WTZ4AC	Allen Gonzales	
XBWQEF	Raymond Butner	
XFRN2L	Raymond Butner	
YGFWD	Phone 1	
YKGK4G	Raymond Butner	
ZVXNQ8	Allen Gonzales	

Question 22: Provide the contact name belonging to the phone number reported in question #21?

Consensus Result: The objective of this question was to identify the last number dialed as context for a group of questions. A consensus was not achieved for question #20 which affected the full series of questions 20-23. A consensus was also not achieved for this question. However, a subset of responses was received for this question and the additional questions in the series which achieved a consensus within the subsets and these results are presented at the end of the report. Question labeled 222 relates to this specific question and Subset 2.

Expected Response Explanation:

Recognizing *61* to be a prefix used on the T-Mobile mobile network for setting up no-answer call forwarding, and keyword searching across the device image for the forwarded-to number, 18056912815, one would discover /USERDATA (ExtX)/Root/data/com.google.android.apps.googlevoice/files/accounts/0/SignupSettings.pb among the configuration files for the Google Voice app and service, in the name of the user.

Reviewing other configuration files for the Google Voice app discovers /USERDATA (ExtX)/Root/data/com.google.android.apps.googlevoice/shared_prefs/accounts.xml which identifies the account name as allengonzo79@gmail.com. The accounts database USERDATA (ExtX)/Root/system_ce/0/accounts_ce.db identifies "Allen Gonzales" as the name associated with the allengonzo79@gmail.com.

TABLE 1

Question 22 - Phone / Messaging

Expected Response Illustration:

Setup file for the Google Voice app

```

Complex = {
  1: = [
    Complex = {
      1: = [
        Complex = {
          1: = [
            LengthValue = +18056912815
          ]
        ]
      ]
    ]
  ]
  3: = [
    Varint = 1
  ]
}
USERDATA (ExtX)/Root/data/com.google.android.apps.googlevoice/files/accounts/0/SignupSettings.pb
    
```

Google Voice App Config. File

```

accounts.xml
Text View  Hex View  File format viewer  File Info
map = {
  0.display_name : string = Allen Gonzales
  0.upgrade_direct_login_to_managed_login : boolean = True
  0.upgrade_remove_account_status : boolean = True
  AccountStore#upgradeAccountCreated : boolean = True
  count : int = 1
  0.gaia_id : string = 112532578259086394667
  0.upgrade_account_status : boolean = True
  0.add_skinny_page_boolean : boolean = True
  0.account_name : string = allengonzo79@gmail.com
  key.com.google.android.apps.googlevoice : int = 0
}
USERDATA (ExtX)/Root/data/com.google.android.apps.googlevoice/shared_prefs/accounts.xml
    
```


TABLE 1

Question 23 - Phone / Messaging	
---------------------------------	--

Question 23: Provide the associated communication service to which the phone number in question #21 belongs?

Manufacturer's User's Google Voice Account

Expected Response:

WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
2B66AE	WhatsApp	
2JDY68	Google Voice	
3LWD98	Google Voice	
3VNPE9	If the question #21 assumes the "***61*" as the last outgoing call, then the associated communication service is a Google Voice voicemail account. If answering with the answer of Raymond Butner (second to last outgoing call), the associated communication service to that phone number are Telegram and WhatsApp.	
63XWWA	Google Voice	
69MBU4	TelephonyConnectionService	
6EKPAN	Samsung/Android telephony	
6PRHA7	WhatsApp	
74MLQ2	WhatsApp	
77WBJY	Telephony	
7RU3AB	Telephony Connection Service	
82DV2X	vnd.sec.contact.phone	
82VLFW	WhatsApp	
8CX7F4	Whatsapp	
8EN7R9	com.google	
8K97CZ	Google Voice	
8NC4K8	WhatsApp	
8NNHGL	T-Mobile	
9ANFQZ	Telegram	
9CUZL3	GSM	
9XT88X	Call Forwarding, Google Voice	
ABE2WW	Google Voice	
AD6282	Metro by T-Mobile	
AEDEP3	Telegram	
B4AJ7X	N/A	
BCMEEEX	Native Phone	
BL9FU8	com.android.phone/com.android.services.telephony.TelephonyConnectionService	

TABLE 1

Question 23 - Phone / Messaging		
WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
C2JJVT	Google Voice	
C9ZCG4	Call forwarding	
CHMD3T	Call forwarding	
CKDDDX	Google Voice	
CMH494	Voicemail	
D7AC7Y	WhatsApp	
EBZ32N	Google Voice	
EHJ79Q	Google Voice	
EQURUZ	Call Forwarding	
EYNXN2	Android Services Telephony Telephoneconnections services	
F27G9V	Google Hangout	
GQ3JZL	Metro by T-Mobile	
H88C8U	Google Voice	
HEPJ4T	WhatsApp	
JP4YCX	TELEPHONY	
LWCVX9	TEXT NOW	
MU3MGV	TextNow	
N9JXHH	Metro PCS	
NGD4BJ	Telephony connection service	
NZ9WWG		
PB49XM	WhatsApp	
PGULYB	WhatsApp and Telegram	
PLMMZP	WhatsApp	
Q29PVJ	com.android.phone/com.android.services.telephony.TelephonyConnectionService	
Q99RM3	Google Voice	
QGJU94	TelephonyConnectionService	
RCRKJC	**61 for T-mobile shows Call Forwarding	
TF4QLP	WhatsApp	
TPBP6E	Call forwarding	
U899KL	Android	
UEREJE	Google Voice com.google.android.apps.googlevoice	
UYQHMY	Android System Calls	

TABLE 1

Question 23 - Phone / Messaging		
WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
V9V7DB	Google Voice	
VA6BPD	**61*18056912815 Call Forwarding service. 7206865455 Call service	
W2UCV3	WhatsApp and Telegram	
W4KC78	WhatsApp and also Telegram (which corresponds to the phone number "+17039407024" "Raymond Butner")	
W4VZYW	T-Mobile Call services (Turn on forwarding if no reply (CF NRY) to a number (unanswered calls ring to alternate number)	
WAMHLA	Google Voice	
WTZ4AC	Google Voice	
XBWQEF	WhatsApp	
XFRN2L	Phone call	
YGFDWD	Google/Bandwidth.com (SVR)	
YKGK4G	WhatsApp	
ZVXNQ8	google voice	

Question 23: Provide the associated communication service to which the phone number in question #21 belongs?

Consensus Result: A consensus was not achieved. The objective of this question was to search for the forwarded-to number 18056912815 which would identify configuration files for the Google Voice service.

Expected Response Explanation:

Recognizing *61* to be a prefix used on the T-Mobile mobile network for setting up no-answer call forwarding, and keyword searching across the device image for the forwarded-to number, 18056912815, would discover /USERDATA (ExtX)/Root/data/com.google.android.apps.googlevoice/files/accounts/0/SignupSettings.pb among the configuration files for the Google Voice service.

Expected Response Illustration:

Google Voice App Config. File

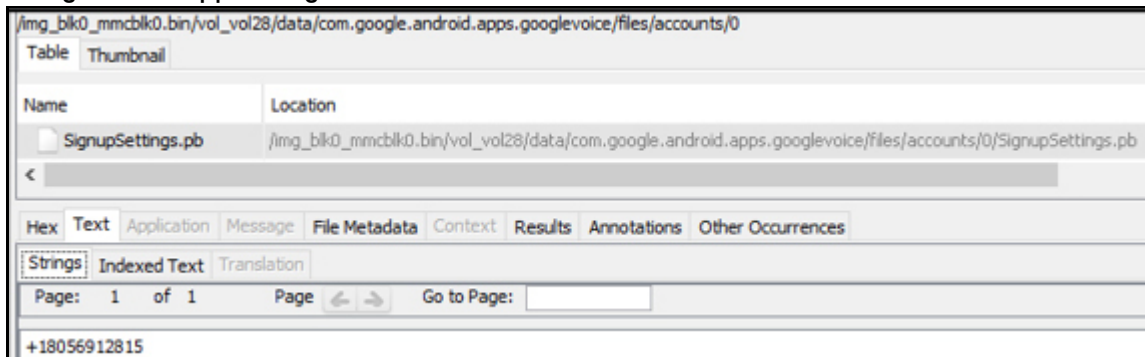


TABLE 1

Question 24 - Phone Metadata / Navigation	
---	--

Question 24: What are the location coordinates for the photograph of the Christmas tree taken with the phone's camera? Provide your response using the following format: Latitude, Longitude (to 6 decimal places)

Manufacturer's 38.888611, -77.005000

Expected Response:

WebCode	Response
2B66AE	38.888611, -77.005000
2JDY68	38.888611, -77.005000
3LWD98	38.888611, -77.005000
3VNPE9	Lat, Lon: 38.888611, -77.005000
63XWWA	38.888611,-77.005000
69MBU4	38.8886, -77.0050
6EKPAN	38.888611 / -77.005000
6PRHA7	38.888611, -77.005000
74MLQ2	38.888611, -77.005000
77WBJY	38.888611, -77.005000
7RU3AB	38.888611, -77.005000
82DV2X	38.888611, -77.005000
82VLFW	38.888611, -77.005000
8CX7F4	38.888611 / -77.005000
8EN7R9	38.888611 / -77.005000
8K97CZ	38.888611, -77.005000
8NC4K8	38.888611, -77.005000
8NNHGL	38.888611 / -77.005000
9ANFQZ	38.888611, -77.005000
9CUZL3	38.888611, -77.005000
9XT88X	38.888611, -77.005000
ABE2WW	38.888611, -77.005000
AD6282	38.888611, -77.005000
AEDEP3	38.888611, -77.005000
B4AJ7X	38.888611, -77.005000
BCMEEEX	38.888611, -77.005000
BL9FU8	38.888611, -77.005000
C2JJVT	38.888611, -77.005000

TABLE 1

Question 24 - Phone Metadata / Navigation	
WebCode	Response
C9ZCG4	38.888611, -77.005000
CHMD3T	38.888611, -77.005000
CKDDDX	38.888611, -77.005000
CMH494	38.888611, -77.005000
D7AC7Y	38.888611, -77.005000
EBZ32N	(38.888611, -77.005000)
EHJ79Q	38.888611, -77.005000
EQURUZ	38.888611 / -77.005000
EYNXN2	Latitude 38.888611 Longitude -77.005000
F27G9V	(38.888611, -77.005000)
GQ3JZL	38.888611, -77.005000
H88C8U	38.888611, -77.005000
HEPJ4T	38.888611, -77.005000
JP4YCX	38.888611,-77.005000
LWCVX9	38.888611,-77.005000
MU3MGV	38.888611, -77.005000
N9JXHH	38.888611, -77.005000
NGD4BJ	38.888611, -77.005000
NZ9WWG	38.888611, -77.005000
PB49XM	38.888611, -77.005000
PGULYB	38.888611, -77.005000
PLMMZP	38.888611, -77.005000
Q29PVJ	38.888611, -77.005000
Q99RM3	Lat N 38, 53, 19 – Long W 77, 0, 18
QGJU94	38.888611, -77.005000
RCRKJC	38.888611, -77.005000
TF4QLP	38.888611, -77.005000
TPBP6E	38.888611, -77.005000
U899KL	38.888610, -77.004998
UEREJE	38.888611, -77.005000
UYQHMY	38.888611 / -77.005000
V9V7DB	38.888611, -77.005000

TABLE 1

Question 24 - Phone Metadata / Navigation	
WebCode	Response
VA6BPD	38.8886, -77.0050
W2UCV3	38.888611, -77.005000
W4KC78	38.888611, -77.005000
W4VZYW	Latitude/Longitude : 38.888611 / -77.005000
WAMHLA	38.888611, -77.005000
WTZ4AC	38.888611, -77.005000
XBWQEF	38.888611,-77.005000
XFRN2L	38.888611, -77.005000
YGFDWD	38.888611 / -77.005000
YK GK4G	N 38.888611 / W 77.005000
ZVXNQ8	38.888611, -77.005000

Question 24: What are the location coordinates for the photograph of the Christmas tree taken with the phone's camera? Provide your response using the following format: Latitude, Longitude (to 6 decimal places)

Consensus Result: 38.888611, -77.005000

Expected Response Explanation:

Location coordinates associated with photos can be found by filtering image files for those containing location metadata. This search reveals only one photograph containing location metadata, a Christmas tree.

Expected Response Illustration:

Image File Metadata

The screenshot shows a file explorer interface with three image thumbnails. The first thumbnail is a Christmas tree, which is highlighted with a blue dashed border. Below the thumbnails is a metadata table for the selected image file.

Type	Value
Date Created	2019-12-13 14:31:04
Latitude	38.88861111111111
Longitude	-77.005
Device Model	SM-J260T1
Device Make	samsung
Source File Path	/img_blk0_mmcbk0.bin/vol_vol28/media/0/DCIM/Camera/20191213_143104.jpg
Artifact ID	-9223372036854775615

TABLE 1

Question 24 - Phone Metadata / Navigation

Image File Metadata



Name: 20191213_143104.jpg
Type: Images
Size (bytes): 2195614
Path: USERDATA (ExtX)/Root/media/0/DCIM/Camera/20191213_143104.jpg
Created: 12/13/2019 2:31:04 PM(UTC-5)
Accessed: 12/13/2019 2:31:04 PM(UTC-5)
Modified: 12/13/2019 2:31:05 PM(UTC-5)
Deleted:
Extraction: Physical
MD5: 9afe5085e2d4f4fc4e202779b6912988
Source file: [20191213_143104.jpg](#)

Metadata

Camera Make: samsung
Camera Model: SM-J260T1
Capture Time: 12/13/2019 2:31:04 PM
Pixel resolution: 3264x1836
Resolution: 72x72 (Unit: Inch)
Orientation: Rotate 90 CW
Lat/Lon: 38.888611 / -77.005000

TABLE 1

Question 25 - Phone Metadata / Navigation

Question 25: According to the text in the file with MD5 hash 7a4860b10c8f6e73813b2d28f4b42893, what does the first amendment not cover?

Manufacturer's Burping

Expected Response:

WebCode	Response
2B66AE	BURPING
2JDY68	BURPING
3LWD98	BURPING
3VNPE9	Burping
63XWWA	Burping
69MBU4	Burping
6EKPAN	Burping
6PRHA7	Burping
74MLQ2	burping
77WBJY	Burping
7RU3AB	BURPING
82DV2X	BURPING
82VLFW	Burping
8CX7F4	Burping
8EN7R9	BURPING
8K97CZ	BURPING
8NC4K8	"burping"
8NNHGL	BURPING
9ANFQZ	burping
9CUZL3	BURPING
9XT88X	Burping
ABE2WW	burping
AD6282	Burping
AEDEP3	BURPING
B4AJ7X	The First Amendment does not cover burping.
BCMEEX	burping
BL9FU8	THE FIRST AMENDMENT DOES NOT COVER BURPING
C2JJVT	Burping

TABLE 1

Question 25 - Phone Metadata / Navigation	
WebCode	Response
C9ZCG4	Burping
CHMD3T	Burping
CKDDDX	Burping
CMH494	Burping
D7AC7Y	Burping
EBZ32N	Burping
EHJ79Q	Burping
EQURUZ	Burping
EYNXN2	Burping
F27G9V	Burping
GQ3JZL	BURPING
H88C8U	BURPING
HEPJ4T	Burping
JP4YCX	BURPING
LWCVX9	Burping
MU3MGV	burping
N9JXHH	burping
NGD4BJ	Burping (The first amendment does not cover burping)
NZ9WWG	Burping
PB49XM	Burping
PGULYB	Burping
PLMMZP	Burping
Q29PVJ	BURPING
Q99RM3	burping
QGJU94	Burping
RCRKJC	Burping
TF4QLP	Burping
TPBP6E	Burping
U899KL	BURPING
UEREJE	The First Amendment Does Not Cover Burping
UYQHMY	Burping
V9V7DB	BURPING

TABLE 1

Question 25 - Phone Metadata / Navigation	
WebCode	Response
VA6BPD	BURPING
W2UCV3	burping
W4KC78	Burping
W4VZYW	BURPING
WAMHLA	burping
WTZ4AC	The first amendment does not cover burping.
XBWQEF	BURPING
XFRN2L	BURPING
YGFDWD	It does not cover burping
YK GK4G	Burping
ZVXNQ8	BURPING

Question 25: According to the text in the file with MD5 hash 7a4860b10c8f6e73813b2d28f4b42893, what does the first amendment not cover?

