Evidence Collection Worksheet

**Group Members: Ben Halpern, Ehab Moustafa, Barzeen Soroudi, Joe Lam, Elija**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Artifact #** | **Timestamp** | **Information** | **Summary** | **Evidence Location** |
| 1 | July 6 2012 | Stamp Insurance PDF | An insurance policy on the stamps at the National Gallery | INBOX.MBOX/Attachments/61/3/docs  Tracys emails |
| 2 | July 06 2012 | A list of supplies “needed to” to break into the national gallery.  Referred to in an email between [patsumtwelve@gmail.com](mailto:patsumtwelve@gmail.com), [coralbluetwo@hotmail.com](mailto:coralbluetwo@hotmail.com),  [Throne1966@hotmail.com](mailto:Throne1966@hotmail.com)  ( see needs.txt ) | List of items they “need to break into the National Gallery” | INBOX.mbox/Attachments/needs.txt |
| 3 | July 10 2012 | In the email file, there is a conversation between Tracy and Pat, where Pat “found the right guy for us to do the job”. Tracy in this same email thread corresponds the list of things to need. | Incriminating email conversation, showing Pat and Tracy blackmailing King | INBOX.mbox/Messages/9F0508B8-04FB-490E-A7-3E23B0E7C59B.emlx |
| 4 | 1341689795 epoch time | A potential fishing link disguised as a target raffle drawing  “ enter ‘702’ in target.com.trdz.biz” | A fishing link disguised as a target raffle drawing | Vol\_vol5/mobile/Library/SMS/Sms.db |
| 5 |  | <https://plus.google.com/app/plus/oob/mp/571/?login=1>  <https://plus.google.com/app/plus/mp/571/#~loop:view=activity&aid=z13sefxiuunsefxry04cjlhqczrgfh4b51k>  <https://plus.google.com/app/plus/mp/571/?login=1>  <https://plus.google.com/app/plus/oob/mp/571/?login=1>  <https://accounts.google.com/ServiceLoginAuth>  <https://plus.google.com/app/plus/mp/571/?login=1>  <http://www.google.com/search?q=gorgonzola&ie=UTF-8&oe=UTF-8&hl=en&client=safari_> | Tracy browsing history hex dump  Doesn’t result much about the heist, her browsing history contains communication links between another person( however it requires a log in )  The rest of her browsing history consists of recipes and news articles. | Vol\_vol5/mobile/Library/safari/History.plist |
| 6 | 2012 07 10 | Her last 2 searches were a cvs in the area:  “ 152 North Quaker Lane  Alexandira, VA 22302” – cvs pharmacy near the location of the National Gallery | Shows her ma search history | Vol\_vol5/mobile/Library/maps/History.plist |
| 7 | 2012 06 14 | In the DCIM folder contains photos of stamps, as well as photos of the front sign of the National Gallery. There are timestamps on all of these photos, | DCIM images of the photos on Tracys phone. In them it contains images of stamps ( possibly the stamps that Tracy intends to steal ) | Vol\_vol5/mobile/media/DCIM/ |
| 8 | 2012 06 06 | The following files shows Tracy’s gps WiFi location history along with timestamps of each longitude and longitude.  Along with the timestamps and each of the locations, the mac address is also listed upon the database. The mac addresses can be resolved dictating which service she connected to. | Whenever she connected to the WiFi it was recorded along with the time and location of the connection | Vol\_vol5/root/Caches/locationd/consolidated.db |
| 9 | 2012 06 06 | A generated KML file contains the GPS location of the photos taken on Tracy’s phone. They map her around the city and in other countries. Using those locations it is able to map out her path, and where she was when those photos were taken. | WiFi connection history  KML file | Reports/Tracy\_ihone…/ReportKML.kml …/…/…/ style.kml |
| 10 | 2012 07 06 | This Database contains data listing the numbers called and who Tracy corresponded with. Through this data as well as the sms.db file from earlier, it is possible to identify different users as Tracy’s daughter, Pat, and another person of interest. | Call history log | Vol\_vol5/wireless/Library/CallHistory/call\_history.db |
| 11 | 2012 07 12 | In this sqlite database, it contains the contacts of Terry, Carry, and Pat, all associated and or Tracy’s family. Through these contacts it is possible to confirm a name resolution of the numbers called and collaborating with Tracy. |  | Vol\_vol5/mobile/library/AddressBook |
|  |  |  |  |  |
| Tools |  |  |  |  |
| 1 | 2019 06 07 | Kali Linux | Operating System |  |
| 2 | 2019 06 07 | Autopsy | Forensics tool |  |
| 3 | 2019 06 07 | Google Maps | A GPS Mapper |  |
| 4 | 2019 06 07 | LeafPad | Text Editor |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |