IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

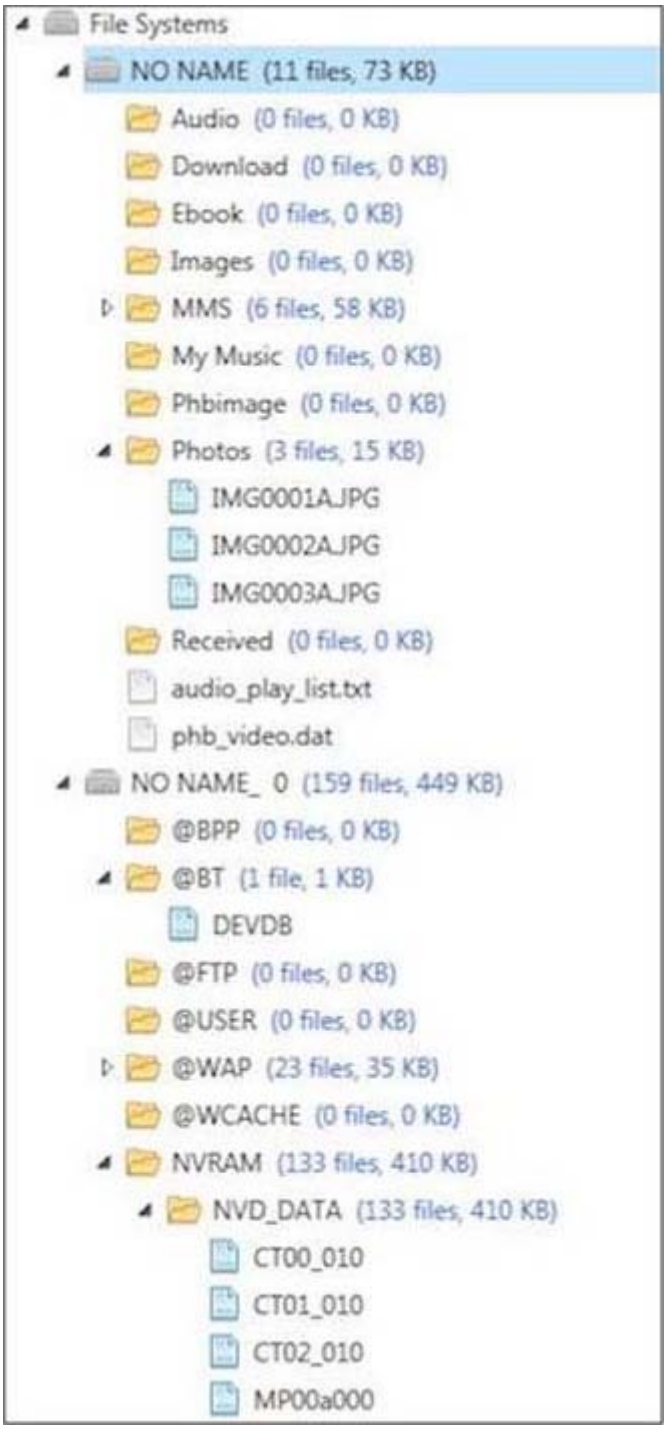
http://www.itrenzheng.com

Exam : **GASF**

Title : GIAC Advanced Smartphone Forensics

Version : DEMO

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



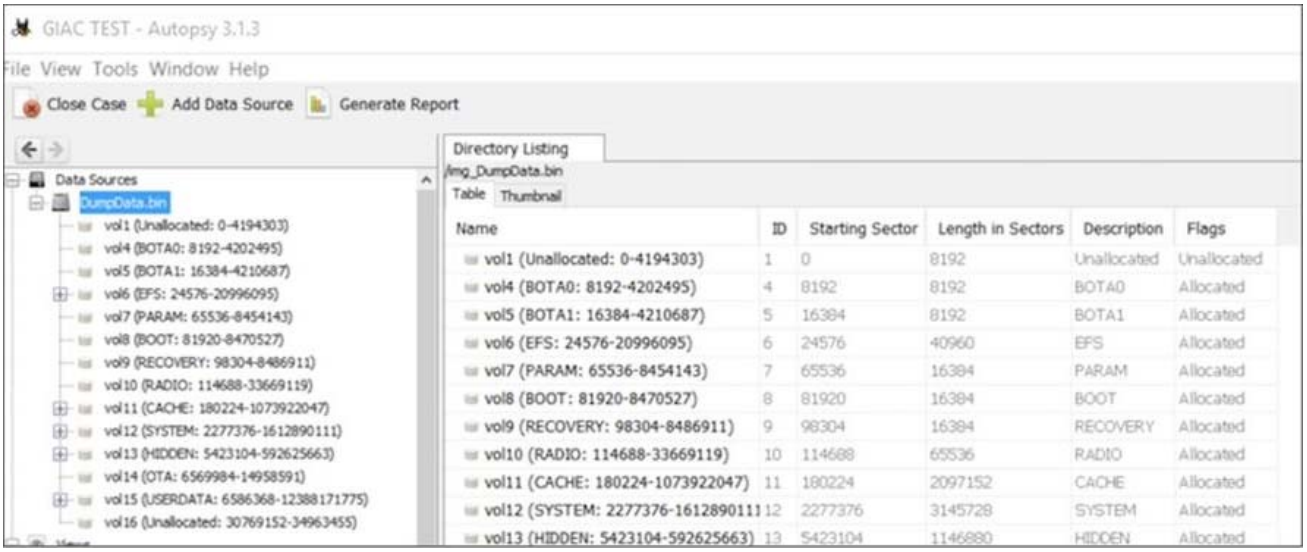
A. Chinese knock-off
B. Windows
C. Android
D. Blackberry

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?



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/