Evidence Collection Worksheet

Sharon Rivas

Artifact #
Timestamp
Information
Summary
Evidence Location

Artifact #	Timestamp	Information	Summary	Evidence location
1	7-12-2012	Md5 hash	2197711773d92f305bc52449a79723e4	/img_tracy-phone-2012-07-15-final.EO1
2	07-15-2012	Device model	iPhone1.2	vol/5/mobile/Library/Logs/AppleSupport/general.log
3	07-15-2012	Device serial number	86004482Y7H	vol/5/mobile/Library/Logs/AppleSupport/general.log
4	07-15-2012	OS version number	4.2.1	vol/5/mobile/Library/Logs/AppleSupport/general.log
5	07-15-2012	Installation time stamp	7-12-2012 16:50:27	vol/5/mobile/Library/Logs/AppleSupport/general.log
6	07-15-2012	Integrated circuit card ID number	89014103255195342366	vol/logs/lockdown.log.1
7	07-15-2012	Tracy's phone number	703-340-9661	vol5/logs/lockdown.log.1
8	07-15-2012	Tracy's email addresses	tracy.sumtwelve@nationalgallerydc.org, tracysumtwelve@gmail.com, coralbluetwo@gmail.com	vol/5/mobile/Library/Mail
9	7-12-2012	Things to break in with or wear	Incriminating message	In attachments under needs.txt

10	**7-6-2012**	**Planning heist with coralbluetwo@hotmail.com and throne1966@hotmail.com**	**Discussed plan to heist and blackmail**	**9F5050 messages**
11	**7-6-2012**	**Text to 571-308-3236 her brother Pat says hey sis he is talking about needs.txt changing it to a pdf to read**	**Related to needs.txt being tricky**	**Sms database #23**
12	**7-6-2012**	**Text to 202-725-2124 possibly Carry or Alex**	**Says how's the flashmob going**	**Sms database #32**
13	**7-6-2012**	**Terry her daughter the phone number is 703-829-6071**	**She talks about "I would rather live with dad than not go to the same school" Prufock)**	**Sms database #13**
14	**7-6-2012**	**Message from 206-910-0932 could be possibly relevant**	**The extension is odd could be from Alex it's trdt.biz**	**Sms database #22**
15	**7-08-2012**	**Photo of the stamps**	**IMG_0049**	**vol_vol5/mobile/media/DCIM/100APPLE**
16	**7-08-2012**	**Photo of a foreign stamp**	**IMG_0050**	**vol_vol5/mobile/media/DCIM/100APPLE**
17	**7-08-2012**	**Photo of a kazakstan stamp**	**IMG_0051**	**vol_vol5/mobile/media/DCIM/100APPLE**
18	**7-08-2012**	**Photo of douglas macarthur stamps**	**IMG_0054**	**vol_vol5/mobile/media/DCIM/100APPLE**
19	**7-08-2012**	**Photo of a kazakstan stamp**	**IMG_0055**	**vol_vol5/mobile/media/DCIM/100APPLE**
20	**7-08-2012**	**Photo of an armed forces stamp**	**IMG_0056**	**vol_vol5/mobile/media/DCIM/100APPLE**

		Photo of brady & co stamp	**IMG_0057**	**vol_vol5/mobile/media/DCIM/100APPLE**
21	**7-08-2012**	**Photo of foreign stamps**	**IMG_0058**	**vol_vol5/mobile/media/DCIM/100APPLE**
22	**7-08-2012**	**Photo of foreign stamps more zoomed in**	**IMG_0059**	**vol_vol5/mobile/media/DCIM/100APPLE**
23	**7-08-2012**	**Same photo as #22 but blurry as if taken in a rush**	**IMG_0060**	**vol_vol5/mobile/media/DCIM/100APPLE**
24	**7-08-2012**	**Same as photo #23 but a different angle**	**IMG_0061**	**vol_vol5/mobile/media/DCIM/100APPLE**
25	**7-08-2012**	**Photo of foreign stamps**	**IMG_0062**	**vol_vol5/mobile/media/DCIM/100APPLE**
26	**7-08-2012**	**Photo of foreign stamps more zoomed in**	**IMG_0063**	**vol_vol5/mobile/media/DCIM/100APPLE**
27	**7-08-2012**	**Photo of a foreign stamp sederland**	**IMG_0065**	**vol_vol5/mobile/media/DCIM/100APPLE**
28	**7-08-2012**	**Photo of a foreign stamp close up**	**IMG_0066**	**vol_vol5/mobile/media/DCIM/100APPLE**
29	**7-08-2012**	**Photo of a different foreign stamp close up**	**IMG_0066**	**vol_vol5/mobile/media/DCIM/100APPLE**
30	**7-08-2012**	**Photo of another foreign stamp close up**	**IMG_0067**	**vol_vol5/mobile/media/DCIM/100APPLE**
31	**7-08-2012**	**Blurry photo of a foreign stamp**	**IMG_0068**	**vol_vol5/mobile/media/DCIM/100APPLE**
32	**7-08-2012**	**Blurry photo of foreign stamps**	**IMG_0069**	**vol_vol5/mobile/media/DCIM/100APPLE**

33	**7-12-2012**	**Call log-** **1. 650-870-0260** **2. 703-829-6191** **3. 1571-308-3236** **4. 571-245-8517** **5. 571-308-3236**	**Tracy's call log**	**vol_vol5/wireless/Library/CallHistory/call_history.db**
34	**7-12-2012**	**WiFi location**	**3.6130688, 38.880558** **Borena, Ethiopia**	**vol_vol5/root/Library/Caches/locationd/consolidated.db**
35	**7-12-2012**	**carrysum2012@yahoo.com**	**Address book- Carry**	**vol_vol5/root/Library/AddressBook/AddressBook.sqlitedb**
36	**7-12-2012**	**patsumtwelve@gmail.com**	**Address book- Pat**	**vol_vol5/root/Library/AddressBook/AddressBook.sqlitedb**
37	**7-12-2012**	**Awen.Throsam@m57biz**	**Address book- Unnamed contact**	**vol_vol5/root/Library/AddressBook/AddressBook.sqlitedb**

Equipment/Tools used: Nano, Autopsy, Kali Linux