K. J. Somaiya School of Engineering, Mumbai-77

Batch: A-4	**Roll No.:** 16010122151
Experiment No. 08	
Signature of the Staff In-charge with date	

TITLE: Illustrate and Compare network security mechanisms

AIM: Working with sample real life cases related to Network security and forensics using tool – Wireshark and Network Miner.

OUTCOME: Student will be able to

CO4: Illustrate and Compare network security mechanisms

Theory: Write about wireshark and Network Miner

S

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 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

K. J. Somaiya School of Engineering, Mumbai-77

https://www.netresec.com/?page=TutorialNMP
https://www.youtube.com/watch?v=qTaOZrDnMzQ
https://www.youtube.com/watch?v=nC5m2WO8JJk

Output(s):

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

A: Sec558user1

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

A: 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?

A: recipe.docx

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

A: 504b0304

5. What was the MD5sum of the file?

A:8350582774e1d4dbe1d61d64c89e0ea1

6. What is the secret recipe?

Recipe for Disaster:

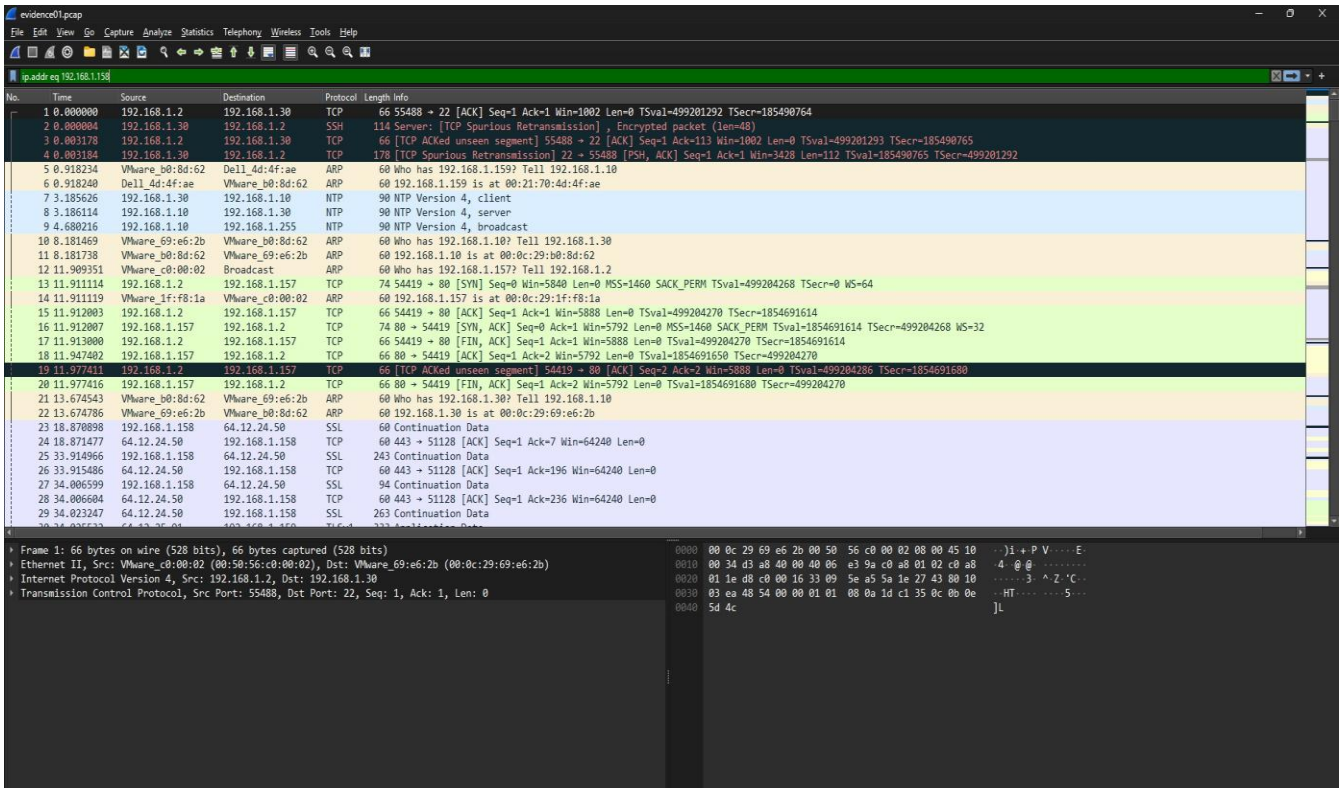
1 serving

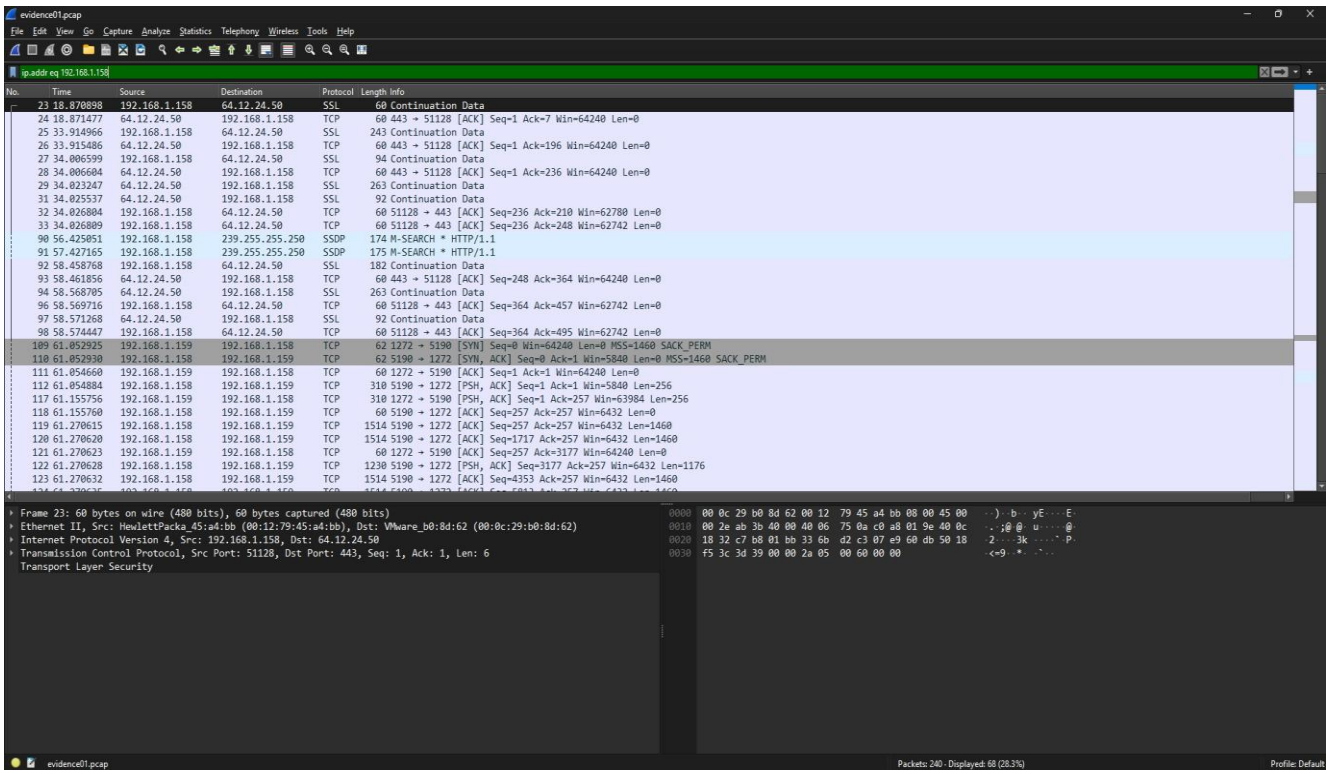
Ingredients:

4 cups sugar

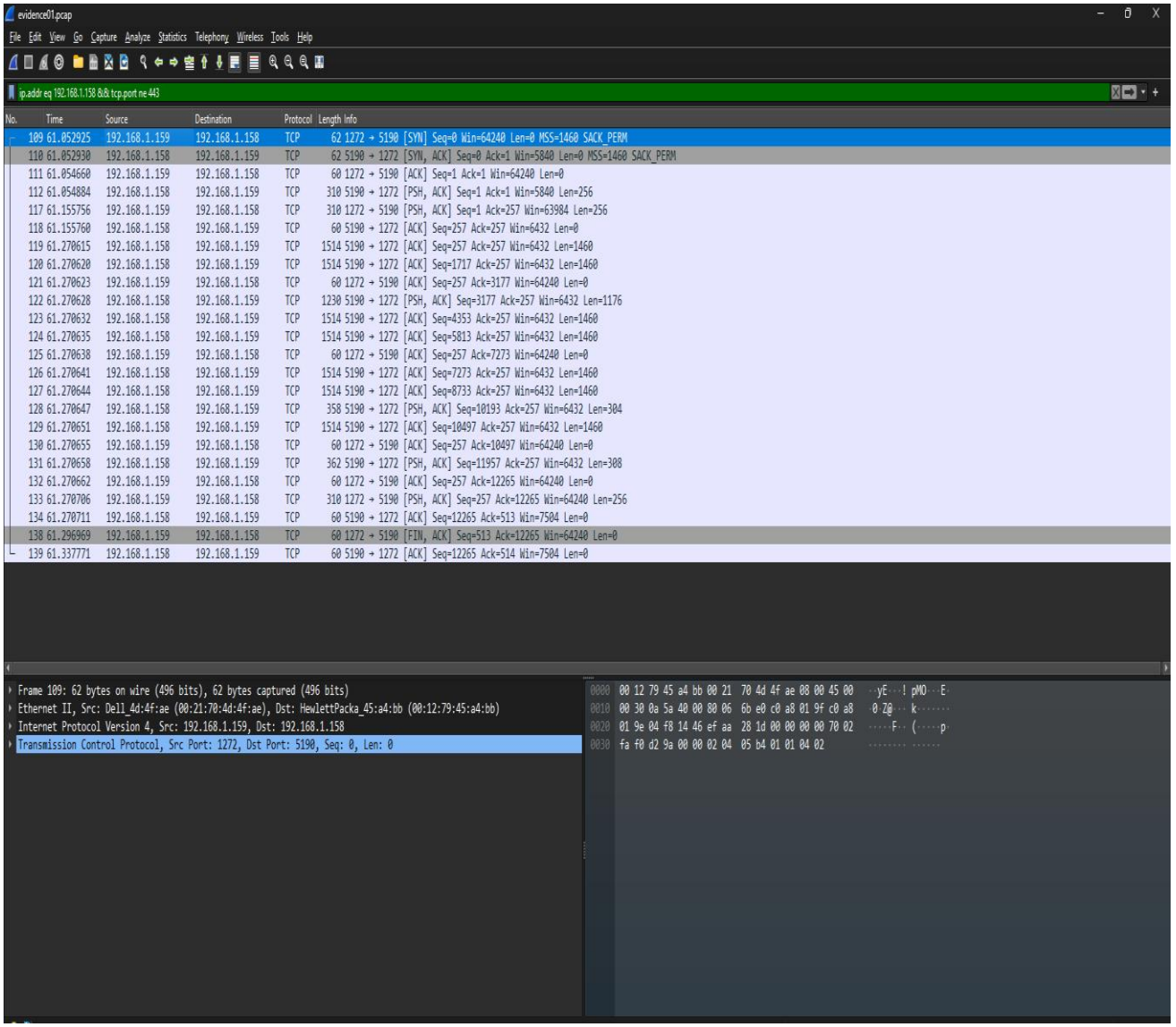
2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

