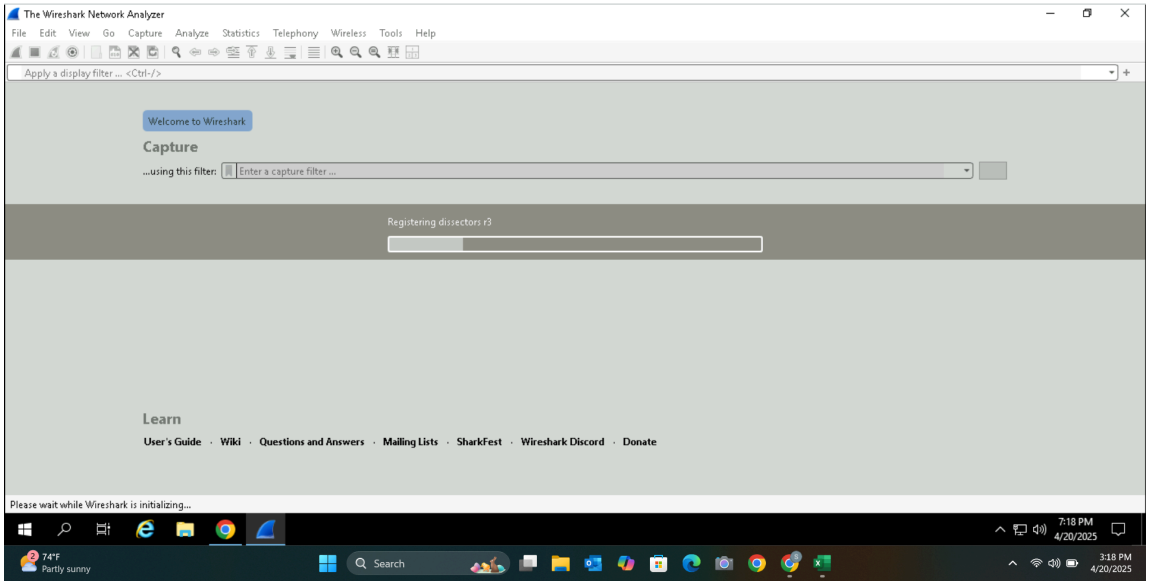
Saeed Rafee
Network Traffic Analysis

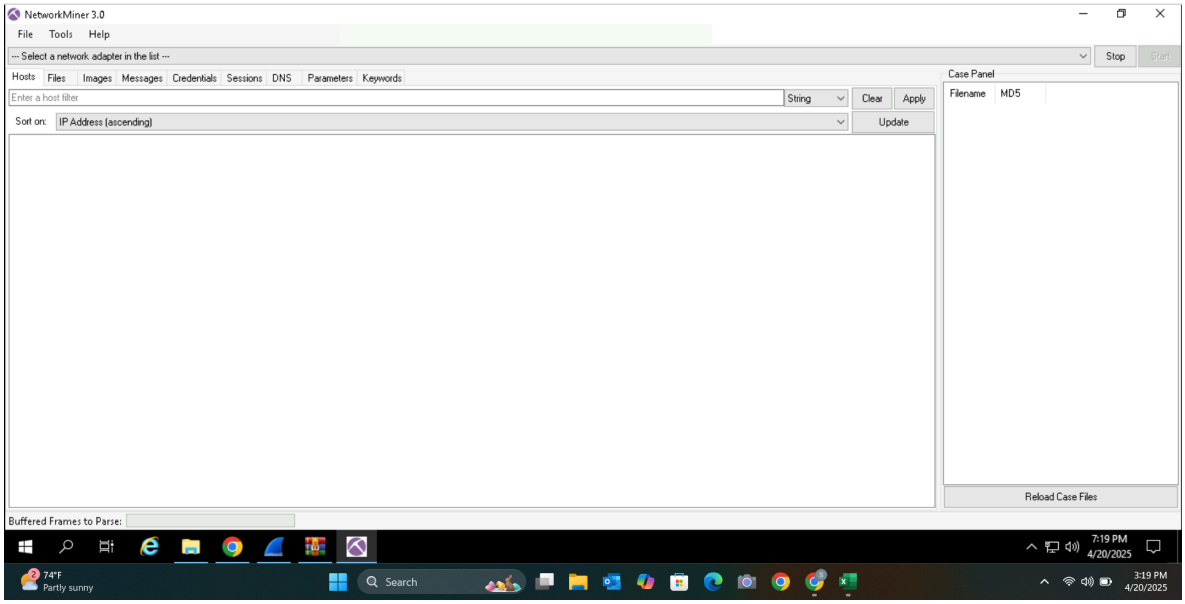
Objective

This lab demonstrates my ability to conduct a hands-on network traffic analysis using tools like **Wireshark** and **NetworkMiner**. I worked through a simulated insider threat investigation by analyzing packet captures, identifying communication patterns, and recovering evidence. The goal was to uncover key details such as usernames, file transfers, and message content—showcasing my approach to forensic analysis and investigative thinking.

