

DUMPSBOSS.COM

GIAC Advanced Smartphone Forensics (GASF)

GIAC GASF

Version Demo

Total Demo Questions: 10

Total Premium Questions: 75

Buy Premium PDF

<https://dumpsboss.com>

support@dumpsboss.com

dumpsboss.com

QUESTION NO: 1

Review the message database below.

Database Structure Browse Data Edit Pragma Execute SQL								
Table: chat_history_message								New Record
id	chs_id	type	timestamp	server_timestamp	direction	route_type	from_id	
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	
1 2	2	0	1487692685....	1	0	3	1487692685.188047_2486	
2 3	2	0	1487692709....	1	0	3	1487692709.882862_658	
3 5	2	1	1487692863....	1	4	3	1487692861.956361_3691	
4 6	2	3	1487692893....	1	1	3	221160132374479	
5 7	2	0	1487699198....	1	0	3	1487699197.953165_2981	
6 8	2	1	1487699208....	1	4	3	1487699206.634783_9850	
7 9	2	0	1487699214....	1	0	3	1487699213.994157_9282	

What can be determined based on the information provided?

- A. There are no deleted messages in this database
- B. The interrupted sequence in the id column could indicate deleted messages
- C. The messages in this table are “outgoing”
- D. The messages contain attachments
- E. The messages in this table are only “incoming”

ANSWER: B

Explanation:

:

QUESTION NO: 2

Review the two highlighted sections in the hex output below from the file MP0c_000.



Convert the phone number found in raw format extracted from a Chinese knock-off device.

- A. 3494044495
- B. 7034241991
- C. 6174429119
- D. 4349404459

ANSWER: B

Explanation:

:

QUESTION NO: 3

Exhibit:

Name	Path
locksettings.db-shm	/app/sys.android.gYABgKAOw1czf6neiAT725GO.ns/appdata/data/apdata/system/
sysmon2.db-shm	/app/sys.sysmon.gYABgB0kStA2fqDfeIFBK.Bhe34/_startup_data/data/
cookieCollection.db-wal	/app/com.evernote.gYABgI0JwqeZrkDqNAqXPZrYxT8/appdata/data/
browser2.db-wal	/app/sys.android.gYABgKAOw1czf6neiAT725GO.ns/appdata/data/apdata/data/com.android.browser/databases/
external.db-wal	/app/sys.android.gYABgKAOw1czf6neiAT725GO.ns/appdata/data/apdata/data/com.qnx.providers.media/databases/
internal.db-wal	/app/sys.android.gYABgKAOw1czf6neiAT725GO.ns/appdata/data/apdata/data/com.qnx.providers.media/databases/
locksettings.db-wal	/app/sys.android.gYABgKAOw1czf6neiAT725GO.ns/appdata/data/apdata/system/
cookieCollection.db-wal	/app/sys.frstiaunch.gYABgE1L_jf.sjW8SE1SCBQsrco/appdata/data/

Where can an analyst find data to provide additional artifacts to support the evidence in the highlighted file?

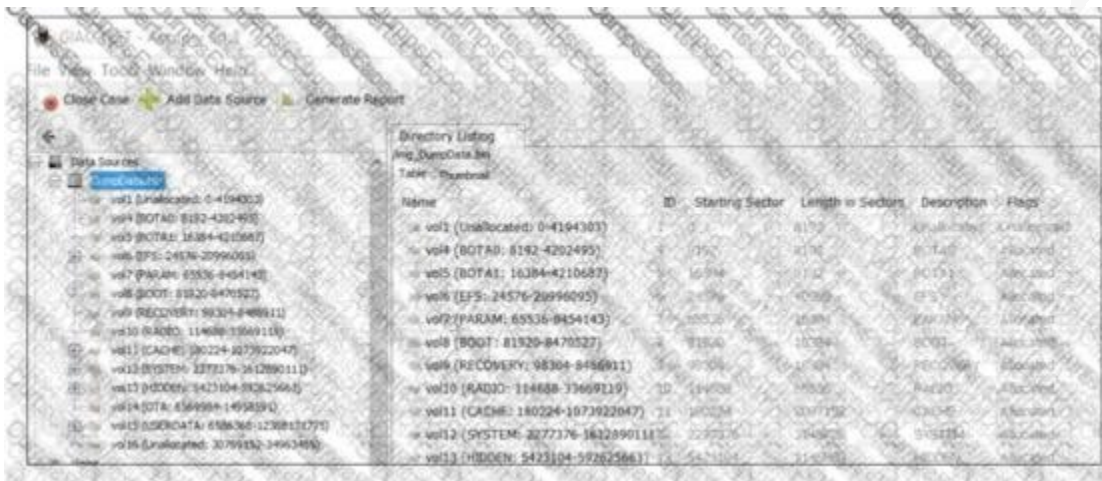
- A. internal.db-wal

- B. browser2.db
- C. sysmon2.db-shm
- D. external.db

ANSWER: A

QUESTION NO: 4

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


QUESTION NO: 5

Analyze the two tables (Albums and Photos) provided from the Facebook database on an Android device located at the path: /data/data/com.facebook.katana/databases/fb.db.