Consensus Result: Burping

Expected Response Explanation:

To find the file associated with a specific hash, search for a file by hash 7a4860b10c8f6e73813b2d28f4b42893. This search reveals the following image file: USERDATA (ExtX)/Root/media/0/DCIM/Camera/20191213_122019.jpg.

Expected Response Illustration:

Image File



TABLE 1

Question 26 - Phone Metadata / Navigation	
---	--

Question 26: What is the creation date and time (using time zone set for this device) of this file with MD5 hash 7a4860b10c8f6e73813b2d28f4b42893? Provide your response in the following format: MM/DD/YYYY, HH:MM AM/PM

Manufacturer's 12/13/2019 12:20 PM

Expected Response:

WebCode	Response
2B66AE	12/13/2019, 12:20 PM
2JDY68	12/13/2019 12:20 PM
3LWD98	12/13/2019 12:20 PM
3VNPE9	12/13/2019, 12:20 PM
63XWWA	13/12/2019 12:20 PM (UTC-05:00)
69MBU4	12/13/2019 12:20 PM
6EKPAN	12/13/2019 12:20 pm
6PRHA7	12/13/2019, 12:20 PM
74MLQ2	12.13.2019 12:20 PM
77WBJY	12/13/2019, 12:20 PM
7RU3AB	12/13/2019, 12:20 PM
82DV2X	12/13/2019, 12:20 PM
82VLFW	12/13/2019, 12:20 PM
8CX7F4	12/13/2019, 12:20 PM
8EN7R9	12/13/2019, 12:20 PM
8K97CZ	12/13/2019, 12:20 PM
8NC4K8	12/13/2019 12:20
8NNHGL	12/13/2019, 12:20 PM
9ANFQZ	12/13/2019 12:20 PM
9CUZL3	12/13/2019, 12:20:19 (- 5 UTC)
9XT88X	12/13/2019, 12:20 PM
ABE2WW	12/13/2019, 12:20 PM
AD6282	12/13/2019 12:20:19 PM
AEDEP3	12/13/2019, 12:20 PM
B4AJ7X	12/13/2019 12:20:19 PM
BCMEEX	12/13/2019, 12:20 PM
BL9FU8	12/13/2019 12:20 PM
C2JJVT	12/13/2019, 12:20 PM

TABLE 1

Question 26 - Phone Metadata / Navigation	
WebCode	Response
C9ZCG4	12/13/2019 12:20
CHMD3T	12/13/2019 12:20 PM
CKDDDX	12/13/2019 12:20 PM
CMH494	12/13/2019 12:20 PM
D7AC7Y	12/13/2019 12:20:19 PM (UTC-5)
EBZ32N	12/13/2019, 12:20 PM(UTC-5)
EHJ79Q	12/13/2019 12:20:19 PM(UTC-5)
EQURUZ	12/13/2019 17:20 PM
EYNXN2	12/13/2019 12:12 PM
F27G9V	12/13/2019, 12:20 PM
GQ3JZL	12/13/2019, 12:20 PM
H88C8U	12/13/2019 12:20 PM
HEPJ4T	12/13/2019, 12:20 PM
JP4YCX	12/13/2019 12:20 PM
LWCVX9	12/13/2019, 12:20 PM
MU3MGV	12/13/2019 12:20 PM
N9JXHH	12/13/2019, 12:20 PM
NGD4BJ	12/13/2019, 00:20 PM
NZ9WWG	12/13/2019, 05:20 PM
PB49XM	12/13/2019, 12:20 PM
PGULYB	12/13/2019, 12:20:19 PM
PLMMZP	12/13/2019, 12:20 PM
Q29PVJ	12/13/2019, 12:20 PM
Q99RM3	12/13/2019 05:20 p.m. (UTC+0)
QGJU94	12/13/2019, 12:20 PM
RCRKJC	12/13/2019 12:20 PM
TF4QLP	12/13/2019, 12:20 PM
TPBP6E	12/13/2019 5:20 PM(UTC+0)
U899KL	12/13/2019 12:20 PM
UEREJE	12/13/2019 12:20 PM (-5 UTC)
UYQHMY	13/12/2019 12:20 PM
V9V7DB	12/13/2019, 12:20 PM

TABLE 1

Question 26 - Phone Metadata / Navigation	
WebCode	Response
VA6BPD	12/13/2019, 12:20 PM
W2UCV3	12/13/2019, 12:20 PM
W4KC78	12/13/2019 12:20 PM
W4VZYW	12/13/2019 12:20 PM
WAMHLA	12/13/2019 12:20:19 PM
WTZ4AC	12/13/2019, 12:20 PM (UTC-5)
XBWQEF	12/13/2019, 12:20 PM
XFRN2L	12/13/2019, 12:20 PM
YGFDDW	12/13/2019 12:20 PM
YK GK4G	12/13/2019 12:20(UTC-5) (PM)
ZVXNQ8	12/13/2019, 12:20 PM

Question 26: What is the creation date and time (using time zone set for this device) of this file with MD5 hash 7a4860b10c8f6e73813b2d28f4b42893? Provide your response in the following format: MM/DD/YYYY, HH:MM AM/PM

Consensus Result: 12/13/2019, 12:20 PM and all formatting styles which represent the same information. In addition, the same date with the time 05:20 PM which represents the same time but in UTC+0 was also accepted.

Expected Response Explanation:

To find the creation date and time of a file associated with a specific hash, initiate a search for a file by hash 7a4860b10c8f6e73813b2d28f4b42893. This search locates the following file: USERDATA (ExtX)/Root/media/0/DCIM/Camera/20191213_122019.jpg

Expected Response Illustration:

File Name Search


filename Search Results:			
Table		Thumbnail	
Name	Location	MD5 Hash	Created Time
 20191213_122019.jpg	/img_blk0_mmcbk0.bin/vol_vol28/media	7a4860b10c8f6e73813b2d28f4b42893	2019-12-13 12:20:19 EST

TABLE 1

Question 26 - Phone Metadata / Navigation


Image Details

Contacts (34) × contacts2.db ×

Images Go

Details

Events (0)



Name:	20191213_122019.jpg
Type:	Images
Size (bytes):	2508926
Path:	USERDATA (ExtX)/Root/media/0/DCIM/Camera/20191213_122019.jpg
Created:	12/13/2019 12:20:19 PM(UTC-5)
Accessed:	12/13/2019 12:20:19 PM(UTC-5)
Modified:	12/13/2019 12:20:19 PM(UTC-5)
Deleted:	
Extraction:	Physical
MD5:	7a4860b10c8f6e73813b2d28f4b42893
Source file:	20191213_122019.jpg

TABLE 1

Question 27 - Phone Metadata / Navigation

Question 27: What is the name of the saved parking location in the Google Maps app?

Manufacturer's Citgo

Expected Response:

WebCode	Response
2B66AE	
2JDY68	Citgo
3LWD98	Citgo
3VNPE9	In the XRY tool used, a bookmarked location was decoded for the coordinates, latitude 37.683784 and longitude -77.45198. Upon mapping the coordinates, the marker is placed in the middle of a freeway. The closest store with a parking lot is the "Green Top Hunt Fish". In Cellebrite, the same bookmarked location cannot be found. There is a "parking_location.cs" file that contains unreadable data. The only words made out from that file was "Citgo".
63XWWA	citgo
69MBU4	Citgo
6EKPAN	Citgo
6PRHA7	Citgo
74MLQ2	Citgo
77WBJY	Citgo
7RU3AB	Citgo
82DV2X	Citgo
82VLFW	Citgo
8CX7F4	Citgo
8EN7R9	Citgo
8K97CZ	Citgo
8NC4K8	Citgo
8NNHGL	Citgo
9ANFQZ	Citgo
9CUZL3	Citgo
9XT88X	Citgo
ABE2WW	Citgo
AD6282	Citgo
AEDEP3	Citgo
B4AJ7X	work
BCMEEX	Want to go
BL9FU8	Citgo

TABLE 1

Question 27 - Phone Metadata / Navigation	
WebCode	Response
C2JJVT	Citgo
C9ZCG4	Citgo
CHMD3T	Citgo
CKDDDX	Citgo
CMH494	Citgo
D7AC7Y	Citgo
EBZ32N	Citgo
EHJ79Q	Citgo
EQURUZ	Citgo
EYNXN2	ABC Supplies (Tulsa)
F27G9V	Green Top Hunt Fish Parking (N 37.6837840, W 77.4519800)
GQ3JZL	Olive Garden Italian Restaurant. 27501 Broken Branch Ln, Old Town Manassas, VA 20109
H88C8U	Citgo
HEPJ4T	Citgo
JP4YCX	CITGO
LWCVX9	Citgo, Midlothian, VA 23112
MU3MGV	Dumfries Market
N9JXHH	Citgo
NGD4BJ	Quarles Truck Stop
NZ9WWG	Citgo
PB49XM	Citgo
PGULYB	Citgo
PLMMZP	Citgo
Q29PVJ	Citgo
Q99RM3	Citgo
QGJU94	Citgo
RCRKJC	Citgo
TF4QLP	This is beyond the scope of reporting
TPBP6E	Citgo
U899KL	None located
UEREJE	Citgo
UYQHMY	Citgo

TABLE 1

Question 27 - Phone Metadata / Navigation	
WebCode	Response
V9V7DB	Citgo
VA6BPD	Citgo
W2UCV3	Citgo
W4KC78	Citgo Note: When using XRY, there is only one saved location in the Google Maps app which can also be seen in the Locations tab under Bookmarks and it does not have a name associated with it. It has the latitude of 37.683784, and longitude of -77.45198. I used Google Maps to obtain a satellite view of the location and it pin-points to a location in the middle of the intersection of "I-95" and "Kings Acres Rd" in Virginia. It is not a parking location; the nearest-by parking lot corresponds to a facility labeled "Green Top Hunt Fish."
W4VZYW	Citgo
WAMHLA	citgo
WTZ4AC	Citgo
XBWQEF	Citgo
XFRN2L	Citgo
YGFDWD	Citgo
YK GK4G	Citgo
ZVXNQ8	Citgo

Question 27: What is the name of the saved parking location in the Google Maps app?

Consensus Result: Citgo

Expected Response Explanation:

A review of installed apps in /Root/data/com.android.vending/databases/localappstate.db gives the identifier as com.google.android.apps.maps. In this directory is a file named "parking_location.cs". The only name in this file is "Citgo".

Expected Response Illustration:

Parking_Location File

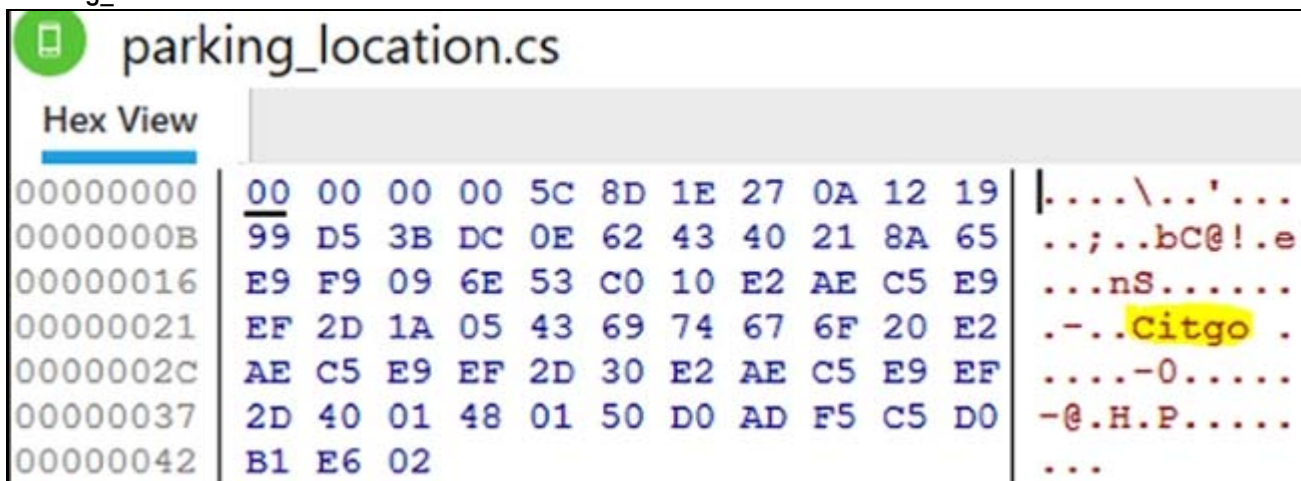


TABLE 1

Question 28 - Applications & Web History

Question 28: What is the name of the cryptocurrency related app installed on this phone?

Manufacturer's BitPay

Expected Response:

WebCode	Response
2B66AE	BitPay – Secure Bitcoin Wallet
2JDY68	BitPay – Secure Bitcoin Wallet
3LWD98	BitPay
3VNPE9	Bitpay
63XWWA	BitPay – Secure Bitcoin Wallet
69MBU4	BitPay
6EKPAN	Bitpay
6PRHA7	BitPay-Secure Bitcoin Wallet
74MLQ2	BitPay – Secure Bitcoin Wallet
77WBJY	Bitpay
7RU3AB	BTC
82DV2X	BitPay – Secure Bitcoin Wallet
82VLFW	BitPay – Secure Bitcoin Wallet
8CX7F4	BitPay-Secure Bitcoin Wallet
8EN7R9	BitPay – Secure Bitcoin Wallet
8K97CZ	Bitpay
8NC4K8	BitPay
8NNHGL	BitPay – Secure Bitcoin Wallet (com.bitpay.wallet)
9ANFQZ	BitPay – Secure Bitcoin Wallet
9CUZL3	BitPay
9XT88X	BitPay – Secure Bitcoin Wallet
ABE2WW	BitPay – Secure Bitcoin Wallet
AD6282	BitPay – Secure Bitcoin wallet
AEDEP3	BitPay
B4AJ7X	BitPay - Secure Bitcoin Wallet
BCMEEEX	BitPay
BL9FU8	BitPay
C2JJVT	BitPay
C9ZCG4	BitPay

TABLE 1

Question 28 - Applications & Web History	
WebCode	Response
CHMD3T	Bitpay - Secure Bitcoin Wallet
CKDDDX	BitPay – Secure Bitcoin Wallet
CMH494	BitPay – Secure Bitcoin Wallet
D7AC7Y	Bit Pay- Secure Bitcoin Wallet
EBZ32N	BitPay
EHJ79Q	BitPay - Secure Bitcoin Wallet
EQURUZ	BitPay
EYNXN2	BitPay
F27G9V	BitPay
GQ3JZL	BitPay – Secure Bitcoin Wallet
H88C8U	BitPay
HEPJ4T	BitPay
JP4YCX	BITPAY - SECURE BITCOIN WALLET.
LWCVX9	BitPay – Secure Bitcoin Wallet
MU3MGV	BitPay - Secure Bitcoin Wallet
N9JXHH	BitPay
NGD4BJ	BitPay - Secure Bitcoin Wallet.
NZ9WWG	BitPay
PB49XM	BitPay - Secure Bitcoin Wallet
PGULYB	BitPay – Secure Bitcoin Wallet
PLMMZP	BitPay - Secure Bitcoin Wallet
Q29PVJ	BitPay – Secure Bitcoin Wallet
Q99RM3	Bitpay-Secure Bitcoin Wallet
QGJU94	BitPay - Secure Bitcoin Wallet
RCRKJC	BitPay – Secure Bitcoin Wallet
TF4QLP	BitPay - Secure Bitcoin Wallet
TPBP6E	BitPay – Secure Bitcoin Wallet
U899KL	BitPay – Secure Bitcoin Wallet
UEREJE	BitPay-Secure Bitcorn Wallet com.bitpay.wallet
UYQHMY	Bitpay
V9V7DB	BitPay
VA6BPD	BitPay-Secure Bitcoin Wallet

TABLE 1

Question 28 - Applications & Web History	
WebCode	Response
W2UCV3	BitPay
W4KC78	BitPay - Secure Bitcoin Wallet (BitPay Wallet)
W4VZYW	BitPay (com.bitpay.wallet)
WAMHLA	BitPay - Secure Bitcoin Wallet
WTZ4AC	BitPay - Secure Bitcoin Wallet
XBWQEF	BitPay - Secure Bitcoin Wallet
XFRN2L	BitPay
YGFDWD	Bitpay
YK GK4G	BitPay
ZVXNQ8	BitPay - Secure Bitcoin Wallet

Question 28: What is the name of the cryptocurrency related app installed on this phone?