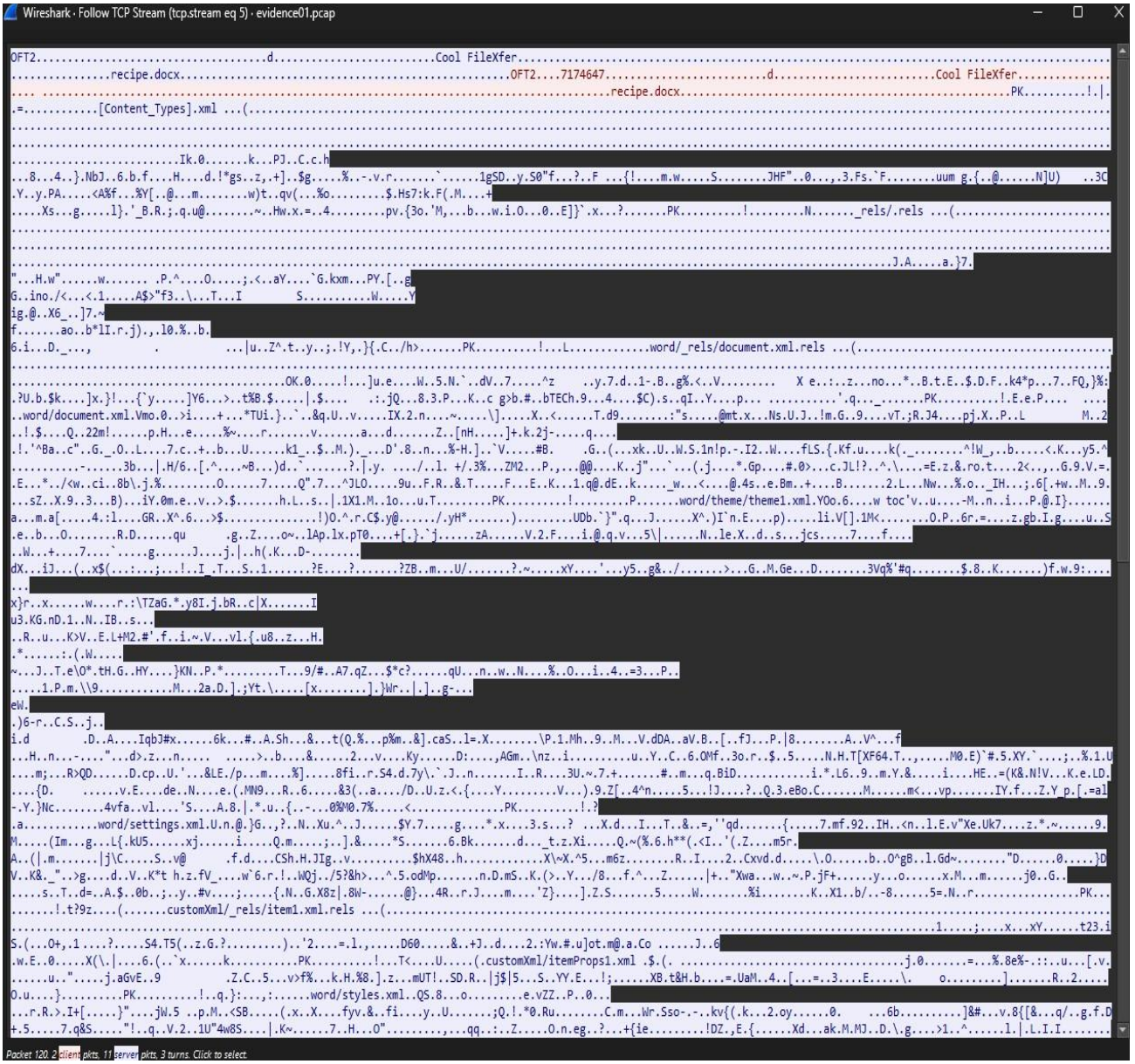

evidence01.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr eq 192.168.1.158
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.2 192.168.1.30 TCP 66 55488 → 22 [ACK] Seq=1 Ack=1 Win=1002 Len=0 TSval=499201292 TSecr=185490764
2 0.000004 192.168.1.30 192.168.1.2 SSH 114 Server: [TCP Spurious Retransmission] , Encrypted packet (len=48)
3 0.003178 192.168.1.2 192.168.1.30 TCP 66 [TCP ACKed unseen segment] 55488 → 22 [ACK] Seq=1 Ack=113 Win=1002 Len=0 TSval=499201293 TSecr=185490765
4 0.003184 192.168.1.30 192.168.1.2 TCP 178 [TCP Spurious Retransmission] 22 → 55488 [PSH, ACK] Seq=1 Ack=1 Win=3428 Len=112 TSval=185490765 TSecr=499201292
5 0.918234 VMware_b0:8d:62 Dell_4d:4f:ae ARP 60 Who has 192.168.1.159? Tell 192.168.1.10
6 0.918240 Dell_4d:4f:ae VMware_b0:8d:62 ARP 60 192.168.1.159 is at 00:21:70:4d:4f:ae
7 3.185626 192.168.1.30 192.168.1.10 NTP 90 NTP Version 4, client
8 3.186114 192.168.1.10 192.168.1.30 NTP 90 NTP Version 4, server
9 4.680216 192.168.1.10 192.168.1.255 NTP 90 NTP Version 4, broadcast
10 8.181469 VMware_69:e6:2b VMware_b0:8d:62 ARP 60 Who has 192.168.1.10? Tell 192.168.1.30
11 8.181738 VMware_b0:8d:62 VMware_69:e6:2b ARP 60 192.168.1.10 is at 00:0c:29:b0:8d:62
12 11.909351 VMware_c0:00:02 Broadcast ARP 60 Who has 192.168.1.157? Tell 192.168.1.2
13 11.911114 192.168.1.2 192.168.1.157 TCP 74 54419 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=499204268 TSecr=0 WS=64
14 11.911119 VMware_1f:f8:1a VMware_c0:00:02 ARP 60 192.168.1.157 is at 00:0c:29:1f:f8:1a
15 11.912003 192.168.1.2 192.168.1.157 TCP 66 54419 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=499204270 TSecr=1854691614
