Free Questions for GASF by dumpssheet

Shared by Manning on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- HFS

B- NTFS

C- Yaffs2

D- FAT

Answer:

D

Question 2

Question Type: MultipleChoice

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

Options:

A- Deleted images

B- Contacts

C- SMS messages

D- Phone numbers

Answer:

C

Question 3

Question Type: MultipleChoice

While analysis in BlackBerry application list 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?

Options:

A- BlackBerry NV Items

B- Content Store

C- Event logs

D- BBThumbs.dat

Answer:

C

Question 4

Question Type: **MultipleChoice**

What is the essential piece of information is most often required in order to decrypt the contents of BlackBerry OS 10 handsets?

Options:

A- BlackBerry Blend username/pin

B- BlackBerry Balance username/password

C- BlackBerry Link ID/password

D- BBM pin

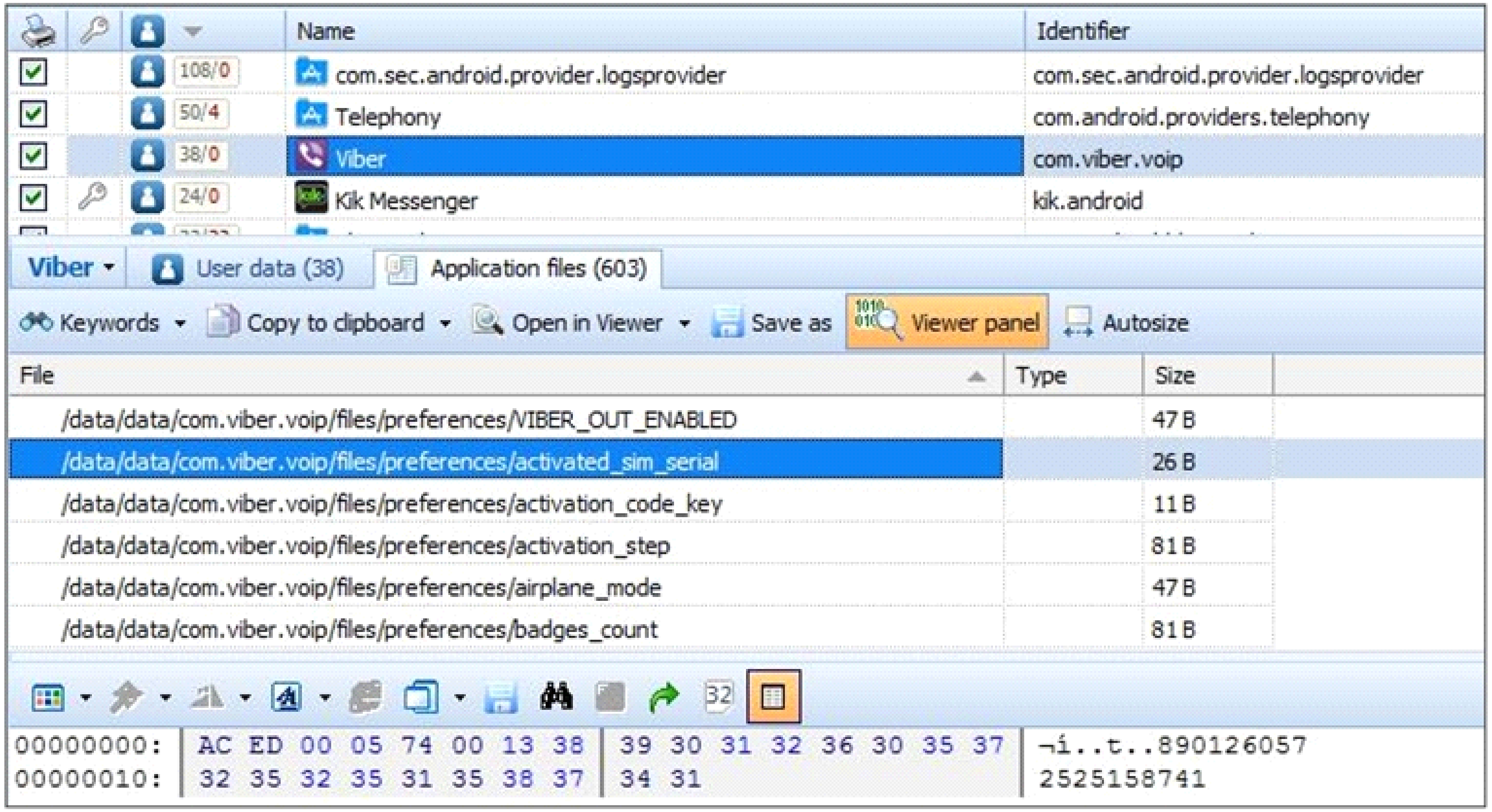
Answer:

