

Case Identifier: US-RU-2023-444

Case Investigator: Dr. Katherine Chang, Forensic Analyst

Identity of the Submitter: Dr. Katherine Chang, Forensic Analyst

Date of Receipt: 04/24/24

---

## Items for Examination:

- Cellular Device
    - Make: Samsung
    - Model: Galaxy S4 64GB (Black)
    - Serial Number: S2346FW091538361
  - Personal Laptop Computer
    - Make: Hewlett-Packard (HP)
    - Model: Pavilion x360
    - Serial Number: HPLC457834SD938
- 

## Findings and Report (Forensic Analysis):

- Cellular Device:
  - On today's date, I retrieved a search warrant through the US District Courts in Washington D.C.
  - Acquire tools for examination of mobile device:
    - SIM card reader
    - Oxygen Forensics Detective (Digital Mobile Forensic Software)
  - Once the tools were acquired and the search warrant was retrieved, the examination began.
    - Because the device was still on and locked, the first step I took to examine the phone was bypassing the screen lock using the forensic software and then isolating it from the current network and disabling the screen lock to remove any passwords that are placed on the phone.
    - Using the SIM card reader, I conducted a thorough examination and successfully retrieved the missing telephone numbers along with a handful of text messages. This data provided some additional insight into the communication patterns of the individual in question, upon careful analysis, the messages that were extracted do seem to have a suspicious lingo underlining the conversation.
    - Each phone number and text message extracted from the cellular device, I meticulously documented the details, including the phone number itself and the accompanying text message content. This comprehensive approach ensured that each piece of communication was thoroughly recorded and analyzed for any potential relevance to the investigation. By meticulously cataloging these details, I aimed to provide a comprehensive overview of the individual's communication history and interactions, thereby facilitating a deeper understanding of their activities and associations.

Case Identifier: US-RU-2023-444

Case Investigator: Dr. Katherine Chang, Forensic Analyst

Identity of the Submitter: Dr. Katherine Chang, Forensic Analyst

Date of Receipt: 04/24/24

- I took action by using the Oxygen Forensics to delve into the digital footprint of the cellular device. With this tool, I conducted a systematic examination, carefully scrutinizing the device's storage, applications, and network connections. Through the software's capabilities, I extracted crucial data, including call logs, text messages, internet browsing history, and application usage patterns. Utilizing Oxygen Forensics Detective was pivotal in uncovering valuable insights into the individual's activities and communications, aiding in the identification of pertinent evidence for the ongoing investigation.
- Documented Message:
  - Phone Number: +7 (922) 555-1543
  - Contact Name: Red Ralph
  - Message: Hey Red Ralph, Just wanted to remind you to keep our conversation about the deal strictly confidential. We can't afford any leaks or slips. Remember, discretion is key. Looking forward to our next meeting to discuss further details. Regards, Senator.
- Personal Computer:
  - On today's date, I began the forensic acquisition/imaging process of the personal computer attributed to the individual under investigation. Employing industry-standard procedures and utilizing specialized forensic imaging software, I systematically captured a bit-by-bit copy of the computer's storage media, ensuring the preservation of all digital evidence in a forensically sound manner. This meticulous approach aimed to capture not only the visible files and folders but also any hidden or deleted data that could potentially hold significance to the investigation. Throughout the acquisition process, strict adherence to chain of custody protocols was maintained to guarantee the integrity and admissibility of the obtained evidence in any legal proceedings.
    - Additionally, I documented the computer's hardware and software configurations, noting any peculiarities or deviations from standard settings. This information provides context for understanding the environment in which the digital evidence was generated and can be crucial for interpreting the findings accurately. By meticulously documenting these details, I aim to provide a comprehensive overview of the computer's setup, facilitating a deeper understanding of its usage patterns and potential relevance to the investigation.
  - After connecting the original media in the laptop to the hardware write-blocker via USB 3.0 to my examination machine, I began the imaging process.
    - Verified the integrity of the original media by calculating and comparing its hash value before proceeding with imaging.
    - Initiated the imaging process using forensic imaging software to create a forensic copy of the entire storage media, including all partitions and unallocated space.
    - Verified the integrity of the forensic image by calculating its hash value and comparing it to the original media's hash value to ensure a bit-for-bit copy.