Consensus Result: BitPay

Expected Response Explanation:

Review of all installed applications in /Root/data/com.android.vending/databases/localappstate.db shows only one app related to cryptocurrency, Bitpay.

Expected Response Illustration:

Installed Applications

Decoded by	Name	Version	Description	Identifier
	BitPay - Secure Bitcoin Wallet	7.1.7		com.bitpay.wallet

Installed Applications

/img_blk0_mmcbk0.bin/vol_vol28/data/com.android.vending/databases

Name	Location	S	C	Modified Time	Change
localappstate.db	/img_blk0_mmcbk0.bin/vol_vol28/data/com.android.vending...			2019-12-15 13:20:45 EST	2019-12-
localappstate.db-journal	/img_blk0_mmcbk0.bin/vol_vol28/data/com.android.vending...			2019-12-15 13:20:45 EST	2019-12-

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Table	appstate	52 entries	Page 1 of 1	Export to CSV
account	allengonzo79@gmail.com	Android Accessibility Suite	0	60104040
title	allengonzo79@gmail.com	BitPay - Secure Bitcoin Wallet	0	80010000
flags	allengonzo79@gmail.com	Briefing	0	3094

TABLE 1

Question 29 - Applications & Web History

Question 29: Within the app data for the installed cryptocurrency app (reported in question #28), what BTC address is indicated as last by the app?

Manufacturer's 1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m

Expected Response:

WebCode	Response
2B66AE	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
2JDY68	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
3LWD98	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
3VNPE9	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
63XWWA	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
69MBU4	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
6EKPAN	881825ea-cd77-4268-8de1-43bc06f486da
6PRHA7	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9
74MLQ2	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
77WBJY	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
7RU3AB	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
82DV2X	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
82VLFW	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
8CX7F4	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
8EN7R9	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
8K97CZ	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
8NC4K8	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
8NNHGL	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
9ANFQZ	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
9CUZL3	i7c8kvthedc-wnvsucg_q=-0
9XT88X	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
ABE2WW	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
AD6282	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
AEDEP3	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
B4AJ7X	N/A
BCMEEX	
BL9FU8	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
C2JJVT	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m

TABLE 1

Question 29 - Applications & Web History	
WebCode	Response
C9ZCG4	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
CHMD3T	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
CKDDDX	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
CMH494	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
D7AC7Y	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
EBZ32N	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
EHJ79Q	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
EQURUZ	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
EYNXN2	1fjjkpusoosww3atgxab4utegzizonl9m
F27G9V	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
GQ3JZL	3AxHqGSiHujeuRrhasWWMvyyzZUiyBLUg
H88C8U	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
HEPJ4T	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
JP4YCX	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
LWCVX9	com.bitpay.wallet
MU3MGV	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
N9JXHH	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
NGD4BJ	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
NZ9WWG	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
PB49XM	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
PGULYB	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
PLMMZP	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
Q29PVJ	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
Q99RM3	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
QGJU94	
RCRKJC	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
TF4QLP	This is beyond the scope of reporting
TPBP6E	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
U899KL	None located
UEREJE	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
UYQHMY	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
V9V7DB	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m

TABLE 1

Question 29 - Applications & Web History	
WebCode	Response
VA6BPD	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
W2UCV3	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
W4KC78	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
W4VZYW	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
WAMHLA	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
WTZ4AC	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
XBWQEF	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
XFRN2L	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
YGFWD	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
YK GK4G	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m
ZVXNQ8	1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m

Question 29: Within the app data for the installed cryptocurrency app (reported in question #28), what BTC address is indicated as last by the app?

Consensus Result: 1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m

Expected Response Explanation:

The Bitpay app record in /Root/data/com.android.vending/databases/localappstate.db indicates com.bitpay.wallet to be the application identifier. Looking in USERDATA (ExtX)/Root/data/com.bitpay.wallet/files/ discovers a file, lastAddress-881825ea-cd77-4268-8de1-43bc06f486da, containing the address: 1fjjkpUsooSWw3ATgXaB4uTEGzizonL9m.

Expected Response Illustration:

Bitpay App Record

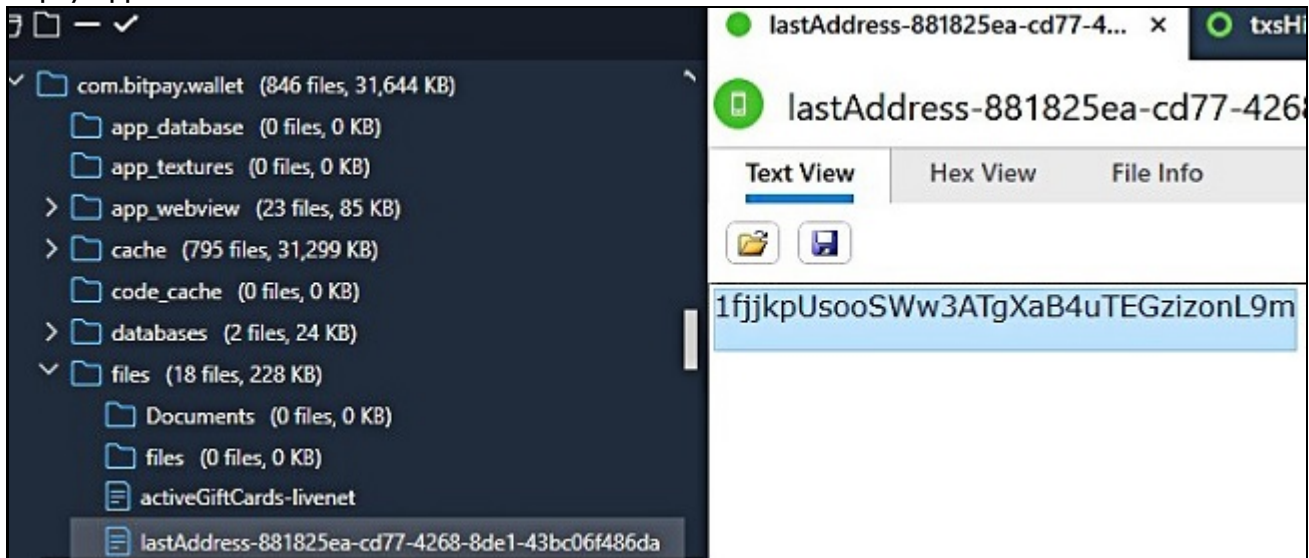


TABLE 1

Question 30 - Applications & Web History

Question 30: What was the amount (in USD) of the last transaction in the cryptocurrency app (reported in question #28)?

Manufacturer's \$1

Expected Response:

WebCode	Response
2B66AE	
2JDY68	1.00 USD
3LWD98	1.00 USD
3VNPE9	\$1.00
63XWWA	1.00 USD
69MBU4	1.00 USD
6EKPAN	\$1
6PRHA7	1.01 USD
74MLQ2	1
77WBJY	1.00
7RU3AB	1.00 USD
82DV2X	1
82VLFW	1.00
8CX7F4	1.00 USD
8EN7R9	1.00 USD
8K97CZ	\$1.00
8NC4K8	1.00
8NNHGL	1.00 USD
9ANFQZ	1
9CUZL3	0.000139 BTC
9XT88X	1.00 USD
ABE2WW	1.01
AD6282	1.01USD
AEDEP3	1
B4AJ7X	N/A
BCMEEX	
BL9FU8	1.00 USD
C2JJVT	1.00

TABLE 1

Question 30 - Applications & Web History	
WebCode	Response
C9ZCG4	1.00
CHMD3T	1.00 USD
CKDDDX	1.00
CMH494	1.01 USD
D7AC7Y	1.00 USD
EBZ32N	1.00USD
EHJ79Q	\$1.00 USD
EQURUZ	1.00
EYNXN2	US\$1
F27G9V	1.00 USD
GQ3JZL	
H88C8U	1.00 USD
HEPJ4T	1.00 USD
JP4YCX	\$1.00
LWCVX9	1.01 USD
MU3MGV	1
N9JXHH	1.00
NGD4BJ	1 USD
NZ9WWG	
PB49XM	1.00 USD
PGULYB	\$1.00 USD
PLMMZP	\$1.00
Q29PVJ	1.00
Q99RM3	1 USD
QGJU94	
RCRKJC	1.00 USD
TF4QLP	This is beyond the scope of reporting
TPBP6E	{"updatedOn":1576208432,"balance":"0.000139 BTC"} alternativeAmountStr = "1.00 USD"
U899KL	None located
UEREJE	1.00 USD The following BTC was located 0.000139
UYQHMY	1.00 USD
V9V7DB	1.00

TABLE 1

Question 30 - Applications & Web History	
WebCode	Response
VA6BPD	\$1.00
W2UCV3	\$1
W4KC78	1.00 USD
W4VZYW	1.01USD (0.000139BTC)
WAMHLA	1.00
WTZ4AC	1.00 USD
XBWQEF	1.00
XFRN2L	1 USD
YGFDWD	1.00 USD
YK GK4G	1.00
ZVXNQ8	1.00 USD in file 1.01 USD in the picture

Question 30: What was the amount (in USD) of the last transaction in the cryptocurrency app (reported in question #28)?

Consensus Result: \$1 and all formatting styles which represent the same information.

Expected Response Explanation:

Located in the same directory noted in question 29, /USERDATA (ExtX)/Root/data/com.bitpay.wallet/files/txsHistory-881825ea-cd77-4268-8de1-43bc06f486da is the last (only) transaction and associated amount.

Expected Response Illustration:

txsHistory-881825ea-cd77-4268-8de1-43bc06f486da Directory

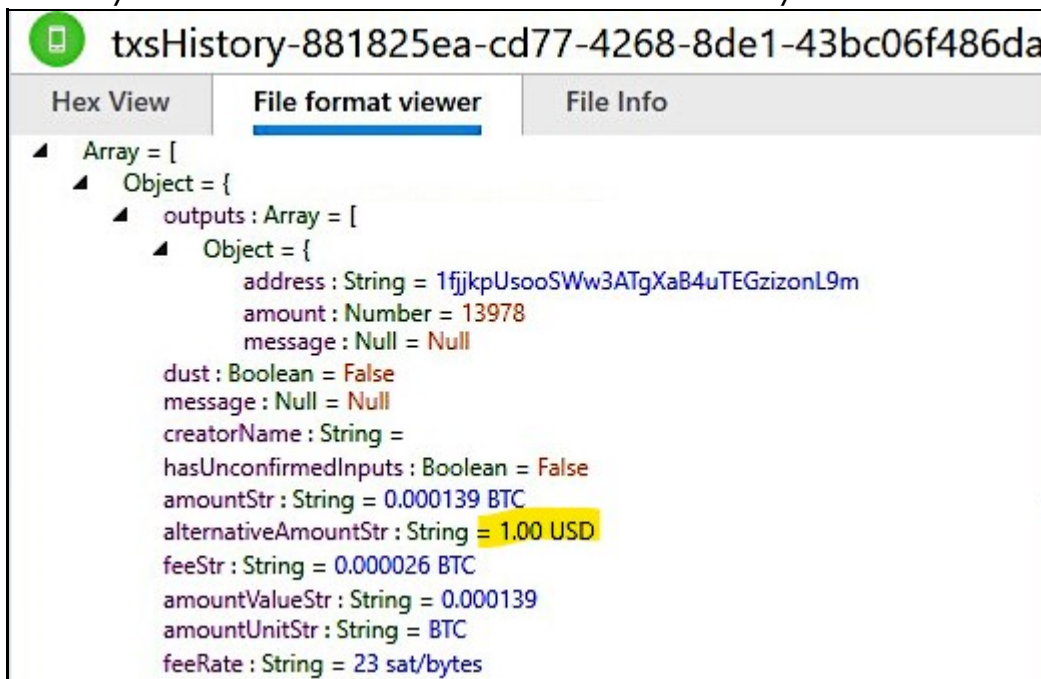


TABLE 1

Question 31 - Applications & Web History

Question 31: At what time (device local time) was the Starbucks app used to conduct a transaction at a Starbucks store on 12/15/2019? Provide your response in the following format: HH:MM AM/PM

Manufacturer's 02:33 PM

Expected Response:

WebCode	Response
2B66AE	09:37 PM
2JDY68	12/15/2019 2:33 PM
3LWD98	02:33 PM
3VNPE9	02:33 PM
63XWWA	14:33 PM
69MBU4	07:33 PM
6EKPAN	07:22 PM
6PRHA7	02:33:57 PM
74MLQ2	07:33 PM
77WBJY	02:33 PM
7RU3AB	02:33 PM
82DV2X	02:33 PM
82VLFW	12/15/2019 02:33 PM
8CX7F4	7:33 PM
8EN7R9	19:33 PM
8K97CZ	14:33 PM
8NC4K8	2:33 PM
8NNHGL	02:33 PM
9ANFQZ	2:33 PM
9CUZL3	07:33 PM
9XT88X	02:33 PM
ABE2WW	02:33 PM
AD6282	14:33 PM
AEDEP3	14:33 PM
B4AJ7X	N/A
BCMEEX	04:37 PM
BL9FU8	02:33 PM
C2JJVT	2:33 PM

TABLE 1

Question 31 - Applications & Web History	
WebCode	Response
C9ZCG4	2:33 PM
CHMD3T	2:33 PM
CKDDDX	02:33 PM
CMH494	02:33 PM
D7AC7Y	7:33:20 PM (UTC-5)
EBZ32N	07:33 PM
EHJ79Q	7:33: PM
EQURUZ	14:33 PM
EYNXN2	02:33 PM
F27G9V	02:33 PM
GQ3JZL	09:37 PM
H88C8U	02:33 PM
HEPJ4T	02:33 PM
JP4YCX	02:33 PM
LWCVX9	07:33 PM
MU3MGV	09:37 PM
N9JXHH	02:33 PM
NGD4BJ	07:33 PM
NZ9WWG	07:33 PM
PB49XM	07:33 PM
PGULYB	14:33 PM
PLMMZP	07:33 PM
Q29PVJ	02:33 PM
Q99RM3	02:33 (PM)
QGJU94	14:33 PM
RCRKJC	02:33 PM
TF4QLP	This is beyond the scope of reporting
TPBP6E	"2019-12-15T 19:33:57 PM
U899KL	12/15/2019 2:17 PM
UEREJE	02:33 PM (Local Date)
UYQHMY	14:33 PM
V9V7DB	02:33 PM

TABLE 1

Question 31 - Applications & Web History	
WebCode	Response
VA6BPD	02:33 PM
W2UCV3	02:33 PM
W4KC78	02:33 PM
W4VZYW	2:33 PM
WAMHLA	09:37 PM
WTZ4AC	2:33 PM
XBWQEF	02:33 PM
XFRN2L	02:33 PM
YGFDWD	16:37 PM
YK GK4G	14:33 PM
ZVXNQ8	02:33 PM

Question 31: At what time (device local time) was the Starbucks app used to conduct a transaction at a Starbucks store on 12/15/2019? Provide your response in the following format: HH:MM AM/PM

Consensus Result: 02:33PM and all formatting styles which represent the same information. In addition, the time of 07:33 PM which represents the same time but in UTC+0 was also accepted.