16 11.912007 192.168.1.157 192.168.1.2 TCP 74 80 → 54419 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=1854691614 TSecr=499204268 WS=32
17 11.913000 192.168.1.2 192.168.1.157 TCP 66 54419 → 80 [FIN, ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=499204270 TSecr=1854691614
18 11.947402 192.168.1.157 192.168.1.2 TCP 66 80 → 54419 [ACK] Seq=1 Ack=2 Win=5792 Len=0 TSval=1854691650 TSecr=499204270
19 11.977411 192.168.1.2 192.168.1.157 TCP 66 [TCP ACKed unseen segment] 54419 → 80 [ACK] Seq=2 Ack=2 Win=5888 Len=0 TSval=499204286 TSecr=1854691680
20 11.977416 192.168.1.157 192.168.1.2 TCP 66 80 → 54419 [FIN, ACK] Seq=1 Ack=2 Win=5792 Len=0 TSval=1854691680 TSecr=499204270
21 13.674543 VMware_b0:8d:62 VMware_69:e6:2b ARP 60 Who has 192.168.1.30? Tell 192.168.1.10
22 13.674786 VMware_69:e6:2b VMware_b0:8d:62 ARP 60 192.168.1.30 is at 00:0c:29:69:e6:2b
23 18.870898 192.168.1.158 64.12.24.50 SSL 60 Continuation Data
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 SSL 243 Continuation Data
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 SSL 94 Continuation Data
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 SSL 263 Continuation Data
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: VMware_c0:00:02 (00:50:56:c0:00:02), Dst: VMware_69:e6:2b (00:0c:29:69:e6:2b)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.30
Transmission Control Protocol, Src Port: 55488, Dst Port: 22, Seq: 1, Ack: 1, Len: 0
0000 00 0c 29 69 e6 2b 00 50 56 c0 00 02 08 00 45 10
0010 00 34 d3 a8 40 00 40 06 e3 9a c0 a8 01 02 c0 a8
0020 01 1e d8 c0 00 16 33 09 5e a5 5a 1e 27 43 80 10
0030 03 ea 48 54 00 00 01 01 08 0a 1d c1 35 0c 0b 0e
0040 5d 4c


