Case Identifier: 01-06-2022-1000-1000-1337
Case Investigator: Chris Evans CYSE 407
Identity of Submitter: District Attorneys Office for the U.S. District Court of Washington D.C.
Date of Receipt: June 5th, 2022 , 10:30 PM

ITEMS FOR EXAMINATION:

- Cellular Telephone device
  - Samsung Galaxy S22 Smartphone
  - Model Number: SM S901B
  - Carrier: Verizon Wireless Network
- Personal Laptop Computer
  - Lenovo IdeaPad Flex 5
  - Samsung 980 M.2 2280 1TB NVME Solid State Drive
  - 16 GB of DDR4 Memory card

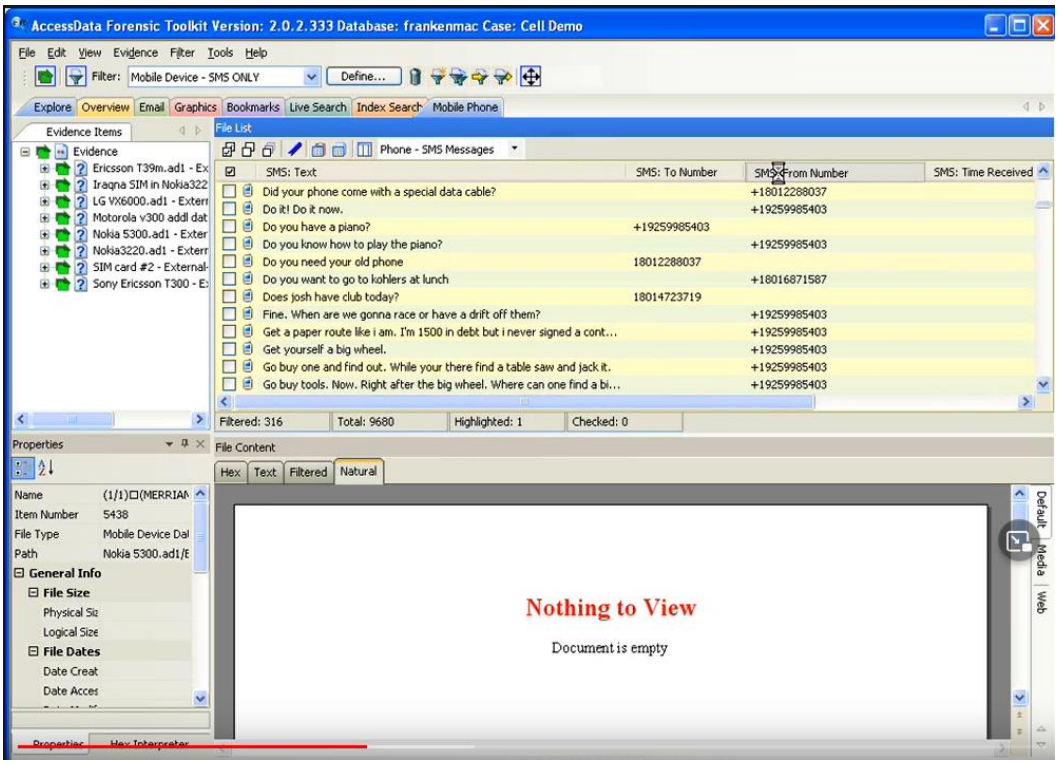
FINDINGS AND REPORT:

- Cellular Device:
  - On today's date, June 6th, 2022, I retrieved a search warrant through the US District Courts In Washington D.C. and began examining the cellular device in question.

  - Tools used for forensic examination of the mobile device:
    - SIM card reader
    - Access Data FTK Imager- Mobile digital forensics software tool

  - After tools and search warrant were retrieved the examination proceeded as below.
    - I connected the cell phone to the my forensic workstation with a USB-C to USB 3.0 connector. Next I opened the AccessData FTK Imager software.
    - AccessData FTK Imager was used to create a forensic image of the cell phone, which is a copy of all the data currently on the cellphones data storage. FTK Imager also simultaneously creates a hash, which is a unique identifier number of the drive in its current state. A hash was also generated for the original phones data drive. Both hashes are the same unique identifier string, meaning that the drive image file FTK Imager created is an exact copy of the files found on the cellular device in question and will allow me a working copy to analyze while preserving the data on the cellphone
    - Next FTK Imager was able to mount the drive image and allow access to the files in the image for a manual extraction using the Mobile Phone Examiner software suite. I was able to go to the Mobile Phone tab and search through all the SMS messages sent. I narrowed the search with a string search choosing only messages sent on 12/15/2021 and was able to discover the confirming lunch text. Below is a picture of that search results.

