Course Name:	**Information Security (116U01L602)**	**Semester:**	**VI**

Somaiya Vidyavihar University
K J Somaiya School of Engineering

Date of Performance :	**24 / 03 /2025**	**DIV/ Batch No:**	**B2**
Student Name:	**Akshat Yadav**	**Roll No:**	**16010122221**

Title: Illustrate and Compare network security mechanisms

Objectives:

To write a program to convert plain text into cipher text using Caesar cipher and Transposition cipher

Related Theory:

Write about wireshark and Network Miner

1. Network based attacks.
2. Network Security tools.
3. Wireshark – Purpose and importance in network security.
4. Network Miner - Purpose and importance in network security.
5. Case Study using Wireshark.
6. Implementation of the same Case study using Network Miner.
7. Comparison of results of both tools.

Link to Case Study: https://forensicscontest.com/2009/09/25/puzzle-1-anns-bad-aim (Evidence file part of the case study document).
Address the questions as specified in the case study.

References:

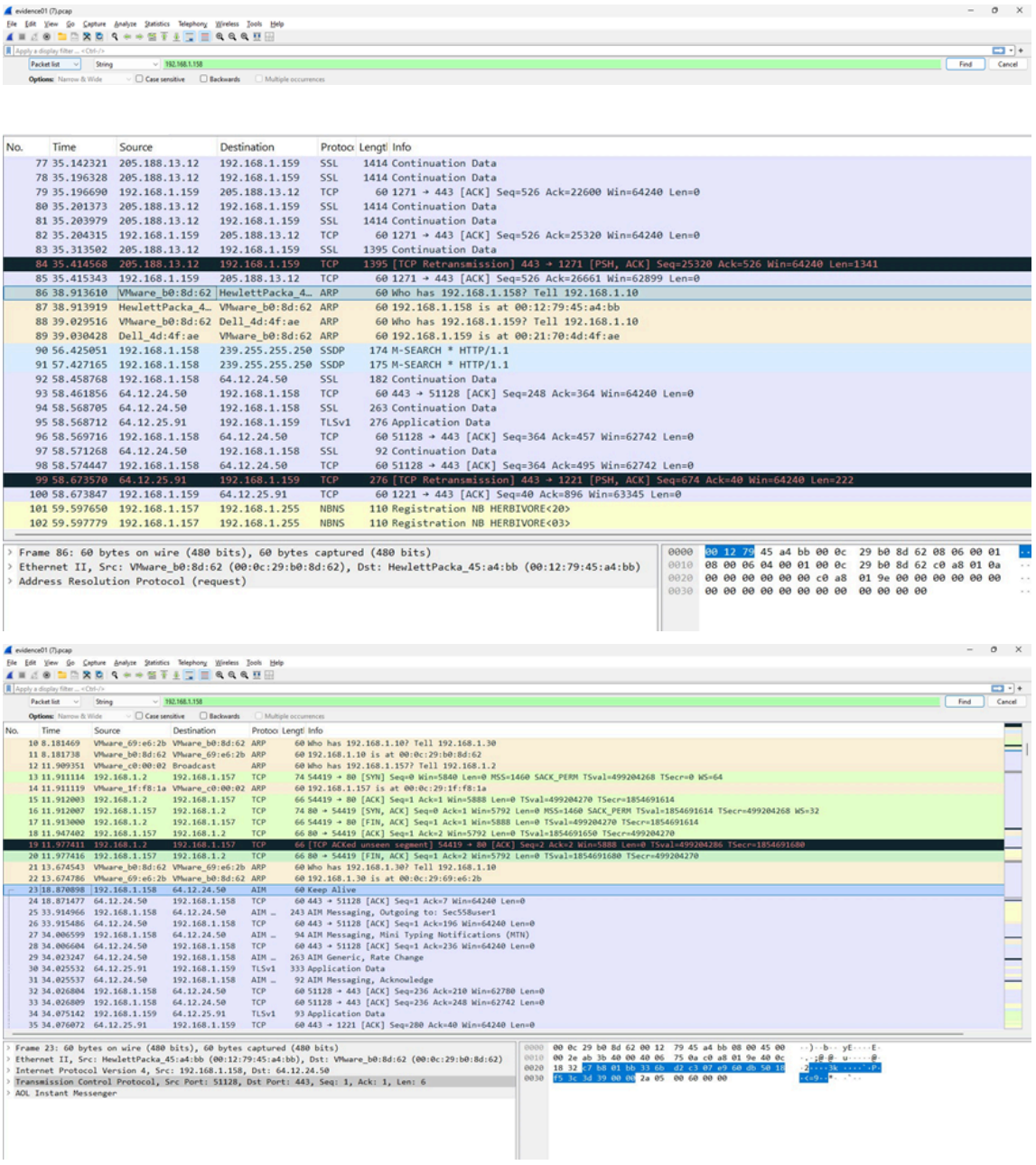
https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html
https://www.netresec.com/?page=TutorialNMP
https://www.youtube.com/watch?v=qTaOZrDnMzQ
https://www.youtube.com/watch?v=nC5m2WO8JJk

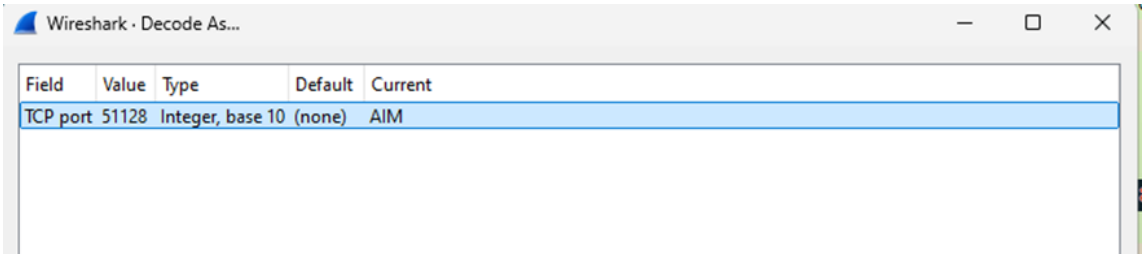
Implementation Details:

