Table of Contents

Belle, the Cockapoo has been kidnapped!

Belle is a black Cockapoo; she was last seen wearing a pink collar with a green tag. The tag contains her owner Mary Smith's information.

- (1/28/2018 ~3:15 pm)
- Victim – Mary Smith

1. Lead System Administrator at Dominion Energy
2. smithmaryj1996@gmail.com
3. 410-849-9508

- Initial Information

1. Ransom demand note came as a text from 703-261-9220

Lab Objectives:

1. Analyze the extracted cell phone image to identify the subject and owner of the Samsung phone dropped by the kidnapper during the ransom drop.

2. Determine the search location to find Belle, the kidnapped dog, based on the analysis of the phone's data.

3. Identify potential phone numbers, including Google Voice numbers, from the phone's contacts and call logs to aid in the investigation.

4. Gather information about the phone's email addresses, communication contacts, and chat applications to trace any possible leads or accomplices involved in the kidnapping.

5. Investigate the phone's call history to find numbers dialed and cross-reference them with the contacts to identify any possible associates or contacts of the suspect.

6. Utilize internet search tools, including Google, to gather additional information such as addresses and location data that might assist in locating Belle and uncovering the suspect intention

The lab participants will work in teams, focusing on specific questions related to the case, and will receive updates and new questions throughout the session. They are encouraged to use the search function within the forensic software and utilize external resources, such as Google, to overcome challenges and progress in the investigation.

Agent Briefing:

Agent,

January 28, 2018, 3:15 pm, operation "Rescue Belle" initiated. Belle, codename for Mary Smith's beloved dog, kidnapped. Suspects threatening to disrupt power grid near major hospital. Terrorism implications. Urgent action required.

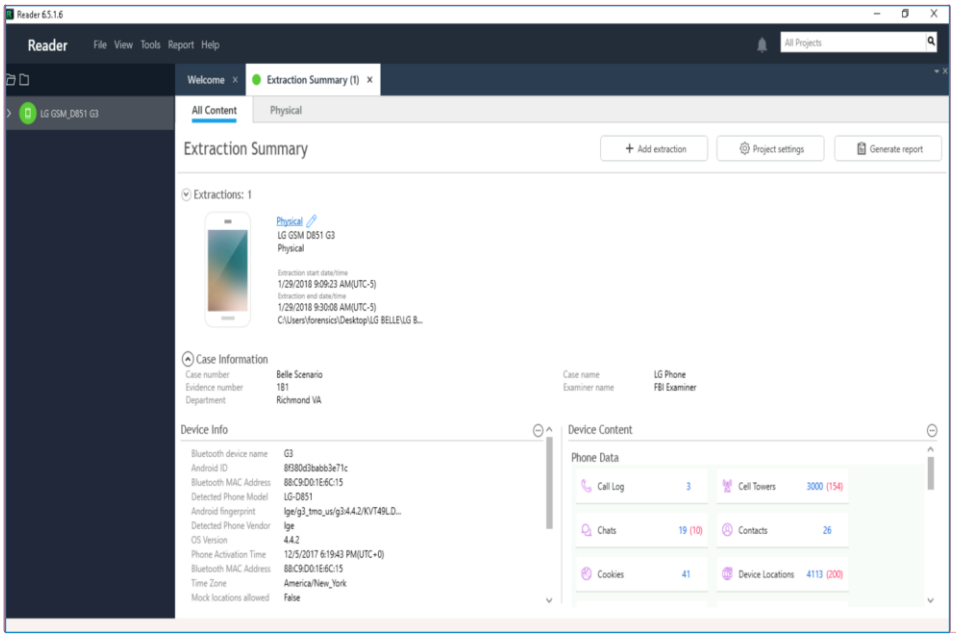
Undercover FBI Agents Susan Wright and Linsey Stem activated Digital Evidence Team. Phone extraction successful. Analyze Samsung phone for subject identification, owner, and Belle's search location.

Proceed with extreme caution. Belle's life at stake. Await further instructions. Time is of the essence.