Step 1: Install Wireshark and NetworkMiner

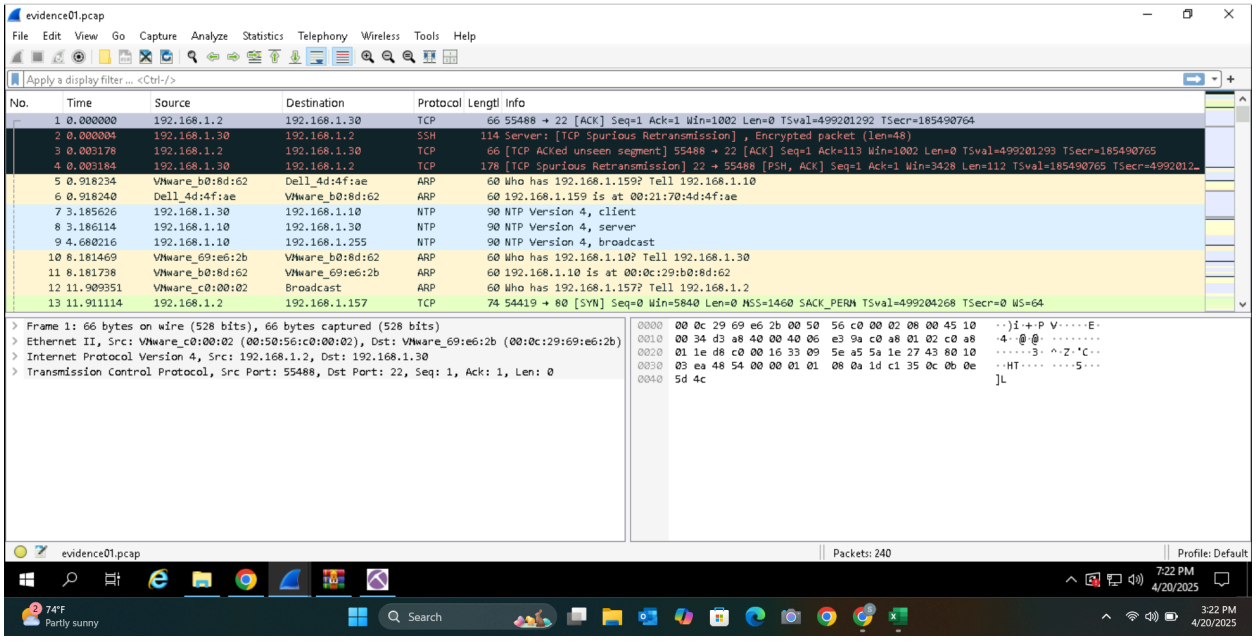
To begin the analysis, I installed two core network forensic tools: **Wireshark** and **NetworkMiner**. Wireshark was used for capturing and inspecting network packets, while NetworkMiner helped extract and organize key artifacts from the same traffic. These tools provided both visual and data-layer perspectives, making it easier to examine the behavior of specific hosts and sessions.