Expected Response Explanation:

Starbucks app data is stored in /USERDATA (ExtX)/Root/data/com.starbucks.mobilecard. The transaction data can be found in the following database: USERDATA (ExtX)/Root/data/com.starbucks.mobilecard/databases/com.starbucks.mobilecard.db. There are three records in the account_history table for this database. Only one contains full information for an actual transaction at an identified Starbucks store. In this record is the svcTransaction field; the localDate tag contains the correct local time of the transaction

TABLE 1

Question 31 - Applications & Web History

Expected Response Illustration:

com.starbucks.mobilecard.db Account History

The screenshot displays the 'com.starbucks.mobilecard.db' application interface. It features a 'Database View' tab and a list of records under the 'account_history' table. The selected record is expanded to show a detailed JSON object with the following fields:

- cardId : String = 876F75FB9CD21EAC9E
- currency : String = USD
- historyId : Number = 13772300906
- historyType : String = SvcTransactionWithPoints
- isoDate : Date = 12/15/2019 7:33:57 PM
- localCurrency : String = USD
- localTotalAccruableAmount : Number = 15.91
- localTotalAmount : Number = 16.75
- modifiedDate : Date = 12/15/2019 9:37:56 PM
- points : Array = []
- svcTransaction : Object = {
 - brandName : String = Starbucks
 - checkId : String = BSVY8wucKO
 - currency : String = USD
 - isVoid : Boolean = False
 - localCurrency : String = USD
 - localDate : Date = 12/15/2019 2:33:57 PM
 - localTransactionAccruableAmount : Number = 15.91
 - localTransactionAmount : Number = 16.75
 - localizedStoreName : String = Fredericksburg, Warrenton Road
 - newBalance : Number = 3.25
 - storeId : String = 23175
 - storeNumber : String = 23175
 - storeType : String = Physical

TABLE 1

Question 31 - Applications & Web History

com.starbucks.mobilecard.db Account History

img_bk0_nmcbl0.bin/vol_vo128\data/com.starbucks.mobilecard/databases

Name	Location	S	C	Modified Time	Change Time
apptentive	/img_bk0_nmcbl0.bin/vol_vo128\data/com.starbucks.mobi...			2019-12-15 19:33:26 EST	2019-12-16 09:00:01 EST
apptentive-journal	/img_bk0_nmcbl0.bin/vol_vo128\data/com.starbucks.mobi...			2019-12-15 13:19:19 EST	2019-12-15 13:19:19 EST
apptimize.db	/img_bk0_nmcbl0.bin/vol_vo128\data/com.starbucks.mobi...			2019-12-15 19:34:06 EST	2019-12-15 19:34:06 EST
apptimize.db-journal	/img_bk0_nmcbl0.bin/vol_vo128\data/com.starbucks.mobi...			2019-12-15 19:34:06 EST	2019-12-15 19:34:06 EST
apptimize_tmp.db	/img_bk0_nmcbl0.bin/vol_vo128\data/com.starbucks.mobi...			2019-12-15 13:19:21 EST	2019-12-15 14:12:41 EST
apptimize_tmp.db-journal	/img_bk0_nmcbl0.bin/vol_vo128\data/com.starbucks.mobi...			2019-12-15 13:19:21 EST	2019-12-15 13:19:21 EST
com.starbucks.mobilecard.db	/img_bk0_nmcbl0.bin/vol_vo128\data/com.starbucks.mobi...			2019-12-15 19:33:20 EST	2019-12-15 19:33:20 EST
com.starbucks.mobilecard.db-journal	/img_bk0_nmcbl0.bin/vol_vo128\data/com.starbucks.mobi...			2019-12-15 14:17:12 EST	2019-12-15 14:17:12 EST

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Matches on page: 1 of 1 Match < > Page: 1 of 1 Page < > 100% Reset

```

android_metadata
  locale
  en_US
account_history
  historyId modified data
  13772136951 2019-12-15T19:17:15.0470000Z {"cardId":"876F75FB5CD21D85D","currency":
"USD","historyId":13772136951,"historyType":"SvcTransaction","isoDate":"2019-12-15T19:17:14.5342785Z",
"localCurrency":"USD","localTotalAccruableAmount":0,"localTotalAmount":0,"modifiedDate":
"2019-12-15T19:17:15.0470000Z","svcTransaction":{"brandName":"Starbucks","currency":"USD","isVoid":false,
"localCurrency":"USD","localDate":"2019-12-15T11:17:14.0624662-08:00","localTransactionAccruableAmount":
0,"localTransactionAmount":0,"newBalance":0,"storeId":"10","storeNumber":"10","storeType":"Starbucks.
com","tax":0,"tipInfo":{"amount":0,"status":"None","tipTransactionId":0,"tippable":false},"transactionAmount":
0,"transactionType":"Activation"},"totalAmount":0}|13772300906 2019-12-15T21:37:56.7630000Z
{"cardId":"876F75FB5CD21EAC5E","currency":"USD","historyId":13772300906,"historyType":"SvcTransactionWithPoints",
"isoDate":"2019-12-15T19:33:57.0000000Z","localCurrency":"USD","localTotalAccruableAmount":15.91,"localTotalAmount":16.75,
"modifiedDate":"2019-12-15T21:37:56.7630000Z","points":{"amount":16.75,"currency":0,"expirationDate":"2020-0
7-02T06:59:59.0000000Z","pointCategory":"Reward","pointType":"Purchases","pointsEarned":31,"promotionName":
"Starbucks Reward Points Accrual","status":"Processed","storeNumber":"023175","totalPointsEarned":31.82}|}.
"svcTransaction":{"brandName":"Starbucks","checkId":"BSVY8wucK0","currency":"USD","isVoid":false,"localCurrency":
"USD","localDate":"2019-12-15T21:33:57.0000000Z","localTransactionAccruableAmount":15.91,"localTransactionAmount":
16.75,"localizedStoreName":"Fredericksburg, Warrenton Road","newBalance":3.25,"storeId":"23175","storeNumber":"23175",
"storeType":"Physical","tax":0,"tipInfo":{"amount":1,"status":"Success","tipTransactionId":13773395493,"tippable":true,
"tippableEndDate":"2019-12-15T21:33:57.0000000Z"},"transactionAmount":16.75,"transactionType":"Redemption"},"totalAmount":16.75}
    
```


TABLE 1

Question 32 - Applications & Web History

Question 32: What was the transaction amount of the Starbucks transaction mentioned in question #31 (in USD, not counting tip)?

Manufacturer's 16.75

Expected Response:

WebCode	Response
2B66AE	1 USD
2JDY68	\$16.75
3LWD98	15.91 USD
3VNPE9	\$16.75 including tax and not tips.
63XWWA	16.75
69MBU4	15,91
6EKPAN	16.75
6PRHA7	\$16.75
74MLQ2	15,91
77WBJY	16.75
7RU3AB	16.75 USD
82DV2X	16.75
82VLFW	16.75
8CX7F4	15.91
8EN7R9	16.75 USD
8K97CZ	\$16.75
8NC4K8	15.91
8NNHGL	15,91
9ANFQZ	16.75
9CUZL3	15.91
9XT88X	16.75
ABE2WW	16.75
AD6282	15.91USD
AEDEP3	16,75
B4AJ7X	N/A
BCMEEX	\$15.91
BL9FU8	16.75
C2JJVT	16.75

TABLE 1

Question 32 - Applications & Web History	
WebCode	Response
C9ZCG4	16.75
CHMD3T	16.75
CKDDDX	15.75
CMH494	16.75
D7AC7Y	\$15.91
EBZ32N	\$16.75
EHJ79Q	\$16.75
EQURUZ	15.91
EYNXN2	16.75
F27G9V	16.75 USD
GQ3JZL	16.75
H88C8U	15.91
HEPJ4T	16.75
JP4YCX	\$16.75
LWCVX9	USD 15.91
MU3MGV	16.75
N9JXHH	15.91
NGD4BJ	16,75 USD
NZ9WWG	16.75
PB49XM	15.91
PGULYB	\$15.91 USD
PLMMZP	\$15.91
Q29PVJ	16.75
Q99RM3	15,75 USD
QGJU94	15.91
RCRKJC	\$15.91
TF4QLP	This is beyond the scope of reporting
TPBP6E	15.91
U899KL	\$17.75
UEREJE	The "local transaction amount" was 16.75.
UYQHMY	16.75
V9V7DB	16.75

TABLE 1

Question 32 - Applications & Web History	
WebCode	Response
VA6BPD	\$16.75
W2UCV3	\$16.75
W4KC78	\$15.91 (before taxes) \$16.75 (tax included)
W4VZYW	16.75 (USD)
WAMHLA	15,91\$
WTZ4AC	16.75
XBWQEF	15.91
XFRN2L	15,91
YGFDWD	1.00 USD
YKGK4G	\$16.75
ZVXNQ8	16.75

Question 32: What was the transaction amount of the Starbucks transaction mentioned in question #31 (in USD, not counting tip)?

Consensus Result: 16.75 and all formatting styles which represent the same information. In addition, the value 15.91 which is the transaction before taxes was also accepted due to the ambiguity of the question.

Expected Response Explanation:

The Starbucks app data is stored in /USERDATA (ExtX)/Root/data/com.starbucks.mobilecard. Transaction data can be found in /USERDATA (ExtX)/Root/data/com.starbucks.mobilecard/databases/com.starbucks.mobilecard.db. There are three records in the account_history table for this database. Only one contains full information for an actual transaction at an identified Starbucks store. In this record in the svcTransaction field, the localTotalAccruableAmount or the localTotalAmount tag contains the requested information.

TABLE 1

Question 32 - Applications & Web History

Expected Response Illustration:

Starbucks database

mg_blk0_mmcbk0.bin/vol_vol28/data/com.starbucks.mobilecard/databases

Table		Thumbnail		
Name	Location	S	C	Modified Time
apptentive	/img_blk0_mmcbk0.bin/vol_vol28/data/com.starbucks.mobi...			2019-12-15 19:33:26 ES
apptentive-journal	/img_blk0_mmcbk0.bin/vol_vol28/data/com.starbucks.mobi...			2019-12-15 13:19:19 ES
apptimize.db	/img_blk0_mmcbk0.bin/vol_vol28/data/com.starbucks.mobi...			2019-12-15 19:34:06 ES
apptimize.db-journal	/img_blk0_mmcbk0.bin/vol_vol28/data/com.starbucks.mobi...			2019-12-15 19:34:06 ES
apptimize_tmp.db	/img_blk0_mmcbk0.bin/vol_vol28/data/com.starbucks.mobi...			2019-12-15 13:19:21 ES
apptimize_tmp.db-journal	/img_blk0_mmcbk0.bin/vol_vol28/data/com.starbucks.mobi...			2019-12-15 13:19:21 ES
com.starbucks.mobilecard.db	/img_blk0_mmcbk0.bin/vol_vol28/data/com.starbucks.mobi...			2019-12-15 19:33:20 ES
com.starbucks.mobilecard.db-journal	/img_blk0_mmcbk0.bin/vol_vol28/data/com.starbucks.mobi...			2019-12-15 14:17:12 ES

Strings Indexed Text Translation

```

android_metadata
  locale
  en_US
account_history
  historyId modified data
  13772136951 2019-12-15T19:17:15.0470000Z {"cardId":"876F75FB9CD21DAB9D","currency":"USD",
localCurrency":"USD","localTotalAccruableAmount":0,"localTotalAmount":0,"modifiedDate":"2019-12-15
urrency":"USD","localDate":"2019-12-15T11:17:14.0524662-08:00","localTransactionAccruableAmount":
com","tax":0,"tipInfo":{"amount":0,"status":"None","tipTransactionId":0,"tippable":false},"transa
  13772300906 2019-12-15T21:37:56.7630000Z {"cardId":"876F75FB9CD21EAC9E","currency":"USD
00000Z","localCurrency":"USD","localTotalAccruableAmount":15.91,"localTotalAmount":16.75,"modifie
7-02T06:59:59.0000000Z","pointCategory":"Reward","pointType":"Purchases","pointsEarned":31,"promc
arned":31.82}},{"svcTransaction":{"brandName":"Starbucks","checkId":"BSVY8wacKO","currency":"USD",
ableAmount":15.91,"localTransactionAmount":16.75,"localizedStoreName":"Fredericksburg, Warrenton
fo":{"amount":1,"status":"Success","tipTransactionId":13773385682,"tippable":true,"tippableEndDat
out":16.75}
    
```

TABLE 1

Question 32 - Applications & Web History

com.starbucks.mobilecard.db Account History

The screenshot displays the 'account_history' table within the 'com.starbucks.mobilecard.db' database. The 'data' column contains three rows of JSON data. The selected row is expanded in the 'Text' column, showing the following object structure:

```

Object = {
  cardId : String = 876F75FB9CD21EAC9E
  currency : String = USD
  historyId : Number = 13772300906
  historyType : String = SvcTransactionWithPoints
  isoDate : Date = 12/15/2019 7:33:57 PM
  localCurrency : String = USD
  localTotalAccruableAmount : Number = 15.91
  localTotalAmount : Number = 16.75
  modifiedDate : Date = 12/15/2019 9:37:56 PM
  points : Array = [
  svcTransaction : Object = {
    brandName : String = Starbucks
    checkId : String = BSVY8wucKO
    currency : String = USD
    isVoid : Boolean = False
    localCurrency : String = USD
    localDate : Date = 12/15/2019 2:33:57 PM
    localTransactionAccruableAmount : Number = 15.91
    localTransactionAmount : Number = 16.75
    localizedStoreName : String = Fredericksburg, Warrenton Road
    newBalance : Number = 3.25
    storeId : String = 23175
    storeNumber : String = 23175
    storeType : String = Physical
  }
  ]
}
    
```

TABLE 1

Question 33 - Applications & Web History	
--	--

Question 33: As recorded on the phone, at what Starbucks store was this transaction conducted (transaction from question #31)?

Manufacturer's Fredericksburg, Warrenton Road

Expected Response:

WebCode	Response
2B66AE	Fredericksburg, Warrenton Road
2JDY68	Fredericksburg, Warrenton Road (storeld: 23175)
3LWD98	Store ID 23175
3VNPE9	Fredericksburg, Warrenton Road
63XWWA	Fredericksburg, Warrenton Road
69MBU4	Fredericksburg, Warrenton Road
6EKPAN	Fredericksburg, Warrenton Road
6PRHA7	Fredricksburg, Warrenton Road
74MLQ2	Fredericksburg, Warrenton Road
77WBJY	Store #23175, location Fredericksburg, Warrenton Road.
7RU3AB	Fredericksburg, Warrenton Road
82DV2X	Fredericksburg, Warrenton Road
82VLFW	Store Number: 23175, Store Name: Fredericksburg, Warrenton Road
8CX7F4	Store 23175 Fredericksburg, Warrenton Road
8EN7R9	Fredericksburg, Warrenton Road.
8K97CZ	Fredericksburg, Warrenton Road
8NC4K8	Fredericksburg, Warrenton Road
8NNHGL	Fredericksburg, Warrenton Road
9ANFQZ	Fredericksburg, Warrenton Road
9CUZL3	Store ID 23175
9XT88X	Fredericksburg, Warrenton Road
ABE2WW	Fredericksburg, Warrenton Road
AD6282	Fredericksburg, Warrento
AEDEP3	Fredericksburg, Warrenton Road
B4AJ7X	N/A
BCMEEX	Fredericksburg, Warrenton Road
BL9FU8	Fredericksburg, Warrenton Road
C2JJVT	Fredericksburg, Warrenton Road

TABLE 1

Question 33 - Applications & Web History	
WebCode	Response
C9ZCG4	Fredericksburg, Warrenton Road
CHMD3T	Fredericksburg, Warrenton Road
CKDDDX	Fredericksburg, Warrenton Road
CMH494	Fredericksburg, Warrenton Road
D7AC7Y	Fredericksburg Warrenton Rd Store ID 23175
EBZ32N	"Fredericksburg, Warrenton Road"
EHJ79Q	Fredericksburg, Warrenton Road
EQURUZ	Fredericksburg, Warrenton Road
EYNXN2	Fredericksburg Warrenton Road (Store 23175)
F27G9V	Fredericksburg, Warrenton Road
GQ3JZL	Fredericksburg, Warrenton Road
H88C8U	Store Number: 23175
HEPJ4T	Fredericksburg, Warrenton Road
JP4YCX	Fredericksburg, WARRENTON ROAD (STORE ID 23175)
LWCVX9	Fredericksburg, Warrenton Road
MU3MGV	Fredericksburg, Warrenton Road
N9JXHH	Fredericksburg, Warrenton
NGD4BJ	Fredericksburg, Warrenton Road
NZ9WWG	Fredericksburg, Warrenton Road
PB49XM	Store 23175 Fredricksburg, Warrenton Rd.
PGULYB	Fredericksburg, Warrenton Road
PLMMZP	Fredricksburg, Warrenton Road
Q29PVJ	Fredericksburg, Warrenton Road
Q99RM3	Fredericksburg Warrenton Road
QGJU94	Store number 023175
RCRKJC	Fredericksburg, Warrenton Road
TF4QLP	This is beyond the scope of reporting
TPBP6E	StoreName:"Fredericksburg, Warrenton Road
U899KL	Fredricksburg Warrenton Rd.
UEREJE	Store Number 23175 Fredericksburg, Warrenton Road
UYQHMY	Fredericksburg, Warrenton Road
V9V7DB	Fredericksburg, Warrenton Road

TABLE 1

Question 33 - Applications & Web History	
WebCode	Response
VA6BPD	Fredericksburg, Warrentown Road
W2UCV3	Fredericksburg, Warrenton Road
W4KC78	Fredericksburg, Warrenton Road
W4VZYW	Fredericksburg, Warrenton Road
WAMHLA	Fredericksburg
WTZ4AC	Fredericksburg, Warrenton Road (Store # 23175)
XBWQEF	Fredericksburg, Warrenton Road
XFRN2L	Fredericksburg, Warrenton Road
YGFWD	Store# 23175, FREDERICKSBURG, WARRENTON ROAD
YK GK4G	"storeNumber": "23175" "localizedStoreName": "Fredericksburg, Warrenton Road"
ZVXNQ8	Fredericksburg, Warrenton Road

Question 33: As recorded on the phone, at what Starbucks store was this transaction conducted (transaction from question #31)?

