

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

Department of Computer Engineering

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.

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

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	192.168.1.157	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	34.025537	64.12.24.50	192.168.1.158	SSL	92	Continuation Data

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 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 02 00 00 45 10 ... 1 + P V ... E
 0010 00 34 d3 a8 40 00 40 06 e3 9a c0 a8 01 02 c0 a8 ... 4 @ @ ...
 0020 01 1e d8 c0 00 16 33 09 5e a5 5a 1e 27 43 00 10 ... 3 ^ Z ' C ...
 0030 03 ea 54 00 00 01 01 08 0a 1d c1 35 0c 0e 0e ... HT ... 5 ...
 0040 5d 4c ... J L

evidence01.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr eq 192.168.1.158

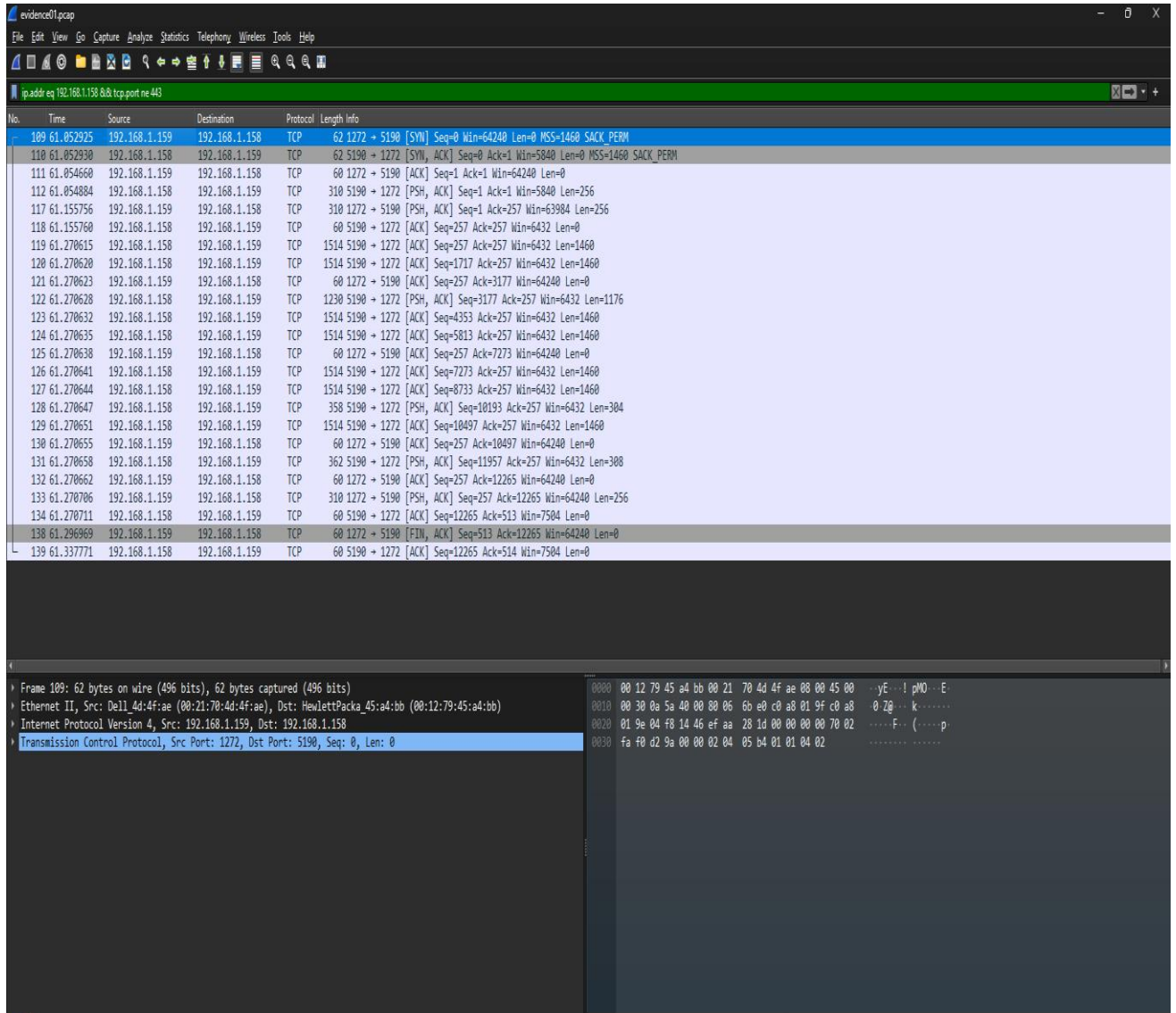
No.	Time	Source	Destination	Protocol	Length	Info
23	18.870898	192.168.1.158	64.12.24.50	SSL	60	Continuation Data
24	18.871477	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=7 Win=64240 Len=0
25	33.914966	192.168.1.158	64.12.24.50	SSL	243	Continuation Data
26	33.915486	64.12.24.50	192.168.1.158	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
30	34.025537	64.12.24.50	192.168.1.158	SSL	92	Continuation Data
31	34.026804	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=210 Win=62780 Len=0
32	34.026809	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=248 Win=62742 Len=0
33	56.250951	192.168.1.158	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
34	56.250951	192.168.1.158	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
35	58.461856	192.168.1.158	64.12.24.50	SSL	182	Continuation Data
36	58.461856	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=248 Ack=364 Win=64240 Len=0
37	58.568705	64.12.24.50	192.168.1.158	SSL	263	Continuation Data
38	58.569716	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=364 Ack=457 Win=62742 Len=0
39	58.571308	64.12.24.50	192.168.1.158	SSL	92	Continuation Data
40	58.574447	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=364 Ack=495 Win=62742 Len=0
41	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
42	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
43	61.054660	192.168.1.159	192.168.1.158	TCP	60	1272 → 5190 [ACK] Seq=1 Ack=1 Win=64240 Len=0
44	61.054884	192.168.1.158	192.168.1.159	TCP	310	5190 → 1272 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=256
45	61.155756	192.168.1.159	192.168.1.158	TCP	310	1272 → 5190 [PSH, ACK] Seq=1 Ack=257 Win=6304 Len=256
46	61.155760	192.168.1.158	192.168.1.159	TCP	60	5190 → 1272 [ACK] Seq=257 Ack=257 Win=6432 Len=0
47	61.170615	192.168.1.159	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=257 Ack=257 Win=6432 Len=1460
48	61.170620	192.168.1.158	192.168.1.159	TCP	1514	5190 → 1272 [ACK] Seq=1717 Ack=257 Win=6432 Len=1460
49	61.170623	192.168.1.159	192.168.1.158	TCP	60	1272 → 5190 [ACK] Seq=257 Ack=3177 Win=64240 Len=0
50	61.170628	192.168.1.158	192.168.1.159	TCP	1230	5190 → 1272 [PSH, ACK] Seq=3177 Ack=257 Win=6432 Len=1176
51	61.170632	192.168.1.158	192.168.1.159	TCP	1514	5190 → 1272 [ACK] Seq=4353 Ack=257 Win=6432 Len=1460
52	61.230235	192.168.1.158	192.168.1.159	TCP	60	5190 → 1272 [ACK] Seq=4353 Ack=257 Win=6432 Len=1460