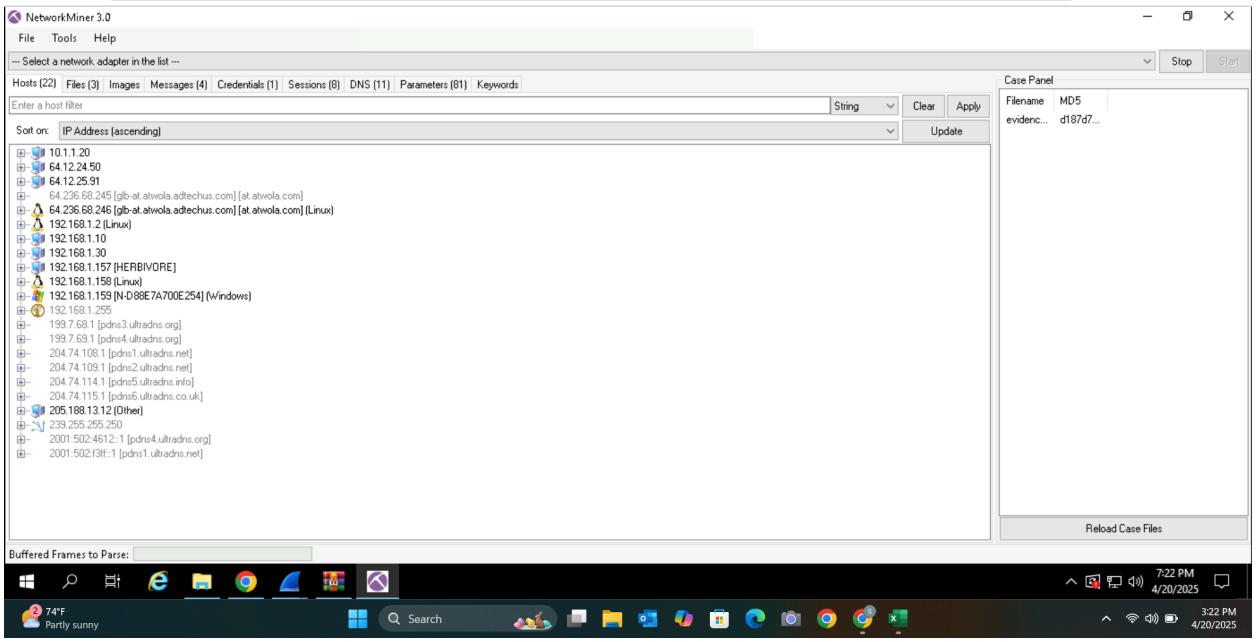




Step 2: Loading the Evidence

With both Wireshark and NetworkMiner ready, I opened the packet capture in each tool. Wireshark allowed me to inspect the traffic flow at the packet level, while NetworkMiner quickly extracted key data like hostnames, files, and communication sessions. Having both views side by side gave me flexibility in how I approached the investigation and helped confirm findings across tools.