Consensus Result: Fredericksburg, Warrenton Road and all formatting styles which represent the same information. Slight variations of the expected result were disregarded as outliers, if they were easily determined to be a spelling error.

Expected Response Explanation:

Starbucks app data is stored in /USERDATA (ExtX)/Root/data/com.starbucks.mobilecard. Transaction data can be found in /USERDATA (ExtX)/Root/data/com.starbucks.mobilecard/databases/com.starbucks.mobilecard.db. There are three records in the account_history table for this database. Only one contains full information for an actual transaction at an identified Starbucks store. In this record in the svcTransaction field, the localizedStoreName tag contains the requested information

Expected Response Illustration:

com.starbucks.mobilecard.db Account History

```

svcTransaction : Object = {
  brandName : String = Starbucks
  checkId : String = BSVY8wucKO
  currency : String = USD
  isVoid : Boolean = False
  localCurrency : String = USD
  localDate : Date = 12/15/2019 2:33:57 PM
  localTransactionAccruableAmount : Number = 15.91
  localTransactionAmount : Number = 16.75
  localizedStoreName : String = Fredericksburg, Warrenton Road
  newBalance : Number = 3.25
  storeId : String = 23175
  storeNumber : String = 23175
  storeType : String = Physical
  tax : Number = 0
    
```


TABLE 1

Question 34 - Applications & Web History

Question 34: Provide the URL the user bookmarked for a dark web website.

Manufacturer's <http://apollon5e246vvhj.onion/login.php>

Expected Response:

WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
2B66AE	http://en.wt1.la/	
2JDY68	http://apollon5e246vvhj.onion/login.php	
3LWD98	http://apollon5e246vvhj.onion/login.php	
3VNPE9	http://apollon5e246vvhj.onion/login.php is listed in the bookmarks of Tor browser. Under the bookmarks of Google Chrome, https://binlist.net and http://en.wt1.la are listed. The question didn't specify which bookmarks to answer, however, both the http://apollon5e246vvhj.onion/login.php and http://en.wt1.la URLs appear to be dark web related.	
63XWWA	http://en.wt1.la/	
69MBU4	http://apollon5e246vvhj.onion/login.php	
6EKPAN	http://apollon5e246vvhj.onion/login.php	
6PRHA7	http://en.wt1.la/	
74MLQ2	http://apollon5e246vvhj.onion/login.php	
77WBJY	http://apollon5e246vvhj.onion/login.php	
7RU3AB	http://apollon5e246vvhj.onion/login.php	
82DV2X	http://apollon5e246vvhj.onion/login.php	
82VLFW	http://apollon5e246vvhj.onion/login.php	
8CX7F4	http://apollon5e246vvhj.onion/login.php	
8EN7R9	http://en.wt1.la/	
8K97CZ	http://apollon5e246vvhj.onion/login.php	
8NC4K8	http://wt1.la/	
8NNHGL	http://en.wt1.la/	
9ANFQZ	http://apollon5e246vvhj.onion/login.php	
9CUZL3	http://apollon5e246vvhj.onion/login.php	
9XT88X	http://apollon5e246vvhj.onion/login.php	
ABE2WW	http://apollon5e246vvhj.onion/login.php	
AD6282	http://apollon5e246vvhj.onion/login.php	
AEDEP3	http://en.wt1.la/	
B4AJ7X	http://grymktgwyxq3sikl.onion	
BCMEEEX	http://en.wt1.la/	
BL9FU8	http://apollon5e246vvhj.onion/login.php	

TABLE 1

Question 34 - Applications & Web History		
WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
C2JJVT	http://apollon5e246vvhj.onion/login.php	
C9ZCG4	http://en.wt1.la/	
CHMD3T	http://apollon5e246vvhj.onion/login.php	
CKDDDX	http://apollon5e246vvhj.onion/login.php	
CMH494	http://en.wt1.la/	
D7AC7Y	http://apollan5e24vvhj.onion/login.php	
EBZ32N	http://apollon5e246vvhj.onion/login.php	
EHJ79Q	http://apollon5e246vvhj.onion/login.php	
EQURUZ	http://apollon5e246vvhj.onion/login.php	
EYNXN2	http://apollon5e246vvhj.onion/login.php	
F27G9V	http://apollon5e246vvhj.onion/login.php	
GQ3JZL	http://en.wt1.la/	
H88C8U	http://apollon5e246vvhj.onion/login.php	
HEPJ4T	http://apollon5e246vvhj.onion/login.php	
JP4YCX	HTTP://APOLLON5E246VWHJ.ONION/LOGIN.PHP	
LWCVX9	http://apollon5e246vvhj.onion/login.php	
MU3MGV	http://en.wt1.la/	
N9JXHH	binlist.net	
NGD4BJ	https://torproject.org	
NZ9WWG	http://www.mocospace.com	
PB49XM	http://apollon5e246vvhj.onion/Login.php	
PGULYB	http://apollon5e246vvhj.onion/login.php	
PLMMZP	http://apollon5e246vvhj.onion/login.php	
Q29PVJ	http://apollon5e246vvhj.onion/login.php http://en.wt1.la/	
Q99RM3	http://en.wt1.la	
QGJU94	http://apollon5e246vvhj.onion/login.php	
RCRKJC	http://en.wt1.la/	
TF4QLP	https://binlist.net/	
TPBP6E	http://en.wt1.la/	
U899KL	https://binlist.net/	
UEREJE	http://apollon5e246vvhj.onion/login.php	
UYQHMY	http://apollon5e246vvhj.onion/login.php - Tor Browser	

TABLE 1

Question 34 - Applications & Web History		
WebCode	Response	** Inconsistencies not highlighted; No consensus achieved **
V9V7DB	http://apollon5e246vvhj.onion/login.php	
VA6BPD	http://en.wt1.la/	
W2UCV3	http://apollon5e246vvhj.onion/login.php	
W4KC78	http://en.wt1.la/ (is the URL that was located as having been bookmarked) http://apollon5e246vvhj.onion/login.php (is a URL that is consistent with a dark web website but was not parsed as a bookmark and was located in the browser.db)	
W4VZYW	http://apollon5e246vvhj.onion/login.php	
WAMHLA	http://apollon5e246vvhj.onion/login.php	
WTZ4AC	http://apollon5e246vvhj.onion/login.php (Login-Apollon Market)	
XBWQEF	http://apollon5e246vvhj.onion/login.php	
XFRN2L	http://apollon5e246vvhj.onion/login.php	
YGFDWD	http://en.wt1.la/	
YK GK4G	http://en.wt1.la/	
ZVXNQ8	http://apollon5e246vvhj.onion/login.php	

Question 34: Provide the URL the user bookmarked for a dark web website.

Consensus Result: A consensus was not achieved. The objective of this question was to have the examiner identify a dark web website URL.

Expected Response Explanation:

Dark web websites are hosted via hidden services on the Tor network, have urls ending in .onion, and are accessed via a specially configured Firefox browser, the Tor browser. Per the following database:

USERDATA (ExtX)/Root/data/com.android.vending/databases/localappstate.db, data for the installed Tor browser is stored at /USERDATA (ExtX)/Root/data/org.torproject.torbrowser.

Bookmarks for the Tor browser are stored in the "bookmarks" table in the browser.db file in /USERDATA (ExtX)/Root/data/org.torproject.torbrowser/files/mozilla/1pv5bhre.default/browser.db. This list contains only one url with a .onion extension, http://apollon5e246vvhj.onion/login.php, the Apollon darknet market. A number of other participants reported http://en.wt1.la/ as the url. This link is for WT1 Store, a carding and dumps marketplace on the regular internet, not a dark web website.

Expected Response Illustration:

Browser Bookmarks

id	title	url
10		http://checkip.amazonaws.com/
9	Login - Apollon Market	http://apollon5e246vvhj.onion/login.php
8	Firefox: Support	https://support.mozilla.org/products/mobile?utm_source=inproduct&utm_medium=default-bo
7	Firefox: Customize with add-ons	https://addons.mozilla.org/android?utm_source=inproduct&utm_medium=default-bookmarks&
6	Firefox: About your browser	about:firefox
5	Other Bookmarks	
4	Tags	
3	Bookmarks Menu	
2	Bookmarks Toolbar	
1	Mobile Bookmarks	

TABLE 1

Question 35 - Applications & Web History

Question 35: What application did the user use to manage PGP keys?

Manufacturer's OpenKeychain

Expected Response:

WebCode	Response
2B66AE	OpenKeychain: Easy PGP
2JDY68	OpenKeychain: Easy PGP
3LWD98	OpenKeychain: Easy PGP
3VNPE9	OpenKeychain: Easy PGP is the installed application on the phone. However, within the email contents, Mailvelope version 4.2.0 was used to manage the emails communicating with PGP keys. Mailvelope appears to be an add-on feature for web browsers rather than an installed application on the phone.
63XWWA	OpenKeychain: Easy PGP
69MBU4	OpenKeychain: Easy PGP
6EKPAN	OpenKeychain: Easy PGP
6PRHA7	OpenKeychain: Easy PGP
74MLQ2	OpenKeychain: Easy PGP
77WBJY	OpenKeychain: Easy PGP
7RU3AB	OpenKeychain: Easy PGP
82DV2X	OpenKeychain: Easy PGP
82VLFW	OpenKeychain: Easy PGP
8CX7F4	OpenKeychain: Easy PGP
8EN7R9	OpenKeychain: Easy PGP
8K97CZ	OpenKeychain: Easy PGP
8NC4K8	OpenKeychain: Easy PGP
8NNHGL	OpenKeychain: Easy PGP
9ANFQZ	OpenKeychain: Easy PGP
9CUZL3	OpenKeyChain: Easy PGP
9XT88X	OpenKeychain: Easy PGP
ABE2WW	OpenKeychain: Easy PGP
AD6282	Open
AEDEP3	OpenKeychain
B4AJ7X	N/A
BCMEEX	OpenKeychain: Easy PGP
BL9FU8	OpenKeychain: Easy PGP
C2JJVT	OpenKeychain: Easy PGP

TABLE 1

Question 35 - Applications & Web History	
WebCode	Response
C9ZCG4	OpenKeychain
CHMD3T	OpenKeychain: Easy PGP
CKDDDX	OpenKeychain: Easy PGP
CMH494	OpenKeychain: Easy PGP
D7AC7Y	OpenKeychain: Easy PGP
EBZ32N	OpenKeychain: Easy PGP
EHJ79Q	OpenKeychain: Easy PGP
EQURUZ	OpenKeychain: Easy PGP
EYNXN2	open keychain (easy PGP)
F27G9V	OpenKeychain: Easy PGP _Version 5.4
GQ3JZL	OpenKeychain: Easy PGP
H88C8U	OpenKeychain: Easy PGP
HEPJ4T	OpenKeychain
JP4YCX	OPENKEYCHAIN:EASY PGP
LWCVX9	OpenKeychain: Easy PGP
MU3MGV	OpenKeychain: Easy PGP
N9JXHH	OpenKeychain
NGD4BJ	OpenKeychain: Easy PGP
NZ9WWG	OpenKeychain
PB49XM	Open Key Chain: EasyPGP
PGULYB	OpenKeychain: Easy PGP
PLMMZP	OpenKeychain: Easy PGP
Q29PVJ	OpenKeychain Version 5.4 (54000)
Q99RM3	OpenKeychain: Easy PGP
QGJU94	OpenKeychain
RCRKJC	OpenKeychain: Easy PGP
TF4QLP	OpenKeychain: Easy PGP
TPBP6E	OpenKeychain
U899KL	Mailvelope
UEREJE	OpenKeychain: Easy PGP org.sufficientlysecure.keychain
UYQHMY	OpenKeychain: Easy PGP
V9V7DB	OpenKeychain

TABLE 1

Question 35 - Applications & Web History	
WebCode	Response
VA6BPD	OpenKeychain: Easy PGP
W2UCV3	OpenKeychain: Easy PGP
W4KC78	OpenKeychain: Easy PGP
W4VZYW	OpenKeychain: Easy PGP
WAMHLA	OpenKeychain: Easy PGP
WTZ4AC	OpenKeyChain: Easy PGP
XBWQEF	OpenKeychain
XFRN2L	OpenKeyChain: Easy PGP
YGFDWD	OpenKeychain: Easy PGP
YK GK4G	OpenKeyChain
ZVXNQ8	OpenKeychain - Easy PGP

Question 35: What application did the user use to manage PGP keys?

Consensus Result: OpenKeychain: Easy PGP

Expected Response Explanation:

The application the user utilized to manage the PGP keys can be found in the following database: USERDATA (ExtX)/Root/data/com.android.vending/databases/localappstate.db. There was only one PGP application installed.