C

Question 5

Question Type: MultipleChoice

Review the information contained within the Viber application running on an Android device. Which of the following can be determined?



			Name	Identifier
☑		108/0	com.sec.android.provider.logsprovider	com.sec.android.provider.logsprovider
☑		50/4	Telephony	com.android.providers.telephony
☑		38/0	Viber	com.viber.voip
☑		24/0	Kik Messenger	kik.android

File	Type	Size
/data/data/com.viber.voip/files/preferences/VIBER_OUT_ENABLED		47 B
/data/data/com.viber.voip/files/preferences/activated_sim_serial		26 B
/data/data/com.viber.voip/files/preferences/activation_code_key		11 B
/data/data/com.viber.voip/files/preferences/activation_step		81 B
/data/data/com.viber.voip/files/preferences/airplane_mode		47 B
/data/data/com.viber.voip/files/preferences/badges_count		81 B

```
00000000: AC ED 00 05 74 00 13 38 | 39 30 31 32 36 30 35 37 | ¬í..t..890126057
00000010: 32 35 32 35 31 35 38 37 | 34 31                   | 2525158741
```

Options:

A- A message containing the string 8901260572525158741 was sent using the Viber application.

B- The Viber account used to send/receive messages can be tied to the user in possession of the SIM card with an IMSI of

8901260572525158741

C- The user account for Viber is 8901260572525158741

D- The Viber account used to send/receive messages can be tied to the user in possession of the SIM card with an ICCID of 8901260572525158741

Answer:

D

Explanation:

it is important to know how many digits make up an ICCID versus an IMSI. ICCIDs are comprised of 19 to 20 digits whereas IMSIs may only contain 14 or 15.

Question 6

Question Type: **MultipleChoice**

Which iOS backup file will contain the last time the device was backed up?

Options:

A- notes.sqlite

B- manifest.mbdb

C- status.plist

D- info.plist

Answer:

D

Explanation:

backed up. The file manifest.mbdb contains a list of data stored in the backup. The file status.plist contains details about the backup including a flag to identify the backup type, date and version. The file notes.sqlite is an android file that contains notes written by the user on the device.

Question 7

Question Type: **MultipleChoice**

You have conducted a keyword search over flash.bin and notice that multiple instances of the same data

appear many times throughout the flash image. What is this an example of?

Options:

A- Flash Translation Layer (FTL)

B- Logical Block Addressing (LBA)

C- NAND degradation

D- Wear-leveling

Answer:

C

Question 8

Question Type: **MultipleChoice**

Which file, located on the Android file system, may be examined to correlate files related to external SD cards that were once used in an Android device?

Options:

A- Internal.db

B- Main.db

C- DataManager. Db

D- external.db

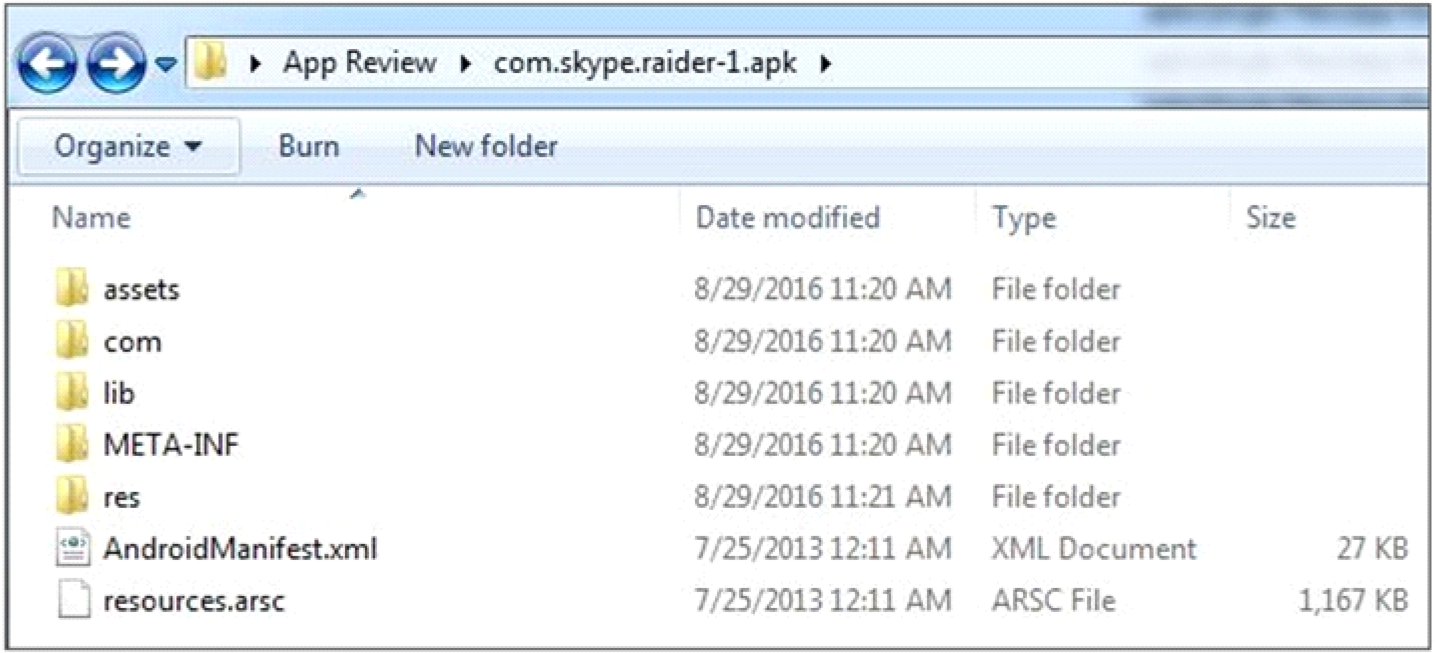
Answer:

D

Question 9

Question Type: **MultipleChoice**

Examine the unpacked Android application below. Which important file, resident in most Android applications, is missing?



Name	Date modified	Type	Size
assets	8/29/2016 11:20 AM	File folder	
com	8/29/2016 11:20 AM	File folder	
lib	8/29/2016 11:20 AM	File folder	
META-INF	8/29/2016 11:20 AM	File folder	
res	8/29/2016 11:21 AM	File folder	
AndroidManifest.xml	7/25/2013 12:11 AM	XML Document	27 KB
resources.arsc	7/25/2013 12:11 AM	ARSC File	1,167 KB

Options:

A- dalvik-cache

B- classes.dex

C- com.skype.raider-1.apk

D- classes-dex2jar.jar

Answer:

B

Question 10

Question Type: **MultipleChoice**

What does access to iOS DFU mode provide an examiner?

Options:

A- Ability to decrypt the SD card of a Symbian device

B- Ability to acquire the info.mkf file on a Blackberry device and brute force the password

C- Ability to root an Android device and perform a physical acquisition

D- Ability to bypass the lock screen of an older iOS device

Answer:

D

Question 11

Question Type: **MultipleChoice**

What is the extension used for BlackBerry 10 backup files?

Options:

A- .APK

B- .BBB

C- .ZIP

D- .IPD

Answer:

B

Question 12

Question Type: **MultipleChoice**

Following the introduction of iMessage with the firmware release iOS 5, devices began storing date/

timestamps in which of the following formats?

Options:

A- UNIXEPOCH

B- PDU SMS timestamp

C- UNIXEPCH

D- Mac epoch

Answer:

A