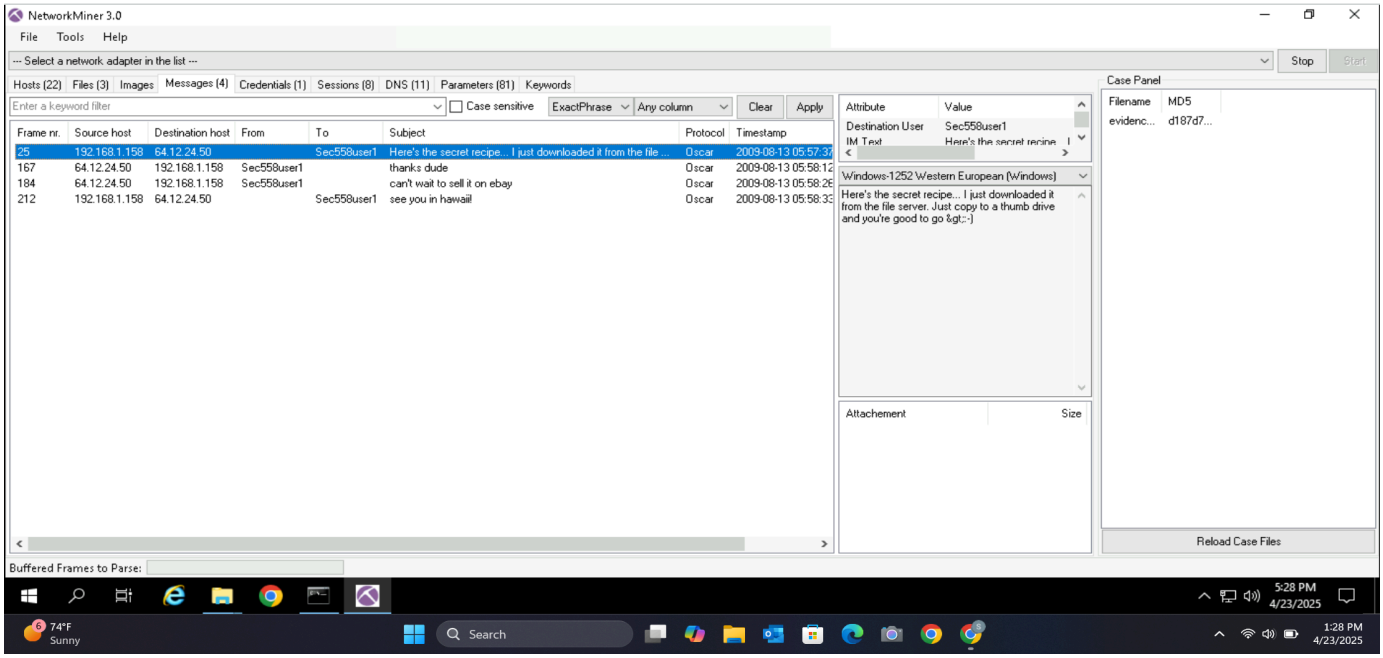


Now that the analysis environment is fully set up, the next phase of this project involves working through a simulated insider threat case. The following scenario outlines the context for the investigation. My task is to examine the network traffic using forensic tools and determine who Ann was communicating with, what was shared, and what evidence can be recovered.

Scenario: Anarchy-R-Us, Inc. suspects that one of their employees, Ann Dercover, is really a secret agent working for their competitor. Ann has access to the company's prized asset, the secret recipe. Security staff are worried that Ann may try to leak the company's secret recipe. Security staff have been monitoring Ann's activity for some time, but haven't found anything suspicious– until now. Today an unexpected laptop briefly appeared on the company wireless network. Staff hypothesize it may have been someone in the parking lot, because no strangers were seen in the building. Ann's computer, (192.168.1.158) sent Instant Messages (IMs) over the wireless network to this computer. The rogue laptop disappeared shortly thereafter. "We have a packet capture of the activity," said security staff, "but we can't figure out what's going on. Can you help?" You are the forensic investigator. Your mission is to figure out who Ann was IM-ing, what she sent, and recover evidence.

Exercise answers:

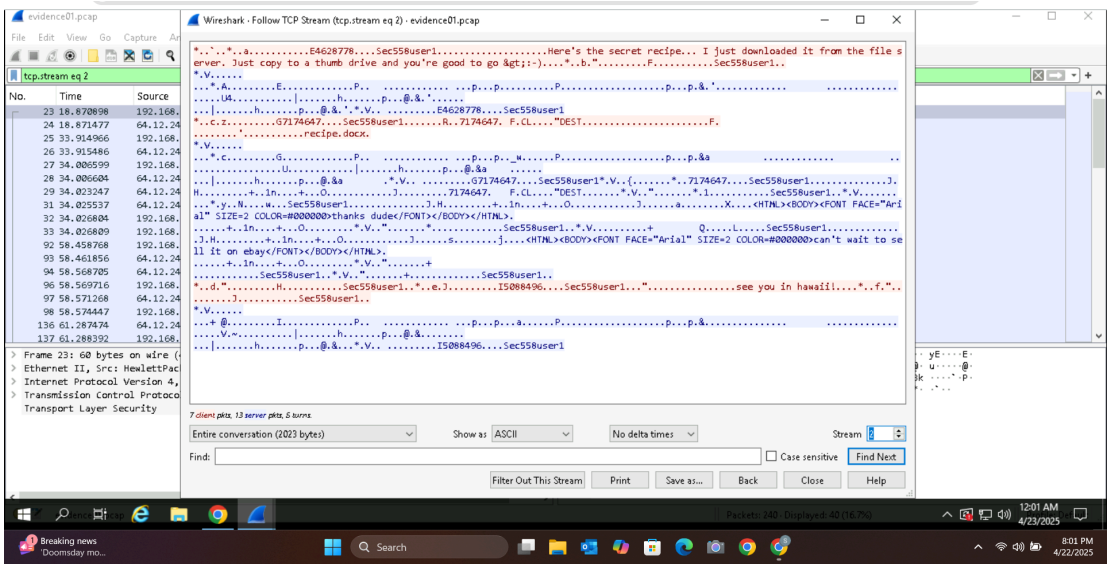
(1) What is the name of Ann's IM buddy?
I opened the evidence file in **NetworkMiner** and navigated to the **"Messages"** tab. From there, I reviewed the captured chat logs and identified the sender and receiver fields. The name **Sec558user1** appeared consistently as the recipient of Ann's messages, confirming the IM buddy's identity.
Answer: Sec558user1