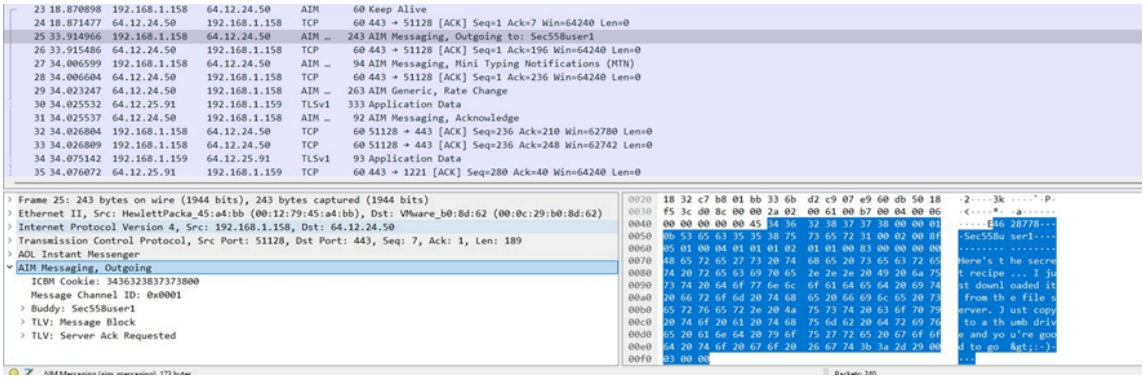
Solving the puzzle-

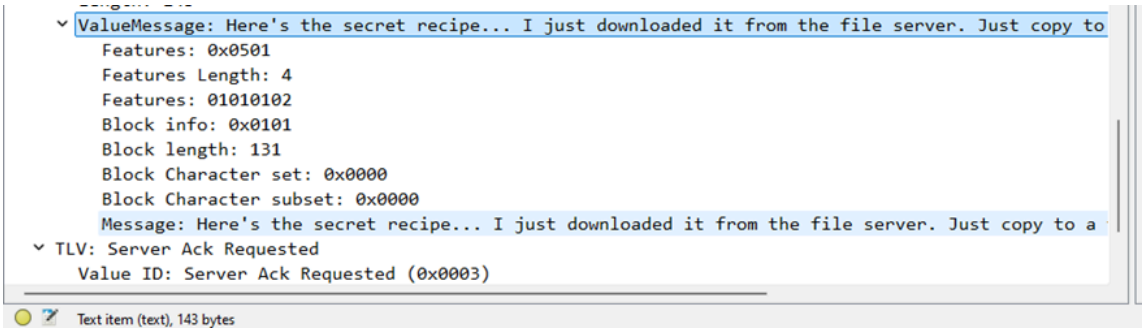
Puzzle #1: Ann's Bad AIM

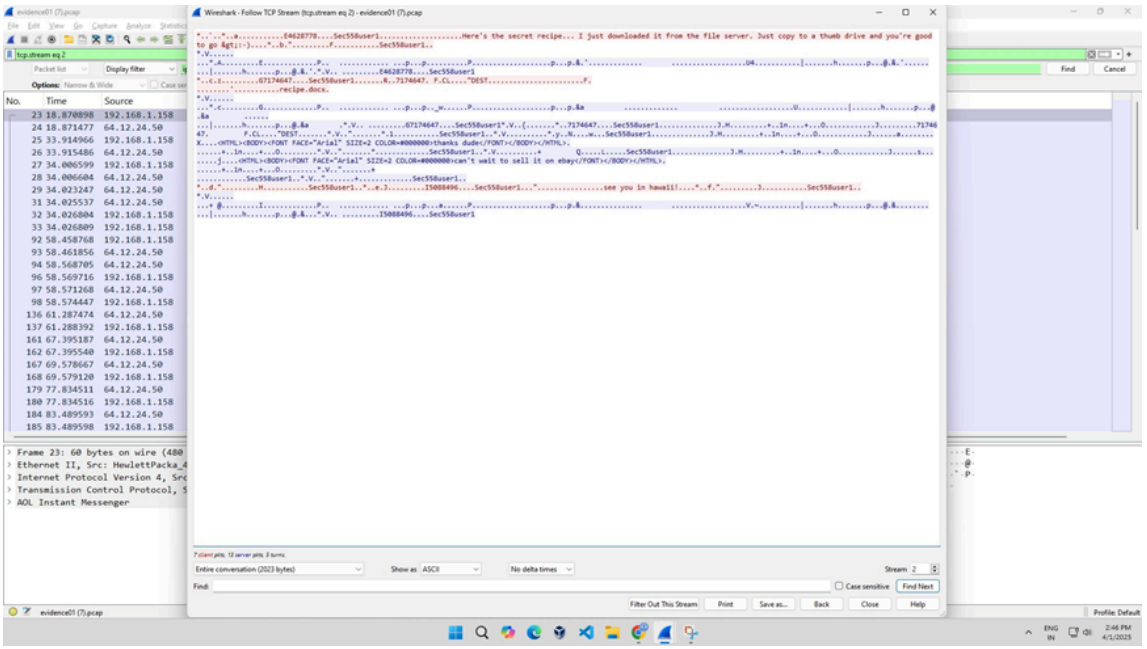
1. What is the name of Ann's IM buddy?

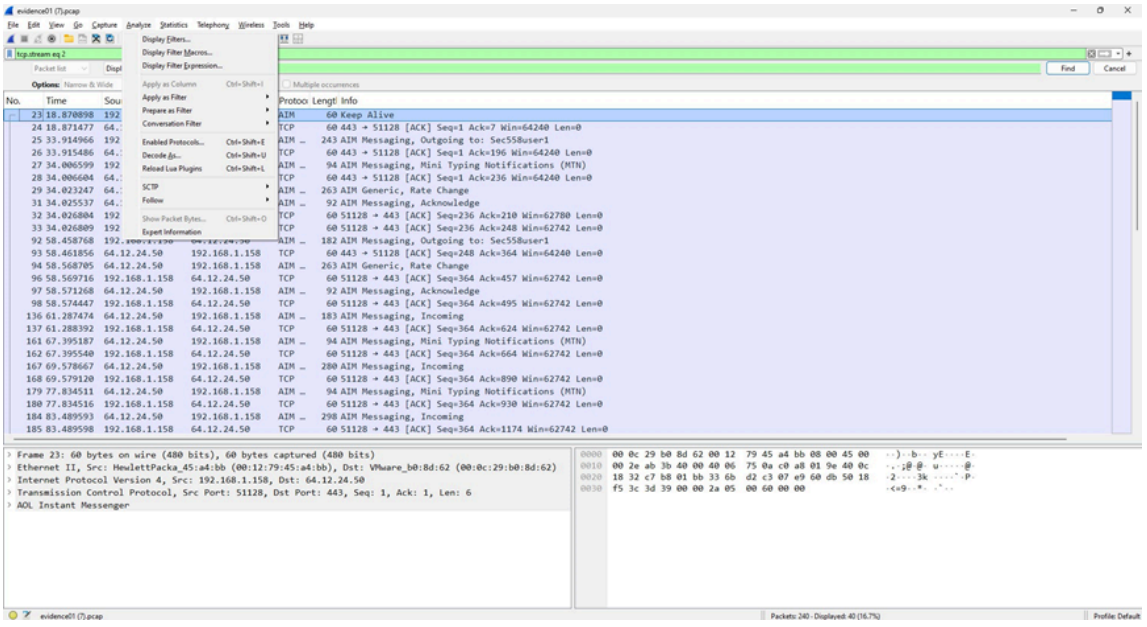


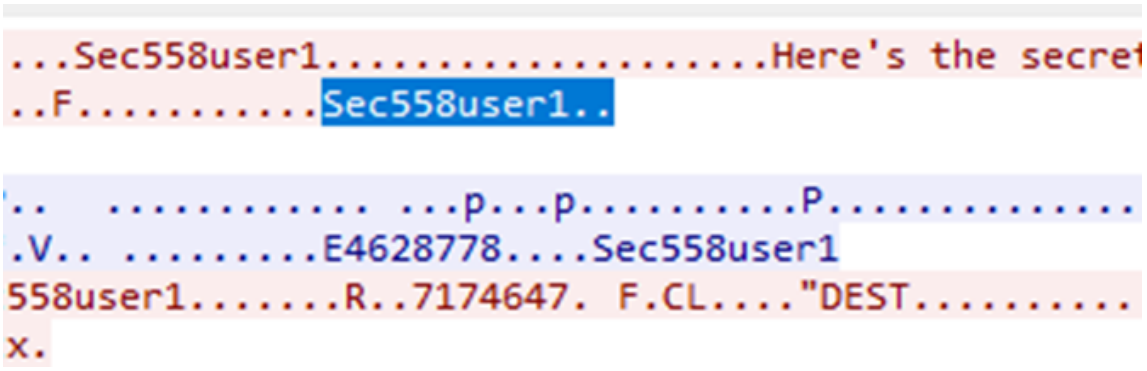

Wireshark · Decode As...
Field
Value
Type
Default
Current
TCP port
51128
Integer, base 10
(none)
AIM


23 18.870898 192.168.1.158 64.12.24.50 AIM 60 Keep Alive
24 18.871477 64.12.24.50 192.168.1.158 TCP 60 443 → 51128 [ACK] Seq=1 Ack=7 Win=64240 Len=0
25 33.914966 192.168.1.158 64.12.24.50 AIM … 243 AIM Messaging, Outgoing to: Sec558user1
26 33.915486 64.12.24.50 192.168.1.158 TCP 60 443 → 51128 [ACK] Seq=1 Ack=196 Win=64240 Len=0
27 34.006599 192.168.1.158 64.12.24.50 AIM … 94 AIM Messaging, Mini Typing Notifications (MTN)
28 34.006604 64.12.24.50 192.168.1.158 TCP 60 443 → 51128 [ACK] Seq=1 Ack=236 Win=64240 Len=0
29 34.023247 64.12.24.50 192.168.1.158 AIM … 263 AIM Generic, Rate Change
30 34.025532 64.12.25.91 192.168.1.159 TLSv1 333 Application Data
31 34.025537 64.12.24.50 192.168.1.158 AIM … 92 AIM Messaging, Acknowledge
32 34.026804 192.168.1.158 64.12.24.50 TCP 60 51128 → 443 [ACK] Seq=236 Ack=210 Win=62780 Len=0
33 34.026809 192.168.1.158 64.12.24.50 TCP 60 51128 → 443 [ACK] Seq=236 Ack=248 Win=62742 Len=0
34 34.075142 192.168.1.159 64.12.25.91 TLSv1 93 Application Data
35 34.076072 64.12.25.91 192.168.1.159 TCP 60 443 → 1221 [ACK] Seq=280 Ack=40 Win=64240 Len=0
Frame 25: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
Ethernet II, Src: HewlettPacka_45:a4:bb (00:12:79:45:a4:bb), Dst: VMware_b0:8d:62 (00:0c:29:b0:8d:62)
Internet Protocol Version 4, Src: 192.168.1.158, Dst: 64.12.24.50
Transmission Control Protocol, Src Port: 51128, Dst Port: 443, Seq: 7, Ack: 1, Len: 189
AOL Instant Messenger
AIM Messaging, Outgoing
ICBM Cookie: 3436323837373800
Message Channel ID: 0x0001
Buddy: Sec558user1
TLV: Message Block
TLV: Server Ack Requested

