DUMPSARENA

GIAC Advanced Smartphone Forensics

GIAC GASF

Version Demo

Total Demo Questions: 10

Total Premium Questions: 75

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

What is a risk to the security of an iPhone backup if the user selects to set a password and encrypt their

backup?

A. The keychain is not captured with the backup and the password can be recovered from the Info.plist file

B. The clear text password will be cached in the user's keychain and can be recovered searching the user's keychain

C. The data is encrypted using a strong key but the password is saved to a file which is encoded using Base64, which is easily reversible

D. The backup file is encrypted and a copy of the keychain is saved in a local file which may be attacked using brute force tools

ANSWER: D

Explanation:

:

When a user creates an iOS backup file they have the option to encrypt the datA. If they select this option a backup of the keychain that contains the encryption password is saved to the file manifest.plist. This file can be examined and the encrypted password can be decrypted, typically through a brute force attack.

QUESTION NO: 2

What does access to iOS DFU mode provide an examiner?

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

Explanation:

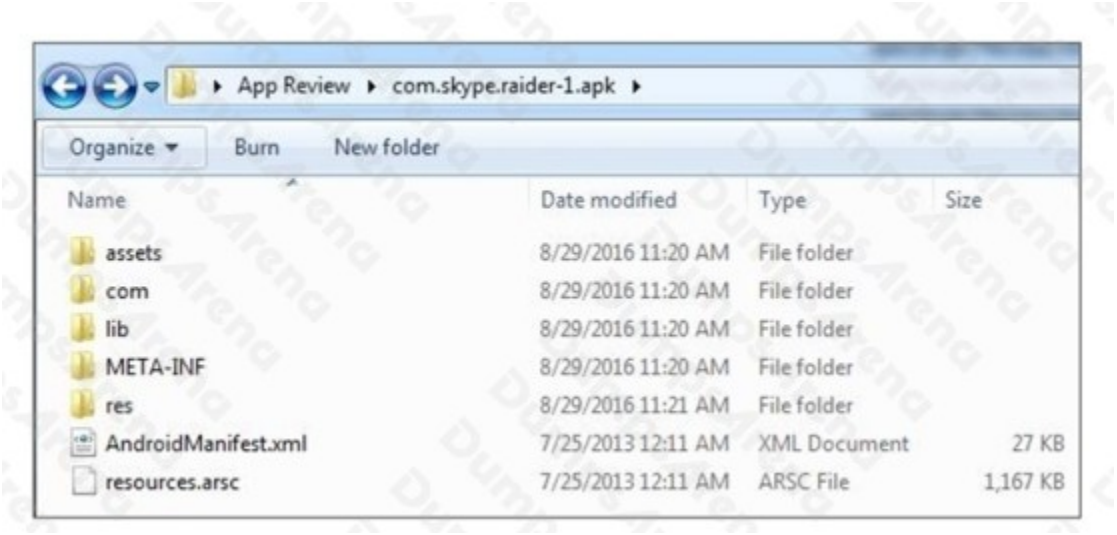
:

Reference: https://www.sciencedirect.com/science/article/pii/B978159749659900002X

QUESTION NO: 3

Examine the unpacked Android application below. Which important file, resident in most

Android applications, is missing?



A. dalvik-cache

B. classes.dex

C. com.skype.raider-1.apk

D. classes-dex2jar.jar

ANSWER: B

Explanation:

:

Reference: https://en.wikipediA.org/wiki/Android_application_package

QUESTION NO: 4

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

ANSWER: A

Explanation:

:

Reference: https://developer.apple.com/library/content/documentation/Darwin/Conceptual/

KernelProgramming/Architecture/Architecture.html

QUESTION NO: 5

Using an emulator and running an application through a series of processes to figure out how it would behave on an actual device is called:

A. Forensic analysis

B. Dynamic analysis

C. Web analysis

D. Static analysis

ANSWER: B

Explanation:

:

Reference:

https://pdfs.semanticscholar.org/90d9/6a3ab48a1b1039573d8a9bfd11e1ab957b82.pdf

QUESTION NO: 6

When analyzing the WhatsApp timestamp “1461184912” in iOS what timestamp conversion should be used?