evidence01.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr eq 192.168.1.158
No. Time Source Destination Protocol Length Info
23 18.870898 192.168.1.158 64.12.24.50 SSL 60 Continuation Data
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 SSL 243 Continuation Data
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 SSL 94 Continuation Data
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 SSL 263 Continuation Data
31 34.025537 64.12.24.50 192.168.1.158 SSL 92 Continuation Data
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
90 56.425051 192.168.1.158 239.255.255.250 SSDP 174 M-SEARCH * HTTP/1.1
91 57.427165 192.168.1.158 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1
92 58.458768 192.168.1.158 64.12.24.50 SSL 182 Continuation Data
93 58.461856 64.12.24.50 192.168.1.158 TCP 60 443 → 51128 [ACK] Seq=248 Ack=364 Win=64240 Len=0
94 58.568705 64.12.24.50 192.168.1.158 SSL 263 Continuation Data
96 58.569716 192.168.1.158 64.12.24.50 TCP 60 51128 → 443 [ACK] Seq=364 Ack=457 Win=62742 Len=0
97 58.571268 64.12.24.50 192.168.1.158 SSL 92 Continuation Data
98 58.574447 192.168.1.158 64.12.24.50 TCP 60 51128 → 443 [ACK] Seq=364 Ack=495 Win=62742 Len=0
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 192.168.1.158 192.168.1.159 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 61.054884 192.168.1.158 192.168.1.159 TCP 310 5190 → 1272 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=256
117 61.155756 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 192.168.1.158 192.168.1.159 TCP 60 5190 → 1272 [ACK] Seq=257 Ack=257 Win=6432 Len=0
119 61.270615 192.168.1.158 192.168.1.159 TCP 1514 5190 → 1272 [ACK] Seq=257 Ack=257 Win=6432 Len=1460
120 61.270620 192.168.1.158 192.168.1.159 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 192.168.1.158 192.168.1.159 TCP 1230 5190 → 1272 [PSH, ACK] Seq=3177 Ack=257 Win=6432 Len=1176
123 61.270632 192.168.1.158 192.168.1.159 TCP 1514 5190 → 1272 [ACK] Seq=4353 Ack=257 Win=6432 Len=1460
Frame 23: 60 bytes on wire (480 bits), 60 bytes captured (480 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: 1, Ack: 1, Len: 6
Transport Layer Security
0000 00 0c 29 b0 8d 62 00 12 79 45 a4 bb 08 00 45 00
0010 00 2e ab 3b 40 00 40 06 75 0a c0 a8 01 9e 40 0c
0020 18 32 c7 b8 01 bb 33 6b d2 c3 07 e9 60 db 50 18
0030 f5 3c 3d 39 00 00 2a 05 00 60 00 00
evidence01.pcap
Packets: 240 · Displayed: 68 (28.3%)
Profile: Default

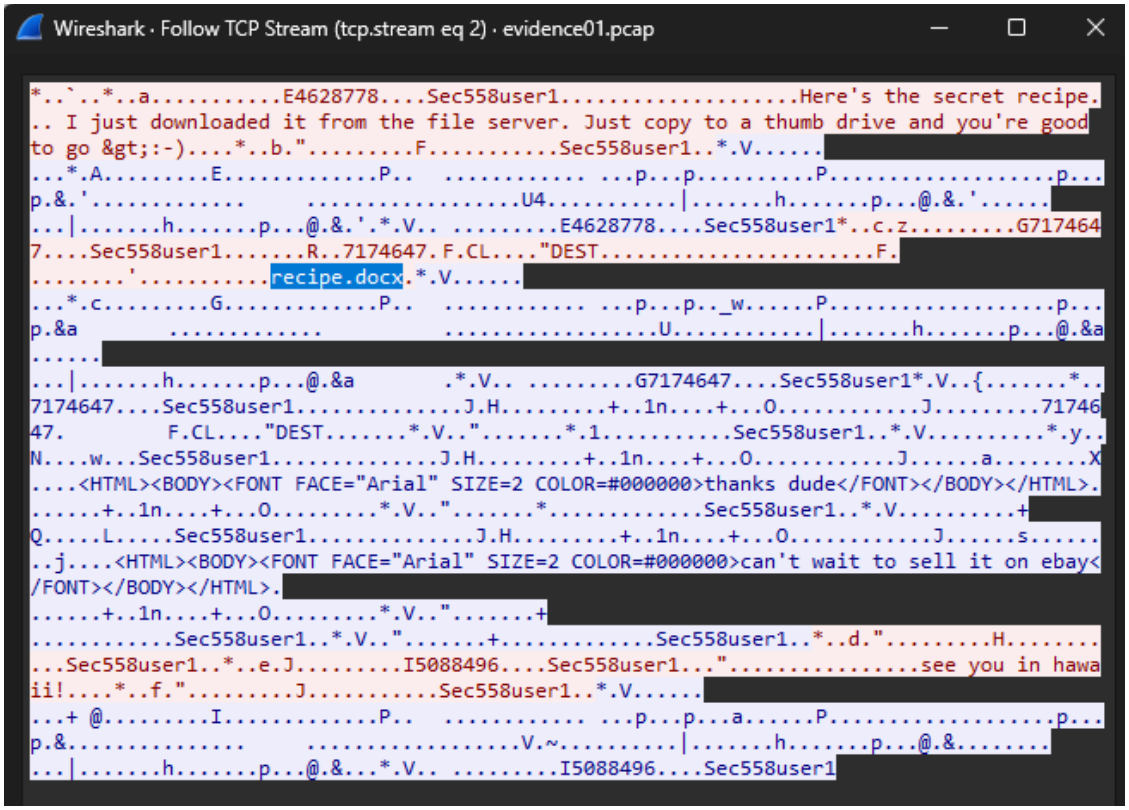
K. J. Somaiya School of Engineering, Mumbai-77