Case Identifier: US-RU-2023-444

Case Investigator: Dr. Katherine Chang, Forensic Analyst

Identity of the Submitter: Dr. Katherine Chang, Forensic Analyst

Date of Receipt: 04/24/24

- Once the imaging had been completed and was then documented, I used Internet Evidence Finder (IEF) software to conduct a thorough examination of the laptop's internet-related activities. This specialized forensic tool allowed me to systematically analyze internet artifacts such as browsing history, downloads, cookies, and cache files. By scrutinizing these digital footprints, I aimed to uncover any online activities or communications that could be pertinent to the investigation. Through the meticulous examination facilitated by IEF, I sought to identify any potential connections to suspicious websites, communication platforms, or individuals of interest. This proactive approach was essential in ensuring that no digital evidence relevant to the case was overlooked, ultimately contributing to a comprehensive forensic analysis of the laptop's digital environment.

```
*****Original Message*****
To: Senator Smith
From: Red Ralph
Date: June 15, 2023 01:22 (- 05:00 EST)

Notify me when you are prepared to discuss plan Bubble Gum.

-----

*****Original Message*****
To: Senator Smith
From: Red Ralph
Date: June 17, 2023 11:43 (- 05:00 EST)

Pleasure meeting with you. Funds should be dispersed at 3:00 on Monday.

-----

*****Original Message*****
To: Senator Smith
From: Red Ralph
Date: June 19, 2023 13:25 (- 05:00 EST)

I appreciate your efforts during this time. I would like to meet with you. Meet at
the blind woman's statue on the second day of Cancer season midday. Everything will
be taken cared of a quarter til the previous hour.]
```

- Once the email was analyzed and documented, I was also able to view previously deleted files from the laptop's storage. Through the utilization of specialized data recovery software and forensic methodologies, I meticulously scanned the allocated and unallocated sectors of the storage media to identify any remnants of deleted files. By reconstructing these fragments, I was able to retrieve a wealth of valuable digital evidence that had been previously hidden or erased from the surface. This comprehensive approach to file recovery enabled me to uncover potential insights into the individual's activities, communications, and interactions, thus further augmenting the depth and scope of the forensic analysis conducted on the laptop.