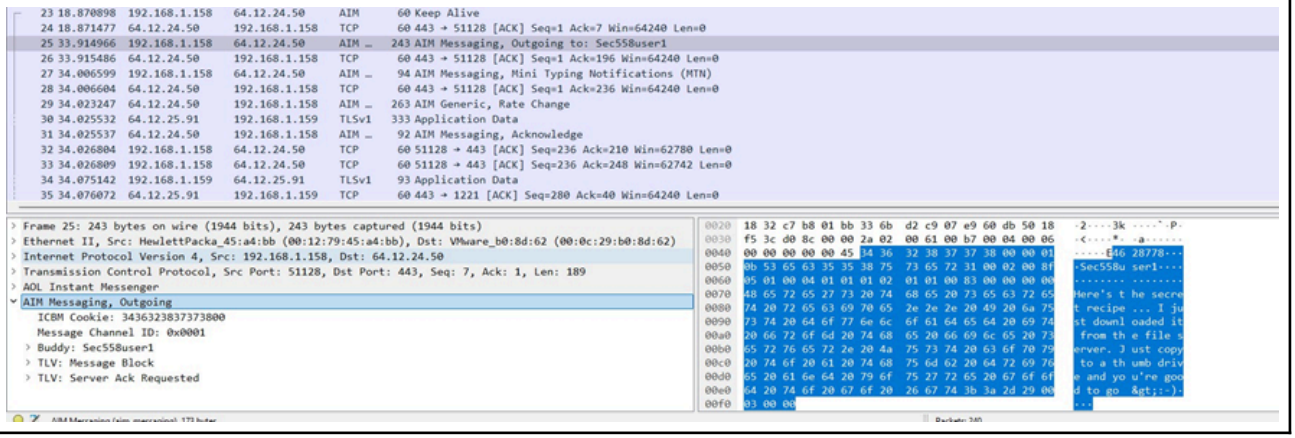

ValueMessage: Here's the secret recipe... I just downloaded it from the file server. Just copy to
Features: 0x0501
Features Length: 4
Features: 01010102
Block info: 0x0101
Block length: 131
Block Character set: 0x0000
Block Character subset: 0x0000
Message: Here's the secret recipe... I just downloaded it from the file server. Just copy to a
TLV: Server Ack Requested
Value ID: Server Ack Requested (0x0003)
Text item (text), 143 bytes

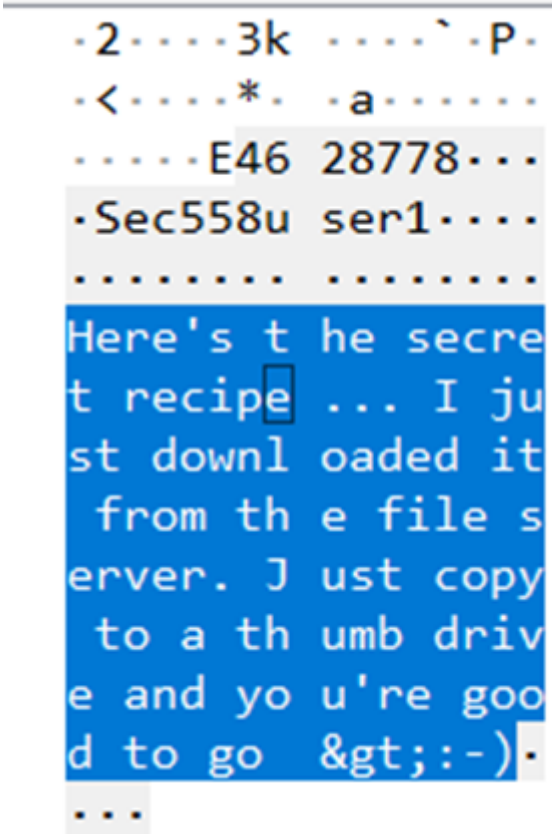

Wireshark · Follow TCP Stream (tcp.stream eq 2) · evidence01 (7).pcap
Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go >:-)
recipe.docx.
thanks dude
can't wait to sell it on ebay
see you in hawaii!

