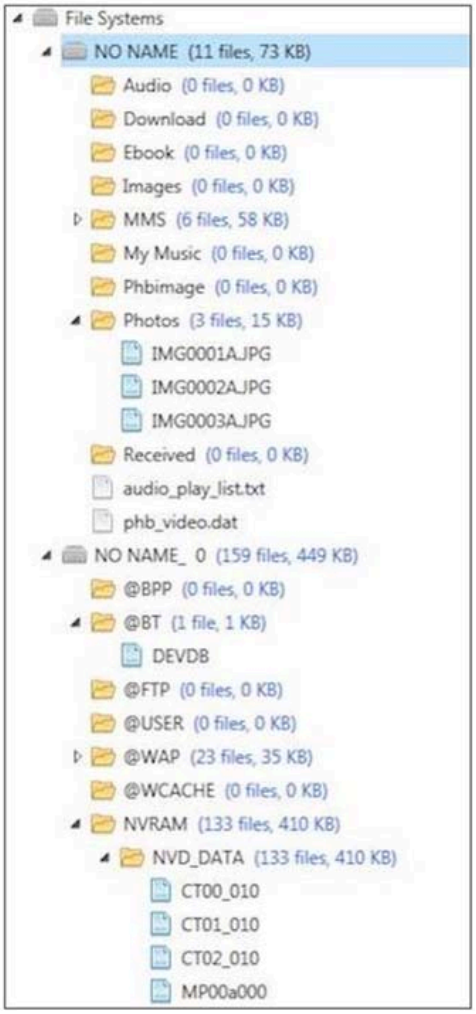
Question #1 *Topic 1*

Based on the image below, which file system is being examined?



A. Chinese knock-off

B. Windows

C. Android

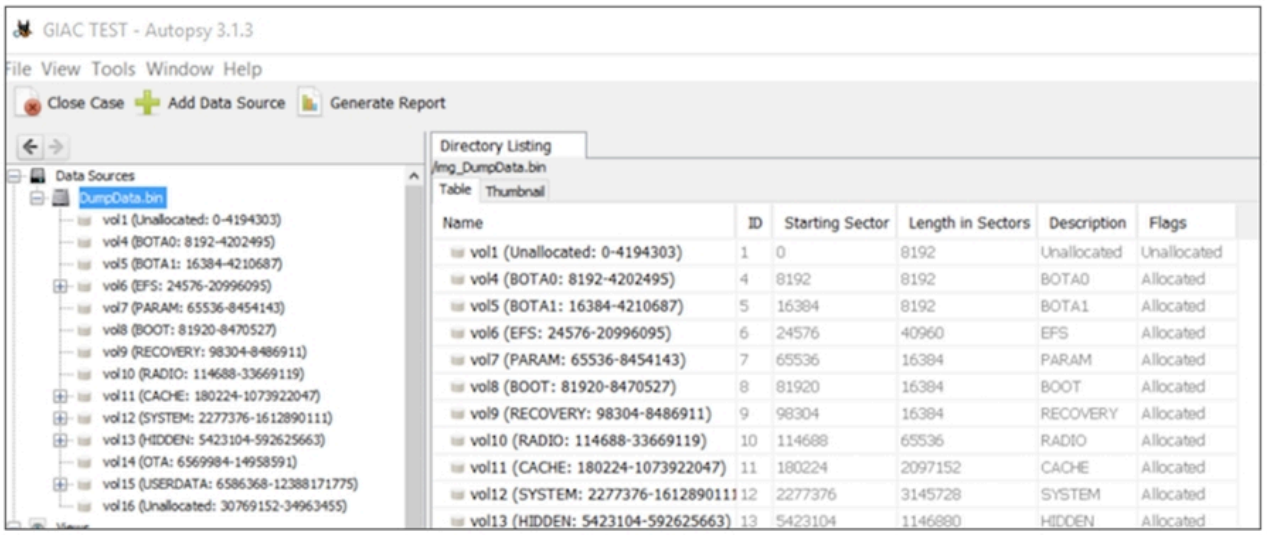
D. Blackberry

Suggested Answer: *A*
Reference:
https://forums.techguy.org/threads/virus-in-china-mobile.992051/

CineFeX 2 years, 11 months ago
No, "Chinese knock-off" is not a file system. It is a term used to describe low-quality, counterfeit products that are made in China and designed to look similar to popular and expensive products from other companies.
upvoted 1 times

Question #2 *Topic 1*

What type of acquisition is being examined in the image below?



