GIAC

GASF Exam

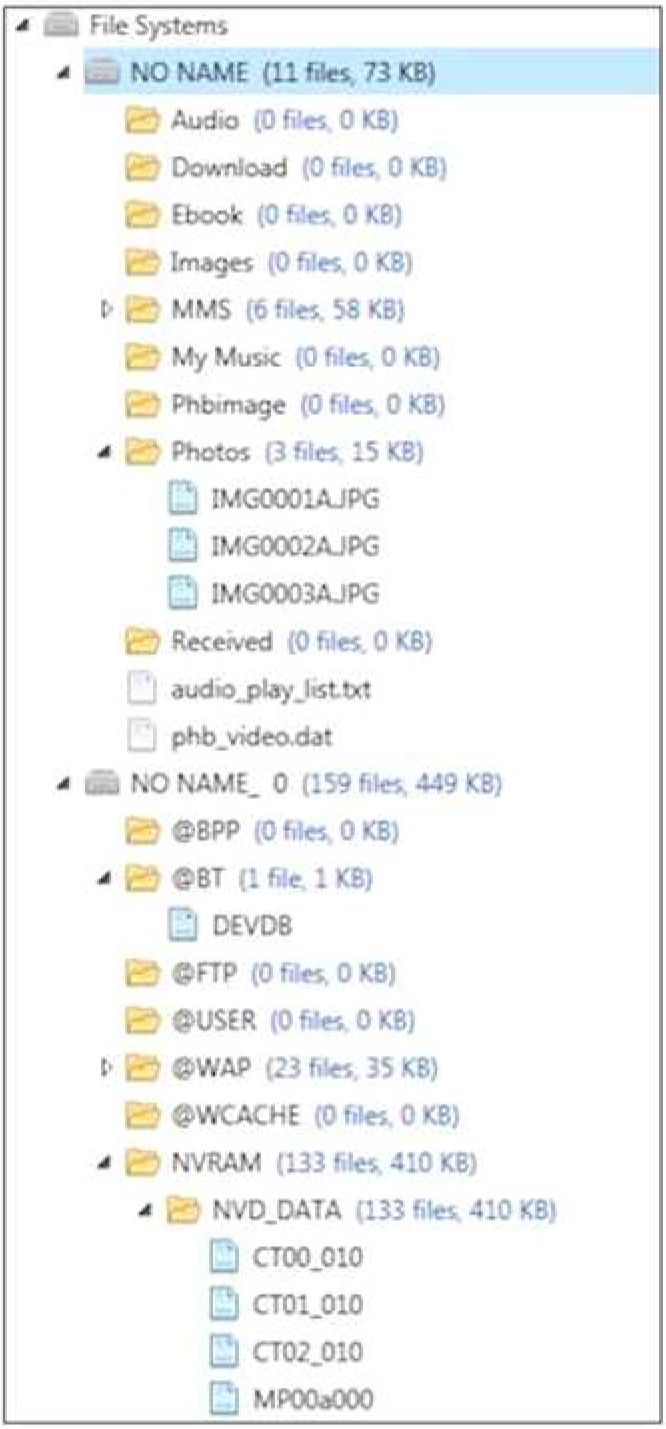
GIAC Advanced Smartphone Forensics

[Questions & Answers Demo]

Version: 8.0

Question: 1

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



```
File Systems
  NO NAME (11 files, 73 KB)
    Audio (0 files, 0 KB)
    Download (0 files, 0 KB)
    Ebook (0 files, 0 KB)
    Images (0 files, 0 KB)
    MMS (6 files, 58 KB)
    My Music (0 files, 0 KB)
    Phbimage (0 files, 0 KB)
    Photos (3 files, 15 KB)
      IMG0001A.JPG
      IMG0002A.JPG
      IMG0003A.JPG
    Received (0 files, 0 KB)
    audio_play_list.txt
    phb_video.dat
  NO NAME_ 0 (159 files, 449 KB)
    @BPP (0 files, 0 KB)
    @BT (1 file, 1 KB)
      DEVDB
    @FTP (0 files, 0 KB)
    @USER (0 files, 0 KB)
    @WAP (23 files, 35 KB)
    @WCACHE (0 files, 0 KB)
    NVRAM (133 files, 410 KB)
      NVD_DATA (133 files, 410 KB)
        CT00_010
        CT01_010
        CT02_010
        MP00a000
```

