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

**Date of submission: 23/04/2025**
**Batch: C1 Roll No.: 16010122323**
**Div: C**
**Student Name: Vedansh Savla**
**Experiment No: 8**
**Staff In-charge: SHIVANI DEOSTHALE**

**TITLE:** Illustrate and Compare network security mechanisms
**AIM**: Working with sample real life cases related to Network security and forensics using tools – Wireshark and Network Miner.
**OUTCOME:** Student will be able to
**CO4:** Illustrate and Compare network security mechanisms

**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

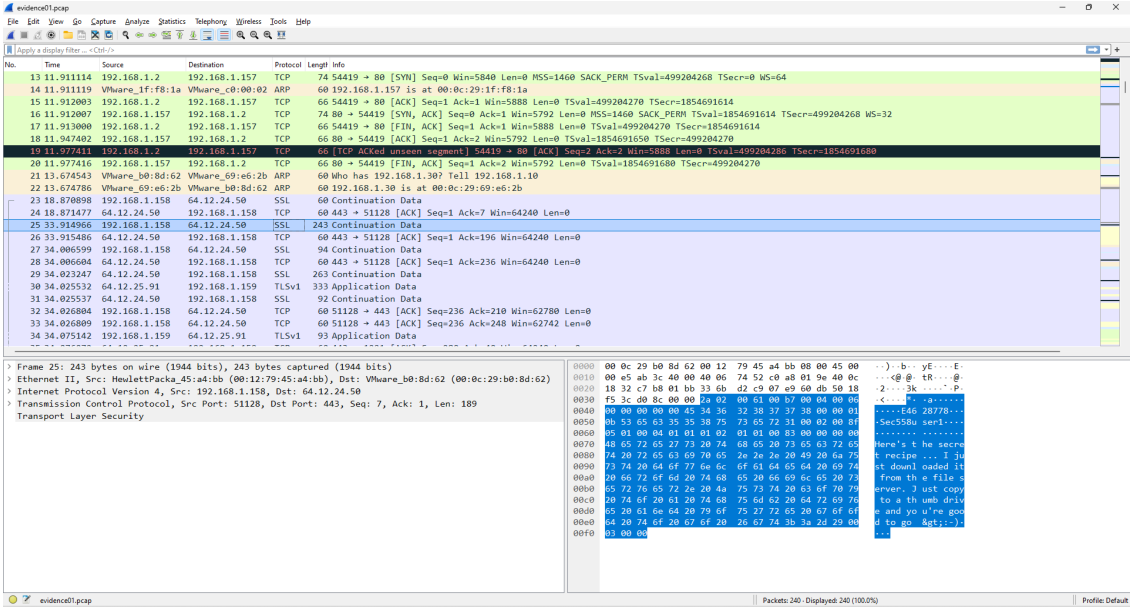
## Output(s):

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

**Ans:** sec558user1

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

**Ans:** 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 >:-)



```
No.  Time       Source            Destination     Protocol Length Info
  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
  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   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
  34 34.075142  192.168.1.159     64.12.25.91     TLSv1    93 Application Data
```