A. iOS bypass lock

B. Blackberry logical

C. Android physical

D. Windows Mobile file system

Suggested Answer: *C*

Reference:

http://www.forensicswiki.org/wiki/How_To_Decrypt_Android_Full_Disk_Encryption

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

Which of the following files contains details regarding the encryption state of an iTunes backup file?

A. Keychain-backup.plist

B. Manifest.mbdb

C. Manifest.plist

D. Status.plist

Suggested Answer: *C*
The Manifest.plist lists if the backup is encrypted. This will come into use and be required should the backup file need to be accessed forensically if it is locked. The Manifest.mbdb contains a listing of data stored in the backup. Even if the backup is encrypted, this data can be parsed for more information.
Reference:
http://resources.infosecinstitute.com/ios-5-backups-part-1/#gref

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

In addition to the device passcode, what other essential piece of information is most often required in order to decrypt the contents of BlackBerry OS 10 handsets?

A. BlackBerry Blend username/pin

B. BlackBerry Balance username/password

C. BlackBerry Link ID/password

D. BBM pin

Suggested Answer: *C*

Special considerations when analyzing data from BlackBerry OS 10 devices:

☞ You must have the device passcode as well as the BlackBerry Link password in order to backup or view this data

☞ This requires an Internet connection on the processing machine because you are authenticating to the BlackBerry Link Server to authenticate the username and password

☞ You may encounter issues when attempting to acquire a BES-enabled device.

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

The device pictured below is in Download Mode to attempt a physical acquisition. What can be ascertained by viewing the Android boot screen below?

A. The Android is not rooted

B. No ROM changes have ever occurred on this device

C. The Original/Factory ROM is booting

D. The Original ROM was at one time modified

Suggested Answer: *C*
Reference:
https://www.digitalforensics.com/blog/physical-acquisition-of-a-locked-android-device/

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

An analyst investigating a Nokia S60 Symbian device wants to know if an Adobe Flash file on the handset is compromised. Which file in the image will best target the Adobe Flash files?

File Size	Path	File Name	Modified
2.42 KB	Z:\system\install	FLASHLITE.sis	3/21/2008 1:21:12 AM
2.96 KB	Z:\system\install	OnlinePrint.sis	3/21/2008 1:21:12 AM
4.14 KB	Z:\resource\apps	saflash.r01	3/21/2008 1:21:12 AM
111 Bytes	Z:\resource\apps	AdobeReader_loc.r04	3/21/2008 1:21:12 AM
713 Bytes	Z:\resource	flashliteplugin.r03	3/21/2008 1:21:12 AM
611 Bytes	C:\System	System.ini	8/27/2013 8:10:12 PM
69 Bytes	C:\System\data\mg2\DB\CData	25.dat	7/24/2013 3:51:38 PM

A. FLASHLITE.sis

B. flashliteplugin.r03

C. saflash.r01

D. OnlinePrint.sis

Suggested Answer: *A*

A sis.file is the package that Symbian uses to install applications on their OS compatible handsets. Knowing that you are investigating an application that is installed on the handset, first narrowing the files down to installer packages, or *.sis files, is a good starting point. Flash is an Adobe product making the most logical of the two remaining* .sis files for review, the FLASHLITE installer package. There are several other files related to "Flash" but as resource files, they provide supporting documentation and will not contain the .app file or code that was possibly malicious.