Expected Response Illustration:

Installed Applications

Installed Applications (176)									
Folder	Icons	Checked	#	Actions	Decoded by	Name	Version		
		<input checked="" type="checkbox"/>	1		Yes	OpenKeychain: Easy PGP	5.4		

TABLE 1

Question 36 - Applications & Web History	
--	--

Question 36: Who's key (other than the user) did the user have stored in his PGP keychain? (provide email address)

Manufacturer's francismilligan599@gmail.com

Expected Response:

WebCode	Response
2B66AE	francismilligan599@gmail.com
2JDY68	francismilligan599@gmail.com
3LWD98	francismilligan599@gmail.com
3VNPE9	francismilligan599@gmail.com
63XWWA	Francismilligan599@gmail.com
69MBU4	francismilligan599@gmail.com
6EKPAN	francismilligan599@gmail.com
6PRHA7	francismilligan599@gmail.com
74MLQ2	francismilligan599@gmail.com
77WBJY	francismilligan599@gmail.com
7RU3AB	francismilligan599@gmail.com
82DV2X	francismilligan599@gmail.com
82VLFW	francismilligan599@gmail.com
8CX7F4	Francismilligan599@gmail.com
8EN7R9	francismilligan599@gmail.com
8K97CZ	Francismilligan599@gmail.com
8NC4K8	francismilligan599@gmail.com
8NNHGL	francismilligan599@gmail.com
9ANFQZ	francismilligan599@gmail.com
9CUZL3	francismilligan599@gmail.com
9XT88X	francismilligan599@gmail.com
ABE2WW	francismilligan599@gmail.com
AD6282	francismilligan599@gmail.com >
AEDEP3	francismilligan599@gmail.com
B4AJ7X	N/A
BCMEEX	francismilligan599@gmail.com
BL9FU8	francismilligan599@gmail.com
C2JJVT	francismilligan599@gmail.com

TABLE 1

Question 36 - Applications & Web History	
WebCode	Response
C9ZCG4	francismilligan599@gmail.com
CHMD3T	francismilligan599@gmail.com
CKDDDX	francismilligan599@gmail.com
CMH494	francismilligan599@gmail.com
D7AC7Y	francismilligan599@gmail.com
EBZ32N	francismilligan599@gmail.com
EHJ79Q	francismilligan599@gmail.com
EQURUZ	francismilligan599@gmail.com
EYNXN2	francismilligan599@gmail.com
F27G9V	francismilligan599@gmail.com
GQ3JZL	francismilligan599@gmail.com
H88C8U	francismilligan599@gmail.com
HEPJ4T	francismilligan599@gmail.com
JP4YCX	FRANCISMILLIGAN599@GMAIL.COM
LWCVX9	francismilligan599@gmail.com
MU3MGV	francismilligan599@gmail.com
N9JXHH	francismilligan599@gmail.com
NGD4BJ	francismilligan599@gmail.com
NZ9WWG	francismilligan599@gmail.com
PB49XM	Francismilligan599@gmail.com
PGULYB	francismilligan599@gmail.com
PLMMZP	francismilligan599@gmail.com
Q29PVJ	francismilligan599@gmail.com
Q99RM3	francismilligan@gmail.com
QGJU94	francismilligan599@gmail.com
RCRKJC	francismilligan599@gmail.com
TF4QLP	francismilligan599@gmail.com
TPBP6E	Milligan <francismilligan599@gmail.com>
U899KL	francismilligan599@gmail.com
UEREJE	francismilligan599@gmail.com
UYQHMY	francismilligan599@gmail.com
V9V7DB	francismilligan599@gmail.com

TABLE 1

Question 36 - Applications & Web History	
WebCode	Response
VA6BPD	francismilligan599@gmail.com
W2UCV3	francismilligan599@gmail.com
W4KC78	francismilligan599@gmail.com FRANCIS MILLIGAN
W4VZYW	francismilligan599@gmail.com
WAMHLA	francismilligan599@gmail.com
WTZ4AC	francismilligan599@gmail.com ("Milligan")
XBWQEF	francismilligan599@gmail.com
XFRN2L	francismilligan599@gmail.com
YGFDWD	francismilligan599@gmail.com
YK GK4G	francismilligan599@gmail.com
ZVXNQ8	francismilligan599@gmail.com

Question 36: Who's key (other than the user) did the user have stored in his PGP keychain? (provide email address)

Consensus Result: francismilligan599@gmail.com

Expected Response Explanation:

Per USERDATA (ExtX)/Root/data/com.android.vending/databases/localappstate.db, the OpenKeychain storage is in org.sufficientlysecure.keychain.
 /USERDATA (ExtX)/Root/data/org.sufficientlysecure.keychain/databases/openkeychain.db contains stored keys. Other than the user, only one other public key is stored in this database.

Expected Response Illustration:

OpenKeyChain database

master_key_id	rank	type	user_id	name	email
-1491894231175803454	0		Milligan <francismilligan599@gmail.com>	Milligan	francismilligan599@gmail.com
-8827840891733830195	0		Al <allengonzo79@gmail.com>	Al	allengonzo79@gmail.com

TABLE 1

Question 37 - Applications & Web History

Question 37: What application did the user utilize to access the bluetooth skimmers?

Manufacturer's Serial Bluetooth Terminal

Expected Response:

WebCode	Response
2B66AE	Serial Bluetooth Terminal
2JDY68	Serial Bluetooth Terminal
3LWD98	Serial Bluetooth Terminal
3VNPE9	Serial Bluetooth Terminal
63XWWA	Serial Bluetooth Terminal 1.28
69MBU4	Serial Bluetooth Terminal
6EKPAN	serial bluetooth terminal
6PRHA7	Serial Bluetooth Terminal
74MLQ2	Serial Bluetooth Terminal
77WBJY	Serial Bluetooth Terminal
7RU3AB	Serial Bluetooth Terminal
82DV2X	Serial Bluetooth Terminal
82VLFW	Serial Bluetooth Terminal
8CX7F4	Serial Bluetooth Terminal
8EN7R9	Serial Bluetooth Terminal
8K97CZ	Serial Bluetooth Terminal
8NC4K8	Serial Bluetooth Terminal
8NNHGL	Serial Bluetooth Terminal
9ANFQZ	Serial Bluetooth Terminal
9CUZL3	Serial Bluetooth Terminal
9XT88X	Serial Bluetooth Terminal
ABE2WW	Serial Bluetooth Terminal
AD6282	Serial Bluetooth terminal
AEDEP3	Serial Bluetooth Terminal
B4AJ7X	N/A
BCMEEEX	Serial Bluetooth Terminal
BL9FU8	Serial Bluetooth Terminal
C2JJVT	Serial Bluetooth Terminal
C9ZCG4	Serial Bluetooth Terminal

TABLE 1

Question 37 - Applications & Web History	
WebCode	Response
CHMD3T	Serial Bluetooth Terminal
CKDDDX	Serial Bluetooth Terminal
CMH494	Serial Bluetooth Terminal
D7AC7Y	Serial Bluetooth Terminal
EBZ32N	Serial Bluetooth Terminal
EHJ79Q	Serial Bluetooth Terminal
EQURUZ	Serial Bluetooth Terminal
EYNXN2	serial bluetooth terminal (e.kai_morich.serial)
F27G9V	Serial Bluetooth Terminal
GQ3JZL	Serial Bluetooth Terminal
H88C8U	Serial Bluetooth Terminal
HEPJ4T	Serial Bluetooth Terminal
JP4YCX	SERIAL BLUETOOTH TERMINAL
LWCVX9	Serial Bluetooth Terminal
MU3MGV	Serial Bluetooth Terminal
N9JXHH	SKMS
NGD4BJ	Serial Bluetooth Terminal
NZ9WWG	Serial Bluetooth Terminal
PB49XM	Serial Bluetooth Terminal
PGULYB	de.kai_morich.serial_bluetooth_terminal
PLMMZP	Serial Bluetooth Terminal
Q29PVJ	Serial Bluetooth Terminal V1.28
Q99RM3	serial bluetooth terminal
QGJU94	Serial Bluetooth Terminal
RCRKJC	Serial Bluetooth Terminal
TF4QLP	This is beyond the scope of reporting
TPBP6E	KnoxBluetooth
U899KL	None located
UEREJE	Serial Bluetooth Terminal de.kai_morich.serial_bluetooth_terminal
UYQHMY	Serial Bluetooth Terminal
V9V7DB	Serial Bluetooth Terminal
VA6BPD	Serial Bluetooth Terminal

TABLE 1

Question 37 - Applications & Web History	
WebCode	Response
W2UCV3	de.kai_morich.serial_bluetooth_terminal
W4KC78	Serial Bluetooth Terminal
W4VZYW	Serial Bluetooth Terminal (de.kai_morich.serial_bluetooth_terminal)
WAMHLA	de.kai_morich.serial bluetooth terminal
WTZ4AC	Serial Bluetooth Terminal (de.kai_morich.serial_bluetooth_terminal)
XBWQEF	Serial Bluetooth Terminal
XFRN2L	Serial Bluetooth Terminal
YGFDWD	Serial Bluetooth Terminal
YK GK4G	Serial Bluetooth Terminal
ZVXNQ8	Serial Bluetooth Terminal

Question 37: What application did the user utilize to access the bluetooth skimmers?

Consensus Result: Serial Bluetooth Terminal

Expected Response Explanation:

Review of installed apps via USERDATA (ExtX)/Root/data/com.android.vending/databases/localappstate.db shows only one Bluetooth specific application. Review of the configuration files for this app in USERDATA (ExtX)/Root/data/de.kai_morich.serial_bluetooth_terminal/shared_prefs/de.kai_morich.serial_bluetooth_terminal_preferences.xml shows device name and MAC address info for one of (the last) skimmers accessed.

Expected Response Illustration:

Installed Applications

The screenshot shows a table of installed applications with the following columns: Name, Version, Description, and Identifier. The application 'Serial Bluetooth Terminal' is highlighted, with version 1.28 and identifier de.kai_morich.serial_bluetooth_ter... The table also shows a total of 32 applications and a search filter for 'bluetooth'.

Decoded by	Name	Version	Description	Identifier
	Serial Bluetooth Terminal	1.28		de.kai_morich.serial_bluetooth_ter...

TABLE 1

Question 37 - Applications & Web History

Preferences

```
de.kai_morich.serial_bluetooth_terminal_preferences.xml
map = {
  pref_device_address : string = 98:D3:71:FD:9A:B6
  pref_device_tab : int = 0
  pref_font_family : string = 0
  pref_timestamp_format : string = HH:mm:ss.SSS
  pref_device_name : string = SKMR9
  pref_show_status : boolean = True
  pref_charset : string = UTF-8
  pref_receive_buffer_size : string = 10000
  pref_font_size : string = 14
  pref_auto_scroll : boolean = True
  pref_receive_display_mode : string = 0
  pref_show_timestamp : boolean = False
  pref_device_le : boolean = False
}
```

TABLE 1

Question 38 - Applications & Web History

Question 38: In what directory was the data downloaded from the bluetooth skimmers stored?

Manufacturer's USERDATA

Expected Response: (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/

WebCode	Response
2B66AE	
2JDY68	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
3LWD98	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
3VNPE9	/USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
63XWWA	/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
69MBU4	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
6EKPAN	USERDATA/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
6PRHA7	de.kai_morich.serial_bluetooth_terminal/files
74MLQ2	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
77WBJY	/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
7RU3AB	USERDATA/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
82DV2X	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
82VLFW	/USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
8CX7F4	(ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
8EN7R9	USERDATA(ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
8K97CZ	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
8NC4K8	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
8NNHGL	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
9ANFQZ	/data/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
9CUZL3	data\de.kai_morich.serial_bluetooth_terminal
9XT88X	/storage/emulated/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
ABE2WW	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
AD6282	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
AEDEP3	/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
B4AJ7X	N/A
BCMEEX	USERDATA/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
BL9FU8	/root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
C2JJVT	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
C9ZCG4	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/

TABLE 1

Question 38 - Applications & Web History	
WebCode	Response
CHMD3T	/storage/emulated/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
CKDDDX	/storage/emulated/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
CMH494	(ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
D7AC7Y	Root/Media/0/Android/Data/de.Kai_morich.serial_bluetooth_terminal/files
EBZ32N	"files"
EHJ79Q	Files
EQURUZ	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/Files
EYNXN2	root/media/0/android/data/de.kai_morich.serial_bluetooth_terminal/files/
F27G9V	/data/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
GQ3JZL	USERDATA(ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
H88C8U	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
HEPJ4T	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
JP4YCX	USERDATA(EXT)/ROOT/MEDIA/0/ANDROID/DATA/DE.KAI.MORICH.SERIAL-BLUETOOTH_TERMINAL/FILES/
LWCVX9	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
MU3MGV	USERDATA/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
N9JXHH	com.skms.android.agent
NGD4BJ	/storage/emulated/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
NZ9WWG	
PB49XM	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
PGULYB	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
PLMMZP	USERDATA(ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
Q29PVJ	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal
Q99RM3	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
QGJU94	
RCRKJC	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
TF4QLP	This is beyond the scope of reporting
TPBP6E	data/com.samsung.android.knox.containeragent/
U899KL	None located
UEREJE	de.kai_morich.serial_bluetooth_terminal/files There were 15 files located in the "files" folder that contained data.
UYQHMY	de.kai_morich.serial_bluetooth_terminal/files
V9V7DB	USERDATA/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files

TABLE 1

Question 38 - Applications & Web History	
WebCode	Response
VA6BPD	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
W2UCV3	\media\0\Android\data\de.kai_morich.serial_bluetooth_terminal\files\
W4KC78	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
W4VZYW	/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
WAMHLA	/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
WTZ4AC	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
XBWQEF	/storage/emulated/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
XFRN2L	/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
YGFDWD	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files
YK GK4G	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/
ZVXNQ8	USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/

Question 38: In what directory was the data downloaded from the bluetooth skimmers stored?

Consensus Result: USERDATA (ExtX)/Root/media/0/Android/data/de.kai_morich.serial_bluetooth_terminal/files/ and all formatting styles which represent the same information.

Expected Response Explanation:

Searching for files or directories named “serial” or “terminal” will locate the target directory.

Expected Response Illustration:

Directory Search

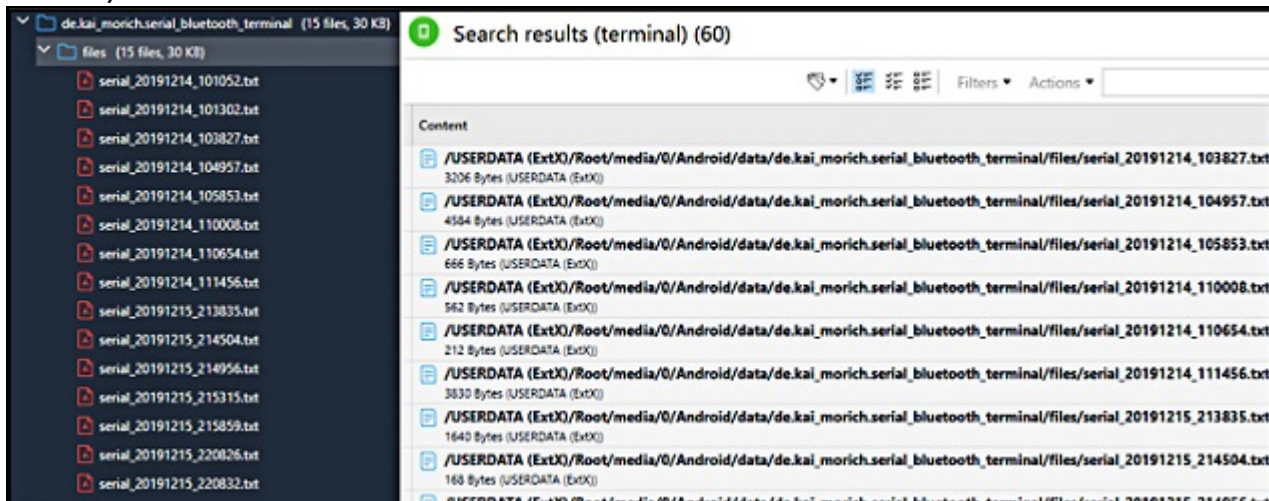


TABLE 1

Question 39 - Applications & Web History

Question 39: What did the user last search on Amazon?