(2) What was the first comment in the captured IM conversation?

In Wireshark, I filtered by the source IP address, located the TCP stream for the IM traffic, then followed the stream to view the full chat. The first message was clearly shown at the top of the conversation. This message confirmed Ann's intent to leak sensitive data.

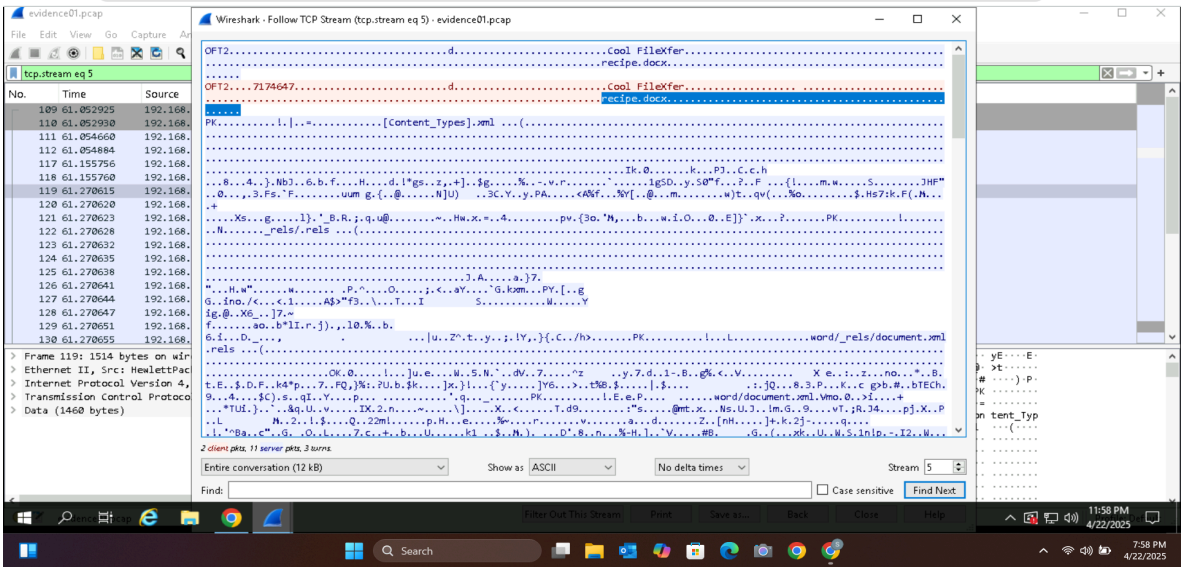
Answer:Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go



(3) What is the name of the file Ann transferred?

In Wireshark, I followed multiple TCP streams until I located the one containing file transfer data. When I reached **Stream 5**, I found the filename **recipe.docx** clearly embedded in the content of the transfer.