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

As part of your analysis of a legacy BlackBerry device, you examine the installed applications list and it appears that no third-party applications were installed on the device. Which other file may provide you with additional information on applications that were accessed with the handset?

A. BlackBerry NV Items

B. Content Store

C. Event logs

D. BBThumbs.dat

Suggested Answer: *C*
Analyzing both the Event Logs (which are accessible in Oxygen Forensic Suite) and/or the Installed Applications (which is a feature available in Cellebrite Physical Analyzer) may lead you to additional data. If applications of interest were located in the Event Logs, a Keyword Search across the media may reveal more data related to the application.

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Which artifact must be carved out manually when examining a file system acquisition of an Android device?

A. Deleted images

B. Contacts

C. SMS messages

D. Phone numbers

Suggested Answer: *C*

JMH2710 5 years, 1 month ago

the giac practice test we got says that this answer is "Deleted Images" !.... This si the second answer out of 10 that doenst match the practice tests

upvoted 1 times

Question #9 *Topic 1*

When conducting forensic analysis of an associated media card, one would most often expect to find this particular file system format?

A. HFS

B. NTFS

C. Yaffs2

D. FAT

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Cellebrite Physical Analyzer uses Bit Defender to scan for malware by flagging files who have known bad hash values. This is an example of which type of mobile malware detection?

A. Specific-based malware detection

B. Signature-based detection

C. Behavioral-based detection

D. Cloud based malware detection

Suggested Answer: *B*
Reference:
https://security.stackexchange.com/questions/95186/what-is-the-precise-difference-between-a-signature-based-vs-behavior-based-antiv

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Which of the following is required in addition to the Apple ID of the custodian to access IOS backup files that are stored in ICloud?

A. iTunes password

B. Device passcode

C. Manifest.plist

D. Keychain-backup.plist

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

In 2015, Apples iTunes store was found to be hosting several malicious applications that were infected as a result of hacked version of the developer toolkit used to create applications. Which Apple developer suite was targeted?

A. Xcode

B. ADB

C. Momentics IDE

D. Xamarin

Suggested Answer: *A*
Reference:
http://money.cnn.com/2015/09/21/technology/apple-xcode-hack/index.html

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

An Android device user is known to use Facebook to communicate with other parties under examination. There is no evidence of the Facebook application on the phone. If there was Facebook usage where would an examiner expect to find these artifacts?

A. com.android.chrome/app_chrome/Default/Local Storage

B. dmappmgr.db

C. /data/system/packages.xml

D. AndroidManifest.xml

Suggested Answer: *B*
Reference:
https://www.ctsforensics.com/assets/news/35550_Web-update.pdf

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

Physical Analyzer provides a function to narrow down a search based on a timestamp, a type, a party or date. What is the name of this advanced searching capability?