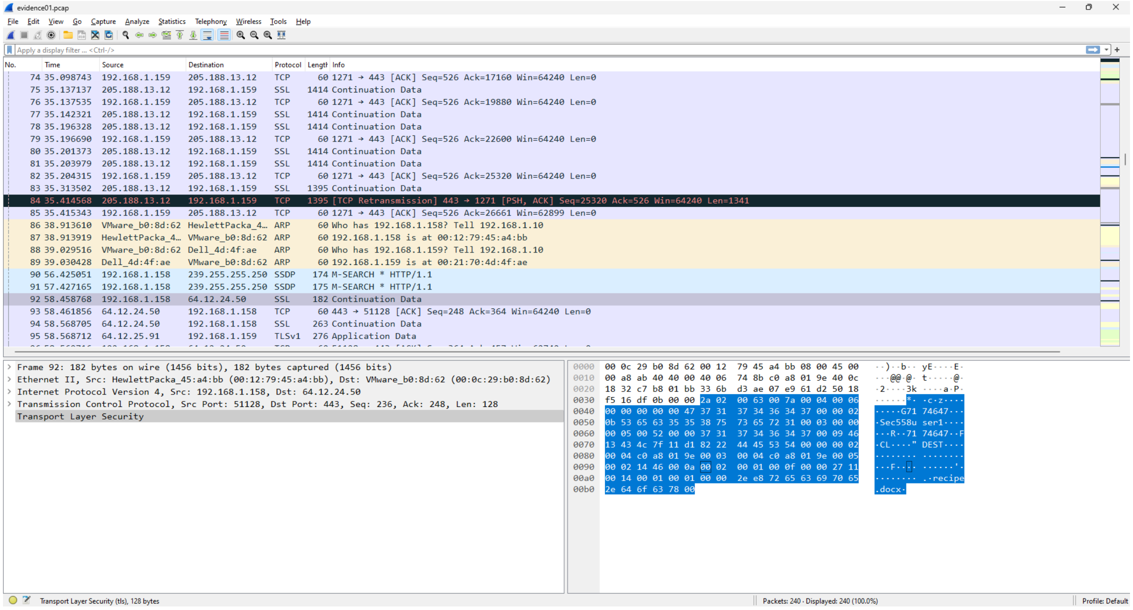
```
> Frame 25: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
> Ethernet II, Src: HewlettPacka_45:a4:bb (00:12:79:45:a4:bb), Dst: VMware_b0:8d:62 (00:0c:29:b0:8d:62)
> Internet Protocol Version 4, Src: 192.168.1.158, Dst: 64.12.24.50
> Transmission Control Protocol, Src Port: 51128, Dst Port: 443, Seq: 7, Ack: 1, Len: 189
  Transport Layer Security
```

```
0000  00 0c 29 b0 8d 62 00 12  79 45 a4 bb 08 00 45 00   ··)··b·· yE····E·
0010  00 e5 ab 3c 40 00 40 06  74 52 c0 a8 01 9e 40 0c   ···<@·@· tR····@·
0020  18 32 c7 b8 01 bb 33 6b  d2 c9 07 e9 60 db 50 18   ·2····3k ····`·P·
0030  f5 3c d0 8c 00 00 2a 02  00 61 00 b7 00 04 00 06   ·<····*· ·a······
0040  00 00 00 00 00 45 34 36  32 38 37 37 38 00 00 01   ·····E46 28778···
0050  0b 53 65 63 35 35 38 75  73 65 72 31 00 02 00 8f   ·Sec558u ser1····
0060  05 01 00 04 01 01 01 02  01 01 00 83 00 00 00 00   ········ ········
0070  48 65 72 65 27 73 20 74  68 65 20 73 65 63 72 65   Here's t he secre
0080  74 20 72 65 63 69 70 65  2e 2e 2e 20 49 20 6a 75   t recipe ... I ju
0090  73 74 20 64 6f 77 6e 6c  6f 61 64 65 64 20 69 74   st downl oaded it
00a0  20 66 72 6f 6d 20 74 68  65 20 66 69 6c 65 20 73    from th e file s
00b0  65 72 76 65 72 2e 20 4a  75 73 74 20 63 6f 70 79   erver. J ust copy
00c0  20 74 6f 20 61 20 74 68  75 6d 62 20 64 72 69 76    to a th umb driv
00d0  65 20 61 6e 64 20 79 6f  75 27 72 65 20 67 6f 6f   e and yo u're goo
00e0  64 20 74 6f 20 67 6f 20  26 67 74 3b 3a 2d 29 00   d to go  &gt;:-)·
00f0  03 00 00                                           ···
```

```
evidence01.pcap        Packets: 240 · Displayed: 240 (100.0%)        Profile: Default
```