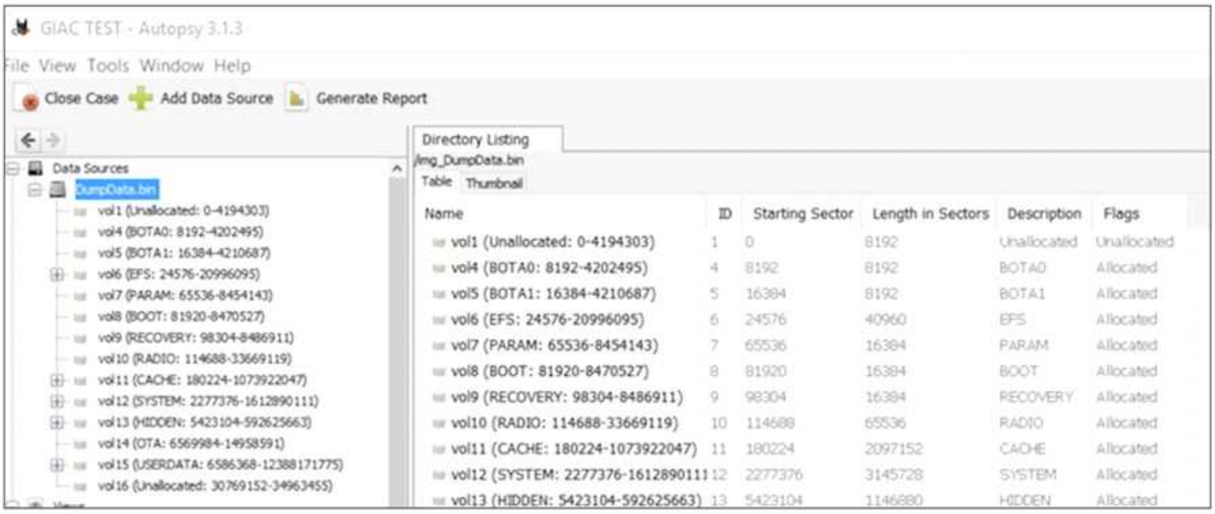
A. Chinese knock-off
B. Windows
C. Android
D. Blackberry

Answer: A

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

Question: 2

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



Data Sources
DumpData.bin
- vol1 (Unallocated: 0-4194303)
- vol4 (BOTA0: 8192-4202495)
- vol5 (BOTA1: 16384-4210687)
- vol6 (EFS: 24576-20996095)
- vol7 (PARAM: 65536-8454143)
- vol8 (BOOT: 81920-8470527)
- vol9 (RECOVERY: 98304-8486911)
- vol10 (RADIO: 114688-33669119)
- vol11 (CACHE: 180224-1073922047)
- vol12 (SYSTEM: 2277376-1612890111)
- vol13 (HIDDEN: 5423104-592625663)
- vol14 (OTA: 6569984-14958591)
- vol15 (USERDATA: 6586368-12388171775)
- vol16 (Unallocated: 30769152-34963455)

/img_DumpData.bin

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-4194303)	1	0	8192	Unallocated	Unallocated
vol4 (BOTA0: 8192-4202495)	4	8192	8192	BOTA0	Allocated
vol5 (BOTA1: 16384-4210687)	5	16384	8192	BOTA1	Allocated
vol6 (EFS: 24576-20996095)	6	24576	40960	EFS	Allocated
vol7 (PARAM: 65536-8454143)	7	65536	16384	PARAM	Allocated
vol8 (BOOT: 81920-8470527)	8	81920	16384	BOOT	Allocated
vol9 (RECOVERY: 98304-8486911)	9	98304	16384	RECOVERY	Allocated
vol10 (RADIO: 114688-33669119)	10	114688	65536	RADIO	Allocated
vol11 (CACHE: 180224-1073922047)	11	180224	2097152	CACHE	Allocated
vol12 (SYSTEM: 2277376-1612890111	12	2277376	3145728	SYSTEM	Allocated
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

Question: 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
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

Question: 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?

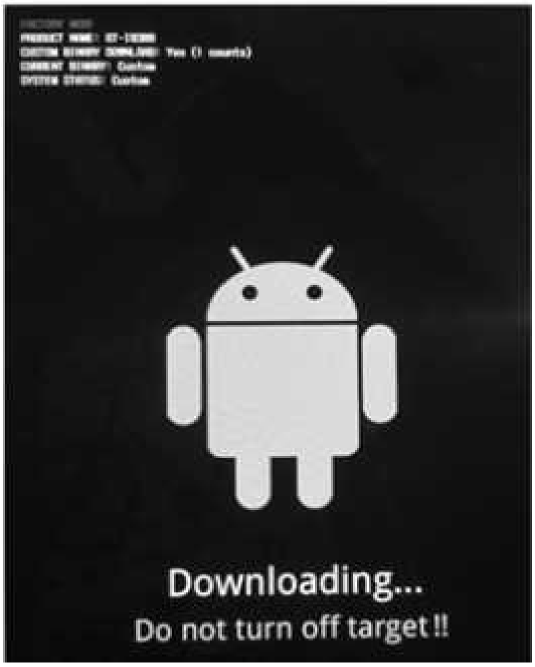
A. BlackBerry Blend username/pin
B. BlackBerry Balance username/password
C. BlackBerry Link ID/password
D. BBM pin

Answer: C

Explanation
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.

Question: 5

The device pictured below is in Download Mode to attempt a physical acquisition.



```
[illegible]
PRODUCT NAME: GT-I9300
CUSTOM BINARY DOWNLOAD: Yes (1 counts)
CURRENT BINARY: Custom
SYSTEM STATUS: Custom
```

Downloading...
Do not turn off target!!