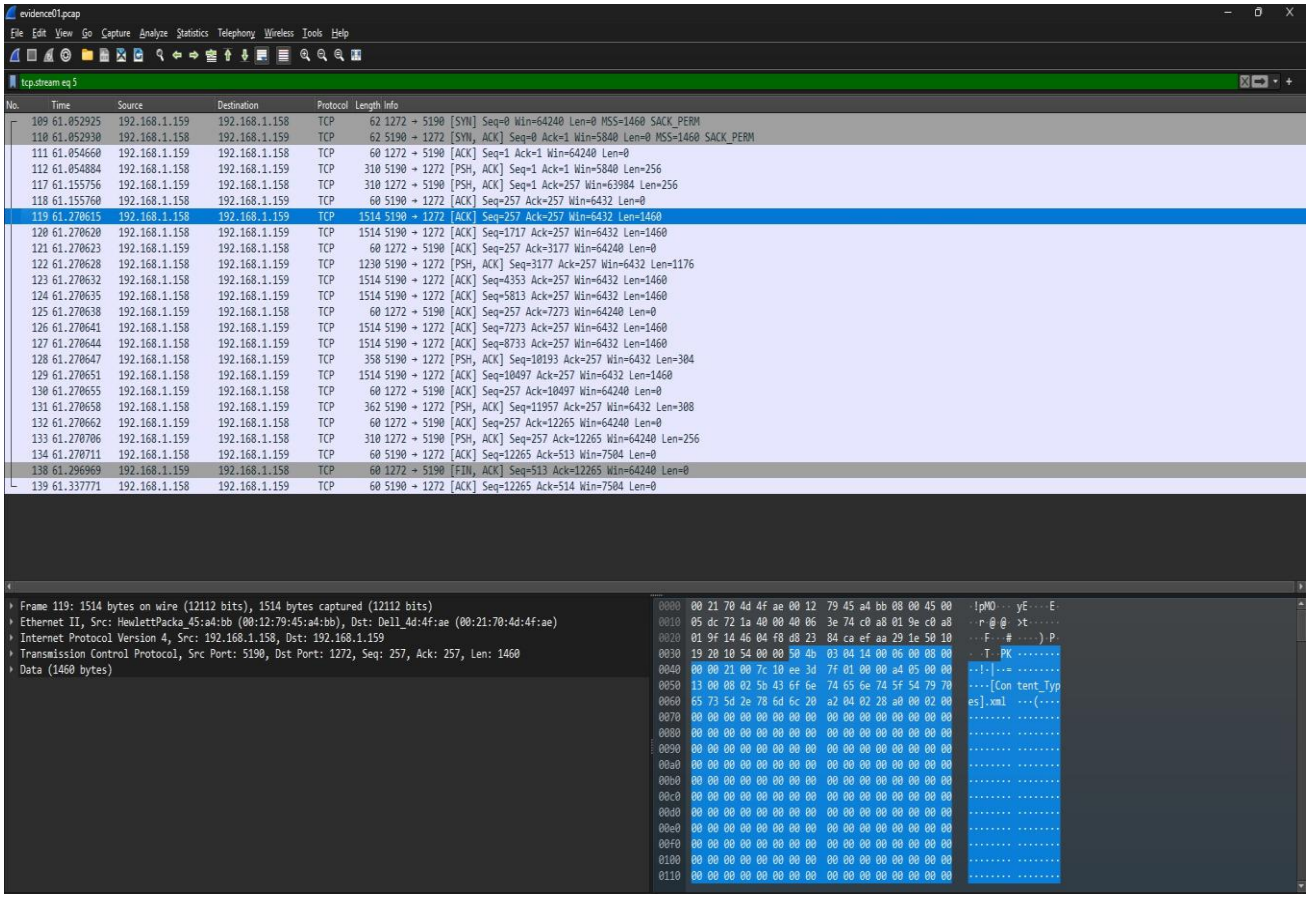
K. J. Somaiya School of Engineering, Mumbai-77