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

**Ans:** recipe.docx



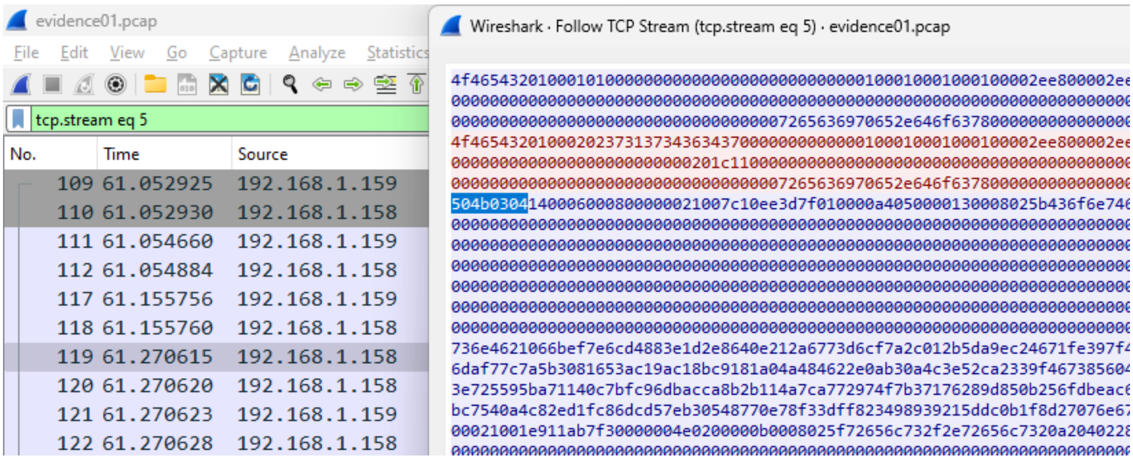
```
No.  Time       Source            Destination       Protocol Length Info
  74 35.098743  192.168.1.159     205.188.13.12     TCP       60 1271 → 443 [ACK] Seq=526 Ack=17160 Win=64240 Len=0
  75 35.137137  205.188.13.12     192.168.1.159     SSL     1414 Continuation Data
  76 35.137535  192.168.1.159     205.188.13.12     TCP       60 1271 → 443 [ACK] Seq=526 Ack=19880 Win=64240 Len=0
  77 35.142321  205.188.13.12     192.168.1.159     SSL     1414 Continuation Data
  78 35.196328  205.188.13.12     192.168.1.159     SSL     1414 Continuation Data
  79 35.196690  192.168.1.159     205.188.13.12     TCP       60 1271 → 443 [ACK] Seq=526 Ack=22600 Win=64240 Len=0
  80 35.201373  205.188.13.12     192.168.1.159     SSL     1414 Continuation Data
  81 35.203979  205.188.13.12     192.168.1.159     SSL     1414 Continuation Data
  82 35.204315  192.168.1.159     205.188.13.12     TCP       60 1271 → 443 [ACK] Seq=526 Ack=25320 Win=64240 Len=0
  83 35.313502  205.188.13.12     192.168.1.159     SSL     1395 Continuation Data
  84 35.414568  205.188.13.12     192.168.1.159     TCP     1395 [TCP Retransmission] 443 → 1271 [PSH, ACK] Seq=25320 Ack=526 Win=64240 Len=1341
  85 35.415343  192.168.1.159     205.188.13.12     TCP       60 1271 → 443 [ACK] Seq=526 Ack=26661 Win=62899 Len=0
  86 38.913610  VMware_b0:8d:62   HewlettPacka_4…   ARP       60 Who has 192.168.1.158? Tell 192.168.1.10
  87 38.913919  HewlettPacka_4…   VMware_b0:8d:62   ARP       60 192.168.1.158 is at 00:12:79:45:a4:bb
  88 39.029516  VMware_b0:8d:62   Dell_4d:4f:ae     ARP       60 Who has 192.168.1.159? Tell 192.168.1.10
  89 39.030428  Dell_4d:4f:ae     VMware_b0:8d:62   ARP       60 192.168.1.159 is at 00:21:70:4d:4f:ae
  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
  95 58.568712  64.12.25.91       192.168.1.159     TLSv1    276 Application Data
```

```
> Frame 92: 182 bytes on wire (1456 bits), 182 bytes captured (1456 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: 236, Ack: 248, Len: 128
  Transport Layer Security
```

```
0000  00 0c 29 b0 8d 62 00 12  79 45 a4 bb 08 00 45 00   ··)··b·· yE····E·
0010  00 a8 ab 40 40 00 40 06  74 8b c0 a8 01 9e 40 0c   ···@@·@· t·····@·
0020  18 32 c7 b8 01 bb 33 6b  d3 ae 07 e9 61 d2 50 18   ·2····3k ····a·P·
0030  f5 16 df 0b 00 00 2a 02  00 63 00 7a 00 04 00 06   ······*· ·c·z····
0040  00 00 00 00 00 47 37 31  37 34 36 34 37 00 00 02   ·····G71 74647···
0050  0b 53 65 63 35 35 38 75  73 65 72 31 00 03 00 00   ·Sec558u ser1····
0060  00 05 00 52 00 00 37 31  37 34 36 34 37 00 09 46   ···R··71 74647··F
0070  13 43 4c 7f 11 d1 82 22  44 45 53 54 00 00 00 02   ·CL····" DEST····
0080  00 04 c0 a8 01 9e 00 03  00 04 c0 a8 01 9e 00 05   ········ ········
0090  00 02 14 46 00 0a 00 02  00 01 00 0f 00 00 27 11   ···F···· ······'·
00a0  00 14 00 01 00 01 00 00  2e e8 72 65 63 69 70 65   ········ ..recipe
00b0  2e 64 6f 63 78 00                                  .docx·
```

```
Transport Layer Security (tls), 128 bytes        Packets: 240 · Displayed: 240 (100.0%)        Profile: Default
```

**4.** What is the magic number of the file you want to extract (first four bytes)?
**Ans:** 0x504b0304



tcp.stream eq 5

| No. | Time | Source |
|---|---|---|
| 109 | 61.052925 | 192.168.1.159 |
| 110 | 61.052930 | 192.168.1.158 |
| 111 | 61.054660 | 192.168.1.159 |
| 112 | 61.054884 | 192.168.1.158 |
| 117 | 61.155756 | 192.168.1.159 |
| 118 | 61.155760 | 192.168.1.158 |
| 119 | 61.270615 | 192.168.1.158 |
| 120 | 61.270620 | 192.168.1.158 |
| 121 | 61.270623 | 192.168.1.159 |
| 122 | 61.270628 | 192.168.1.158 |

Wireshark · Follow TCP Stream (tcp.stream eq 5) · evidence01.pcap

```
4f465432010001010000000000000000000000000001000100010001000002ee800002ee
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000007265636970652e646f6378000000000000000
4f46543201000202373137343634370000000000000100010001000100002ee800002ee
0000000000000000000000000201c11000000000000000000000000000000000000000
0000000000000000000000000000000007265636970652e646f6378000000000000000
504b0304140006000800000021007c10ee3d7f010000a405000013000802 5b436f6e746
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
736e4621066bef7e6cd4883e1d2e8640e212a6773d6cf7a2c012b5da9ec24671fe397f4
6daf77c7a5b3081653ac19ac18bc9181a04a484622e0ab30a4c3e52ca2339f4673856O4
3e725595ba71140c7bfc96dbacca8b2b114a7ca772974f7b37176289d850b256fdbeac6
bc7540a4c82ed1fc86dcd57eb30548770e78f33dff823498939215ddc0b1f8d27076e67
00021001e911ab7f30000004e0200000b0008025f72656c732f2e72656c7320a2040228
0000000000000000000000000000000000000000000000000000000000000000000000
```