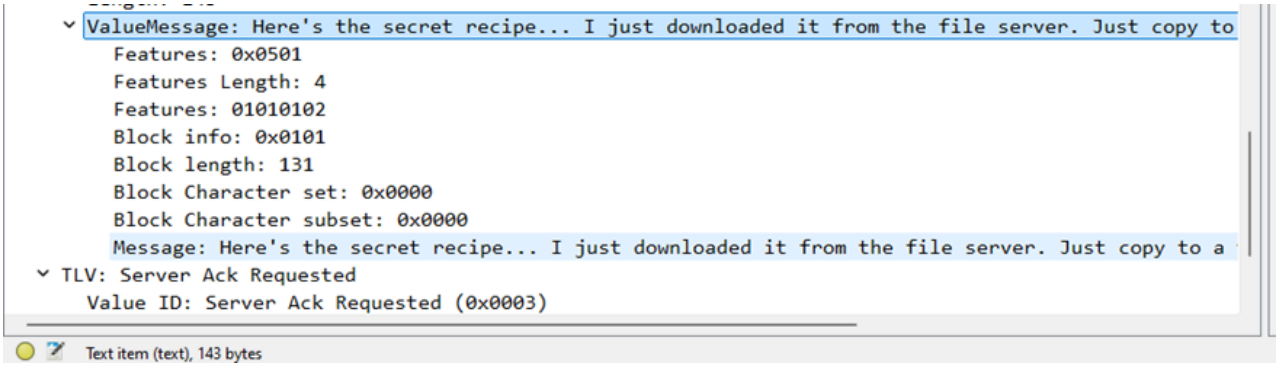


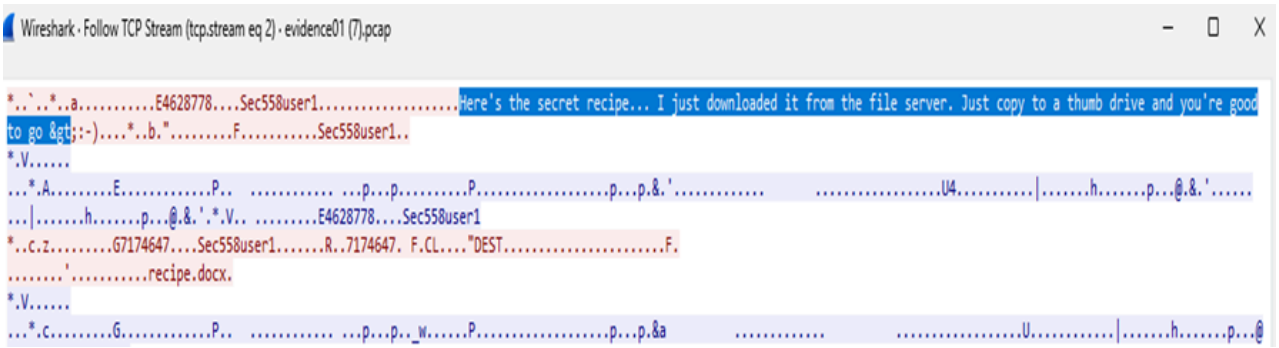


2. What was the first comment in the captured IM conversation?

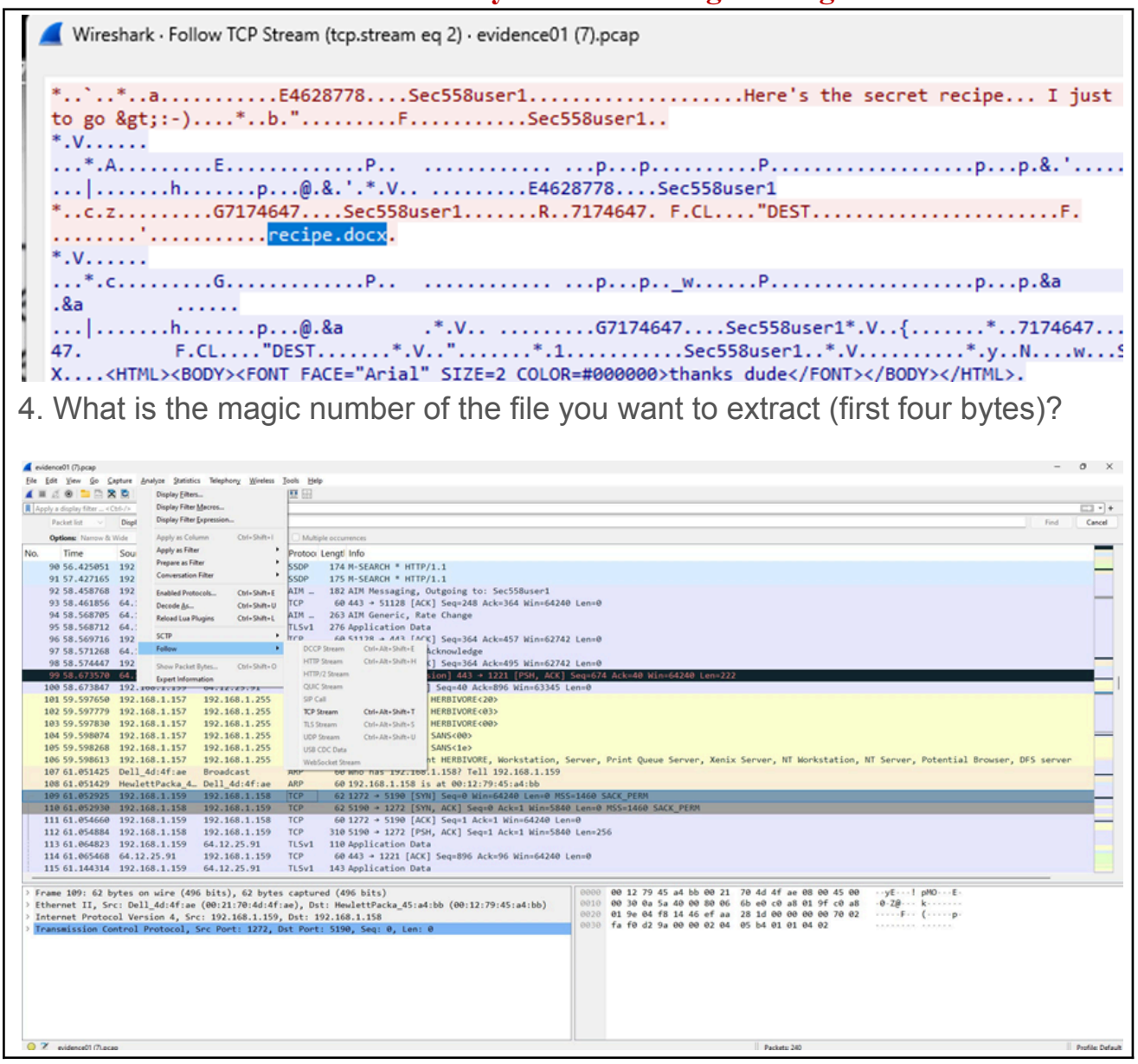




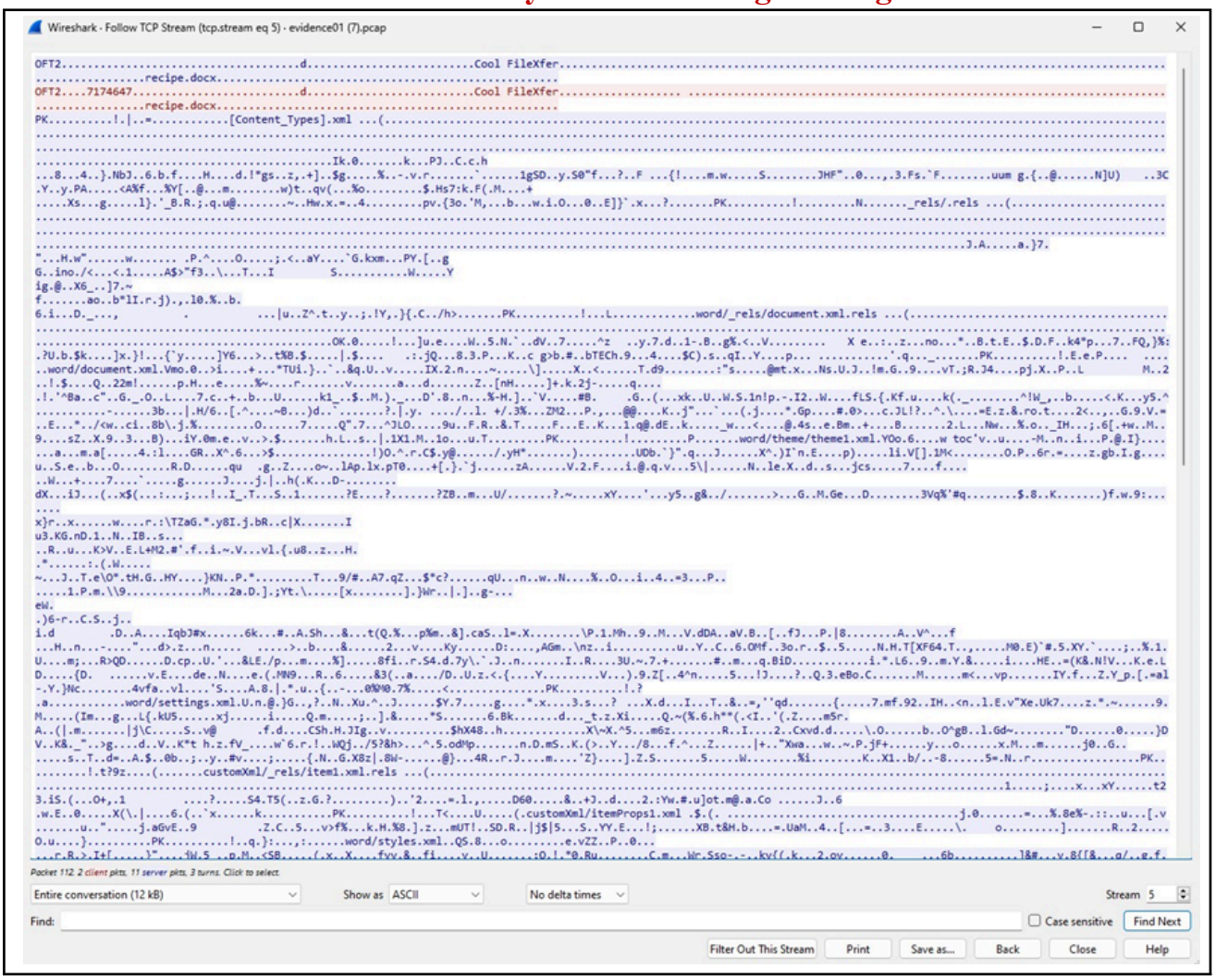


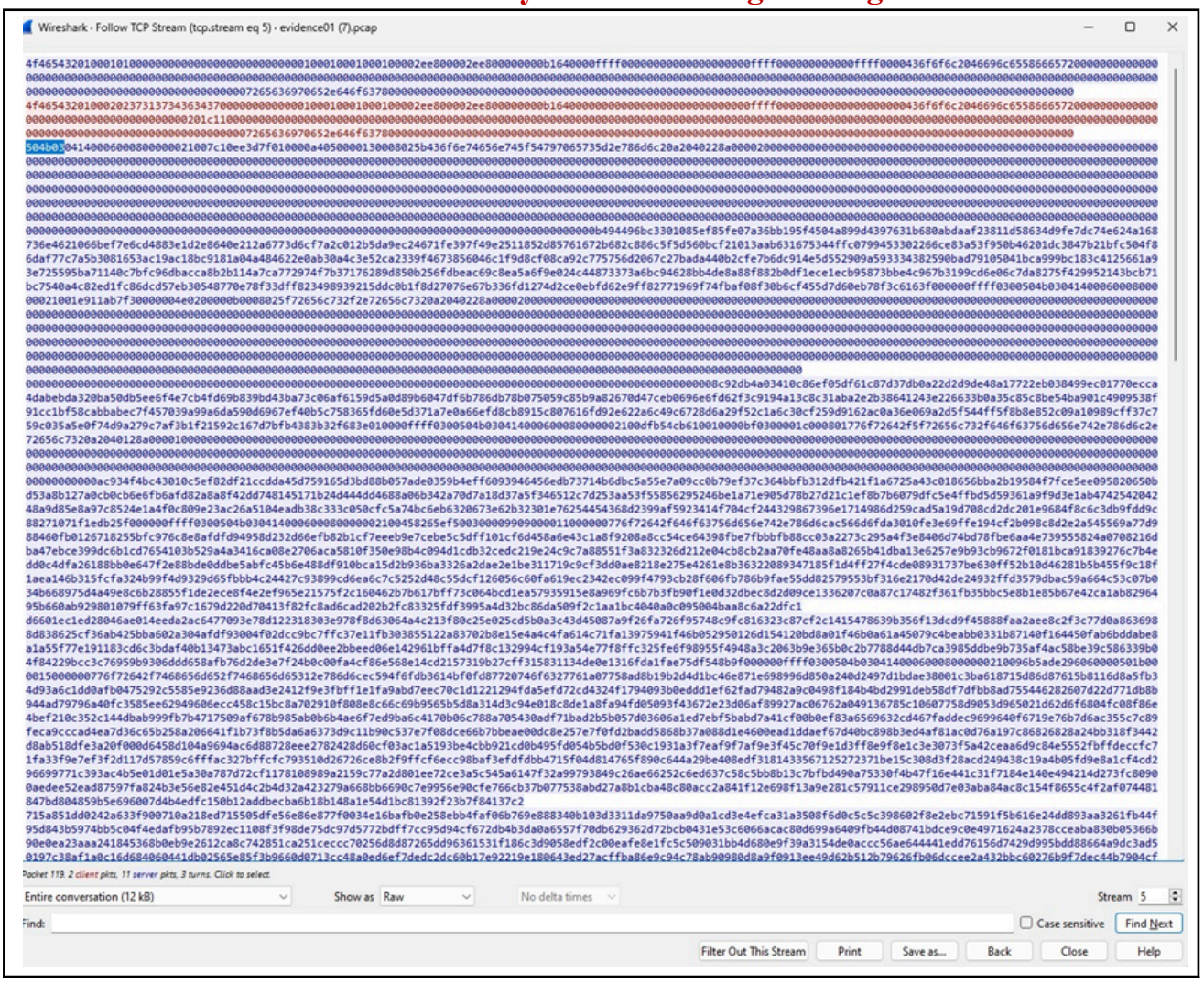


3. What is the name of the file Ann transferred?

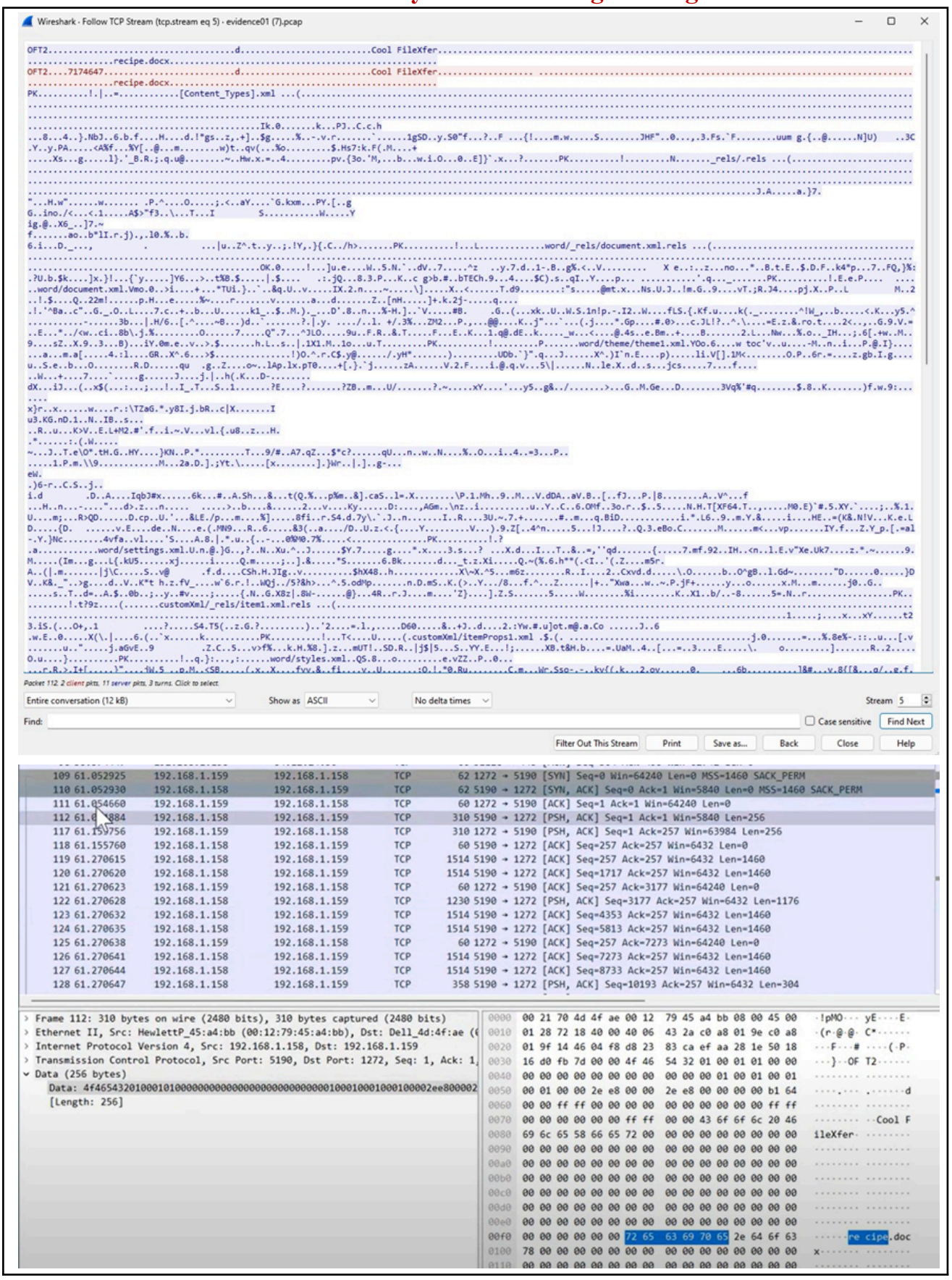


