Case Identifier: 82759022

Case Investigator: Bryant Watkins

Identity of Submitter: Bryant Watkins

Date of Receipt: 4/21/2024

Items Submitted for Examination

Cellular Device - Base transceiver station, Base station controller, Mobile switching center, and SIM Card components specifically of a Samsung Galaxy S22 Ultra. **S/N** - S385637401839

Laptop – Hard Drive, USB Drive, and Physical possession of Microsoft Surface Pro laptop device. **S/N** – M8475601228746

Steps Taken

Cellular Device

- A search warrant from the U.S Federal District Courts was issued and received on today's date of 4/21/2024
- Acquisition of the following digital forensic tools - SIM Card Reader (MOBILedit Forensic), Secure View 3, and a passcode cracker (SV Strike).
- Unlocking of Device – Used the advanced scripting capability of SV Strike to successfully discover the correct PIN and thus gain access to the device.
- SIM Card – MOBILedit forensic contains a built-in write-blocker, after connecting to the cellular device directly via Bluetooth I was able to read the SIM card by using the provided SIM reader.

Case Identifier: 82759022

Case Investigator: Bryant Watkins

Identity of Submitter: Bryant Watkins

Date of Receipt: 4/21/2024

Laptop

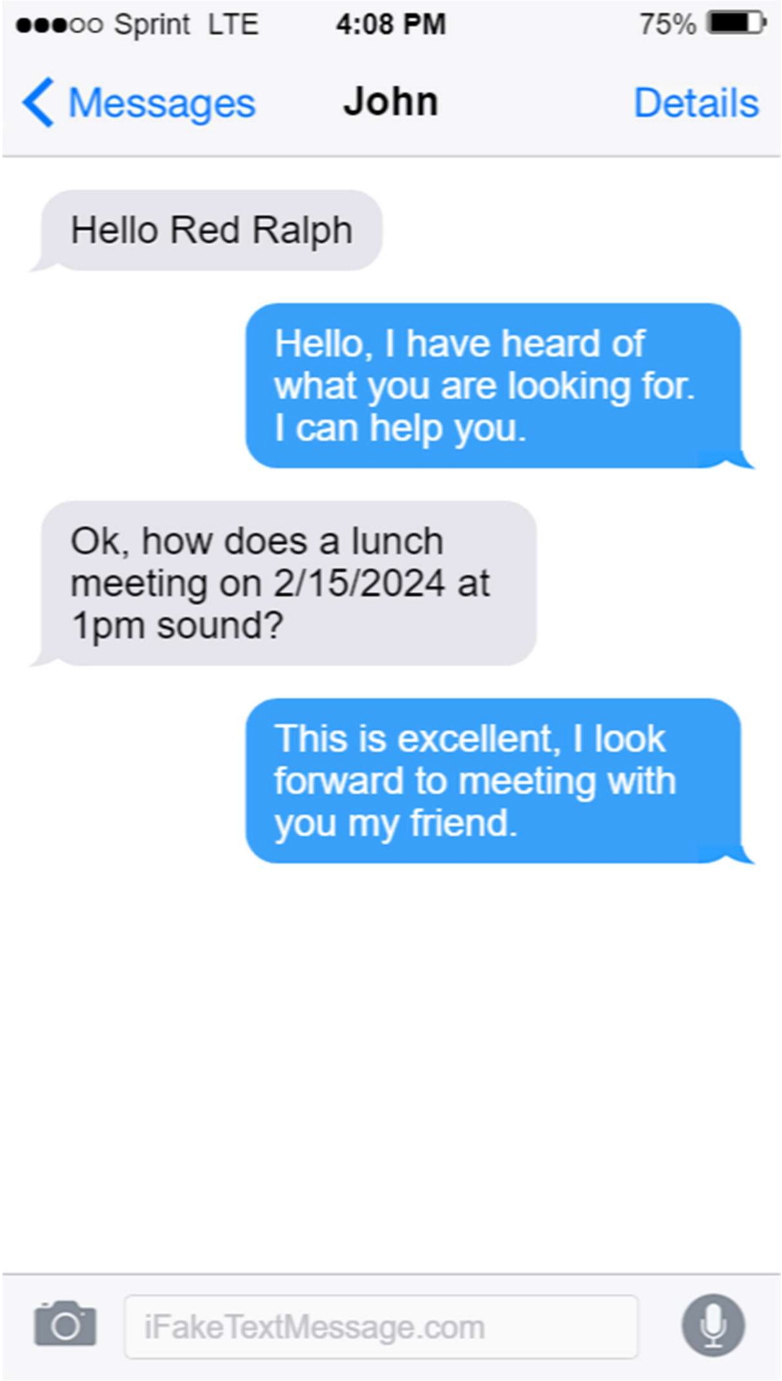
- A search warrant from the U.S Federal District Courts was issued and received on today's date of 4/21/2024
- Acquisition of the following digital forensic tools – www.internic.com, and OSForensics.
- I utilized www.internic.com to find the domain's IP address and point of contact for this investigation.
- Then I proceeded compare e-mail logs with the messages (acquired through usage of OSForensics) to verify the e-mail account, message ID, IP address, as well as date and time stamp.
- OSForensics was also capable of successfully recovering previously deleted zip files that, upon close examination, contain pertinent data and information for the purposes of this investigation.
- The headers and encoding at the beginning and ending of the e-mail(s) in question were traced which allowed me to monitor the route the e-mails took through the server. I then used this information to determine who really sent the e-mails in question through pinpointing the sender's true location.