**5.** What was the MD5sum of the file?
**Ans:** 8350582774e1d4dbe1d61d64c89e0ea1

**6.** What is the secret recipe?
**Ans:**

<u>Recipe for Disaster:</u>

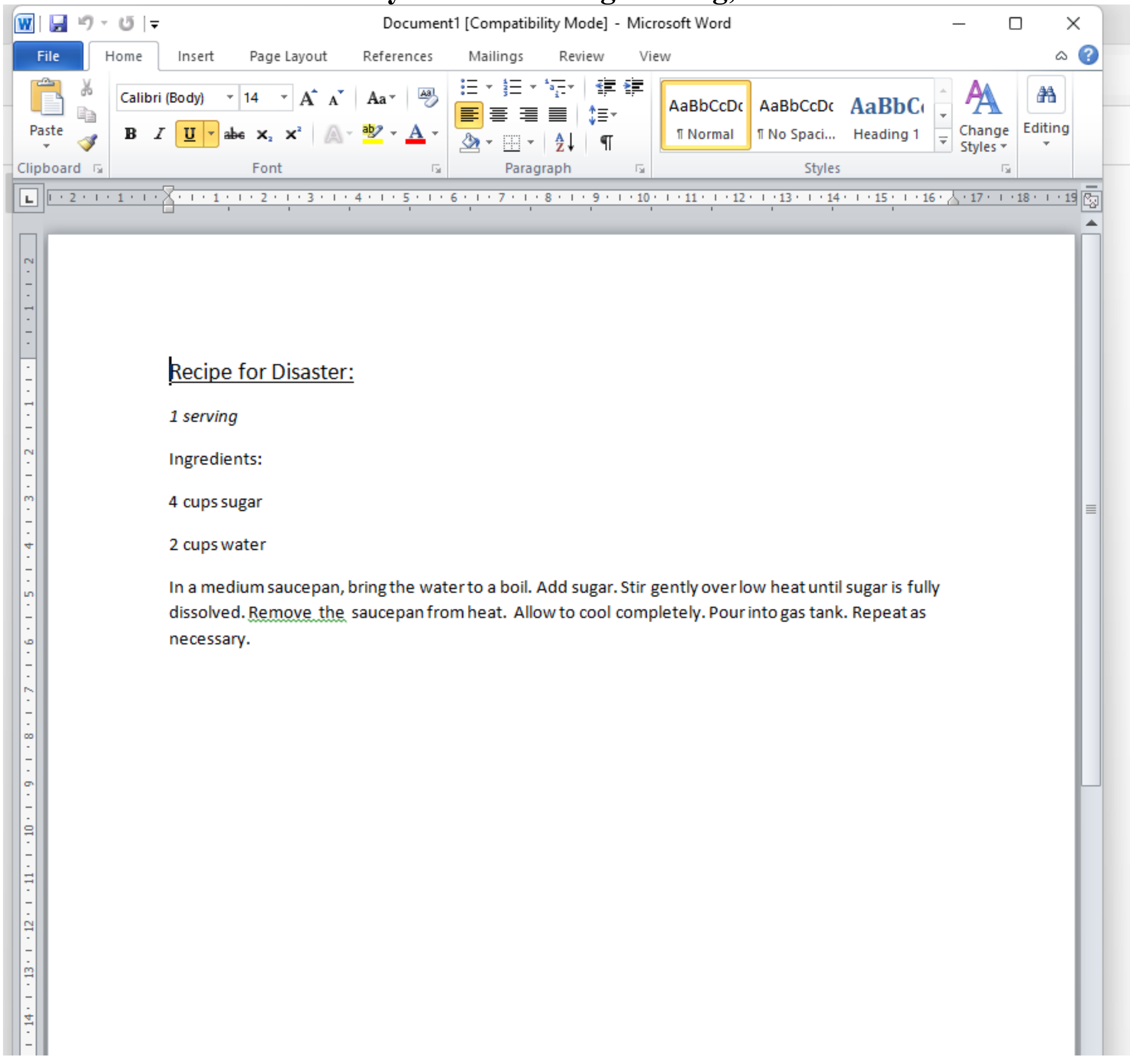
*1 serving*

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.



