TRUXTON

Findings

This report was generated on Wednesday, February 8, 2017 3:00:21 PM for the Sugar LLC investigation opened Wednesday, February 8, 2017 2:55:21 PM.

Summary

These are the items found to be interesting during the investigation of the seized media.

Items Found

1. SSID "SUGARCORP" [definition 2, source 2]
2. A Facebook Message event that occurred on 2015-02-25T20:18:12. I got it. Meet me downstairs. [source 3].
3. A Facebook Message event that occurred on 2015-02-20T13:13:13. We really need to get together for drinks [source 3].
4. A Facebook Message event that occurred on 2015-02-20T13:16:59. You will not be disappointed! [source 3].
5. A Program Executed event that occurred on 2015-02-27T16:57:11. DELETEANY_TRACKS.EXE executed for the third time. [source 4].
6. A Program Executed event that occurred on 2015-02-27T04:33:44. DELETEANY_TRACKS.EXE executed for the second time. [source 4].
7. A Program Executed event that occurred on 2015-02-26T22:44:55. DELETEANY_TRACKS.EXE executed for the first time. [source 4].
8. A Microsoft Excel 2007 spreadsheet file named "118-16 Evaluation Matrix Final Rankings- BAFO.xlsx" MD5: 57422570EB1F7495F1E2CF2E8672600A from media "Bob's Laptop" [source 1].
9. A Microsoft Word 2007 document file named "BAFO-Request-Form.docx" MD5: 7310042C7B8719B2D3D7920095B41FCC from media "Bob's Laptop" [source 1].
10. A Windows 8 Prefetch file named "DELETEANY_TRACKS.EXE-81BEDE19.pf" MD5: 0FFC6E9AFD0084DB10875BFD10BA7F7B from media "Bob's Laptop" [source 1].
11. A Windows Shortcut file named "SugarLLC BAFO.lnk" MD5: 8F0B0C648D251544D983DBAAA30E0E40 from media "Bob's Laptop" [source 1].
12. A hash value of 7310042C7B8719B2D3D7920095B41FCC.
13. Location: Latitude 38.963233855205 Longitude -77.397849510551 [source 3].
14. Location: Latitude 38.963233855205 Longitude -77.397849510551 [source 3].
15. Location: Latitude 38.963233855205 Longitude -77.397849510551 [source 3].
16. Location: Latitude 38.969789855205 Longitude -77.386595510551 [source 3].
17. A SMS message dated 2015-02-24T17:40:43 subject "Just put it on a td" [source 6].
18. A SMS message dated 2015-02-24T17:42:59 subject "I'll park next door then walk it over." [source 6].
19. A Facebook message dated 2015-02-25T20:18:12 subject "I got it. Meet me downstairs." [source 3].
20. A Facebook message dated 2015-02-20T13:15:59 subject "Really?" [source 3].
21. A Facebook message dated 2015-02-20T13:18:12 subject "See you at 5" [source 3].
22. A Facebook message dated 2015-02-20T13:13:13 subject "We really need to get together for drinks" [source 3].
23. A Facebook message dated 2015-02-20T13:16:59 subject "You will not be disappointed!" [source 3].
24. A Facebook message dated 2015-02-25T20:18:12 subject "On my way" [source 3].

Sources

Sources are where items come from. The following is a list of places where the above items were found.

1. Media: Bob's Laptop - Directory "Seized Media\Laptop", 49 files, 945,052,953 bytes (901.27MB).
2. A WPA Supplicant Configuration file from media "Bob's Laptop" [1] named "wpa_supplicant.conf" MD5: 817FC8807003BFF4C022D06A81244ADA starting 368 bytes from the beginning of the file.
3. A Facebook Orca Database file from media "Bob's Laptop" [1] named "orca2.db" MD5: 4724B517408A22CD9F62AA2759DD0A89, the offset from the beginning of the file is not known.
4. A Windows 8 Prefetch file from media "Bob's Laptop" [1] named "DELETEANY_TRACKS.EXE-81BEDE19.pf" MD5: 0FFC6E9AFD0084DB10875BFD10BA7F7B, the offset from the beginning of the file is not known.
5. Media: Bob's Phone - Directory "Seized Media\Phone", 3 files, 33,635 bytes (32.85KB).
6. A Cellebrite 2.0 Report file from media "Bob's Phone" [5] named "Cellebrite 2.0 report.xml" MD5: 460CE6C0E6A7402426086CA235625B21, the offset from the beginning of the file is not known.

Definitions

1. MD5

An MD5 hash is a fingerprint for a file's contents. Every byte in the file is run through a mathematical formula that computes a very large number representing those unique contents. Slight differences in the value or order of the bytes in the file will result is a vastly different hash value. For example, the three letters in "Sam" results in an MD5 hash value of BA0E0CDE1BF72C28D435C89A66AFC61A. "Sma" hashes to 5688E3BDCB34C6325D69261854B14210 and "sam" (lower case s) hashes to 332532DCFAA1CBF61E2A266BD723612C. The hash of nothing, zero bytes, is D41D8CD98F00B204E9800998ECF8427E.

2. SSID

A Service Set Identifier (SSID) is a name given to a WiFi access point. This is also known as a 'network name' and usually created by the owner of the access point.

Files Referenced

1. Bob's Laptop

Directory "Seized Media\Laptop", 49 files, 945,052,953 bytes (901.27MB)

1. Name wpa_supplicant.conf
   Directory Load.Root\Media\Folder\WiFi\Android\Backup
   MD5 817FC8807003BFF4C022D06A81244ADA
   Created 2017-01-22T15:31:55

2. Name orca2.db
   Directory Load.Root\Media\Folder\Facebook
   MD5 4724B517408A22CD9F62AA2759DD0A89
   Created 2017-01-22T15:30:39

3. Name DELETEANY_TRACKS.EXE-81BEDE19.pf
   Directory Load.Root\Media\Folder\Prefetch\8
   MD5 0FFC6E9AFD0084DB10875BFD10BA7F7B
   Created 2017-01-22T15:30:43

4. Name 118-16 Evaluation Matrix Final Rankings- BAFO.xlsx
   Directory Load.Root\Media\Folder\Documents
   MD5 57422570EB1F7495F1E2CF2E8672600A
   Created 2017-01-22T15:30:39

5. Name BAFO-Request-Form.docx
   Directory Load.Root\Media\Folder\Documents
   MD5 7310042C7B8719B2D3D7920095B41FCC
   Created 2017-01-22T15:30:39

6. Name SugarLLC BAFO.lnk
   Directory Load.Root\Media\Folder\USB
   MD5 8F0B0C648D251544D983DBAAA30E0E40
   Created 2017-01-22T15:30:49

2. Bob's Phone

Directory "Seized Media\Phone", 3 files, 33,635 bytes (32.85KB)

Name Cellebrite 2.0 report.xml
Directory Load.Root\Media\Folder
MD5 460CE6C0E6A7402426086CA235625B21
Created 2017-01-22T15:31:55