Final Paper

Kobe Coleman

CYSE 407: Digital Forensic

April 24, 2024

Case Scenario

You were hired as a forensic expert to investigate alleged contact between US and Russian officials. The owner of the laptop and phone has "lawyered up" and is not saying anything about what they were doing or any meetings that may have happened. You performed a forensic analysis on the laptop and cell phone of a high ranking US government official.

Case Identifier: DFL-2024-18780

Case Investigator: Kobe Coleman

Identify of the Submitter: Alan Yamato

Date of Receipt: 4/15/2024

Items of Examinations:

iPhone 15

- 256 GB
- Color: Blue
- Serial Number: 9i5l06Y4DWqI
- Software: iOS 17.3.5
- Made in USA: 09/22/2023

Dell Precision 5680 Workstation

- Storage: 4 TB
- Memory: 64 GB: 2 x 32 GB, LPDDR5, 6000 MT/s
- Operating System: Windows 11 Pro
- Processor: Intel Core i9-13900H
- Made in China
- Color: Black

Legal Protocols

- There have been continuous questions about the behavior of government official Alan Yamato, both inside and outside of the office.
- Fortunately, we secured a warrant from Judge Jenkins Sanders that allows us to collect the suspect's electronics, including his iPhone and laptop, to advance our investigation.
- To avoid any interference, we will impose mandatory paid time off on him, ensuring that he doesn't know of any strange activity during this period.

- During his absence, an government official with the same GS ranking will take up his tasks while the probe continues.

Software Used in Investigation:

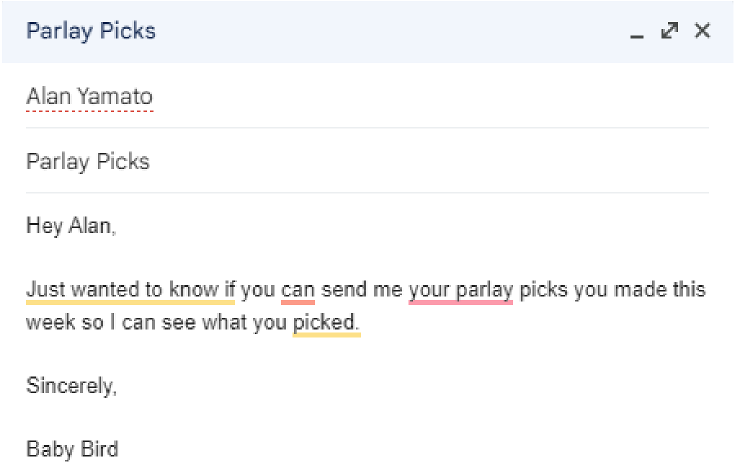
1. The Sleuth Kit: allows you to analyze volume and file system data.
2. EnCase: provides extensive capabilities for obtaining, analyzing, and reporting digital evidence from a variety of devices and platforms.
3. Cellebrite UFED: This software specializes in mobile device forensics and can be used to extract and analyze data from the iPhone 15, including messages, call logs, and other digital artifacts that may reveal communication.
4. VMware: creates a virtual environment to extract data without affecting the operating system.
5. Mail Pro+: allows the user to examine, look for, and convert multiple email files.
6. Aid4Mail- this tool helps to recover emails that are deleted and has better filtering then other tools.
7. Ophcrack- This is a tool that is used to get into a laptop or computer, from digital investigators.

How the Software will be used in the Investigations:

In the investigation, a combination of software tools will be utilized to gather, analyze, and interpret digital evidence from the devices under scrutiny. The Sleuth Kit will be useful in investigating volume and file system data, revealing vital information about the structure and contents of storage medium. EnCase, known for its extensive capabilities, will play a critical role in gathering and analyzing digital evidence from a variety of devices and platforms, ensuring a full analysis of the data contained on those devices. Cellebrite UFED will specialize in mobile device forensics, extracting and analyzing data from the iPhone 15 to discover texts, call logs, and other digital artifacts pertinent to the case. VMware will establish a virtual environment, allowing investigators to extract data without modifying the underlying operating system, thereby protecting the evidence's integrity. Mail Pro+ will streamline the examination and conversion of multiple email files, facilitating the analysis of email communications pertinent to the case. Finally, Volatility will be used to do memory forensics on the machine, revealing hidden programs, network connections, and other artifacts that would be difficult to detect with typical disk analysis. Together, these technological tools will constitute a comprehensive arsenal to help untangle the investigation's intricacies.

Analyzing The Laptop

The Dell laptop was analyzed with Ophcrack and The Sleuth Kit. This allowed us to access and inspect the laptop's contents easily. Our effort moved to finding and recovering emails exchanged between the government official and the Russian spy. Next, we used Mailpro+ software to expose communication between the two individuals from December 6, 2023 to April 20, 2024 without notice or suspicion. They employed covert code names like "baby bird" to avoid suspicion, allowing them to discuss sensitive matters such as “What parlay picks did you make for this week." "In reality, these files were highly classified documents. They concealed this by referring to them as 'the parlay picks,' implying the number of top-secret files transferred to 'baby bird.' Despite recovering the emails, we had to ensure that none were erased. Aid4Mail proved useful in this endeavor, uncovering around five emails erased by a government officer, all of which included top-secret files. Here are the emails in which they pretended to be lottery numbers."