Recipe for Disaster:

*1 serving*

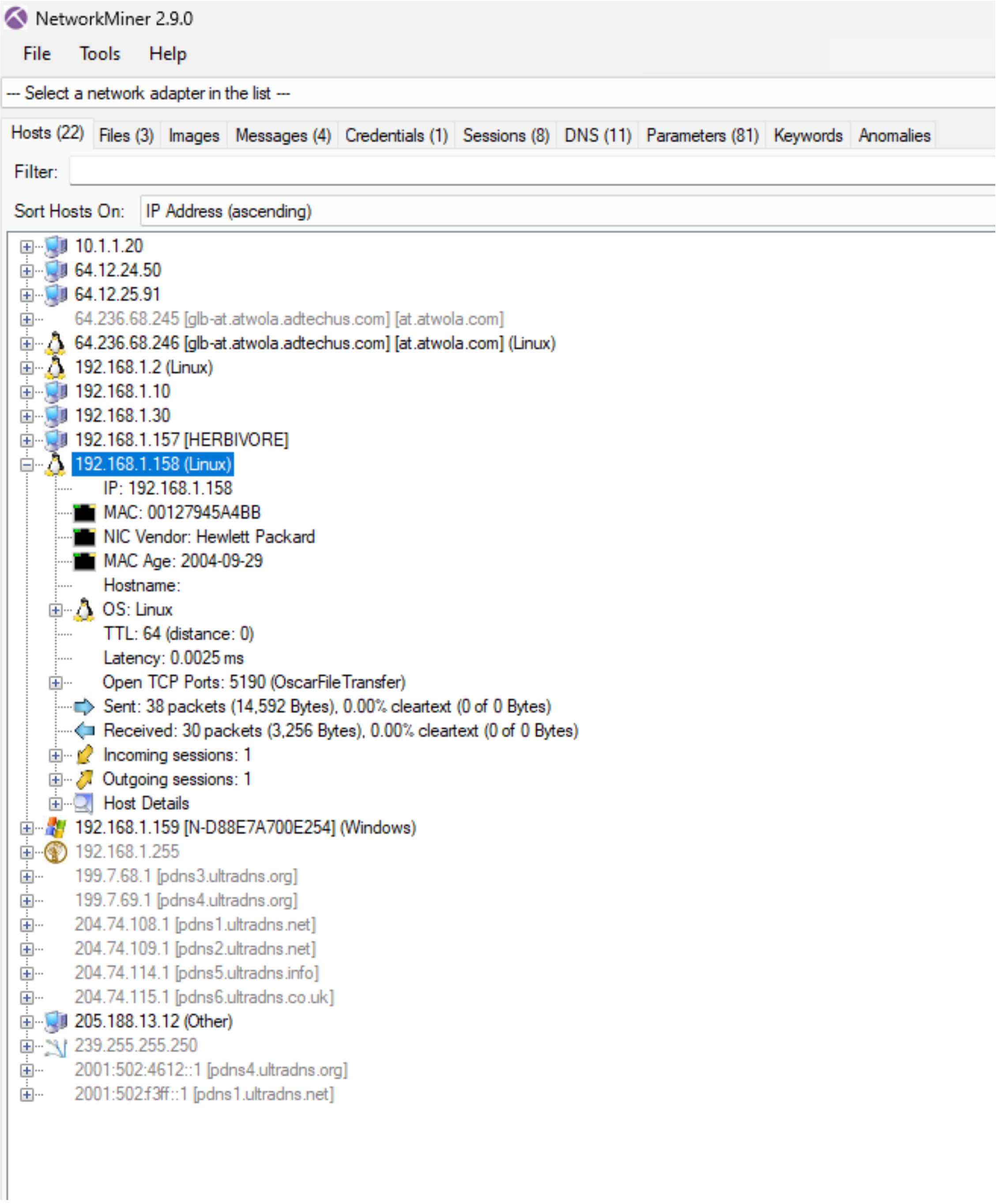
Ingredients:

4 cups sugar

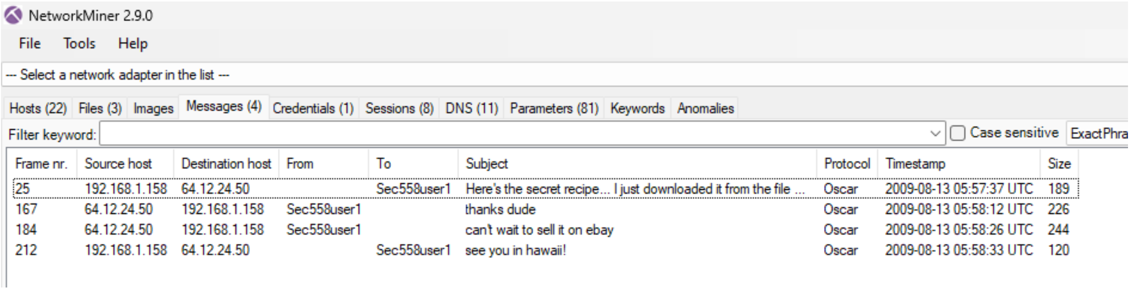
2 cups water

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.