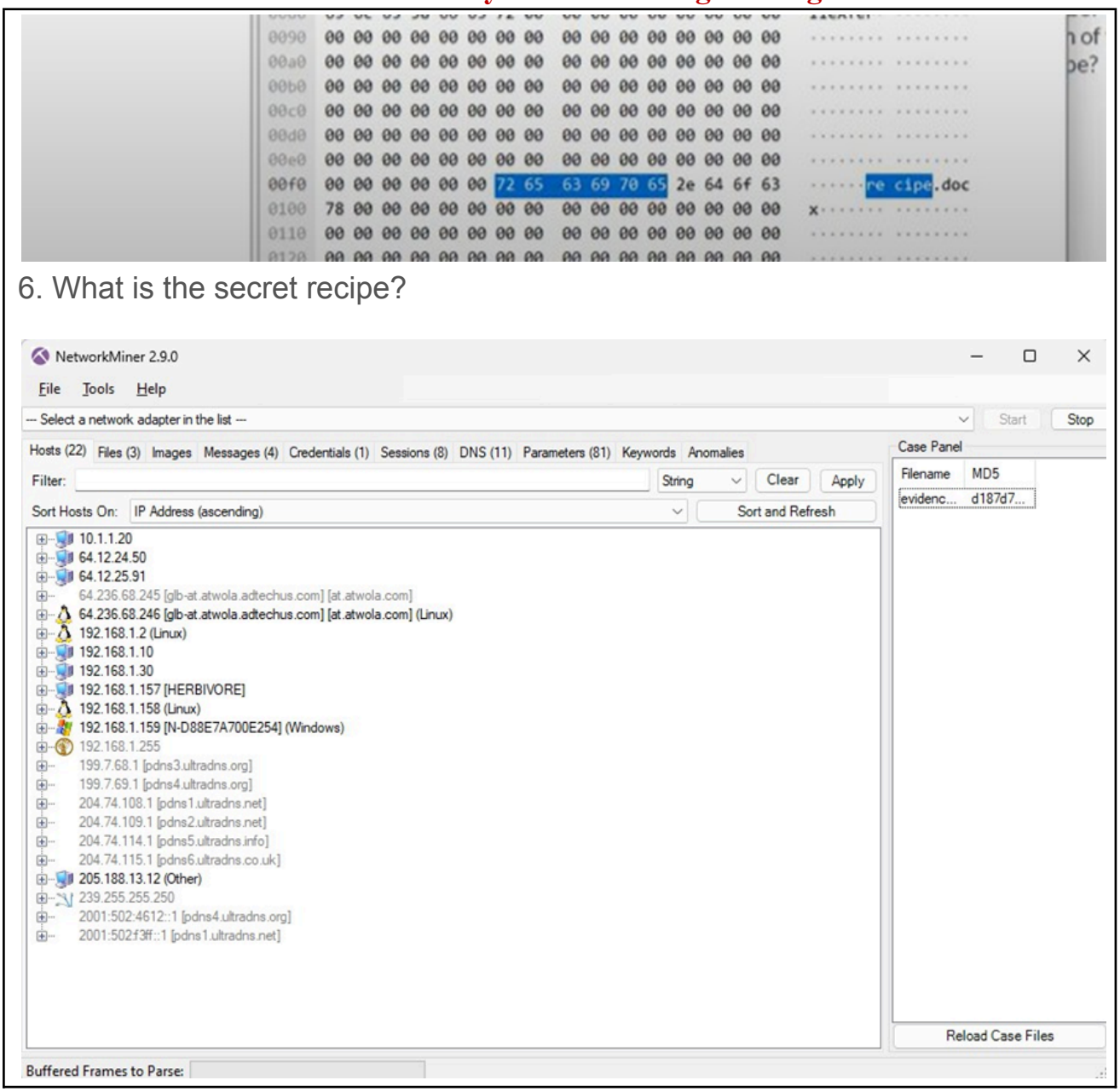
4. What is the magic number of the file you want to extract (first four bytes)?


Wireshark · Follow TCP Stream (tcp.stream eq 5) · evidence01 (7).pcap
Packet 112. 2 client pkts, 11 server pkts, 3 turns. Click to select.
Entire conversation (12 kB)
Show as ASCII
No delta times
Stream 5
Find:
Case sensitive