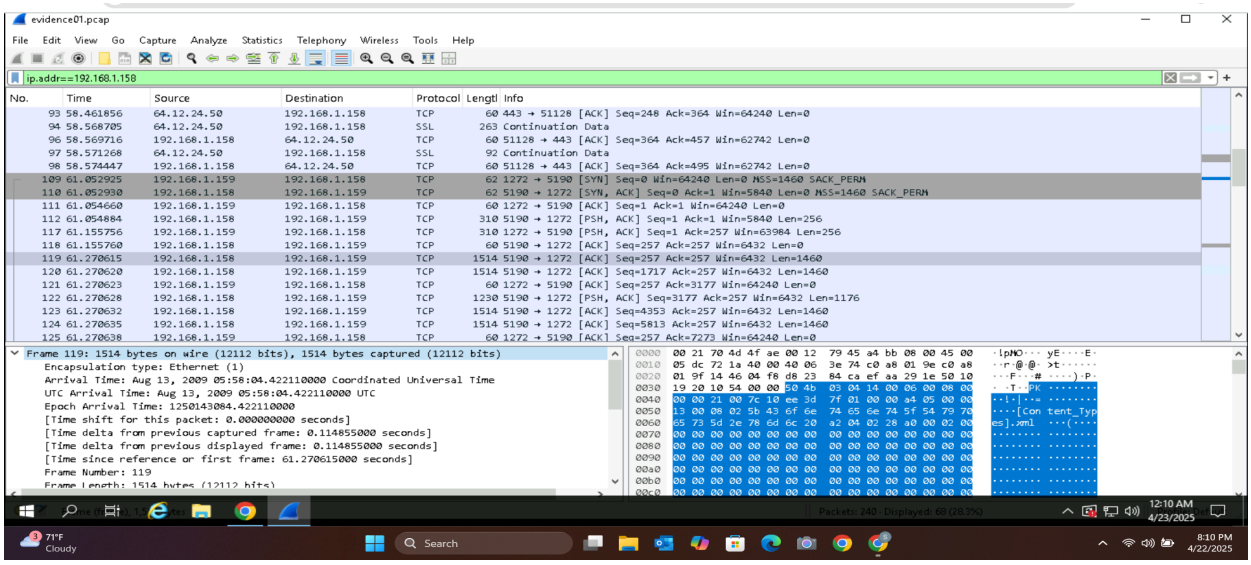
Answer: recipe.docx



(4) What is the magic number of the file you want to extract (first four bytes)?

In Wireshark, I followed the TCP stream from the file transfer and opened the **Hex View** of a packet carrying the file payload. At the beginning of the hex pane, I observed the first four bytes: 50 4B 03 04.These bytes are a known file signature indicating a .docx (ZIP-based) document, confirming it as the start of the transferred file.