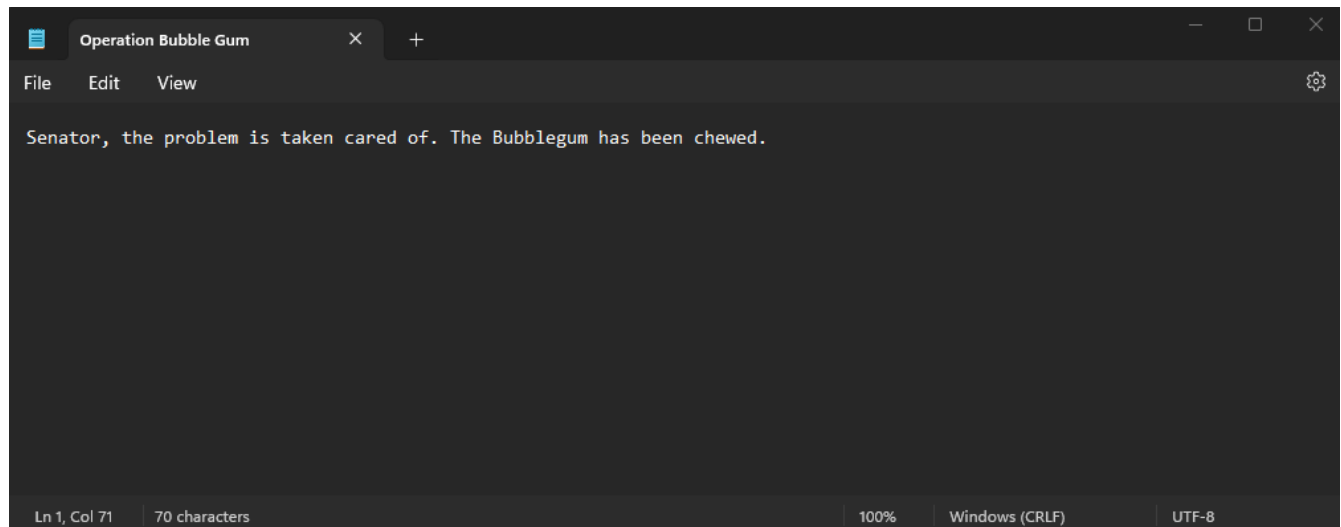
Case Identifier: US-RU-2023-444

Case Investigator: Dr. Katherine Chang, Forensic Analyst

Identity of the Submitter: Dr. Katherine Chang, Forensic Analyst

Date of Receipt: 04/24/24

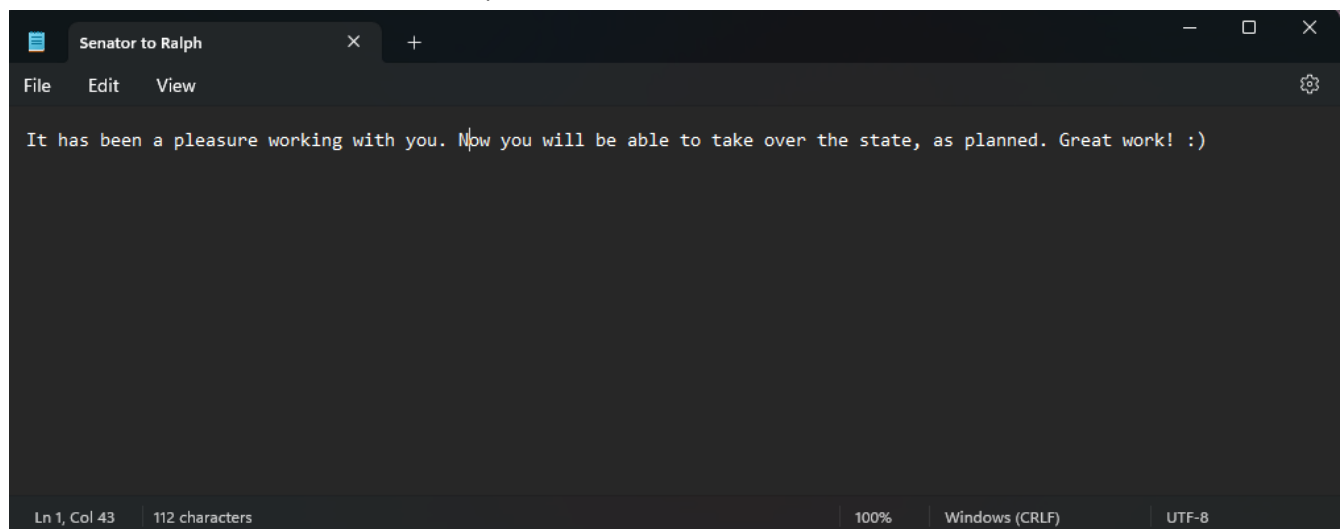
- File named "Operation Bubblegum"



A screenshot of a text editor window with a dark theme. The title bar shows the file name "Operation Bubble Gum" and standard window controls. The menu bar includes "File", "Edit", and "View". The text area contains a single line of text: "Senator, the problem is taken cared of. The Bubblegum has been chewed." The status bar at the bottom indicates "Ln 1, Col 71", "70 characters", "100%", "Windows (CRLF)", and "UTF-8".

```
Senator, the problem is taken cared of. The Bubblegum has been chewed.
```

- File named "Senator to Ralph"



A screenshot of a text editor window with a dark theme. The title bar shows the file name "Senator to Ralph" and standard window controls. The menu bar includes "File", "Edit", and "View". The text area contains a single line of text: "It has been a pleasure working with you. Npw you will be able to take over the state, as planned. Great work! :)" where "Npw" is a typo for "Now". The status bar at the bottom indicates "Ln 1, Col 43", "112 characters", "100%", "Windows (CRLF)", and "UTF-8".

```
It has been a pleasure working with you. Npw you will be able to take over the state, as planned. Great work! :)
```

Case Identifier: US-RU-2023-444

Case Investigator: Dr. Katherine Chang, Forensic Analyst

Identity of the Submitter: Dr. Katherine Chang, Forensic Analyst

Date of Receipt: 04/24/24

## Conclusion:

- In conclusion to the report, no original media was damaged, manipulated, or changed in anyway. Refer to the emails and text messages collected in its original state during the investigation. The integrity of the original data, including digital files, documents, and communication logs, remains intact and unaltered throughout the forensic examination process. This assurance is supported by the screenshots taken during the investigation, serving as visual documentation of the condition of the suspect's devices. All forensic procedures were meticulously executed to ensure the preservation of the original media's integrity, and no evidence suggests any tampering or manipulation of the data. Thus, the findings and conclusions drawn from the forensic analysis can be confidently based on the unaltered state of the original media.
- Hardware that was used to recover files:
  - SIM Card Reader: Utilized for extracting missing telephone numbers and text messages from the suspect's cellular device, providing insight into communication activities.
  - Write-Blocker: Employed to prevent any alteration or modification of the original data during the imaging process of the suspect's personal computer, ensuring the integrity of the recovered files.
  - USB 3.0 Connection: Facilitated the secure connection of the suspect's laptop to the examination machine, enabling the forensic imaging process to be conducted without compromising the integrity of the original media.
- Software that was used to recover files:
  - Oxygen Forensics Detective: Employed for digital mobile forensic analysis, allowing comprehensive examination of the suspect's cellular device to recover relevant data such as text messages, call logs, and other communication activities.
  - ProDiscover: Utilized for media imaging and file recovery from the suspect's personal computer, enabling the retrieval of deleted files and examination of email communications and other digital artifacts relevant to the case.
  - Internet Evidence Finder (IEF): Deployed to recover internet browsing history and other online activities from the suspect's devices, providing insights into web-based communications and interactions.

Evidence includes:

Case Identifier: US-RU-2023-444

Case Investigator: Dr. Katherine Chang, Forensic Analyst

Identity of the Submitter: Dr. Katherine Chang, Forensic Analyst

Date of Receipt: 04/24/24

- A text message between the suspect and a user named Red Ralph regarding a conversation that be kept "confidential".
- An email conversation between a user named Red Ralph regarding meetings and payment for "coordinated plans," suggestive of undisclosed transactions or arrangements.
- Deleted zip files containing classified material uploaded to a file-sharing site, raising concerns about unauthorized disclosure of sensitive information.
- Recovery of deleted text messages and call logs from the suspect's cellular device, shedding light on their communication activities and potential contacts.