Manufacturer's Bluetooth Module

Expected Response:

WebCode	Response
2B66AE	Amazon.com: LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino: Computers & Accessories
2JDY68	amazon bluetooth module hc05
3LWD98	bluetooth module hc05
3VNPE9	amazon bluetooth module hc05
63XWWA	LearningTech HC-05 Module Pass Through Communication
69MBU4	amazon bluetooth module hc05
6EKPAN	bluetooth module hc05
6PRHA7	amazon bluetooth module hc05
74MLQ2	amazon bluetooth module hc05
77WBJY	bluetooth module hc05
7RU3AB	bluetooth module hc05
82DV2X	amazon bluetooth module hc05
82VLFW	amazon bluetooth module hc05
8CX7F4	Amazon Bluetooth module hc05
8EN7R9	bluetooth module hc05
8K97CZ	amazon bluetooth module hc05
8NC4K8	bluetooth module hc05 (LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino)
8NNHGL	Amazon.com: LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino: Computers & Accessories
9ANFQZ	LeaningTech HC-05 Module
9CUZL3	amazon bluetooth module hc05
9XT88X	amazon bluetooth module hc05
ABE2WW	amazon bluetooth module hc05
AD6282	Bluetooth module
AEDEP3	bluetooth module hc05
B4AJ7X	Amazon.com: LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino: Computers & Accessories
BCMEEX	amazon bluetooth module hc05
BL9FU8	amazon bluetooth module hc05

TABLE 1

Question 39 - Applications & Web History	
WebCode	Response
C2JJVT	amazon bluetooth module hc05
C9ZCG4	amazon bluetooth module hc05
CHMD3T	LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino: Computers and Accessories.
CKDDDX	LeaningTech HC 05 Module Pass Through Communication
CMH494	amazon bluetooth module hc05
D7AC7Y	Amazon Bluetooth Module hc05
EBZ32N	Amazon.com: LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino: Computers & Accessories
EHJ79Q	LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino: Computers & Accessories
EQURUZ	amazon bluetooth module hc05
EYNXN2	amazon bluetooth module hc05
F27G9V	amazon bluetooth module hc05
GQ3JZL	LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino: Computers & Accessories
H88C8U	Bluetooth module hc05
HEPJ4T	bluetooth module hc05
JP4YCX	BLUETOOTH MODULE HC05
LWCVX9	Amazon.com: LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino: Computers & Accessories
MU3MGV	bluetooth module hc05
N9JXHH	bluetooth module hc05
NGD4BJ	amazon bluetooth module hc05.
NZ9WWG	amazon bluetooth module hc05
PB49XM	Amazon Bluetooth Module hc05
PGULYB	amazon bluetooth module hc05 (LeaningTech HC-05 Module Bluetooth)
PLMMZP	LeaningTech HC-05 Module Bluetooth Serial Pass-through module wireless serial communication
Q29PVJ	LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino
Q99RM3	LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino
QGJU94	bluetooth module hc05
RCRKJC	amazon bluetooth module hc05
TF4QLP	This is beyond the scope of reporting
TPBP6E	bluetooth module hc05

TABLE 1

Question 39 - Applications & Web History	
WebCode	Response
U899KL	amazon bluetooth module hc05
UEREJE	The user performed a search in Google for "amazon Bluetooth module hc05". The user visited the site Amazon (Amazon.com) using the Google search engine and searched for a Leaning Tech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino: Computers & Accessories
UYQHMY	Bluetooth module hc05
V9V7DB	amazon bluetooth module hc05
VA6BPD	remote weblab triggers
W2UCV3	amazon bluetooth module hc05
W4KC78	Amazon bluetooth module hc05
W4VZYW	bluetooth module hc05
WAMHLA	amazon bluetooth module hc05
WTZ4AC	On Amazon, the link was for a Leaning Tech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino; however, the search was through Google, and the search was for amazon Bluetooth module hc05.
XBWQEF	bluetooth module hc05
XFRN2L	Amazon bluetooth module hc05
YGFWD	LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino
YK GK4G	HC-05 Bluetooth module
ZVXNQ8	No searches on Amazon were found. The last item viewed on amazon.com : Amazon.com: LeaningTech HC-05 Module Bluetooth Serial Pass-Through Module Wireless Serial Communication with Button for Arduino: Computers & Accessories The last item search in Google for Amazon : amazon bluetooth module hc05

Question 39: What did the user last search on Amazon?

Consensus Result: Bluetooth Module and all formatting variations that represent the same information.

Expected Response Explanation:

Reviewing the history file for the Chrome web browser, /USERDATA (ExtX)/Root/data/com.android.chrome/app_chrome/Default/History, shows a timeline of web activity including searches. Among them are searches including "amazon" as a search term, the last of these is a google.com search for "amazon bluetooth module hc05".

TABLE 1

Question 39 - Applications & Web History

Expected Response Illustration:

Browser History

The screenshot shows a browser history interface with a title bar 'History' and tabs for 'Database View', 'Hex View', and 'File Info'. Below the tabs, there is a search bar and a list of 47 URLs. The list is sorted by 'last_visit_time' in descending order. The entries include various websites such as weather.gov, donate.torproject.org, google.com, amazon.com, ebay.com, and support.google.com, with timestamps ranging from 12/13/2019 1:08:23 AM to 12/3/2019 6:02:01 PM.

last_visit_time	url
12/13/2019 1:08:23 AM	http://wt1.la/
12/13/2019 1:08:07 AM	https://www.weather.gov/okx/
12/10/2019 8:54:27 PM	https://www.google.com/url?q=https://donate.torproject.org/subscription-confirm?token%3Dmj186ppCOjFKkLVsZhd1NJDxj3SusQEW&source=gm...
12/10/2019 8:54:27 PM	https://donate.torproject.org/subscription-confirm?token=mj186ppCOjFKkLVsZhd1NJDxj3SusQEW
12/10/2019 8:54:27 PM	https://donate.torproject.org/subscribed
12/10/2019 8:40:30 PM	https://www.google.com/search?client=ms-android-mpcs-us-rcv&ei=IQLwXbGmJLKd5wK2wa6IAw&q=NYC+weather+.gov&oq=NYC+weather+.go...
12/10/2019 8:40:23 PM	https://www.google.com/search?q=NYC+weather&oq=NYC+weather&aqs=chrome..69i57j0l3.8923j1j9&client=ms-android-mpcs-us-rcv&sourceid...
12/10/2019 8:39:52 PM	https://www.google.com/search?q=NYC+weather&oq=NYC+weather&aqs=chrome..69i57j0l3.8923j1j9&client=ms-android-mpcs-us-rcv&sourceid...
12/10/2019 8:39:26 PM	https://www.google.com/search?q=dI5953&oq=dI5953&aqs=chrome..69i57j0.7804j0j4&client=ms-android-mpcs-us-rcv&sourceid=chrome-mobile...
12/10/2019 8:38:19 PM	https://news.google.com/?hl=en-US&gl=US&ceid=US:en
12/5/2019 2:54:51 PM	https://www.amazon.com/LeaningTech-HC-05-Module-Pass-Through-Communication/dp/B00INWZRNC
12/5/2019 11:37:44 AM	https://www.aa.com/contact/forms?topic=#/
12/5/2019 11:37:28 AM	https://www.aa.com/i18n/customer-service/contact-american/american-customer-service.jsp
12/3/2019 6:33:12 PM	https://www.amazon.com/errors/validateCaptcha?amzn=m%2FKke5Fz6n5%2FRraz5TLVjQ%3D%3D&amzn-r=%2FLeaningTech-HC-05-Module-Pass-T...
12/3/2019 6:32:57 PM	https://www.google.com/search?client=ms-android-mpcs-us-rcv&ei=OqrmXYTaKsXb5gLcz6XQAg&q=amazon+bluetooth+module+hc05&oq=ama...
12/3/2019 6:32:50 PM	https://www.ebay.com/p/553119340?iid=352221845135&chn=ps&norover=1&mkevt=1&mkrld=711-117182-37290-0&mkcid=2&itemid=35222184...
12/3/2019 6:32:46 PM	https://www.google.com/search?client=ms-android-mpcs-us-rcv&ei=OqrmXYTaKsXb5gLcz6XQAg&q=amazon+bluetooth+module+hc05&oq=ama...
12/3/2019 6:32:46 PM	https://www.google.com/search?client=ms-android-mpcs-us-rcv&ei=OqrmXYTaKsXb5gLcz6XQAg&q=amazon+bluetooth+module+hc05&oq=ama...
12/3/2019 6:32:45 PM	https://www.google.com/search?client=ms-android-mpcs-us-rcv&ei=OqrmXYTaKsXb5gLcz6XQAg&q=amazon+bluetooth+module+hc05&oq=ama...
12/3/2019 6:32:40 PM	https://www.google.com/search?client=ms-android-mpcs-us-rcv&ei=OqrmXYTaKsXb5gLcz6XQAg&q=amazon+bluetooth+module+hc05&oq=ama...
12/3/2019 6:32:33 PM	https://www.google.com/search?q=amazon+bluetooth+module&oq=amazon+bluetooth+mod&aqs=chrome..1.69i57j0l3.9482j0j7&client=ms-andro...
12/3/2019 6:32:32 PM	https://www.google.com/search?q=amazon+bluetooth+module&oq=amazon+bluetooth+mod&aqs=chrome..1.69i57j0l3.9482j0j7&client=ms-andro...
12/3/2019 6:32:32 PM	https://www.google.com/search?q=amazon+bluetooth+module&oq=amazon+bluetooth+mod&aqs=chrome..1.69i57j0l3.9482j0j7&client=ms-andro...
12/3/2019 6:32:28 PM	https://www.google.com/search?q=amazon+bluetooth+module&oq=amazon+bluetooth+mod&aqs=chrome..1.69i57j0l3.9482j0j7&client=ms-andro...
12/3/2019 6:31:56 PM	https://www.ebay.com/itm/MiniDX3-Portable-Magnetic-Credit-Card-Reader-Data-Collector-Shipped-From-The-USA/153702115598?epid=22811046...
12/3/2019 6:31:47 PM	https://support.google.com/android/answer/7521240?p=verify_number&visit_id=637109945298574745-595817420&rd=1
12/3/2019 6:28:48 PM	https://support.google.com/android?p=verify_number
12/3/2019 6:28:48 PM	https://goo.gl/LHCS9W
12/3/2019 6:03:06 PM	https://www.ebay.com/sch/i.html?_nkw=card+readers+magnetic&_trksid=p2334524.m4084.11313.TR1.TRC0.A0.H0.Xcard+readers+m.TR50&_odkw=c...
12/3/2019 6:02:43 PM	https://www.ebay.com/sch/i.html?_sacat=11892&_nkw=card+readers+&_trksid=p2499334.m4084.11313.TR7.TRC1.A0.H0.Xcard+readers.TR50
12/3/2019 6:02:21 PM	https://www.ebay.com/b/Bluetooth-POS-Credit-Card-Terminals-Readers/11892/bn_7116046724
12/3/2019 6:02:01 PM	https://www.google.com/search?client=ms-android-mpcs-us-rcv&ei=26LmXbGeCoXr5gKXlpe4DQ&q=build+bluetooth+card+reader&oq=build+bl...

TABLE 1

Question 120 - Phone / Messaging

Question 120: What was the date and time of the last outgoing call? Provide your response in the time zone set for the device using the following format: MM/DD/YYYY, HH:MM AM/PM (Subset 1)

Manufacturer's 12/15/2019 09:28 PM

Expected Response:

WebCode	Response
2JDY68	12/15/2019 9:28 PM
3LWD98	12/15/2019 09:28 PM
3VNPE9	12/15/2019, 09:28 PM was the last dialed outgoing call made to **61*18056912815, which appears to be a call forwarding service number. If the last call was made to a person or contact, it would be 12/05/2019, 06:35 AM.
63XWWA	12/15/2019, 21:28 PM
69MBU4	12/15/2019, 09:28 PM
6EKPAN	12/15/2019 09:28 pm
74MLQ2	12/15/2019 09:28 PM
7RU3AB	12/15/2019, 09:28 PM
82DV2X	12/15/2019, 09:28 PM
8K97CZ	12/15/2019, 09:28 PM
9XT88X	12/15/2019, 09:28 PM
ABE2WW	12/15/2019, 09:28 PM
AD6282	12/15/2019 21:28 PM
BL9FU8	12/15/2020 09:28 PM
C2JJVT	12/15/2019, 9:28 PM
C9ZCG4	12/15/2019 09:28 PM
CHMD3T	12/15/2019 9:28 PM
CKDDDX	12/15/2019 21:28 PM
EBZ32N	12/15/2019, 09:28 PM(UTC-5)
EHJ79Q	12/15/2019 9:28:53 PM(UTC-5)
EQURUZ	12/15/2019 2128 PM
EYNXN2	12/15/2019 09:28 PM
F27G9V	12/15/2019, 09:28 PM
GQ3JZL	12/15/2019, 09:28 PM
JP4YCX	12/15/2019 09:28 pm
LWCVX9	12/15/2019, 09:28 PM
MU3MGV	12/15/2019, 09:28 PM

TABLE 1

Question 120 - Phone / Messaging	
WebCode	Response
NGD4BJ	12/15/2019, 09:28 PM
NZ9WWG	12/15/2019, 09:28 PM
Q29PVJ	12/15/2019, 09:28 PM
Q99RM3	12.15.2019 09:28 pm
QGJU94	12/15/2019, 21:28 PM
RCRKJC	12/15/2019, 09:28 PM
TF4QLP	12/15/2019, 09:28 PM (technically last call but this is a call forward) 12/15/2019, 08:55 PM (last true call)
TPBP6E	12/15/2019 9:28:53 PM(UTC-5)
U899KL	12/15/2019 9:28 PM
UEREJE	12/15/2019 09:28 PM
V9V7DB	12/15/2019, 09:28 PM
VA6BPD	12/15/2019, 09:28 PM
W4VZYW	12/15/2019 09:28 PM
WAMHLA	12/15/2019 9:28 PM
WTZ4AC	12/15/2019, 9:28 PM (UTC-5)
YGFDWD	12/15/2019, 21:28:53 PM
ZVXNQ8	12/15/2019, 09:28 PM

Question 120: What was the date and time of the last outgoing call? Provide your response in the time zone set for the device using the following format: MM/DD/YYYY, HH:MM AM/PM (Subset 1)

Consensus Result: Subset 1 of participants for Question #20 reported 12/15/2019 09:28 PM as the consensus answer. This response and all formatting styles which represent the same information were used to group these participants into Subset 1.

Expected Response Explanation:

The last outgoing call date and time can be found in the Call log located in /Root/data/com.samsung.android.providers.contacts/databases/calllog.db-wal

Expected Response Illustration:

Call Log

Parties	Timestamp	Duration	Status
To: 5713130786	11/21/2019 10:19:38 AM(UTC-5)		Unknown
From: +17039407024 Raymond Butner	12/5/2019 6:32:30 AM(UTC-5)	00:00:27	Unknown
To: +17039407024 Raymond Butner	12/5/2019 6:35:03 AM(UTC-5)		Unknown
From: -1	12/15/2019 9:20:22 PM(UTC-5)		Rejected
To: **61*18056912815	12/15/2019 9:28:53 PM(UTC-5)		Unknown
From: Unknown	12/15/2019 9:31:58 PM(UTC-5)		Rejected

TABLE 1

Question 121 - Phone / Messaging

Question 121: The last outgoing call was made to what phone number? (Subset 1)

Manufacturer's **61*18056912815Expected Response:

WebCode	Response
2JDY68	**61*18056912815
3LWD98	**61*18056912815
3VNPE9	1 (805) 691-2815, however, it is listed with the prefix number "***61*". The entire number dialed out is "***61*18056912815". The "***61*" number appears to be a call forwarding service and is going to a Google Voice number. If the last call was made to a person or contact, it would be the phone number 1 (703) 940-7024.
63XWWA	**61*18056912815
69MBU4	+17039407024
6EKPAN	**61*18056912815
74MLQ2	+17039407024
7RU3AB	+17039407024
82DV2X	7206865455
8K97CZ	**61*18056912815
9XT88X	**61*18056912815
ABE2WW	**61*18056912815
AD6282	**61*18056912815
BL9FU8	**61*18056912815
C2JJVT	**61*18056912815
C9ZCG4	**61*18056912815
CHMD3T	**61*18056912815
CKDDDX	**61*18056912815
EBZ32N	**61*18056912815
EHJ79Q	**61*18056912815
EQURUZ	**61*18056912815
EYNXN2	**61*18056912815
F27G9V	**61*18056912815
GQ3JZL	**61*18056912815
JP4YCX	**61*18056912815
LWCVX9	**61*18056912815
MU3MGV	7206865455

TABLE 1

Question 121 - Phone / Messaging	
WebCode	Response
NGD4BJ	+6118056912815
NZ9WWG	**61*18056912815
Q29PVJ	**61*18056912815 **61* entry is a call forwarding service. The last call to an individual was made to 17039407024.
Q99RM3	**61*18056912815
QGJU94	**61*18056912815
RCRKJC	**61*18056912815
TF4QLP	**61*18056912815 (this is a forwarded call) 720-686-5455 (last true call)
TPBP6E	18056912815
U899KL	**61*18056912815
UEREJE	**61*18056912815 (1-805-691-2815)
V9V7DB	**61*18056912815
VA6BPD	The last outgoing call on the phone was **61*18056912815. The last outgoing call in the calllog.db was 7206865455
W4VZYW	**61*18056912815
WAMHLA	**61*18056912815
WTZ4AC	**61*18056912815
YGFDDW	**61*18056912815
ZVXNQ8	**61*18056912815

Question 121: The last outgoing call was made to what phone number? (Subset 1)

Consensus Result: Subset 1 of participants for Question #20 reported **61*18056912815 as the consensus answer.

Expected Response Explanation:

The number associated with the last outgoing call record can be found in the Call log located in /Root/data/com.samsung.android.providers.contacts/databases/calllog.db-wal.