Case Identifier: 01-06-2022-1000-1000-1337
Case Investigator: Chris Evans CYSE 407
Identity of Submitter: District Attorneys Office for the U.S. District Court of Washington D.C.
Date of Receipt: June 5th, 2022 , 10:30 PM



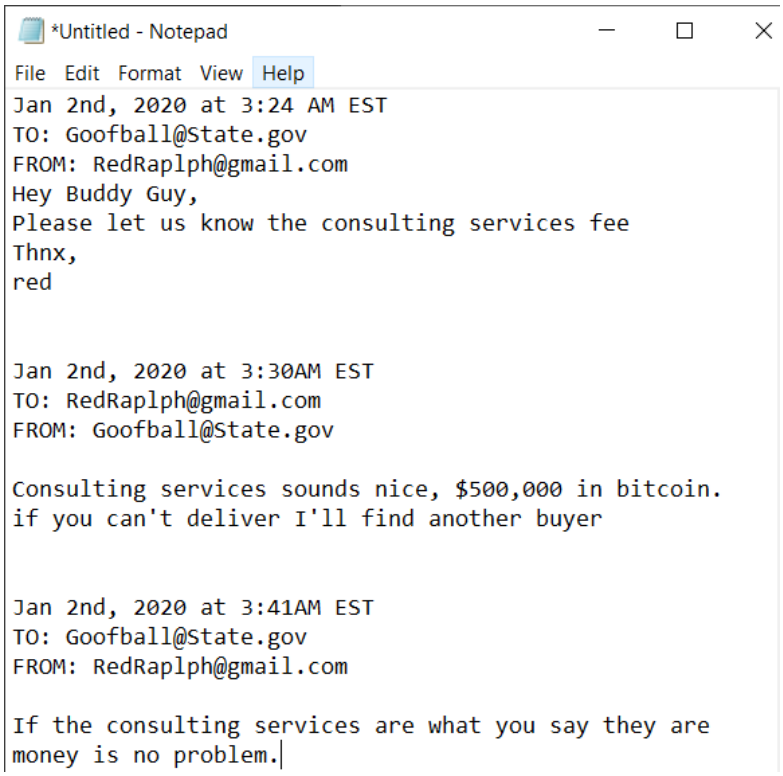
- Documented Message:
  - Phone Number: 18016871587
  - Contact Name: Red Ralph
  - Message: “ Do you want to go to kohlers at lunch “

- Personal Laptop Computer
  - On today's date, June 6th, 2022, I began the forensic imaging process

  - Tools used for forensic examination of the mobile device:
    - Access Data FTK Imager- Mobile digital forensics software tool
    - www.arin.net – Public IP registry website
    - USB 3.0 cord

  - After connecting original media drive in the laptop to the hardware write blocker via USB 3.0 I began the imaging process. I used AccessData FTK Imager software to copy the drive and create a forensic image copy. This copy was also hashed like the cellphone and when compared with the original drive was shown to be identical.
  - Once image was created I used the following process to recover emails and deleted zip files.
    - Email Recovery Process
      - After obtaining the laptop drive image, I opened it with a AccessData FTK Imager software and mounted it to be able to navigate the files.
      - I performed a string search for the keyword “ RedRalph@gmail.com”

- I was able to search through the results and find multiple emails that contained the keyword, “Consulting services” that were addressed to RedRalph@gmail.com. Below is the emails that were discovered and some metadata that were recovered and collected as evidence.



- The emails header also contained IP address routing information and using the search engine google I was able to track back the communication using public registry website WWW.arin.net . The email headers were collected as evidence.

- Deleted ZIP File and Web Log Recovery Process
  - Software used
    - Autopsy
    - www.arin.net
  - Using Autopsy I created a new case, and mounted the data drive image to the case for review. After mounting I opened the file exploer and navigated to section Views, then to Deleted Files, and then to All
  - In the All section I was able to find three .ZIP files that were deleted on January 3rd, 2020 at 9:45 PM EST
  - These files were recovered and collected as evidence.
  - Using the software Windows firewall log I was able to see that the files in question was transmitted to FileBuddy which has an IP address registered to a file sharing website in the Russian Federation. This occurred January 3rd, 2020 at 9:00 PM EST I resolved the IP address found in Windows Firewall log with www.arin.net lookup

to see where the IP was located. These logs were recovered and collected as evidence.

CONCLUSION:

- Conclusion:
  - After using Digital forensic methods and practices in keeping with industry standards like ISO/IEC 17025 I am confident in my analysis of the cellphone and laptop drives and that my software tools have discovered evidence useful to the court. I am confident that on Dec 15, 2021 text messages were exchanged to coordinate a meeting with Red Ralph as the contact was saved in the target cellphone. Then on January 2, 2020 emails between the laptops owners and RedRalph were exchanged containing the keyword "consulting Services". And then lastly on January 3, 2020 ZIP files were uploaded to a file sharing site called FileBuddy with servers located in Russia.

- Hardware used to recover files
  - Forensic workstation computer
  - Data write blocker
  - SIM card reader
  - USB cords

- Software used to recover files
  - Access Data FTK Imager
  - Windows Firewall Log
  - Autopsy

- Evidence includes:
  - Emails from the evidence laptop to Red Ralph containing keywords
  - SMS messages and metadata from the evidence cellphone to Red Ralph containing instructions to meet physically.
  - Deleted ZIP files forensically recovered with classified material as well as logs showing transmission to file share websites.

CONSULTATION FEE

- I was hired by the US District Court of Washington D.C. to offer my expertise as a digital forensic investigator on this case. The services I rendered were mobile data recovery, computer email data recovery, and data carving also known as salvaging of deleted data from a computer. The fee for my time is $150 USD per hour and I worked on this case for 40 hours for a total charge of $6000 USD. This fee includes any court appearances, or testimony necessary to deliver my written report.

Case Identifier: 01-06-2022-1000-1000-1337
Case Investigator: Chris Evans CYSE 407
Identity of Submitter: District Attorneys Office for the U.S. District Court of Washington D.C.
Date of Receipt: June 5th, 2022 , 10:30 PM