Parlay Picks

Alan Yamato

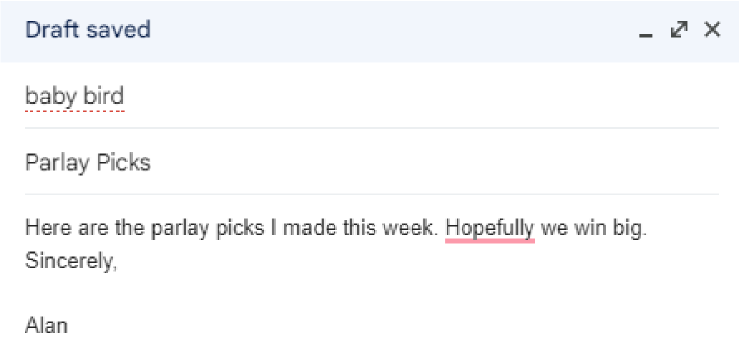
Parlay Picks

Hey Alan,

Just wanted to know if you can send me your parlay picks you made this week so I can see what you picked.

Sincerely,

Baby Bird



Draft saved

baby bird

Parlay Picks

Here are the parlay picks I made this week. Hopefully we win big.
Sincerely,

Alan

These are just two of the countless emails sent between the government official and the Russian spy. They disguised their contact as parlay picks, but the government official was actually sending top-secret data and sensitive information about agency agents, including personal details. Tools such as Sleuth Kit helped to uncover this illegal conduct.

Analyzing The Phone

The process of analyzing the cellphone began with unlocking it, facilitated by the use of Cellebrite UFED and with this tool we were able to find "baby bird" on his contact list. In addition, we discovered that they were texting and calling each other on a daily basis. Next, we recovered the binary format from the mobile device, which enabled us to decipher the text messages being delivered. Among these texts, we discovered plans made with "baby bird," detailing meeting times and locations, including a rendezvous at a steakhouse at 1595 I St NW, Washington.

Baby Bird: Hey can you send me those parlay picks we were talking about earlier this week.

Alan: Yea, but can I just give you to them over lunch at this famous steakhouse.

Baby Bird: Sure where is it at?

Alan: 1595 I St NW, Washington. Its called Rare steakhouse.

Baby Bird: Ok See you there.

The displayed messages are between "baby bird" and a government official named Alan. They propose meeting in person for Alan to pass over the top-secret files, choosing this technique over email to avoid drawing attention. They have already been captured, although they are unaware of this.

Conclusion

After this evidence was presented in court this Alan was given serve punishment because he violated “United States Constitution, Article III, Section 3, “Treason against the United States, shall consist only in levying war against them, or in adhering to their enemies, giving them aid and comfort. No person shall be convicted of treason unless on the testimony of two witnesses to the same overt act, or on confession in open court” (Cornell) and also violated “Section 783 of Title 50, U.S.C., makes it unlawful for any officer or employee of the United States, or of any federal department or agency, to communicate to any person whom he or she knows or has reason to believe to be an agent of a foreign government, any information classified by the President or by the head of such department or agency as affecting the security of the United States, knowing or having reason to know that such information has been so classified. See 50 U.S.C. § 783(b). Conversely, it is unlawful for a foreign agent knowingly to receive classified information from a United States government employee, unless special authorization has been obtained. See 50 U.S.C. § 783(c)" (Justice). Baby Bird is still currently on the run and is being investigated and pursuited by our investigation team and FBI agents.

Reference

2057. synopses of key national defense and national security provisions. Justice Manual | 2057. Synopses Of Key National Defense And National Security Provisions | United States Department of Justice. (2020, January 17). https://www.justice.gov/archives/jm/criminal-resource-manual-2057-synopses-key-national-defense-and-national-security-provisions#:~:text=Section%20783%20of%20Title%2050,or%20by%20the%20head%20of

Admin. (2023, June 12). *Best Mobile Forensics Tools - Top 5 Unlocking digital insights*. Forensics Insider. https://www.forensicsinsider.com/digital-forensics/best-mobile-forensics-tools/

Dell Precision 5680 Mobile Workstation: Dell USA. Dell. (n.d.). https://www.dell.com/en-us/shop/dell-laptops/precision-5680-workstation/spd/precision-16-5680-laptop/xctop5680usvp2?view=configurations

IPhone 15 and iphone 15 plus - technical specifications. Apple. (n.d.). https://www.apple.com/iphone-15/specs/?afid=p238%7CsmtGMaii5-dc_mtid_20925d2q39172_pcrid_686763100025_pgrid_154285222278_pntwk_g_pchan__pexid_100404449063_&cid=wwa-us-kwgo-iphone--slid-foQg6u43--Brand-iPhone15-PostAvail-

Legal Information Institute. (n.d.). *Treason*. Legal Information Institute. https://www.law.cornell.edu/wex/treason#:~:text=According%20to%20the%20United%20States,giving%20them%20aid%20and%20comfort.