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

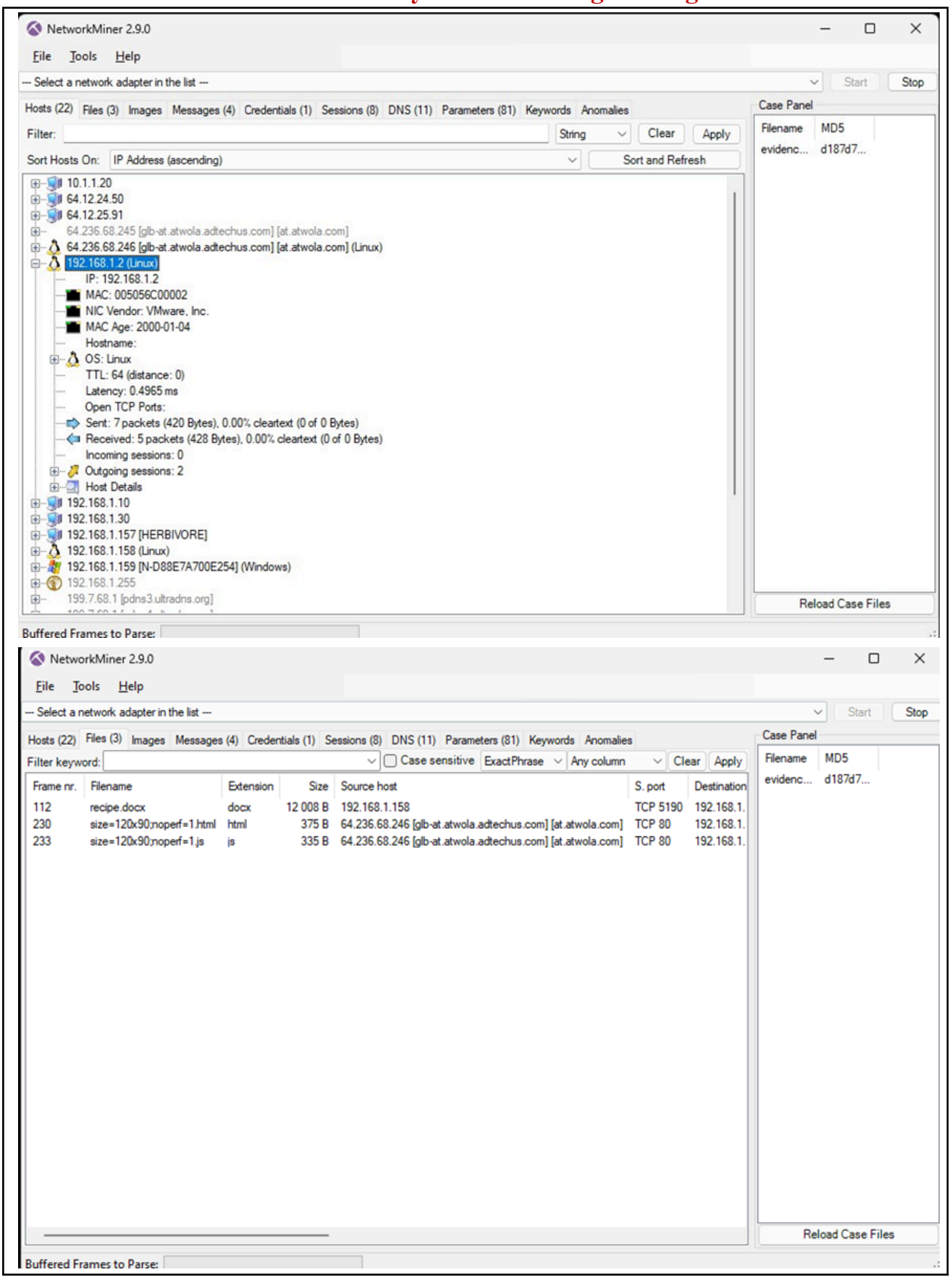

Wireshark · Follow TCP Stream (tcp.stream eq 5) · evidence01 (7).pcap
Packet 119. 2 client pkts, 11 server pkts, 3 turns. Click to select.
Entire conversation (12 kB)
Show as Raw
No delta times
Stream 5
Find:
Case sensitive
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

