

Exam : GASF

Title:GIAC AdvancedSmartphone Forensics

Version : DEMO



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

- A. Chinese knock-off
- B. Windows
- C. Android
- D. Blackberry
- Answer: A

Explanation:

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

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

GIAC TEST - Autopsy 3.1.3							
e View Tools Window Help							
🍘 Close Case 🛖 Add Data Source 📗 Generate I	Report						
€ ⇒	Directory /mg_DumpDa						
	Table Thu						
	Name		ID	Starting Sector	Length in Sectors	Description	Flags
	wol1 (vol1 (Unallocated: 0-4194303)		0	8192	Unallocated	Unallocated
	wol4 (iii vol4 (BOTA0: 8192-4202495)		8192	8192	BOTAD	Allocated
	w vol5 (wol5 (BOTA1: 16384-4210687)		16384	8192	BOTA1	Allocated
	🔤 vol6 (wol6 (EFS: 24576-20996095)		24576	40960	EFS	Allocated
	w vol7 (wol7 (PARAM: 65536-8454143)		65536	16384	PARAM	Allocated
	😑 vol8 (BOOT: 81920-8470527)	8	81920	16384	BOOT	Allocated
vol12 (SYSTEM: 2277376-1612890111)	iii vol9 (RECOVERY: 98304-8486911)	9	98304	16394	RECOVERY	Allocated
vol13 (HDDEN: 5423104-592625663) vol14 (OTA: 6569984-14958591) vol15 (USERDATA: 6586568-12388171775) vol16 (Unallocated: 30769152-34963455)	w vol10	(RADIO: 114688-33669119)	10	114688	65536	RADIO	Allocated
	w vol11	(CACHE: 180224-1073922047)	11	180224	2097152	CACHE	Allocated
	wol12	(SYSTEM: 2277376-1612890111	12	2277376	3145728	SYSTEM	Allocated
	w vol13	(HIDDEN: 5423104-592625663)	13	5423104	1146880	HIDDEN	Allocated

- 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

3. 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

Answer: C

Explanation:

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

4.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

Answer: C

Explanation:

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.

5. 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

Answer: C

Explanation:

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