On 8/13/19, on a report of a dead body, police responded to the Rock Springs area in Florida. At that location, police recovered the body of an apparent homicide victim. Included among items seized that day was a powered off Samsung S6 G920a phone. The police placed the phone in a faraday bag and submitted it for an examination.

Continuing on 8/13/19, an examiner charged the battery of the phone and completed a physical extraction of its contents.

You are to complete an analysis on the extracted data. You are to use all tools you deem appropriate. You have full search authority to find anything that, among other items of investigative interest, identifies the phone’s user, with whom the phone’s user was communicating, and any potential illegal activity with which the phone’s user was involved.

---

1. What is the hash value for the partition that contains user artifacts?

A. AEB075D6ED6A9FB005FEF8DB6B712E12D0131361F0583DE746494A19377FB102

B. 7B5EF155A6E07AD4D5C67FAA65F715552CDB4D5CDA2E8C45B8104E0F63A84EB4

C. 7A8797B97987D7987EE98787A798F97877632220D262514E97754FB986355DC79

D. 9ED5F6783B2F58ADAEC753CD08B1A01F421DC0727DABFE4250AE45E9F93D736D

E. Skip

2. What was set as the phone’s user name?

A. UserID1

B. Jdtest

C. Jd tester

D. Jd.cvult

E. Skip

3. What program was used to discuss a potentially illegal transaction?

A. Whatsap

B. Gmail
C. Burner
D. KiK
E. Skip

4. To what time zone is the phone set?
A. America/Chicago
B. America/Los Angeles
C. America/Goose_Bay
D. America/New_York
E. Skip

5. The file named 20190809_120201.jpg appears to be relevant to the case. In what city was this picture taken?
A. Orlando
B. Dallas
C. Miami
D. Tulsa
E. Skip

6. Regardless of how many were parsed by your tool(s), how many wifi access points did the phone log?
A. 8
B. 6
C. 2
D. 4
E. Skip

7. What file contains data to recover the phone's pattern password?
A. Gesture.key
B. PasswordKeeper_ATT.apk
C. com.google.android.gms.auth.confirm.CredentialsState
D. accounts.db
E. Skip

8. The TOR browser was installed on this phone. When (date and time) was it last used?
A. 8/9/2019, 2:55 PM
B. 8/12/2019, 6:55 PM

C. 8/12/2019, 10:55 PM
D. 8/9/2019, 6:55 PM
E. Skip

9. What phone number can be associated with this device?
A. (918)236-0870
B. (202)538-9455
C. (321)257-9720
D. (571)386-1265
E. Skip

10. What is likely the last name of the person with whom the phone's user was communicating regarding a potential trade of illegal goods?
A. Aarseth
B. Ohlin
C. Vincent
D. Eikemo
E. Skip

11. What was the phone's user researching?
A. Hitman for hire
B. Airfare
C. Credit card fraud
D. Drug and firearm prices
E. Skip

12. What email address is serves as the account for applications installed via the Play store?
A. olve.eikemo.777@gmail.com
B. jd.cvult@gmail.com
C. 12025389455@s.whatsapp.net
D. 19182360870@s.whatsapp.net
E. Skip

13. Did the user try to map directions to where he was supposed to meet someone?
A. Yes

B. No

14. What website was used with TOR to find a listing of deepweb markets?

A. www.therecoveryvillage.com
B. www.deepwebsiteslinks.com
C. www.silkroad.com
D. www.whoishostingthis.com
E. Skip

15. What is the VIN number of the vehicle that connected to the phone via Bluetooth?

A. 1B3EEGHKDK9393980
B. 1C4RAHAB7HC693271
C. 1BDJDW737DH282828
D. None of the above
E. Skip

16. What is the Bluetooth MAC address for the vehicle to which the phone was connected?

A. 00:54:AF:68:D4:F4
B. 00:25:DE:33:D4:A1
C. 9C:B6:D0:FD:8C:E0
D. None of the above
E. Skip

17. There were many search terms recovered, one of which was deleted. What application was used in regard to the deleted search term?

A. Chrome
B. TOR
C. Instagram
D. Play Store
E. Skip

18. The user of the device viewed assorted posts on Instagram. One of them has a picture that includes an envelope. What country is listed on the return address area of the envelope?

A. America

B. Norway
C. Sweden
D. Russia
E. Skip

19. What was a search term conducted within Instagram?
A. burzum
B. ar15
C. mayhemband
D. All of the above
E. Skip

20. What did the user of the phone ask for via gmail?
A. Location of meeting
B. WiFi password
C. Olve's whats app number
D. Extension on loan
E. Skip

21. The user placed a couple items in a shopping cart. What are they?
A. Records
B. Firearms
C. Drugs
D. All of the above
E. Skip

22. Using the time zone settings for the location where the phone was recovered, when were searches for Orlando Springs Park (date and time) recorded by the phone?
A. 8/10/2019 12:35 PM
B. 8/12/2019 5:30 PM
C. 8/10/2019 4:35 PM
D. Both A and B
E. Skip

23. Did the phone's user download anything from Google docs?
A. Yes

B. No
C. Skip

24. Given your knowledge of best practices, were there any potential issues with the device extraction you discovered during your analysis?

A. Yes
B. No
C. Skip