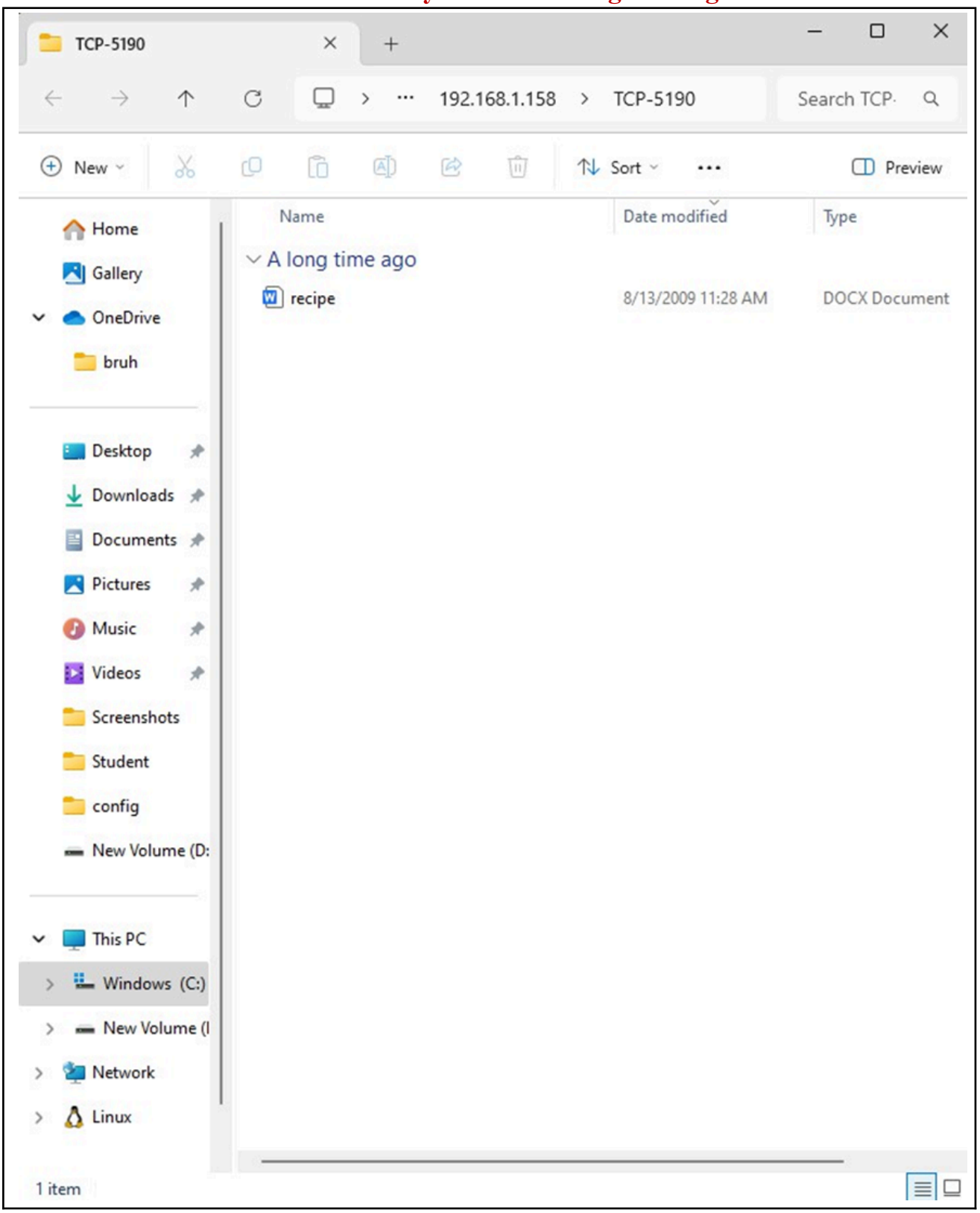
5. What was the MD5sum of the file?

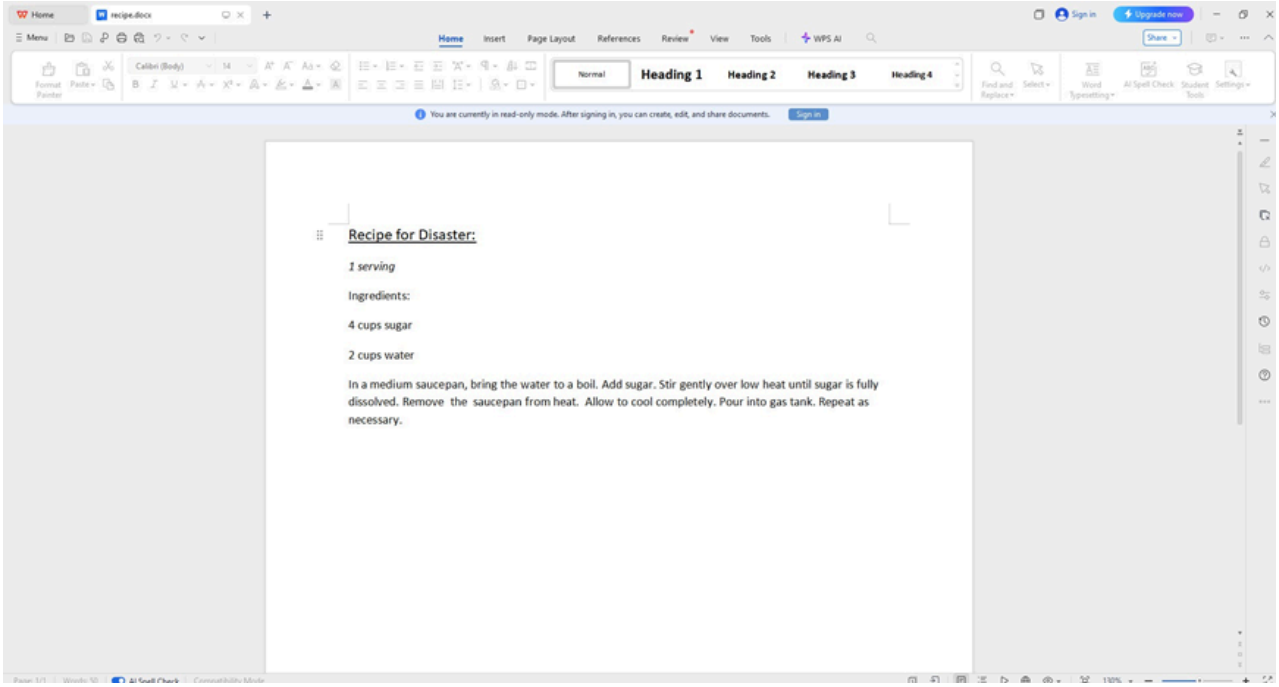

Wireshark · Follow TCP Stream (tcp.stream eq 5) · evidence01 (7).pcap
Entire conversation (12 kB)
Show as ASCII
No delta times
Stream 5
Find:
Case sensitive
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
109 61.052925 192.168.1.159 192.168.1.158 TCP 62 1272 → 5190 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
110 61.052930 192.168.1.159 192.168.1.158 TCP 62 5190 → 1272 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
111 61.054660 192.168.1.159 192.168.1.158 TCP 60 1272 → 5190 [ACK] Seq=1 Ack=1 Win=64240 Len=0
112 61.0 884 192.168.1.159 192.168.1.158 TCP 310 5190 → 1272 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=256
117 61.1 756 192.168.1.159 192.168.1.158 TCP 310 1272 → 5190 [PSH, ACK] Seq=1 Ack=257 Win=63984 Len=256
118 61.155760 192.168.1.159 192.168.1.158 TCP 60 5190 → 1272 [ACK] Seq=257 Ack=257 Win=6432 Len=0
119 61.270615 192.168.1.159 192.168.1.158 TCP 1514 5190 → 1272 [ACK] Seq=257 Ack=257 Win=6432 Len=1460
120 61.270620 192.168.1.159 192.168.1.158 TCP 1514 5190 → 1272 [ACK] Seq=1717 Ack=257 Win=6432 Len=1460
121 61.270623 192.168.1.159 192.168.1.158 TCP 60 1272 → 5190 [ACK] Seq=257 Ack=3177 Win=64240 Len=0
122 61.270628 192.168.1.159 192.168.1.158 TCP 1230 5190 → 1272 [PSH, ACK] Seq=3177 Ack=257 Win=6432 Len=1176
123 61.270632 192.168.1.159 192.168.1.158 TCP 1514 5190 → 1272 [ACK] Seq=4353 Ack=257 Win=6432 Len=1460
124 61.270635 192.168.1.159 192.168.1.158 TCP 1514 5190 → 1272 [ACK] Seq=5813 Ack=257 Win=6432 Len=1460
125 61.270638 192.168.1.159 192.168.1.158 TCP 60 1272 → 5190 [ACK] Seq=257 Ack=7273 Win=64240 Len=0
126 61.270641 192.168.1.159 192.168.1.158 TCP 1514 5190 → 1272 [ACK] Seq=7273 Ack=257 Win=6432 Len=1460
127 61.270644 192.168.1.159 192.168.1.158 TCP 1514 5190 → 1272 [ACK] Seq=8733 Ack=257 Win=6432 Len=1460
128 61.270647 192.168.1.159 192.168.1.158 TCP 358 5190 → 1272 [PSH, ACK] Seq=10193 Ack=257 Win=6432 Len=304
Frame 112: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits)
Ethernet II, Src: HewlettP_45:a4:bb (00:12:79:45:a4:bb), Dst: Dell_4d:4f:ae (
Internet Protocol Version 4, Src: 192.168.1.158, Dst: 192.168.1.159
Transmission Control Protocol, Src Port: 5190, Dst Port: 1272, Seq: 1, Ack: 1,
Data (256 bytes)
Data: 4f4654320100010100000000000000000000000000010001000100010002ee800002
[Length: 256]
0000 00 21 70 4d 4f ae 00 12 79 45 a4 bb 08 00 45 00
0010 01 28 72 18 40 00 40 06 43 2a c0 a8 01 9e c0 a8
0020 01 9f 14 46 04 f8 d8 23 83 ca ef aa 28 1e 50 18
0030 16 d0 fb 7d 00 00 4f 46 54 32 01 00 01 01 00 00
0040 00 00 00 00 00 00 00 00 00 00 01 00 01 00 01 00
0050 00 01 00 00 2e e8 00 00 2e e8 00 00 00 00 b1 64
0060 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 ff ff
0070 00 00 00 00 00 00 ff ff 00 00 43 6f 6f 6c 20 46
0080 69 6c 65 58 66 65 72 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0 00 00 00 00 00 00 72 65 63 69 70 65 2e 64 6f 63
0100 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00