A. Chrome

B. Webkit

C. UNIX Epoch

D. Mac Absolute

ANSWER: C

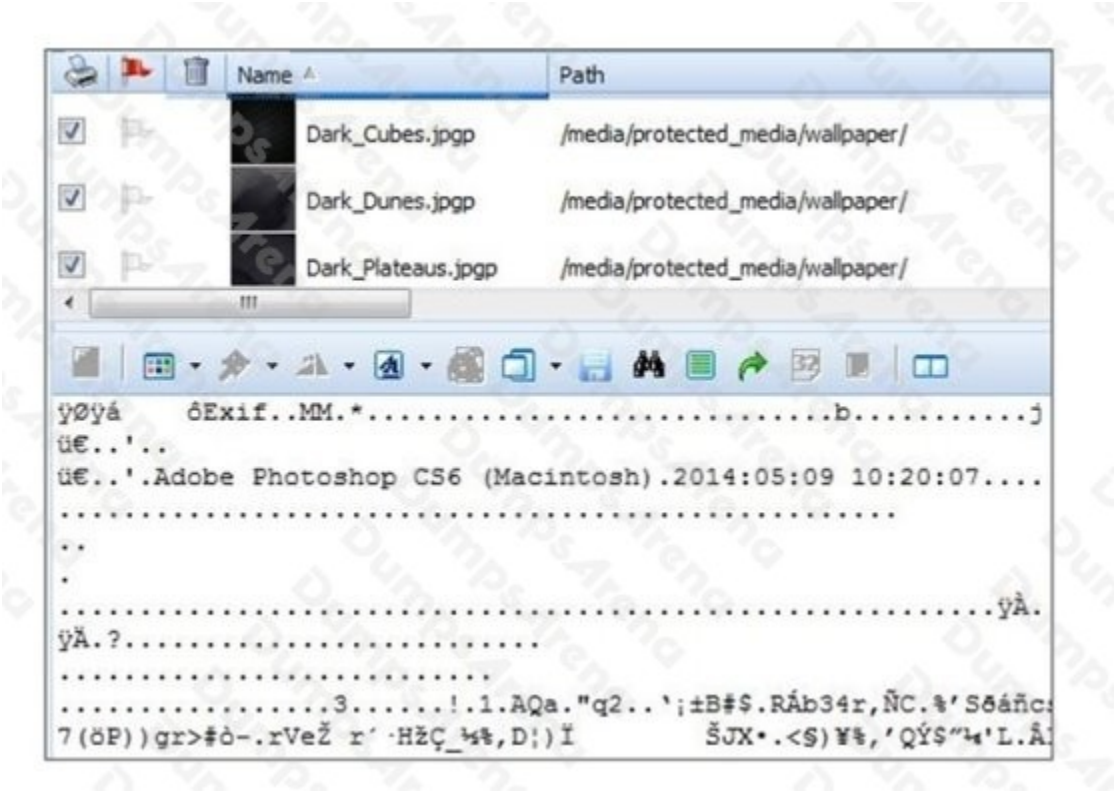
Explanation:

:

Reference: https://arxiv.org/pdf/1507.07739.pdf

QUESTION NO: 7

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

ANSWER: A

Explanation:

:

Reference: https://forums.crackberry.com/blackberry-q10-f272/protected-media-911023/

QUESTION NO: 8

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

ANSWER: D

Explanation:

:

Reference: https://developer.android.com/guide/topics/data/backup.html

QUESTION NO: 9

The jTAG method is designed to acquire data through which of the following?

A. Chip-level access

B. Twister box with RJ45 connection

C. Test Access Ports (TAPs)

D. Chip-level access USB connection

ANSWER: C

Explanation:

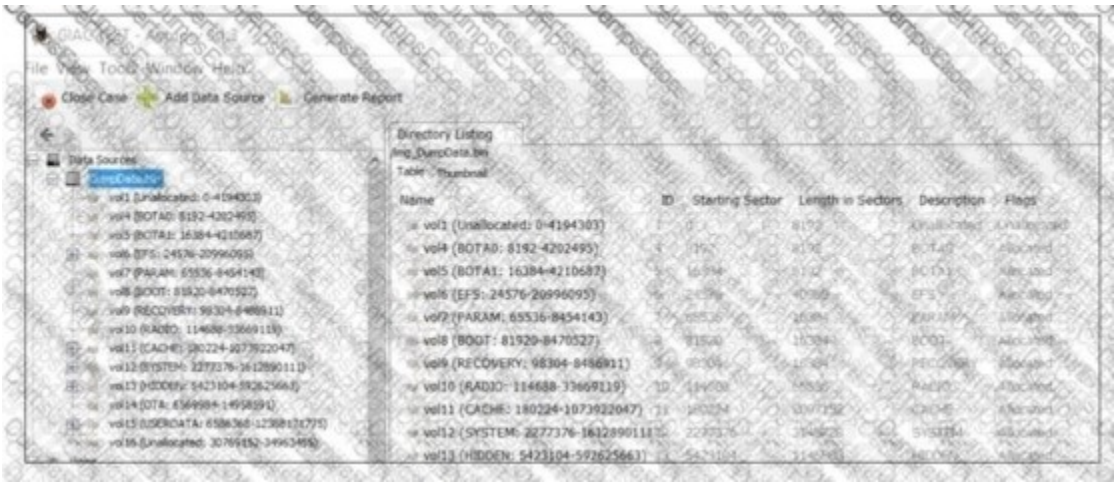
:

The Joint Test Action Group, or JTAG method, is commonly relied upon when forensic and open source tools do not support data acquisition of a smartphone. This type of acquisition can damage a device if done by an untrained examiner. The JTAG method acquires data via the Test Access Ports (TAPs), which requires the device be taken apart, yet remain functional.
Reference:

http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=922

QUESTION NO: 10

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

ANSWER: C

Explanation:

:

Reference:

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