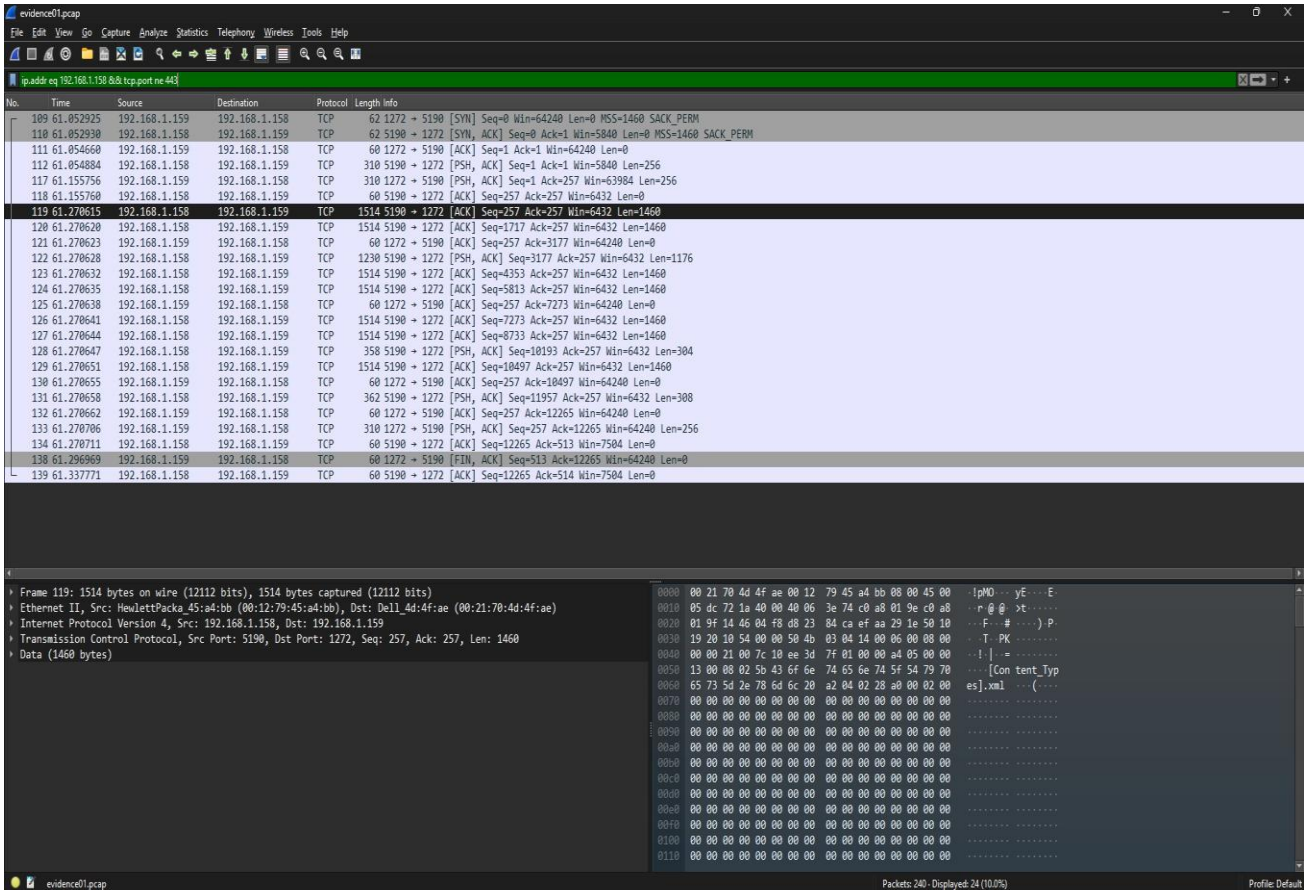


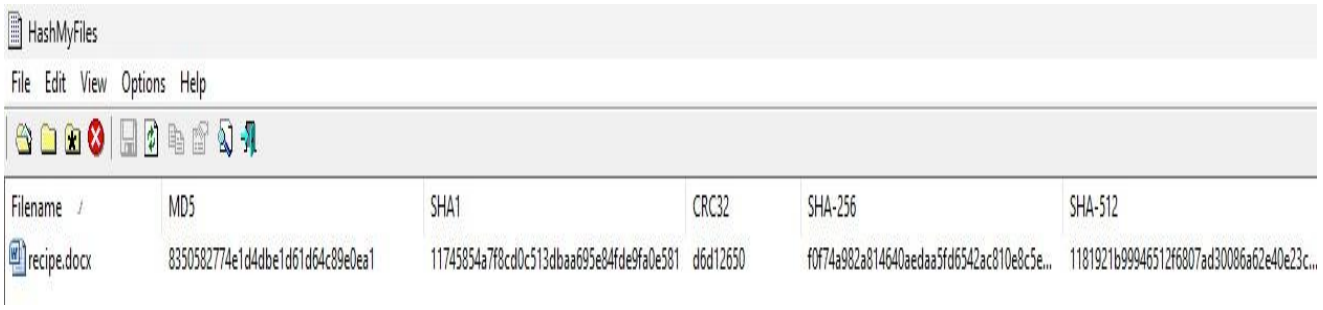
K. J. Somaiya School of Engineering, Mumbai-77



K. J. Somaiya School of Engineering, Mumbai-77







Post Lab Questions:

Q1 Explain the different challenges in handling network based incidents.