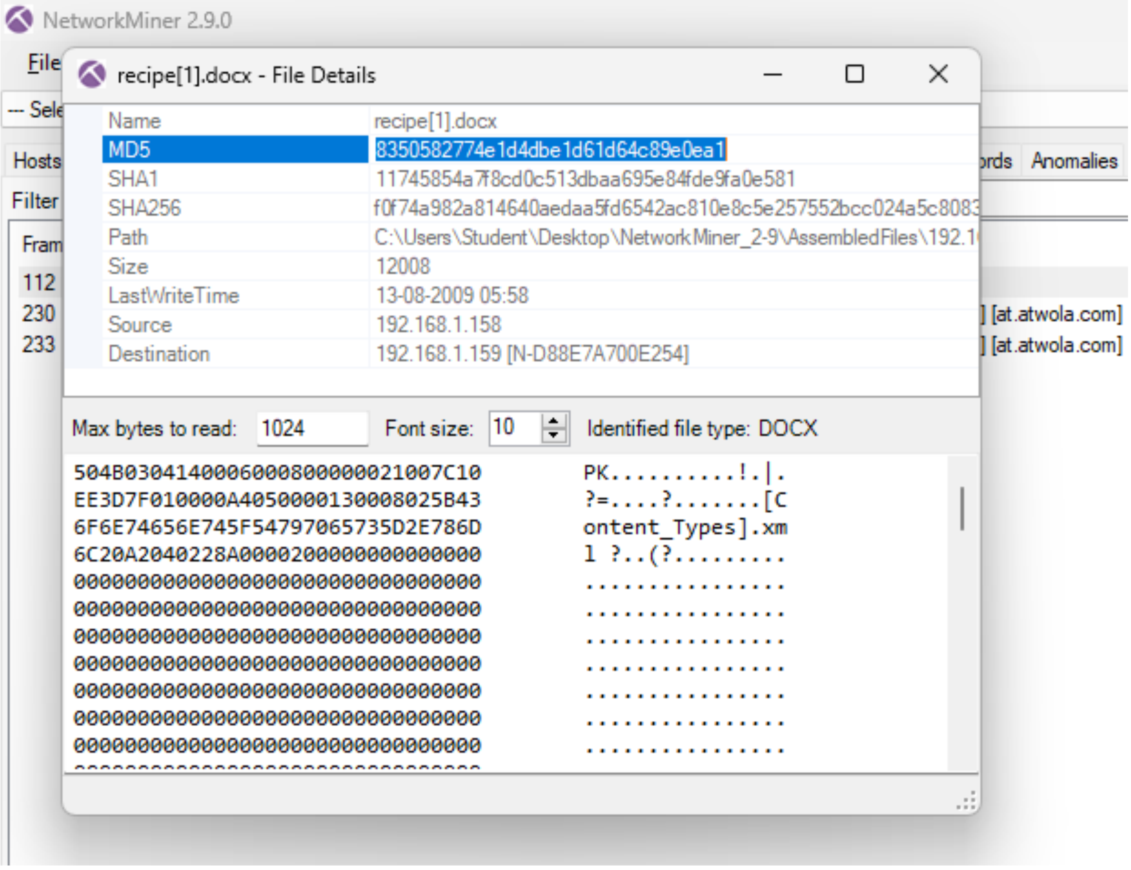
# Using Network Miner:



```
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)
192.168.1.10
192.168.1.30
192.168.1.157 [HERBIVORE]
192.168.1.158 (Linux)
    IP: 192.168.1.158
    MAC: 00127945A4BB
    NIC Vendor: Hewlett Packard
    MAC Age: 2004-09-29
    Hostname:
    OS: Linux
    TTL: 64 (distance: 0)
    Latency: 0.0025 ms
    Open TCP Ports: 5190 (OscarFileTransfer)
    Sent: 38 packets (14,592 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 30 packets (3,256 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Incoming sessions: 1
    Outgoing sessions: 1
    Host Details
192.168.1.159 [N-D88E7A700E254] (Windows)
192.168.1.255
199.7.68.1 [pdns3.ultradns.org]
199.7.69.1 [pdns4.ultradns.org]
204.74.108.1 [pdns1.ultradns.net]
204.74.109.1 [pdns2.ultradns.net]
204.74.114.1 [pdns5.ultradns.info]
204.74.115.1 [pdns6.ultradns.co.uk]
205.188.13.12 (Other)
239.255.255.250
2001:502:4612::1 [pdns4.ultradns.org]
2001:502:f3ff::1 [pdns1.ultradns.net]
```



| Frame nr. | Source host | Destination host | From | To | Subject | Protocol | Timestamp | Size |
|---|---|---|---|---|---|---|---|---|
| 25 | 192.168.1.158 | 64.12.24.50 | | Sec558user1 | Here's the secret recipe... I just downloaded it from the file ... | Oscar | 2009-08-13 05:57:37 UTC | 189 |
| 167 | 64.12.24.50 | 192.168.1.158 | Sec558user1 | | thanks dude | Oscar | 2009-08-13 05:58:12 UTC | 226 |
| 184 | 64.12.24.50 | 192.168.1.158 | Sec558user1 | | can't wait to sell it on ebay | Oscar | 2009-08-13 05:58:26 UTC | 244 |
| 212 | 192.168.1.158 | 64.12.24.50 | | Sec558user1 | see you in hawaii! | Oscar | 2009-08-13 05:58:33 UTC | 120 |