albums

#		_id	aid	cover_pid	owner	name
1	<input checked="" type="checkbox"/>	1	100006274086300_1073741825	100006274086300_1073741833	100006274086300	Profile Pictures
2	<input checked="" type="checkbox"/>	2	100006274086300_1073741827	100006274086300_1073741835	100006274086300	Mobile Uploads
3	<input checked="" type="checkbox"/>	3	100006274086300_1073741828	100006274086300_1073741832	100006274086300	Cover Photos

photos

#		_id	pid	aid	owner
19	<input checked="" type="checkbox"/>	19	106716779501997_1073741832	106716779501997_23395	106716779501997
20	<input checked="" type="checkbox"/>	20	106716779501997_1073741827	106716779501997_23395	106716779501997
21	<input checked="" type="checkbox"/>	21	100006274086300_1073741834	100006274086300_1073741827	100006274086300
22	<input checked="" type="checkbox"/>	22	100003042564055_1073741831	100003042564055_70725	100003042564055
23	<input checked="" type="checkbox"/>	23	100005241790123_1073741832	100005241790123_1073741826	100005241790123
24	<input checked="" type="checkbox"/>	24	100005241790123_1073741833	100005241790123_1073741826	100005241790123
25	<input checked="" type="checkbox"/>	25	100006274086300_1073741835	100006274086300_1073741827	100006274086300
26	<input checked="" type="checkbox"/>	26	100005241790123_1073741834	100005241790123_1073741826	100005241790123
27	<input checked="" type="checkbox"/>	27	100005241790123_1073741837	100005241790123_1073741826	100005241790123
28	<input checked="" type="checkbox"/>	28	100005241790123_1073741836	100005241790123_1073741826	100005241790123
29	<input checked="" type="checkbox"/>	29	100002477682997_1030577	100002477682997_58205	100002477682997

Which photo was added to Facebook by the user of the device?

- A. 106716779501997_1073741827
- B. 100003042564055_1073741835
- C. 100005241790123_1073741832
- D. 100006274086300_1073741835

ANSWER: D

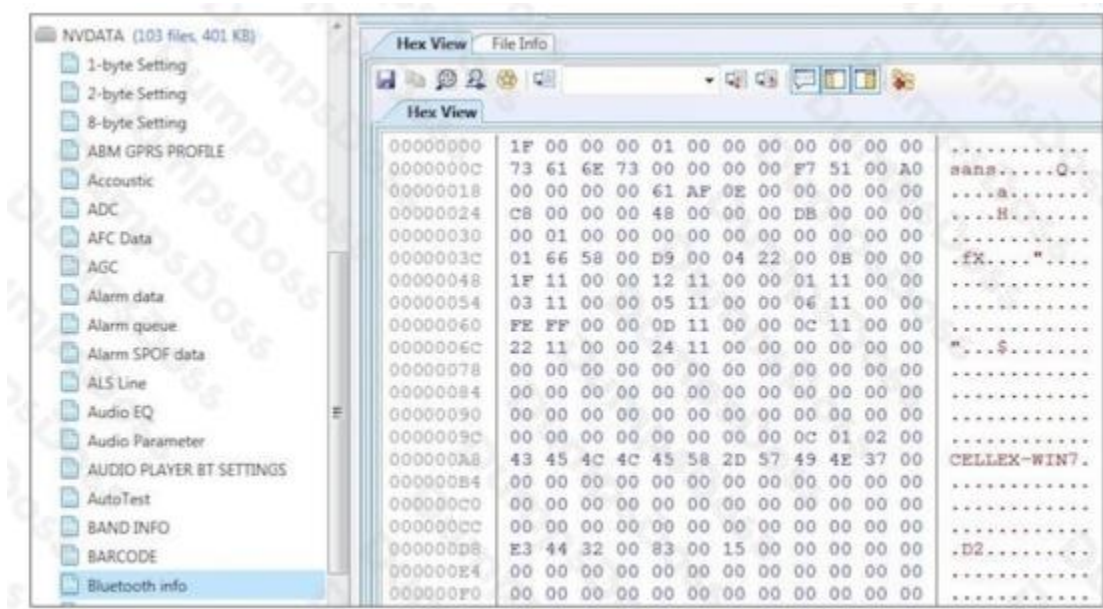
Explanation:

:

Examination of the first table shows user activity related to Cover photos. Mobile uploads and Profile pictures leading to the conclusion that user 100006274086300, is the owner of the device. In the second table, examine the picture's IDs resident in the database. Only one photo shares the Facebook ID that matches the ID of the assumed device owner.

QUESTION NO: 6

Examine the file, Bluetooth, what is the name of the device being examined?



- A. CON
- B. WIN7
- C. CON....M
- D. WIN10

ANSWER: B

Explanation:

:

QUESTION NO: 7

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: 8

What is often more of a challenge with mobile forensics than other areas of forensics?

- A. Analysis and Reporting of Information
- B. Isolation of devices
- C. Identification of evidence
- D. Evidence collection

ANSWER: D**Explanation:**

:

QUESTION NO: 9

What type of acquisition has occurred for this device?



- A. Physical
- B. File system
- C. Bypass lock
- D. Logical

ANSWER: B**Explanation:**

:

Reference: https://archive.org/stream/Defcon20Slides/DEFCON-20-Robinson-Spy-vs-Spy_djvu.txt

QUESTION NO: 10

Which artifact(s) can be extracted from a logical image only if the device the image was acquired from was jailbroken?

- A. SMS/MMS
- B. Email
- C. Call Logs
- D. Photos

ANSWER: B**Explanation:**

:

Photos, SMS/MMS and call logs can be extracted from a logical acquisition of a nonjailbroken device. Once a device has been jailbroken, email can be extracted for review.