ANS: Handling network-based incidents can be complex due to various factors. Some of the main challenges include:

1. **Scale and Complexity**: Modern networks are often large and complex, involving multiple devices, protocols, and communication methods. This makes identifying the origin and scope of an incident difficult, especially in distributed networks.

2. **Anonymity and Obfuscation**: Attackers may use techniques to mask their identity or obscure their activity. This can involve methods like IP spoofing, using VPNs or Tor, or manipulating packet headers, making it harder for network administrators to trace the attacker.

3. **Encrypted Traffic**: The use of encryption protocols like HTTPS and VPNs can make it challenging to inspect network traffic for malicious activities. Although encryption ensures data privacy, it can also prevent security tools from analyzing the content of traffic for threats.

4. **Volume of Data**: Network traffic often involves huge amounts of data. Identifying and isolating malicious traffic from normal traffic within this volume can be overwhelming without the proper tools and methodologies.

5. **Time Sensitivity**: Network-based incidents may require a rapid response to prevent data breaches, loss of service, or damage to systems. This can add pressure to incident responders, requiring them to act quickly, but still accurately, to contain the issue.

6. **Coordination Between Teams**: Dealing with network-based incidents often requires collaboration between different departments (e.g., security, IT, legal, management). Miscommunication or delays in coordination can worsen the impact of the incident.

7. **False Positives and Alerts**: Network monitoring tools can sometimes produce too many alerts, making it difficult for responders to prioritize genuine threats. False positives can lead to wasted resources, and important issues may get overlooked.

8. **Legal and Compliance Issues**: Depending on the nature of the incident, organizations may face legal and compliance challenges. Handling sensitive data during an incident could raise concerns, especially in regulated industries like healthcare or finance.

8.2 Discuss the tools used for monitoring the network traffic.

ANS.: Monitoring network traffic is essential for identifying potential issues, preventing security breaches, and maintaining optimal performance. Some common tools used for network traffic monitoring include:

1. **Wireshark:** A popular packet analyzer used to capture and inspect network packets. It allows detailed examination of the protocol stack and helps troubleshoot network issues.

2. **SolarWinds Network Performance Monitor:** A comprehensive network monitoring solution that helps in identifying performance

issues, outages, and other network-related incidents. It provides real-time monitoring and alerting.

3. **Nagios:** An open-source monitoring tool that provides insights into network traffic, server performance, and uptime. It supports custom plugin integrations for monitoring various network devices and services.

4. **PRTG Network Monitor:** A tool that offers real-time monitoring of bandwidth, network devices, and systems. It can alert administrators to issues like high traffic volume or failures.

5. **Zabbix:** An open-source monitoring solution that tracks network performance, servers, and other hardware. It can alert users to potential issues with network traffic and systems.

6. **ntopng:** An advanced network traffic monitoring tool that provides a detailed, real-time overview of network traffic, highlighting key metrics and potential security risks.

7. **Tcpdump:** A command-line network packet analyzer similar to Wireshark but more lightweight. It is often used for troubleshooting network problems and analyzing network traffic.

8. **WiSpy:** A tool for monitoring and troubleshooting wireless network traffic. It helps network administrators identify congestion, interference, and other issues affecting Wi-Fi performance.

9. **Bro (Zeek):** A powerful open-source network analysis framework that provides real-time monitoring and deep analysis of network traffic, helping detect network intrusions and anomalies.

8.3 What do you understand by packet sniffing?

ANS.: Packet sniffing refers to the process of intercepting and analyzing packets of data that travel over a network. By capturing these packets, network administrators, security professionals, or attackers can analyze the content, identify issues, or discover vulnerabilities in the network. Packet sniffing tools can monitor traffic and capture data such as:

- **Headers:** Metadata like IP addresses, ports, and protocols used.
- **Payloads:** The actual data being transmitted between devices.
- **Traffic Patterns:** Which devices are communicating and how much data is being transferred.

While packet sniffing can be a legitimate method used for network troubleshooting or performance monitoring, it can also be exploited for malicious purposes, such as eavesdropping on sensitive data or intercepting communication. In a cybersecurity context, it's crucial to secure the network and employ encryption protocols to prevent unauthorized packet sniffing activities.

Packet sniffing tools, like Wireshark or Tcpdump, are commonly used for network diagnostics, analyzing network protocols, and detecting potential security threats like Man-in-the-Middle (MITM) attacks or unauthorized data access. However, their use without authorization is illegal and can lead to severe privacy violations.

Conclusion: Thus, from this experiment, we learnt about usage of some network security tools like Wireshark and Network Miner and implemented the same through a case study.