A. Watchlist Editor

B. Tags

C. Timeline

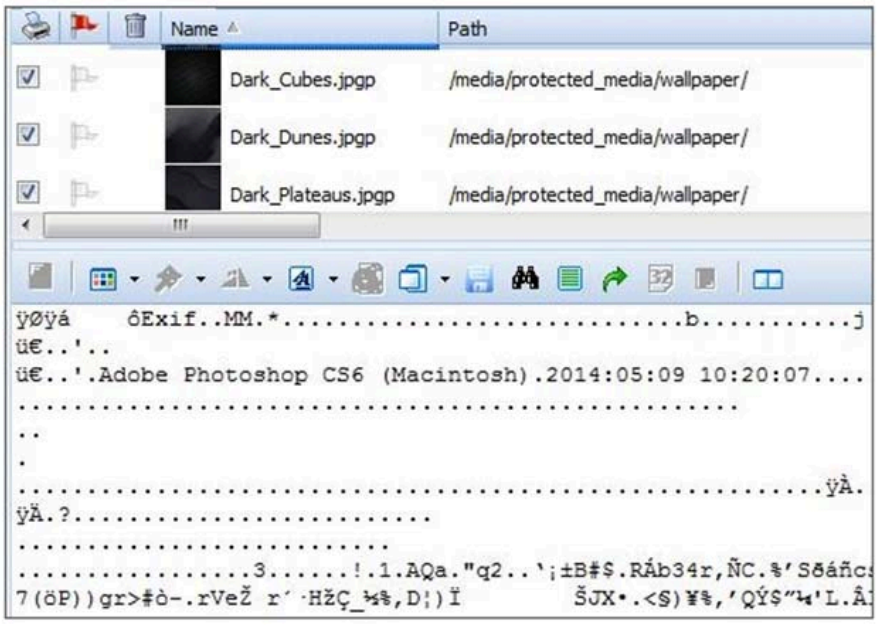
D. Event of Interest

Suggested Answer: *C*
Physical Analyzer offers the Timeline feature to narrow down what happened on the smartphone during a specific time, type, party, etc. This is commonly used to narrow down time periods. Data that is manually carved will not be shown here. There is also an option to create a custom timeline specification.

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

The files pictured below from a BlackBerry OS10 file system have a unique file extension. What can be concluded about these files?



A. Files are protected by the file system, so changing the file system makes them less accessible

B. Files are encrypted to prevent them from being viewed without the decryption key

C. Files are encoded for secure transmitting of data

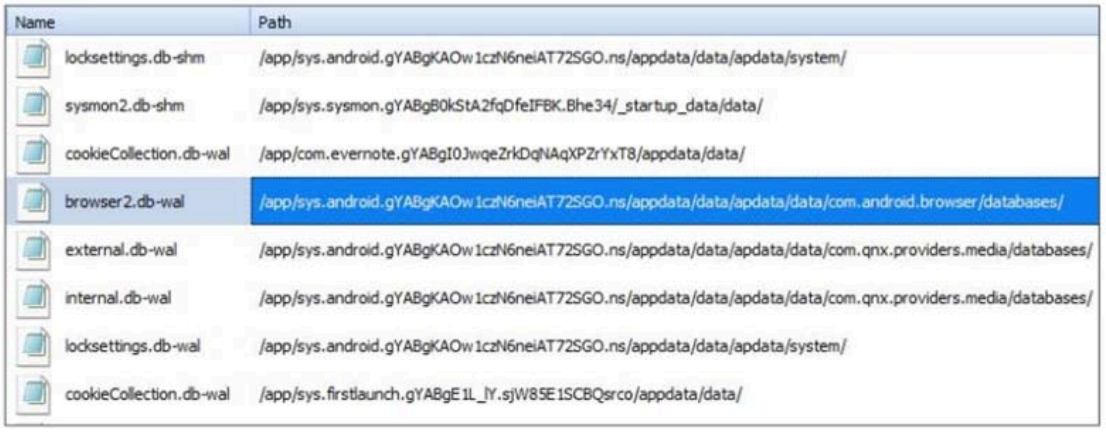
D. Files are located on a media card so they contain a unique file extension

Suggested Answer: *A*
Reference:
https://forums.crackberry.com/blackberry-q10-f272/protected-media-911023/

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

Where can an analyst find data to provide additional artifacts to support the evidence in the highlighted file?



Name	Path
locksettings.db-shm	/app/sys.android.gYABgKAOw1czN6neiAT72SGO.ns/appdata/data/apdata/system/
sysmon2.db-shm	/app/sys.sysmon.gYABgB0kStA2fqDfeIFBK.Bhe34/_startup_data/data/
cookieCollection.db-wal	/app/com.evernote.gYABgI0JwqeZrkDqNAqXPZrYxT8/appdata/data/
browser2.db-wal	/app/sys.android.gYABgKAOw1czN6neiAT72SGO.ns/appdata/data/apdata/data/com.android.browser/databases/
external.db-wal	/app/sys.android.gYABgKAOw1czN6neiAT72SGO.ns/appdata/data/apdata/data/com.qnx.providers.media/databases/
internal.db-wal	/app/sys.android.gYABgKAOw1czN6neiAT72SGO.ns/appdata/data/apdata/data/com.qnx.providers.media/databases/
locksettings.db-wal	/app/sys.android.gYABgKAOw1czN6neiAT72SGO.ns/appdata/data/apdata/system/
cookieCollection.db-wal	/app/sys.firstlaunch.gYABgE1L_JY.sjW85E1SCBQsrco/appdata/data/