Case Identifier: 82759022

Case Investigator: Bryant Watkins

Identity of Submitter: Bryant Watkins

Date of Receipt: 4/21/2024



Hello Red Ralph

Hello, I have heard of what you are looking for. I can help you.

Ok, how does a lunch meeting on 2/15/2024 at 1pm sound?

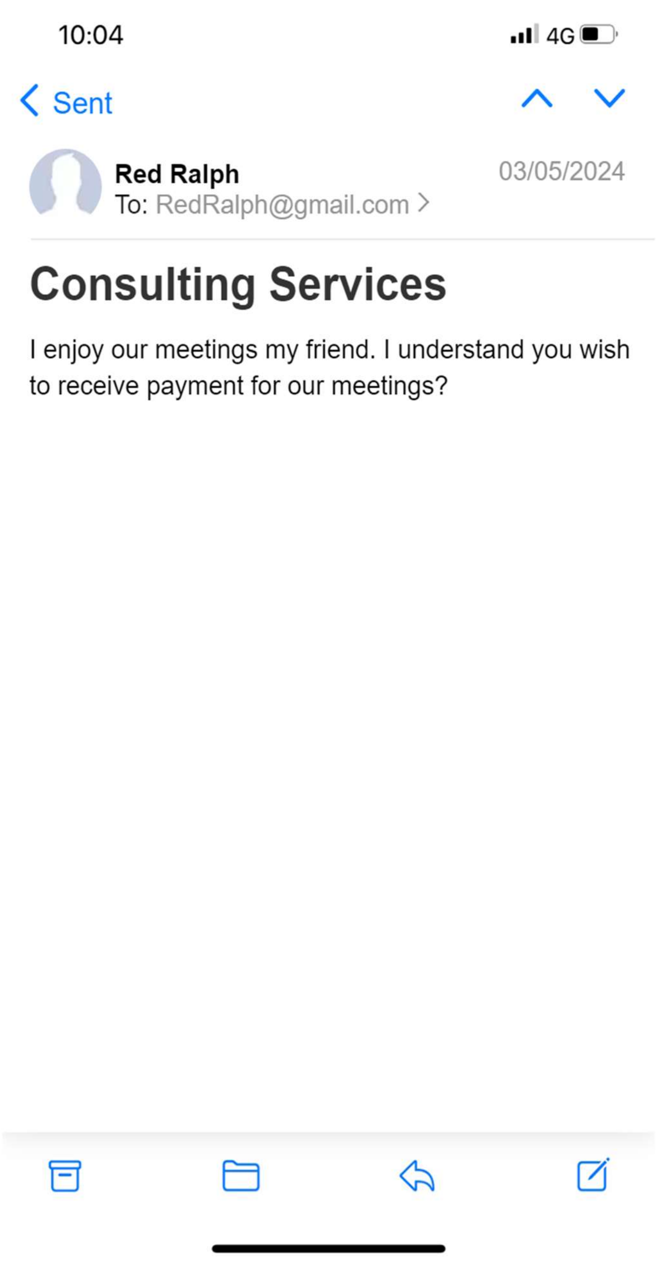
This is excellent, I look forward to meeting with you my friend.