What can be ascertained by viewing the Android boot screen below?

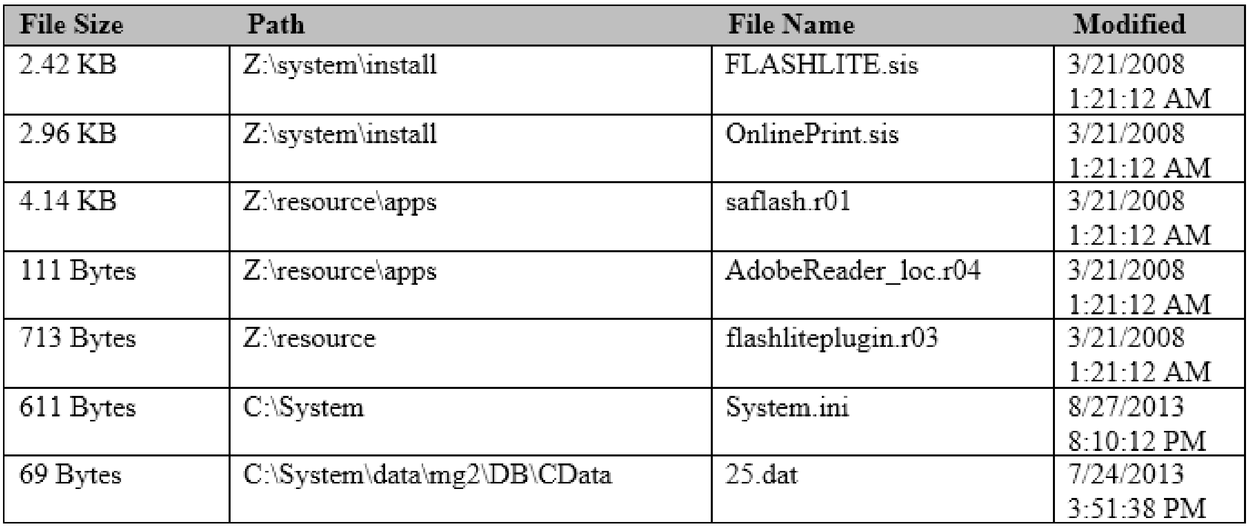
A. The Android is not rooted
B. No ROM changes have ever occurred on this device
C. The Original/Factory ROM is booting
D. The Original ROM was at one time modified

Answer: C

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

Question: 6

An analyst investigating a Nokia S60 Symbian device wants to know if an Adobe Flash file on the handset is compromised.



File Size	Path	File Name	Modified
2.42 KB	Z:\system\install	FLASHLITE.sis	3/21/2008 1:21:12 AM
2.96 KB	Z:\system\install	OnlinePrint.sis	3/21/2008 1:21:12 AM
4.14 KB	Z:\resource\apps	saflash.r01	3/21/2008 1:21:12 AM
111 Bytes	Z:\resource\apps	AdobeReader_loc.r04	3/21/2008 1:21:12 AM
713 Bytes	Z:\resource	flashliteplugin.r03	3/21/2008 1:21:12 AM
611 Bytes	C:\System	System.ini	8/27/2013 8:10:12 PM
69 Bytes	C:\System\data\mg2\DB\CData	25.dat	7/24/2013 3:51:38 PM

Which file in the image will best target the Adobe Flash files?

A. FLASHLITE.sis
B. flashliteplugin.r03
C. saflash.r01
D. OnlinePrint.sis

Answer: A

Explanation
Explanation: A sis.file is the package that Symbian uses to install applications on their OS compatible handsets. Knowing that you are investigating an application that is installed on the handset, first narrowing the files down to installer packages, or *.sis files, is a good starting point. Flash is an Adobe product making the most logical of the two remaining* .sis files for review, the FLASHLITE installer package. There are several other files related to “Flash” but as resource files, they provide supporting documentation and will not contain the .app file or code that was possibly malicious.

Question: 7

As part of your analysis of a legacy BlackBerry device, you examine the installed applications list and 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?

A. BlackBerry NV Items
B. Content Store
C. Event logs
D. BBThumbs.dat

Answer: C

Explanation
Explanation: Analyzing both the Event Logs (which are accessible in Oxygen Forensic Suite) and/or the
Installed Applications (which is a feature available in Cellebrite Physical Analyzer) may lead you to additional
datA. If applications of interest were located in the Event Logs, a Keyword Search across the media may reveal more data related to the application.

Question: 8

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

A. Deleted images
B. Contacts
C. SMS messages
D. Phone numbers

Answer: C

Explanation

Question: 9

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

A. HFS
B. NTFS
C. Yaffs2
D. FAT

Answer: D

Explanation

Question: 10

Cellebrite Physical Analyzer uses Bit Defender to scan for malware by flagging files who have known bad hash values. This is an example of which type of mobile malware detection?

A. Specific-based malware detection
B. Signature-based detection
C. Behavioral-based detection
D. Cloud based malware detection

Answer: B