A. internal.db-wal

B. browser2.db

C. sysmon2.db-shm

D. external.db

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Which of the following is a unique 56 bit number assigned to a CDMA handset?

A. Mobile Station International Subscriber Directory Number (MSISDN)

B. Electronic Serial Number (ESN)

C. International Mobile Equipment Identifier (IMEI)

D. Mobile Equipment ID (MEID)

Suggested Answer: *D*

The Mobile Equipment ID (MEID), also found under the battery cover, is a 56 bit number which replaced the ESN due to the limited number of 32 bit

ESN numbers. The MEID is listed in hex, where the first byte is a regional code, next three bytes are a manufacturer code, and remaining three bytes are a manufacturer-assigned serial number.

Reference:

https://sites.google.com/site/bbayles/index/cdma_hardware_id

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Which of the following files provides the most accurate reflection of the device's date/timestamp related to the last device wipe?

A. /private/var/mobile/Library/AddressBook/AddressBook.sqlitedb

B. /private/var/mobile/Applications/com.apple.mobilesafari/Library/history.db

C. /private/var/mobile/Applications/com.viber/Library/Prefernces/com.viber.plist

D. /private/var/mobile/Applications/net.whatsapp.WhatsApp/Library/pw.dat

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Which of the following is the term for the SMS malware that sends text messages to a premium number generating large service bills for the user of the targeted device?