Case Identifier: 82759022

Case Investigator: Bryant Watkins

Identity of Submitter: Bryant Watkins

Date of Receipt: 4/21/2024

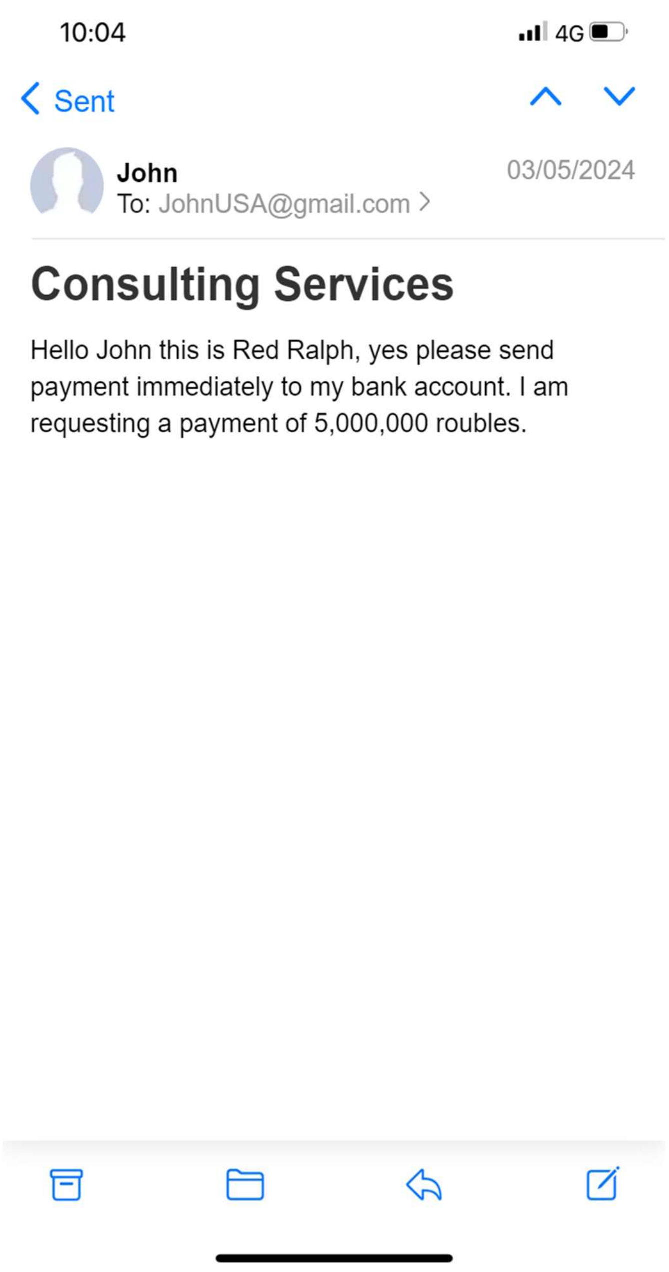


Red Ralph
To: RedRalph@gmail.com

03/05/2024

Consulting Services

I enjoy our meetings my friend. I understand you wish to receive payment for our meetings?



John
To: JohnUSA@gmail.com

03/05/2024

Consulting Services

Hello John this is Red Ralph, yes please send payment immediately to my bank account. I am requesting a payment of 5,000,000 roubles.

Case Identifier: 82759022

Case Investigator: Bryant Watkins

Identity of Submitter: Bryant Watkins

Date of Receipt: 4/21/2024

Conclusion

It is very apparent based on the evidence acquired that the suspect in question, John of the United States, has colluded with a Russian counterpart known by his alias “Red Ralph”. Upon recovering and extracting text messages as well as email communications – multiple messages were uncovered that shed light on an intelligence sharing scheme to undermine United States security and provide insider knowledge to adversary Russia. John from the United States has been observed discussing specific meeting times and details as well as payment correspondence through text and email messages.

The acquired evidence has been confirmed to be completely authenticate as well as confirmed as being sent by the two suspects based on the data integrity protections and IP sourcing components of the forensic tools utilized during this process. This all makes for an incredibly strong case that should move forward accordingly within the United States Federal District Court system and assist in the prosecution of John from the United States as well as the Russian official Red Ralph due to their illegal communications that pertain to sensitive United States intel that heightens national security risks for the United States.

WORK CITED

Nelson, Bill, et al. *Guide to Computer Forensics and Investigations: Processing Digital Evidence*. 6th ed., CENGAGE LEARNING, 2018, *Cengage*, Accessed 20 Feb. 2024.