Demo Questions

GIAC GASF Exam

GIAC Advanced Smartphone Forensics (GASF)

Thank you for downloading GASF Exam PDF

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

Correct Answer: *A*

Reference:

https://forums.techguy.org/threads/virus-in-china-mobile.992051/

Question #2Topic 1

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

GIAC TEST - Autopsy 3.1.3						
le View Tools Window Help						
🕳 Close Case 🛶 Add Data Source 🐚 Generate R	Report					
Data Sources Descharte	A Table Thunbrial					
vol1 (J.nakozsted: 0 -4194303) vol4 (DCTA0: 8192-4302495) vol5 (SCTA1: 55384-4210687) vol6 (DF5: 24578-20996095) vol6 (DF5: 24578-20996095) vol6 (DF5: 24578-20996095) vol8 (DCOT: 81520-6479527) vol9 (BCOTKER: 9304-646912) vol10 (RAEDC: 114688-35669119) III (CAEDC: 114688-3569119)	Name	D	Starting Sector	Length in Sectors	Description	Flags
	wol1 (Unallocated: 0-4194303)	1	0	0192	Unallocated	Unallocated
	= vol4 (BOTA0: 8192-4202495)	4	8192	8192	BOTAD	Allocated
	wol5 (BOTA1: 16384-4210687)	5	16384	8192	BOTA1	Allocated
	wol6 (EFS: 24576-20996095)	6	24576	40960	EPS	Allocated
	= vol7 (PARAM: 65536-8454143)	7	65536	16394	PARAM	Allocated
	wol8 (800T: 81920-8470527)	0	01920	16304	BOOT	Allocated
- vol12 (\$157894: 2277376-3612890111)	woł9 (RECOVERY: 98304-8486911)	9	98304	16394	RECOVERY	Allocated
	wol10 (RADID: 114688-33669119)	10	114600	65536	RADIO	Allocated
	= vol11 (CACHE: 180224-1073922047)	11	180224	2097152	CACHE	Allocated
	wol12 (SYSTEM: 2277376-161289011	112	2277376	3145728	SYSTEM	Allocated
	wol13 (HIDDEN: 5423104-592625663)	13	5423104	1146880	HEDDEN	Allocated

- A. iOS bypass lock
- B. Blackberry logical
- C. Android physical
- D. Windows Mobile file system

Correct Answer: C

Reference:

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

Question #3Topic 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

Correct 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

Question #4Topic 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

Correct 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.

Question #5Topic 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

Correct Answer: C

Reference:

https://www.digitalforensics.com/blog/physical-acquisition-of-a-lo

cked-android-device