A. Trojan

B. Adware

C. Potentially unwanted applications

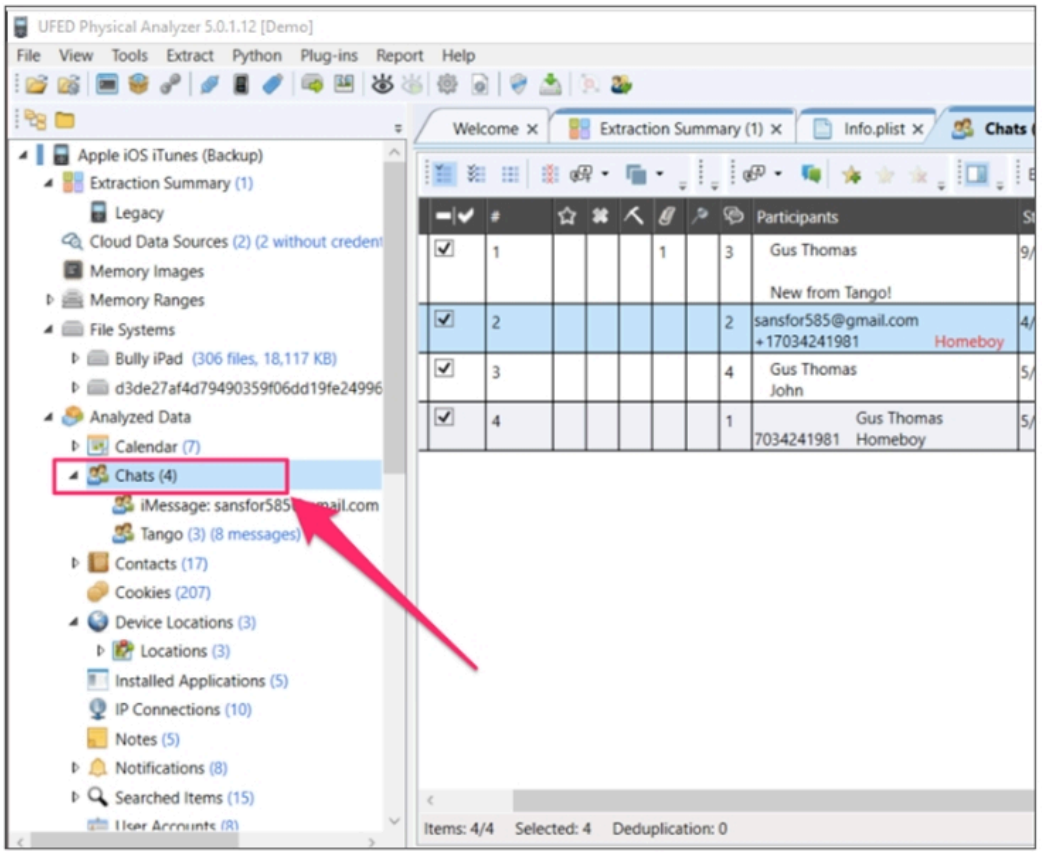
D. Click bait

Suggested Answer: *A*
Reference:
https://pdfs.semanticscholar.org/7f33/9156f47345bd102c9b05f45f9bfe4c182720.pdf

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

When examining the iOS device shown below the tool indicates that there are 4 chat messages recovered from the device. Which of the following locations may contain additional chat information?



A. Memory ranges from a physical dump of the device

B. Databases installed and maintained by the application

C. Internet history plist files found in logical acquisitions

D. IP connections used by the application

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Which of the following can most forensics tools crack on an iOS device?

A. Touch (fingerprint) ID

B. Simple passcode

C. Passphrase

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Which cloud based system can be utilized by Android owners to backup user data?

A. Amazon Web Services (AWS)

B. Samsung Kies

C. Android Device Manager

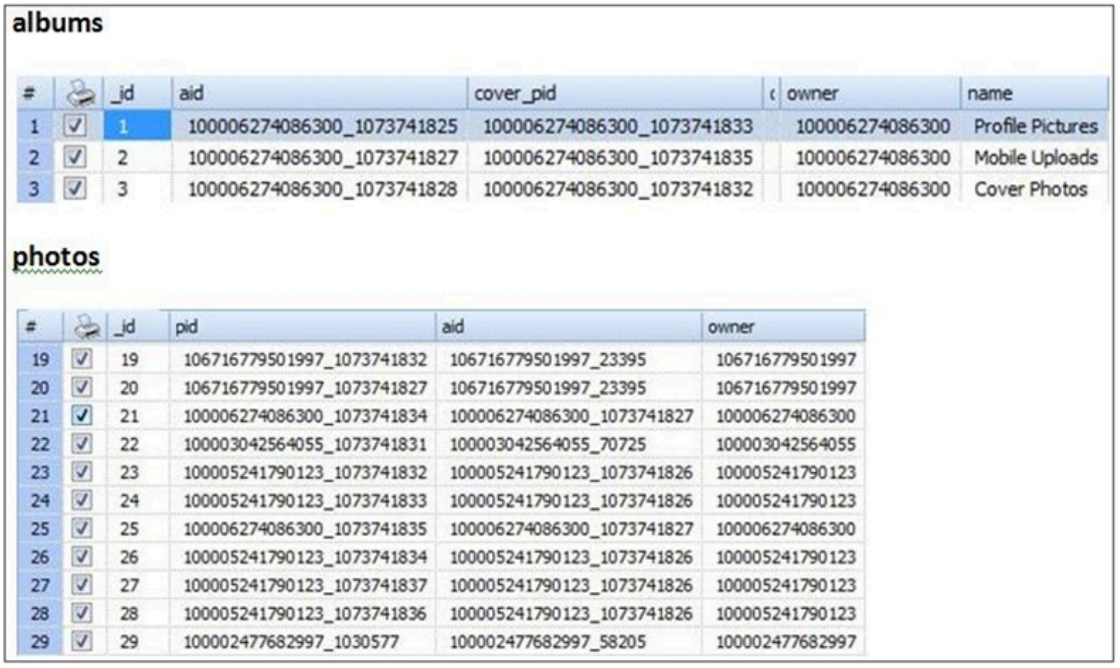
D. Google

Suggested Answer: *D*
Reference:
https://developer.android.com/guide/topics/data/backup.html