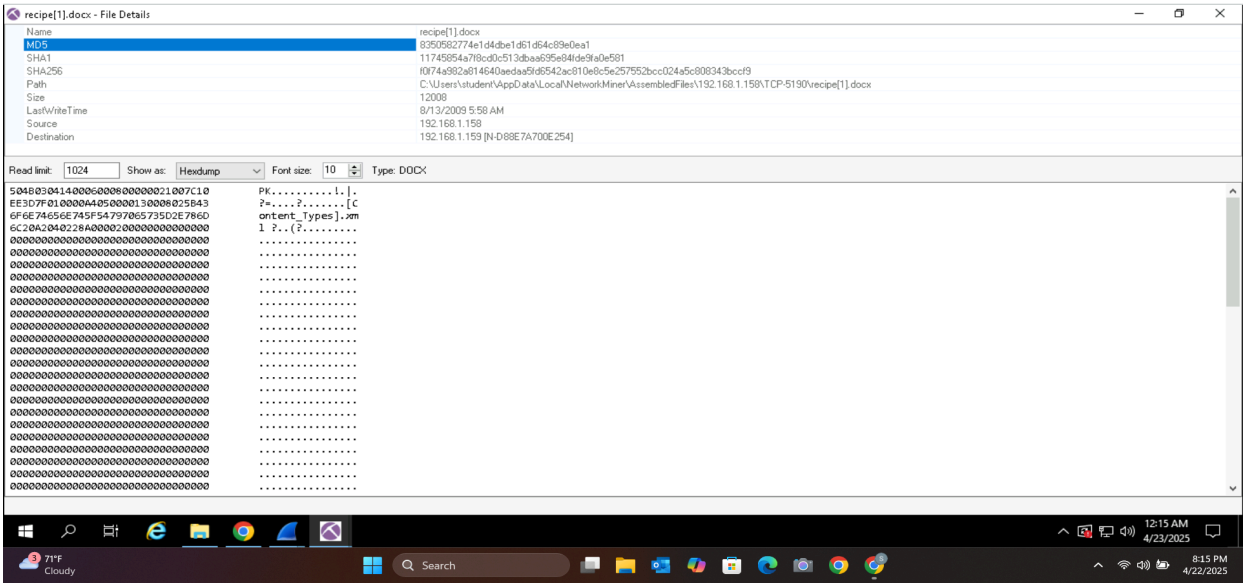
Answer: 50 4B 03 04



(5) What is the MD5sum of the file?

After extracting the file from the packet capture, I calculated its MD5 hash using a hashing tool. This produced a unique fingerprint for the file, which is commonly used for integrity verification and identification.

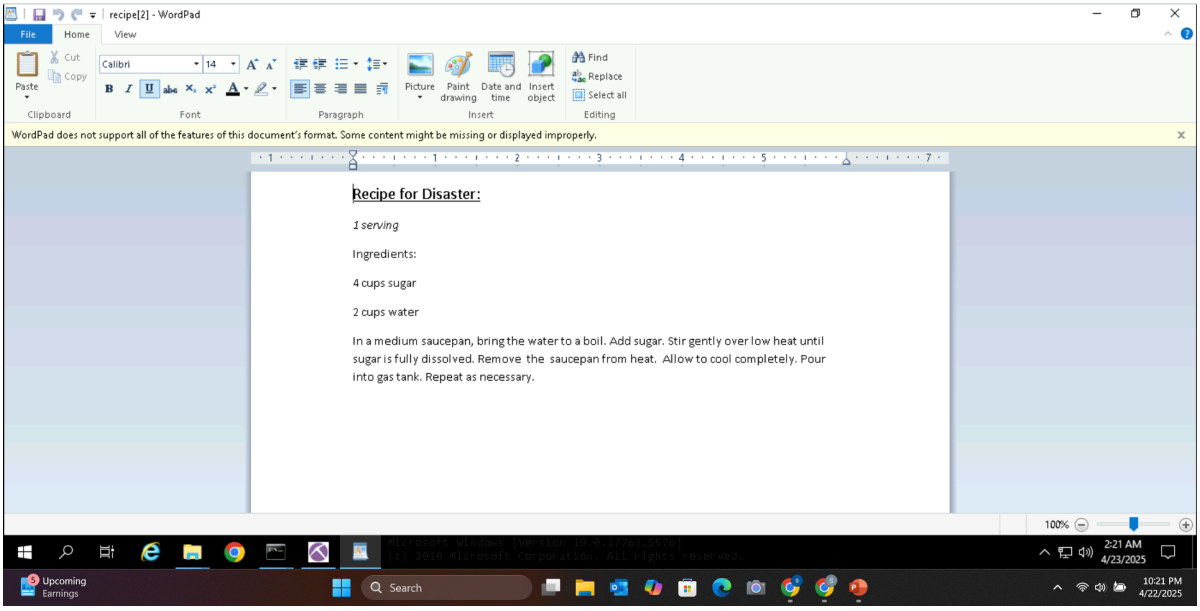
Answer: 8350582774e1d4dbe1d61d64c89e0ea1



(6) What is the secret recipe?

After extracting and opening the transferred .docx file, I found the full contents of the secret recipe inside. The recipe appeared to be disguised as a cooking instruction but likely contained symbolic meaning based on the context of the case.

Answer:



Conclusion

Through this investigation, I successfully identified the IM communication between the suspect and their contact, extracted and reviewed the transferred file, and confirmed the leaked contents. Using Wireshark and NetworkMiner, I was able to trace the timeline of the events, analyze metadata, and extract file-level details from the capture.

Key findings included:

- The identity of the IM buddy
- The first message exchanged
- The transferred file name and content
- The file's hash and signature (magic number)

This analysis highlights my ability to use network forensics tools to investigate suspicious activity, extract meaningful evidence, and document the process clearly and effectively.