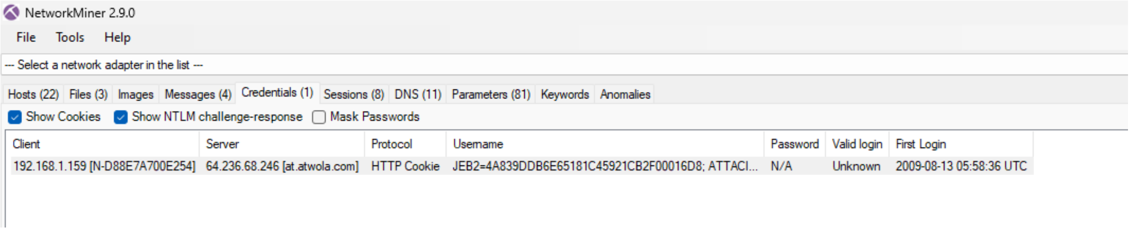
NetworkMiner 2.9.0

recipe[1].docx - File Details

| | |
|---|---|
| Name | recipe[1].docx |
| MD5 | 8350582774e1d4dbe1d61d64c89e0ea1 |
| SHA1 | 11745854a7f8cd0c513dbaa695e84fde9fa0e581 |
| SHA256 | f0f74a982a814640aedaa5fd6542ac810e8c5e257552bcc024a5c8083 |
| Path | C:\Users\Student\Desktop\NetworkMiner_2-9\AssembledFiles\192.1 |
| Size | 12008 |
| LastWriteTime | 13-08-2009 05:58 |
| Source | 192.168.1.158 |
| Destination | 192.168.1.159 [N-D88E7A700E254] |

Max bytes to read: 1024 Font size: 10 Identified file type: DOCX

```
504B0304140006000800000021007C10        PK..........!.|.
EE3D7F010000A4050000130008025B43        ?=....?.......[C
6F6E74656E745F54797065735D2E786D        ontent_Types].xm
6C20A2040228A0000200000000000000        l ?..(?.........
00000000000000000000000000000000        ................
00000000000000000000000000000000        ................
00000000000000000000000000000000        ................
00000000000000000000000000000000        ................
00000000000000000000000000000000        ................
00000000000000000000000000000000        ................
00000000000000000000000000000000        ................
```

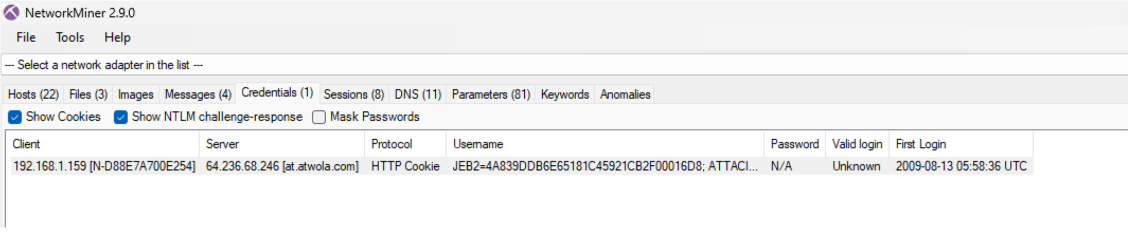


NetworkMiner 2.9.0

File Tools Help
--- Select a network adapter in the list ---
Hosts (22) Files (3) Images Messages (4) Credentials (1) Sessions (8) DNS (11) Parameters (81) Keywords Anomalies

☑ Show Cookies ☑ Show NTLM challenge-response □ Mask Passwords

| Client | Server | Protocol | Username | Password | Valid login | First Login |
|---|---|---|---|---|---|---|
| 192.168.1.159 [N-D88E7A700E254] | 64.236.68.246 [at.atwola.com] | HTTP Cookie | JEB2=4A839DDB6E65181C45921CB2F00016D8; ATTACI... | N/A | Unknown | 2009-08-13 05:58:36 UTC |



NetworkMiner 2.9.0

☑ Show Cookies ☑ Show NTLM challenge-response □ Mask Passwords

| Client | Server | Protocol | Username | Password | Valid login | First Login |
|---|---|---|---|---|---|---|
| 192.168.1.159 [N-D88E7A700E254] | 64.236.68.246 [at.atwola.com] | HTTP Cookie | JEB2=4A839DDB6E65181C45921CB2F00016D8; ATTACI... | N/A | Unknown | 2009-08-13 05:58:36 UTC |

## Post Lab Questions:

## 8.1 Explain the different challenges in handling network-based incidents.

Handling network-based incidents presents various challenges due to the complexity of modern networks and the constantly evolving threat landscape. Some of the key challenges include:

1. **Volume of Data**: Network traffic can generate vast amounts of data, making it

difficult to quickly identify and isolate suspicious activities. Effective analysis requires sophisticated tools and techniques to manage this large volume of data in real-time.

2. **Encryption**: Many network communications are encrypted (e.g., SSL/TLS), which makes it challenging to inspect the content of the data without the proper decryption keys. This complicates detection of malicious activities, such as data exfiltration or malware communication.