6. What is the secret recipe?


NetworkMiner 2.9.0
File Tools Help
-- Select a network adapter in the list --
Start Stop
Hosts (22) Files (3) Images Messages (4) Credentials (1) Sessions (8) DNS (11) Parameters (81) Keywords Anomalies
Filter:
String Clear Apply
Sort Hosts On: IP Address (ascending)
Sort and Refresh
10.1.1.20
64.12.24.50
64.12.25.91
64.236.68.245 [glb-at.atwola.adtechus.com] [at.atwola.com]
64.236.68.246 [glb-at.atwola.adtechus.com] [at.atwola.com] (Linux)
192.168.1.2 (Linux)
IP: 192.168.1.2
MAC: 005056C00002
NIC Vendor: VMware, Inc.
MAC Age: 2000-01-04
Hostname:
OS: Linux
TTL: 64 (distance: 0)
Latency: 0.4965 ms
Open TCP Ports:
Sent: 7 packets (420 Bytes), 0.00% cleartext (0 of 0 Bytes)
Received: 5 packets (428 Bytes), 0.00% cleartext (0 of 0 Bytes)
Incoming sessions: 0
Outgoing sessions: 2
Host Details
192.168.1.10
192.168.1.30
192.168.1.157 [HERBIVORE]
192.168.1.158 (Linux)
192.168.1.159 [N-D88E7A700E254] (Windows)
192.168.1.255
199.7.68.1 [pdns3.ultradns.org]
Case Panel
Filename MD5
evidenc... d187d7...
Reload Case Files
Buffered Frames to Parse:
NetworkMiner 2.9.0
File Tools Help
-- Select a network adapter in the list --
Start Stop
Hosts (22) Files (3) Images Messages (4) Credentials (1) Sessions (8) DNS (11) Parameters (81) Keywords Anomalies
Filter keyword:
Case sensitive ExactPhrase Any column Clear Apply
Frame nr. Filename Extension Size Source host S. port Destination
112 recipe.docx docx 12 008 B 192.168.1.158 TCP 5190 192.168.1.
230 size=120x90;noperf=1.html html 375 B 64.236.68.246 [glb-at.atwola.adtechus.com] [at.atwola.com] TCP 80 192.168.1.
233 size=120x90;noperf=1.js js 335 B 64.236.68.246 [glb-at.atwola.adtechus.com] [at.atwola.com] TCP 80 192.168.1.
Case Panel
Filename MD5
evidenc... d187d7...
Reload Case Files
Buffered Frames to Parse:


TCP-5190
192.168.1.158
TCP-5190
Search TCP-
New
Sort
Preview
Home
Gallery
OneDrive
bruh
Desktop
Downloads
Documents
Pictures
Music
Videos
Screenshots
Student
config
New Volume (D:
This PC
Windows (C:)
New Volume (I
Network
Linux
Name
Date modified
Type
A long time ago
recipe
8/13/2009 11:28 AM
DOCX Document
1 item



Conclusion:

In this lab, we explored the importance of network security tools like Wireshark and Network Miner in identifying and analyzing network-based incidents. Through the case study, we learned how these tools can be used to capture and examine network traffic, extract useful information, and solve real-life security puzzles. By comparing the results from both tools, we observed that while Wireshark offers detailed packet-level analysis, Network Miner provides a more forensic, high-level view of network activities. Ultimately, understanding and utilizing these tools are essential in securing and investigating network environments effectively.

Post-Lab Questions:

8.1 Explain the different challenges in handling network based incidents.
8.2 Discuss the tools used for monitoring the network traffic.
8.3 What do you understand by packet sniffing?

8.1 Explain the different challenges in handling network based incidents.

ANS- Network-based incidents can be difficult to handle due to several factors, including:

1. Scale and Complexity: Modern networks can be vast and complex, consisting of numerous devices, subnets, firewalls, and endpoints. This makes it challenging to quickly identify and isolate incidents.

2. Detection and Visibility: Detecting network-based incidents often requires continuous monitoring, and the attackers may use sophisticated methods to avoid detection. Limited visibility into encrypted traffic or traffic from trusted sources can hinder timely detection.

3. Volume of Traffic: High network traffic volumes can make it difficult to discern between normal and malicious activities, especially during Distributed Denial of Service (DDoS) attacks, where the network is flooded with unnecessary traffic.

4. Attribution: It can be hard to attribute network-based incidents to specific attackers, as they might use anonymizing techniques (e.g., VPNs, proxies, or botnets), obfuscating their identities and location.

5. Response Time: Time-sensitive incidents, such as data breaches or DDoS attacks, require rapid responses to mitigate damage. However, the time required to analyze and respond can be hindered by insufficient resources or a lack of skilled personnel.

6. Legal and Regulatory Compliance: Ensuring that incident handling complies with various legal frameworks and regulatory requirements (like GDPR or HIPAA) can add complexity. For example, when handling sensitive data or monitoring communication, privacy issues might arise.

7. Coordination Across Teams: Network-based incidents may require coordination between various teams, including IT, legal, and security teams, which can be difficult in large organizations or when the network is distributed across multiple locations.

8. Changing Threat Landscape: The tactics, techniques, and procedures (TTPs) of cybercriminals and threat actors are constantly evolving. This means that the tools and processes used to manage incidents may quickly become outdated or ineffective.

8.2 Discuss the tools used for monitoring the network traffic.

ANS-Various tools are used for monitoring network traffic to ensure the integrity, security, and performance of a network. These tools include:

1. Wireshark: This is a popular packet analyzer that captures and inspects network traffic in real-time. It can decode and display protocol information from network packets, which is valuable for troubleshooting and investigating incidents.

2. Snort: A widely used open-source intrusion detection/prevention system (IDS/IPS) that analyzes network traffic for signs of malicious activity or policy violations. Snort can also be configured for network monitoring to detect abnormal traffic patterns.

3. Nagios: A network monitoring tool that provides insights into the status of various network devices (routers, switches, etc.), servers, and services. It can send alerts based on predefined thresholds.

4. SolarWinds Network Performance Monitor: A comprehensive tool that provides real-time monitoring of network traffic, performance metrics, and bandwidth usage. It helps identify bottlenecks and issues in network infrastructure.

5. Tcpdump: Another packet analysis tool that is often used in conjunction with Wireshark. It is command-line-based and captures network traffic, which can then be analyzed to detect suspicious or unauthorized activity.

6. PRTG Network Monitor: A network monitoring solution that tracks traffic, bandwidth, and overall performance. It provides customizable alerts and dashboards, helping administrators monitor network health and detect anomalies.

What do you understand by packet sniffing?

ANS-Packet sniffing is a method of detecting and assessing packet data sent over a network. It can be used by administrators for network monitoring and security.

However, packet sniffing tools can also be used by hackers to spy or steal confidential data.

The packet sniffing process is achieved by analyzing data packets sent through Transmission Control Protocol/Internet Protocol (TCP/IP) — the protocol that connects devices to wired or wireless networks. These data packets can include different types of traffic sent across a network, such as login details and passwords, as well as technical data like IP addresses.

IT professionals use packet sniffers for network troubleshooting by checking for harmful data packets. They also gain insights around bandwidth usage — for example, revealing which applications are the most intensive — to detect hidden issues affecting network performance.

Network administrators can also use packet sniffers to “sniff” websites that are being visited, the type of content being consumed, and communications like email.