Instructions:

After opening your Virtual Machine, please allow some time for the Cellebrite software to automatically launch. Be patient during this process. Once the software is running, make sure to close any pop-up windows that prompt you with inquiries. If you encounter a pop-up asking to change the computer's time zone, select the "No" option to keep the current time zone intact. By following these steps, you can ensure a smooth and efficient start to your Cellebrite data extraction and analysis process.

You have done everything right once you see this screen below



Be sure that you have expanded the lists but clicking the arrow to the left of "LG GSM_D851 G3

Commented [CJ1]: Be sure that you have expanded the lists but clicking the arrow to the left of "LG GSM_D851 G3

Contact Analysis:

- Access the Contacts on the device and review them thoroughly.
- Look for potential phone numbers associated with the subject.
- Specifically, check for any Google Voice Phone Numbers in the contacts.
- If you find a Google Voice Phone Number, note down the actual phone number.
- Conduct a deeper analysis of the device to gather more information related to this number, such as call logs, messages, and any associated applications.

Home Information:

1. Review the contacts on the device:

   - Look for potential phone numbers associated with the subject.

2. Identify work and home information:

   - Check the contacts, notes, or any relevant applications for details about the person's workplace and residence.

Email Analysis:

1. Email Address and Communication Analysis:

- Access the phone's Email application or database.

- Identify all email addresses used on the phone.

- Determine the communication contacts associated with each email address.

Ransom Note:

2. Verification of Ransom Demand Note Number:

- Check the phone's call logs or messages.

- Confirm if the number "703-261-9220" is present on the phone.

- Identify any information related to this number, such as the associated contact

Device Presence:

3. Search for Mary Smith's Name and Phone Number:

- Utilize the search function in the phone's applications or database.

- Look for "Mary Smith" or the phone number "410-849-9508" on the device.

- Record any findings associated with this name or number.

Info Retrieval:

4. Retrieve Information about the Phone's Phone Number:

- Check the phone's settings or SIM card information.

- Search contacts, messages, or emails that may contain the phone number.

- Note any information available about the phone's phone number.

Facebook chats:

5. Investigate Interesting Facebook Chats via Messenger:

- Open the Facebook Messenger application data on the phone.
- Look for conversations that may lead to finding "Belle" or related information.
- Record any relevant details from the chat messages.

SMS Text Messages:

6. Explore Interesting SMS Text Messages and Chat Applications:

   - Review SMS messages on the phone for intriguing conversations.

   - Identify the people involved in the conversations and their phone numbers.

Chat Application:

- Determine chat applications present on the phone and the associated usernames/accounts.

- Attempt to find passwords for these chat applications.

Identity of “LoveCockapoo”:

7. Discover More Information about "lovecockapoo":

- Investigate the phone's data to find references to "lovecockapoo."

- Check for social media profiles or other accounts linked to this name.

- Gather any additional relevant information related to "lovecockapoo."

Call Logs:

8. Check Phone Call History:

- Access the call logs on the phone.

- Identify the phone numbers dialed or received by the device.

- Cross-reference these phone numbers with the phone's contacts.

- Use a search engine to find the owner of any unidentified phone numbers.

Address and Locations:

9. Verify Address Associated with the Owner:

- Search for the owner's address using the phone's data.
- Use a search engine to Google the address for further information.
- Identify the location and any relevant details about the address.

Proceed with caution and adhere to legal and ethical guidelines while performing the investigation. Record all findings for later analysis and potential follow-up actions.

Question set 2:

Dog Park Info:

1. Check for pictures with location data for Short Pump Dog Park.

2. If found, note the date and time the pictures were taken.

Drop site analysis:

1. Look for pictures with location data for Deep Run Park.

2. Identify any pictures taken in a different area of the park than the drop site.

Navigation data:

1. Search for navigation apps with data for Deep Run Park or Short Pump Park.

2. Note the date and time of any navigation data found.

3. Check for pictures or navigation apps showing Kroger with location data.

Location Data Investigation:

1. Locate file 20171215_120600.jpg.

2. Identify the position location (coordinates) associated with the file.

Collars and Locations:

1. Find the location (Map position) for the dog collars and leashes.

2. Use the lat long converter to obtain the coordinates.

3. Record the location shown on the map.

Note: For each question, make sure to document any relevant findings and ensure the accuracy of the data extracted. Pay attention to timestamps and location details to aid in the investigation.