3. **Distributed Attacks**: Network-based incidents often involve distributed attacks (e.g., Distributed Denial of Service (DDoS) attacks), which can make it hard to pinpoint the source of the attack. These attacks use many different sources to overwhelm a target, making them difficult to block or mitigate.

4. **Lack of Visibility**: In some cases, organizations may lack the necessary network monitoring tools or sensors to detect and respond to incidents effectively. This can be particularly problematic in larger, more complex network environments.

5. **Time Sensitivity**: Detecting and mitigating network incidents often requires rapid response times to minimize damage. Delays in identifying the source of an attack or isolating affected systems can lead to greater harm.

6. **False Positives**: Network monitoring tools can generate false alarms, which can lead to resource overload, distract from actual incidents, and waste time. Accurately distinguishing between benign and malicious activity is crucial.

7. **Evolving Threats**: Network-based threats are constantly evolving, with attackers using advanced techniques to evade detection. This requires continuous adaptation and updating of security measures.

8. **Internal Threats**: Insider threats, whether malicious or accidental, can be difficult to identify because the attacker often has legitimate access to the network.

9. **Coordination and Communication**: Network-based incidents often require cross-departmental coordination, including IT, legal, compliance, and management. Effective communication is crucial to ensure a rapid and coordinated response.

## 8.2 Discuss the tools used for monitoring the network traffic.

There are several tools available to help monitor network traffic and ensure the security and performance of a network. Some of the commonly used tools include:

1. **Wireshark**: One of the most popular open-source tools for network protocol analysis. Wireshark allows users to capture and analyze packets on the network in real-time, providing detailed insights into network traffic.

2. **Tcpdump**: A command-line packet analyzer similar to Wireshark but often preferred by users working in a terminal or requiring more lightweight tool functionality. Tcpdump allows you to capture network packets and analyze them.

3. **NetFlow/SFlow**: These are network traffic monitoring protocols that collect data about traffic flows, such as source and destination IPs, and can provide a high-level view of network performance. They are often used in larger enterprise networks.

4. **Nagios**: A comprehensive monitoring solution for networks and servers. It provides real-time alerts and monitoring of network services, hosts, and applications to ensure the availability and performance of network infrastructure.

5. **SolarWinds Network Performance Monitor**: This is a commercial tool that offers deep visibility into network performance. It helps identify performance bottlenecks, troubleshoot network issues, and improve overall network health.

6. **PRTG Network Monitor**: PRTG monitors network infrastructure and traffic in real-time. It provides detailed data visualization, bandwidth monitoring, and alerting for various network parameters.

7. **Snort**: Snort is an open-source intrusion detection and prevention system (IDS/IPS) that analyzes network traffic in real-time to detect and respond to suspicious activity. It can also perform packet capture and deep packet inspection.

8. **Suricata**: Another open-source IDS/IPS tool, Suricata is capable of monitoring network traffic, detecting intrusions, and offering high-performance capabilities with multi-threading and high-speed traffic capture.

9. **Zabbix**: Zabbix is an open-source network monitoring tool that can track the availability and performance of network devices, servers, and applications. It can generate alerts based on specific thresholds and conditions.

10. **OpenNMS**: An open-source network management platform that provides

monitoring, alerting, and performance measurement capabilities for enterprise networks.

These tools help security teams identify malicious activity, network performance issues, and other anomalies, facilitating efficient incident response and proactive network management.

---

### 8.3 What do you understand by packet sniffing?

**Packet sniffing** is the process of capturing and analyzing data packets transmitted over a network. It involves intercepting network traffic and examining the contents of the packets in order to gather information about the communication between devices on the network. This technique is often used for legitimate purposes such as network troubleshooting, performance monitoring, or security analysis. However, it can also be used maliciously by attackers to capture sensitive information like passwords, email content, and other private data.

Packet sniffers (also known as network analyzers or protocol analyzers) can be either hardware devices or software tools. Common examples of packet sniffing tools include **Wireshark** and **Tcpdump**.

Key points about packet sniffing:

1. **Types of Traffic**: Packet sniffing can capture various types of network traffic, such as HTTP, FTP, DNS, or any other protocol. It can capture both inbound and outbound traffic.

2. **Man-in-the-Middle (MitM) Attacks**: Attackers may use packet sniffing as part of a Man-in-the-Middle attack, where they intercept and potentially alter communication between two parties without their knowledge.

3. **Legal and Ethical Issues**: Unauthorized packet sniffing is illegal in many jurisdictions and is considered an invasion of privacy. Sniffing should only be done with proper authorization, typically for network administration or security monitoring purposes.

4. **Encryption**: Encrypted traffic (e.g., HTTPS) makes it difficult for a packet sniffer to view the actual contents of the communication. While the metadata (e.g., source and destination IP addresses) can still be visible, the data itself is protected.

5. **Detection**: Modern networks may use encryption or secure communication

protocols to mitigate the risks of packet sniffing, and intrusion detection systems may alert administrators to suspicious sniffing activity.

**Conclusion:** Analyzed a packet to capture the conversation between two users and obtained their secret messages and file.