TABLE 1

Question 121 - Phone / Messaging

Expected Response Illustration:

Call Log

Call Log (8)							
	<input type="checkbox"/>	#		Parties	↑ Timestamp	Duration	Status
	<input checked="" type="checkbox"/>	1		To: 5713130786	11/21/2019 10:19:38 AM(UTC...		Unknown
	<input checked="" type="checkbox"/>	2		From: +17039407024 Raymond Butner	12/5/2019 6:32:30 AM(UTC-5)	00:00:27	Unknown
	<input checked="" type="checkbox"/>	3		To: +17039407024 Raymond Butner	12/5/2019 6:35:03 AM(UTC-5)		Unknown
	<input checked="" type="checkbox"/>	4		From: -1	12/15/2019 9:20:22 PM(UTC-5)		Rejected
	<input checked="" type="checkbox"/>	5		To: **61*18056912815	12/15/2019 9:28:53 PM(UTC-5)		Unknown
	<input checked="" type="checkbox"/>	6		From: Unknown	12/15/2019 9:31:58 PM(UTC-5)		Rejected
	<input checked="" type="checkbox"/>	7		From: Unknown	12/15/2019 9:33:57 PM(UTC-5)		Rejected
	<input checked="" type="checkbox"/>	8		From: -1	12/15/2019 9:35:13 PM(UTC-5)		Rejected

TABLE 1

Question 220 - Phone / Messaging

Question 220: What was the date and time of the last outgoing call? Provide your response in the time zone set for the device using the following format: MM/DD/YYYY, HH:MM AM/PM (Subset 2)

Manufacturer's 12/05/2019 06:35 AM

Expected Response:

WebCode	Response
2B66AE	12/05/2019, 06:35 AM
77WBJY	12/05/2019, 06:35 AM
82VLFW	12/05/2019, 06:35 AM
8CX7F4	12/05/2019, 6:35:03 AM
8NNHGL	12/05/2019, 06:35 AM
9ANFQZ	12/5/2019 6:35 AM
9CUZL3	12/05/2019, 06:35:03 AM (UTC -5)
AEDEP3	12/05/2019, 06:35:03 AM
BCMEEEX	12/05/2019, 06:35 AM
D7AC7Y	12/5/2019 6:35 AM
HEPJ4T	12/05/2019, 06:35 AM
N9JXHH	12/05/2019, 06:35 AM
PB49XM	12/05/2019, 06:35 AM
PGULYB	12/5/2019, 6:35:03 AM
PLMMZP	12/05/19, 6:35 AM
W4KC78	12/05/2019, 06:35 AM is the date and time of the last outgoing call made to a contact. (This time stamp corresponds to the outgoing call made to "+17039407024" "Raymond Butner") Note: 12/15/2019, 09:28 PM is the date and time of the last outgoing call parsed by both CelleBrite and XRY (which corresponds to the outgoing call to "***61*18056912815") - **61 is a T-mobile/ Metro PCS Short Code to "Turn on forwarding if no reply (CF NRY) to a number (unanswered calls ring to alternate number)".
XBWQEF	12/05/2019, 06:35 AM
XFRN2L	12/05/2019 06:35 AM
YK GK4G	12/5/2019 06:35(UTC-5)

Question 220: What was the date and time of the last outgoing call? Provide your response in the time zone set for the device using the following format: MM/DD/YYYY, HH:MM AM/PM (Subset 2)

Consensus Result: Subset 2 of participants for Question #20 reported 12/05/2019 06:35 AM as the consensus answer. This response and all formatting styles which represent the same information were used to group these participants into Subset 2.

Expected Response Explanation:

The last outgoing call date and time can be found in the Call log located in /Root/data/com.samsung.android.providers.contacts/databases/calllog.db-wal

TABLE 1

Question 220 - Phone / Messaging

Expected Response Illustration:

Call Log

Call Log (8)							
			#		Parties	↑ Timestamp	Duration
		<input checked="" type="checkbox"/>	1		To: 5713130786	11/21/2019 10:19:38 AM(UTC...	
		<input checked="" type="checkbox"/>	2		From: +17039407024 Raymond Butner	12/5/2019 6:32:30 AM(UTC-5)	00:00:27
		<input checked="" type="checkbox"/>	3		To: +17039407024 Raymond Butner	12/5/2019 6:35:03 AM(UTC-5)	
		<input checked="" type="checkbox"/>	4		From: -1	12/15/2019 9:20:22 PM(UTC-5)	

TABLE 1

Question 221 - Phone / Messaging

Question 221: The last outgoing call was made to what phone number? (Subset 2)

Manufacturer's 1-703-940-7024

Expected Response:

WebCode	Response
2B66AE	+17039407024
77WBJY	17039407024
82VLFW	+17039407024
8CX7F4	17039407024
8NNHGL	17039407024
9ANFQZ	+17039407024
9CUZL3	+17039407024
AEDEP3	17039407024
BCMEEEX	1 703 940 7024
D7AC7Y	1-703-940-7024
HEPJ4T	+17039407024
N9JXHH	1-703-940-7024
PB49XM	17039407024
PGULYB	17039407024
PLMMZP	+17039407024
W4KC78	17039407024
XBWQEF	17039407024
XFRN2L	+17039407024
YK GK4G	+17039407024

Question 221: The last outgoing call was made to what phone number? (Subset 2)

Consensus Result: Subset 2 of participants for Question #20 reported 1-703-940-7024 as the consensus answer.

Expected Response Explanation:

The number associated with the last outgoing call record can be found in the Call log located in /Root/data/com.samsung.android.providers.contacts/databases/calllog.db-wal.

Expected Response Illustration:

Call Log

Call ID	Party	Timestamp	Duration
1	To: 5713130786	11/21/2019 10:19:38 AM(UTC-5)	
2	From: +17039407024 Raymond Butner	12/5/2019 6:32:30 AM(UTC-5)	00:00:27
3	To: +17039407024 Raymond Butner	12/5/2019 6:35:03 AM(UTC-5)	

TABLE 1

Question 222 - Phone / Messaging

Question 222: Provide the contact name belonging to the phone number reported in question #21? (Subset 2)

Manufacturer's Raymond Butner

Expected Response:

WebCode	Response
2B66AE	Raymond Butner
77WBJY	Raymond Butner
82VLFW	Raymond Butner
8CX7F4	Raymond Butner
8NNHGL	Raymond Butner
9ANFQZ	Raymond Butner
9CUZL3	Raymond Butner
AEDEP3	Raymond Butner
BCMEEEX	Raymond Butner
D7AC7Y	Raymond Butner
HEPJ4T	Raymond Butner
N9JXHH	Raymond Butner
PB49XM	Raymond Butner
PGULYB	Raymond Butner
PLMMZP	Raymond Butner
W4KC78	Raymond Butner
XBWQEF	Raymond Butner
XFRN2L	Raymond Butner
YK GK4G	Raymond Butner

Question 222: Provide the contact name belonging to the phone number reported in question #21? (Subset 2)

Consensus Result: Subset 2 of participants for Question #20 reported Raymond Butner as the consensus answer.

Expected Response Explanation:

The last outgoing call along with any information such as stored contact name for associated number can be found in the Call log located in /Root/data/com.samsung.android.providers.contacts/databases/calllog.db-wal.

TABLE 1

Question 222 - Phone / Messaging

Expected Response Illustration:

Call Log

Call Log (8)									
				#		Parties	↑ Timestamp	Duration	Status
				1		To: 5713130786	11/21/2019 10:19:38 AM(UTC...		Unknown
				2		From: +17039407024 Raymond Butner	12/5/2019 6:32:30 AM(UTC-5)	00:00:27	Unknown
				3		To: +17039407024 Raymond Butner	12/5/2019 6:35:03 AM(UTC-5)		Unknown
				4		From: -1	12/15/2019 9:20:22 PM(UTC-5)		Rejected

Additional Comments

TABLE 2

WebCode	Additional Comments
2JDY68	Question 21: The last outgoing call is actually a call forwarding command. Question 22: Allen Gonzales is the owner of the Google Voice account associated with allengonzo79@gmail.com. Question 27: The file name suggests that it stores a parking location, however, there was no way to verify this. Question 39: There was no search performed on Amazon's website. This is a Google search. The test included a number of questions which called for the manual parsing of data. Some areas required assumptions about data or app testing (e.g., Google Maps parking location). I think the number of problems asking for this level of detail was unnecessary for a proficiency test.
3VNPE9	Some of my answers to the questions contain justification for the answers submitted. Please refer to them as needed for the reason I answered the questions as I did.
6EKPAN	The PGP encrypted messages sent via K9 were accessed by exporting the OpenKeyChain backup to a PC and importing it using the backup key present in a screenshot. Some of the messages concerning the skimming operation. However there were no questions about this and so all this cleverness was wasted!
9XT88X	There are two interpretations for answering the series of Questions 20-23, all based off of the interpretation of the initial question in the series. Option 1 assumes the entry used to enable call forwarding on the device (**61* call) is considered the last outgoing call since it was the last interaction with the phone function of the device. This is listed as the last outgoing call in both Axiom and UFED PA, but presents difficulty and confusion with answering questions 21-23. Option 2 assumes the last outgoing call is understood to be the last time the phone was used to complete an outgoing voice call. This allows for a much more straight forward interpretation of questions 21-22, but leaves Question 23 in limbo with possible answers of Telegram, WhatsApp, or T-Mobile depending on the interpretation of "communication service".
BCMEEEX	Regarding Question 20, there was a later call placed to **61*#, but this is a call forwarding request, so it was not selected. In actual casework, we are rarely, if ever, asked what app a user used; investigators usually know what apps they are interested in and ask for specific app data.
C2JJVT	When answering question #14 and question #16 I used the number presented by Physical Analyzer (v7.32.0.16). I used the overall number of messages found on the phone, minus any duplicated messages. In short for question #14 I selected SMS Messages and filtered on "Parties/From: +17206865455 Francis Milligan and found 24 total listings with 18 duplications. For question #16 selected "SMS Messages" and used the filter on the "Status" category which listed 32 results with 24 duplications. With an earlier version of Physical Analyzer (v7.29.0.152) the duplication results were slightly different (question #14 had 18 total with 6 "identified" duplications and question #16 had 32 total with 16 duplications). When answering question #21 I simply copied out the entire number (including the call forwarding pretext. When answering question# 30 I entered the amount located in the USERDATA (ExtX)/Root/data/com.bitpay.wallet/files/txsHistory-881825ea-cd77-4268-8de1-43bc06f486d a which contains the transaction history for the application. I also noticed the amount "1.01" in a snapshot (image file) that was created after the date of the txsHistory. The 1.01 amount could reflect the transaction with the added cost of completing the transaction, however; I felt the question was geared towards the txsHistory file. On question #38 the folder containing the text files with the skimmer data was simply labeled "files". I entered the file path for the question.
C9ZCG4	Prior to examination the hash values for the exhibit were confirmed against those provided in

TABLE 2

WebCode	Additional Comments
	the question Question 1 the hash value was read from the UFD file as well as being hashed separately.
CKDDDX	Google Voice was a little confusing and lead me down an unusual path as we do not have access to this in the UK. The **61* indicates potential call forwarding command and the contact number 1805691281 appears to be linked to Google Voice and the handset.
EBZ32N	The questions were not germane to a "real world" investigation and were unnecessarily complicated for the sake of a proficiency test.
EHJ79Q	There are several questions relating to skimmer data that are very specific and would require a more in-depth analysis than normal case work would require. This test asks questions that require the analyst to conduct extensive research and goes beyond a normal proficiency test. Other questions seem too vague and require the analyst to make assumptions about what is being asked.
EYNXN2	This PT came at a difficult period due to COVID-19 and the reduction in time available. It appears that some files may have been manually changed so that they cannot be dealt with as normal by the various mobile device forensic software packages. Some of the questions appeared to be ambiguous. I dont think a 'US' set up device is appropriate to our needs.
TF4QLP	Numbers 20 and 21 should be worded differently. Looking at the last outgoing call in the database shows a forward call which does not provide any information on the forwarded phone number. **61* indicates a forward call so this question can result in an incorrect answer even though it was literally the last outgoing call.
TPBP6E	thanks
U899KL	I am using UFED Physical analyzer 7.33.0.30 and the information requested is not in the file I downloaded. I did confirm the SHA1 Hash value for the file. This leaves 12 answers blank.
UEREJE	I think that this PT should contain less questions. This is the longest test of all of the CTS PT's.
V9V7DB	Once again this year/s test lacks the shine and polish that is expected of professional work product. And this iteration required a level of effort more suited for a Certification Examination vice an annual Proficiency. Several of the Questions presented specific challenges due to wording ambiguity and/or lack of formatting consistency. Question 2 asks for the "model name" of the device. This is confusing. Since model and name could be interpreted as separate descriptors. Whereas device model could be "SM-J260T1" and device name could be "Galaxy J2". Question 38 uses the term "directory". This is ambiguous and could reference any of the parent folders or sub/folders containing the apparent skimmer data. Such as "0", "Android", or "data". The term "path" should be used if the full path to the files is the desired answer vice the directory in which they are stored. Question 39 is poorly worded. Since the wording of this question gives an expectation of finding a search conducted directly through the Amazon website vice a Google search of the Amazon website. And leaves you wondering whether the term "amazon" should be included in the answer. And Questions 20, 21, 22, and 23 gave me quite a headache. The term "contact name" is ambiguous. And could refer to "Owner" or "(owner)". Or "User 0" or "User" or "0". Or "Allen Gonzalez" or "allengonzo79@gmail.com". The term "phone number" could include the Google Voice number, the short code, or both. And the term "communication service" only compounds the confusion. As this could refer to either Google Voice or T-Mobile. Why not just select a more straightforward call log entry for this series of test Questions? Rather than try to "stump the chump".
W2UCV3	Question 17: Ambiguous question. Technically the communication service used was the SMS

TABLE 2

WebCode	Additional Comments
	<p>service. The communication service provider or company who sent the SMS is Google Voice. Question 20 to 23: The last outgoing call log is technically the call that starts with "***61*" followed by a number.. however there is no contact in relation to this. The next outgoing call is approx. 10 days earlier however has multiple contact entries (question 23) relating to this number. Question 27: The saved parking location located in the file parking_location.cs is mostly unreadable: "™ Ö;ÜbC@!Šeéù nSÂâ®Áéï-Citgo â®Áéï-0â®Áéï-@HPĐ-õÁĐ±æ. However Citgo can be identified as well as prior searches relating to Citgo including the address "Citgo, Midlothian, VA 23112" but this cannot be confirmed as the correct name of the saved location. Question 39: The question is ambiguous. Is the question asking what did the user last browse/view on Amazon? Or what did the user last search on google relating to Amazon?</p>
W4KC78	<p>Question #20: 12/15/2019, 09:28 PM is the time of the last outgoing call parsed by both CelleBrite and XRY (which corresponds to the outgoing call to "***61*18056912815"). **61 is a T-mobile/ Metro PCS Short Code to "Turn on forwarding if no reply (CF NRY) to a number (unanswered calls ring to alternate number)". Question #21: 18056912815 is the number of the last outgoing call parsed by both CelleBrite and XRY. However, it was dialed with the prefix **61* What was dialed was "***61*18056912815" Note: If we consider 18056912815 as reported by both CelleBrite and XRY to be the number to which the last outgoing call was dialed to, then I cannot answer the follow-up questions #22 and #23. The number "18056912815" does not appear to be associated to any contact, and I was unable to find any additional information about it (and actually it also affects the possible answer for question #20). For this reason I am assuming that this call forwarding-type call may not have been considered the last outgoing call and therefore including the call made on 12/05/2019, 06:35 AM (which corresponds to the outgoing call to "+17039407024" "Raymond Butner") as an alternate answer.</p>
XFRN2L	<p>Though a huge overall improvement in this test, some of the questions are misleading (i.e. 21, 22, 23, 32 & 39). The challenge should be a technical one, not one based on how to interpret what is asked.</p>
YK GK4G	<p>note for Question #20. There was a forwarded call (using **61*) to 1-805-691-2815 at 21:28 on 12/15/2019, which I'm assuming is not the intention of this question)</p>

-End of Report-
(Appendix may follow)