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

Analyze the two tables (Albums and Photos) provided from the Facebook database on an Android device located at the path: /data/data/com.facebook.katana/ databases/fb.db.
Which photo was added to Facebook by the user of the device?



albums

#	_id	aid	cover_pid	owner	name
1	1	100006274086300_1073741825	100006274086300_1073741833	100006274086300	Profile Pictures
2	2	100006274086300_1073741827	100006274086300_1073741835	100006274086300	Mobile Uploads
3	3	100006274086300_1073741828	100006274086300_1073741832	100006274086300	Cover Photos

photos

#	_id	pid	aid	owner
19	19	106716779501997_1073741832	106716779501997_23395	106716779501997
20	20	106716779501997_1073741827	106716779501997_23395	106716779501997
21	21	100006274086300_1073741834	100006274086300_1073741827	100006274086300
22	22	100003042564055_1073741831	100003042564055_70725	100003042564055
23	23	100005241790123_1073741832	100005241790123_1073741826	100005241790123
24	24	100005241790123_1073741833	100005241790123_1073741826	100005241790123
25	25	100006274086300_1073741835	100006274086300_1073741827	100006274086300
26	26	100005241790123_1073741834	100005241790123_1073741826	100005241790123
27	27	100005241790123_1073741837	100005241790123_1073741826	100005241790123
28	28	100005241790123_1073741836	100005241790123_1073741826	100005241790123
29	29	100002477682997_1030577	100002477682997_58205	100002477682997

A. 106716779501997_1073741827

B. 100003042564055_1073741835

C. 100005241790123_1073741832

D. 100006274086300_1073741835

Suggested Answer: *D*
Examination of the first table shows user activity related to Cover photos. Mobile uploads and Profile pictures leading to the conclusion that user
100006274086300, is the owner of the device. In the second table, examine the pictures IDs resident in the database. Only one photo shares the Facebook ID that matches the ID of the assumed device owner.

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Which file will indicate if Siri was active on an iOS device?

A. private/var/Library/Preferences/com.apple.suggestions.plist

B. private/var/Library/SpringBoard/PushStore/com.apple.reminders.pushstore

C. private/var/Library/Preferences/com.apple.SpeakSelection.plist

D. private/var/Library/Preferences/com.apple.SiriViewService.plist

Suggested Answer: *B*

The first step in searching for traces of Siri use should be to validate if the user was using Siri. To do this, simply search for iSiri in the tool or navigate to Library/Prefernces/com.apple.SiriViewService.plist. If active, this status will be reflected in the plist file as "StatusActive." Siri stores information in the common files related to each task (calendar.sqlitedb, call_history.db, etc.)

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Which of the following is one potential risk of using the ALWAYS OFF rule for handling cell phones?

A. Overwriting data

B. Engaging password or PIN protection mechanism

C. Destruction of call logs and cell tower information

D. Improper handling by the user

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

What type of storage does an iOS device use for user data?

A. SSD

B. SIM

C. NAND

D. NOR

Suggested Answer: *C*
Reference:
https://www.ifixit.com/Answers/View/230162/Recovering+data+stored+on+NAND+chip+on+iPhone+6

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

Which of the following items is found in the Kernel Space for an iOS device?

A. Cocoa Touch framework

B. System Area

C. Applications

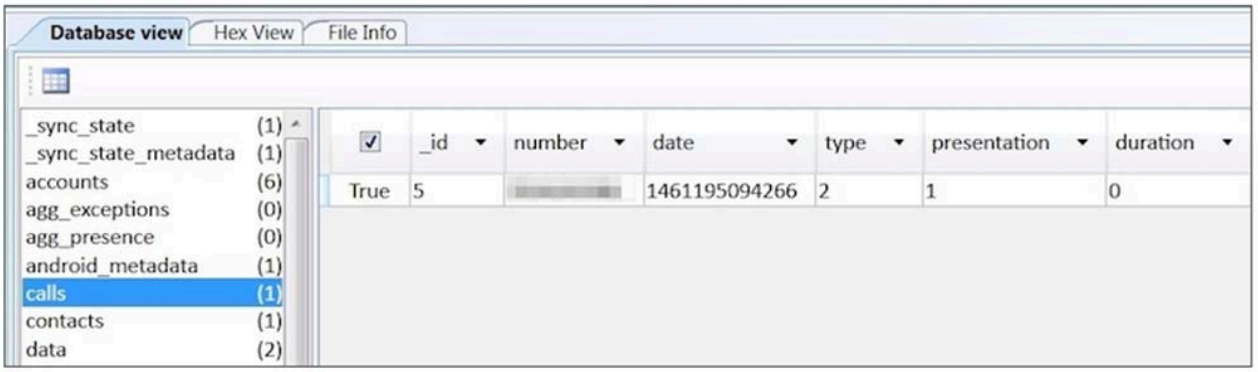
D. Core Services

Suggested Answer: *A*
Reference:
https://developer.apple.com/library/content/documentation/Darwin/Conceptual/KernelProgramming/Architecture/Architecture.html

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

What is being shown in the image below?



A. An outgoing call that was not answered

B. A call that was answered but immediately hung up

C. A missed Skype message on an android device

D. A call that was answered and lasted 5 seconds

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

Where would an examiner find evidence of an iOS update to device from one version to another?

A. NOR memory

B. System partition

C. Data partition

D. SIM card

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Which of the following chipsets is commonly found in knock-off handsets?

A. Invidia Tegra

B. MediaTek (MTK)

C. A8

D. Qualcomm Snapdragon

Suggested Answer: *B*
Reference:
https://www.stuff.tv/features/7-chinese-smartphones-youve-never-heard-will-definitely-want

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

What type of acquisition has occurred for this device?

A. Physical

B. File system

C. Bypass lock

D. Logical

Suggested Answer: *B*
Reference:
https://archive.org/stream/Defcon20Slides/DEFCON-20-Robinson-Spy-vs-Spy_djvu.txt

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

How would an examiner review items deleted from a SQLITE database?

A. Using a Hex Viewer

B. Converting the database to a txt file

C. Reviewing the file header

D. Selecting the raw data from the table

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

Which of the following devices below runs the Apple iOS operating system?

A. Apple TV

B. MacBook Pro

C. iPod Touch

D. Apple Watch

Suggested Answer: *C*

iOS devices can be defined as Apple products running the Apple iPhone operating system including the iPhone, iPad and iPod Touch. The Apple watch runs Watch OS, which is similar to iOS. MacBook Pros run Mac OSX and the Apple TV is using a new operating system called tvOS.

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

Which of the following is a backup tool for smartphones?

A. Ovi Suite

B. Lifeblog

C. Absinthe

D. Mbackup

Suggested Answer: *A*
The only tool in the list that will create a backup is the Ovi Suite. Absinthe and Mbackup are malware and the application Lifeblog is a timelinening tool for Nokia users.

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

When dealing with mobile devices and flash memory, and the fact that data in memory constantly changes even when the device is simply powered on. It is best practice to:

A. Only acquire from devices in an OFF state

B. Document those changes that were made to the device during the forensic process

C. Always use a write-blocker when dealing with mobile devices

D. Always remove the battery from a device before acquisition

Suggested Answer: *B*
Mobile devices are constantly changing when powered on, and there is no way to write block a mobile device because they communicate using modern protocols such as AT commands and others. Because of these factors, the goal in forensic becomes to make as little change as possible, and to document those changes that were made to the device during the forensic process.

Currently there are no comments in this discussion, be the first to comment!