Frame 23: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: Hewlett-Packard_45:a4:b8 (08:12:79:45:a4:b8), 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 b8 00 45 00 ... b y E ... E
 0010 00 2e a0 3b 40 00 40 06 75 0a e0 a8 01 9a 40 0c ... 0 @ u ... @
 0020 18 32 c7 b8 01 b8 33 6b d2 c3 07 e9 60 db 50 18 ... 2 ... 3k ... P
 0030 f5 3c 3d 39 00 00 2a 05 00 60 00 00 ... c-9 * ...

Packets: 240 - Displayed: 68 (28.3%) Profile: Default

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



The image shows a Wireshark packet capture analysis of a TCP connection. The top pane displays a list of packets, and the bottom pane shows the details of the selected packet (Frame 189).

No.	Time	Source	Destination	Protocol	Length	Info
189	61.852925	192.168.1.159	192.168.1.158	TCP	62	1272 → 5190 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
110	61.852930	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	61.854660	192.168.1.159	192.168.1.158	TCP	60	1272 → 5190 [ACK] Seq=1 Ack=1 Win=64240 Len=0
112	61.854884	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
124	61.270635	192.168.1.158	192.168.1.159	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	192.168.1.158	192.168.1.159	TCP	1514	5190 → 1272 [ACK] Seq=7273 Ack=257 Win=6432 Len=1460
127	61.270644	192.168.1.158	192.168.1.159	TCP	1514	5190 → 1272 [ACK] Seq=8733 Ack=257 Win=6432 Len=1460
128	61.270647	192.168.1.158	192.168.1.159	TCP	358	5190 → 1272 [PSH, ACK] Seq=10193 Ack=257 Win=6432 Len=304
129	61.270651	192.168.1.159	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=10497 Ack=257 Win=6432 Len=1460
130	61.270655	192.168.1.159	192.168.1.158	TCP	60	1272 → 5190 [ACK] Seq=257 Ack=10497 Win=64240 Len=0
131	61.270658	192.168.1.158	192.168.1.159	TCP	362	5190 → 1272 [PSH, ACK] Seq=11957 Ack=257 Win=6432 Len=308
132	61.270662	192.168.1.159	192.168.1.158	TCP	60	1272 → 5190 [ACK] Seq=257 Ack=12265 Win=64240 Len=0
133	61.270706	192.168.1.159	192.168.1.158	TCP	310	1272 → 5190 [PSH, ACK] Seq=257 Ack=12265 Win=64240 Len=256
134	61.270711	192.168.1.158	192.168.1.159	TCP	60	5190 → 1272 [ACK] Seq=12265 Ack=513 Win=7504 Len=0
138	61.296969	192.168.1.159	192.168.1.158	TCP	60	1272 → 5190 [FIN, ACK] Seq=513 Ack=12265 Win=64240 Len=0
139	61.337771	192.168.1.158	192.168.1.159	TCP	60	5190 → 1272 [ACK] Seq=12265 Ack=514 Win=7504 Len=0

Frame 189: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
 Ethernet II, Src: Dell_4d:4f:ae (00:21:70:4d:4f:ae), Dst: Hewlett-Packard_45:a4:bb (00:12:79:45:a4:bb)
 Internet Protocol Version 4, Src: 192.168.1.159, Dst: 192.168.1.158
 Transmission Control Protocol, Src Port: 1272, Dst Port: 5190, Seq: 0, Len: 0

0000 00 12 79 45 a4 bb 00 21 70 4d 4f ae 00 00 45 00 ..yE...l pM...E
 0010 00 30 0a 5a 40 00 06 6b e0 c0 a8 01 9f c0 a8 0 7g...k.....
 0020 01 9e 04 f8 14 46 ef aa 28 1d 00 00 00 70 02F... (....p
 0030 fa f0 d2 9a 00 00 02 04 05 b4 01 01 04 02

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

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

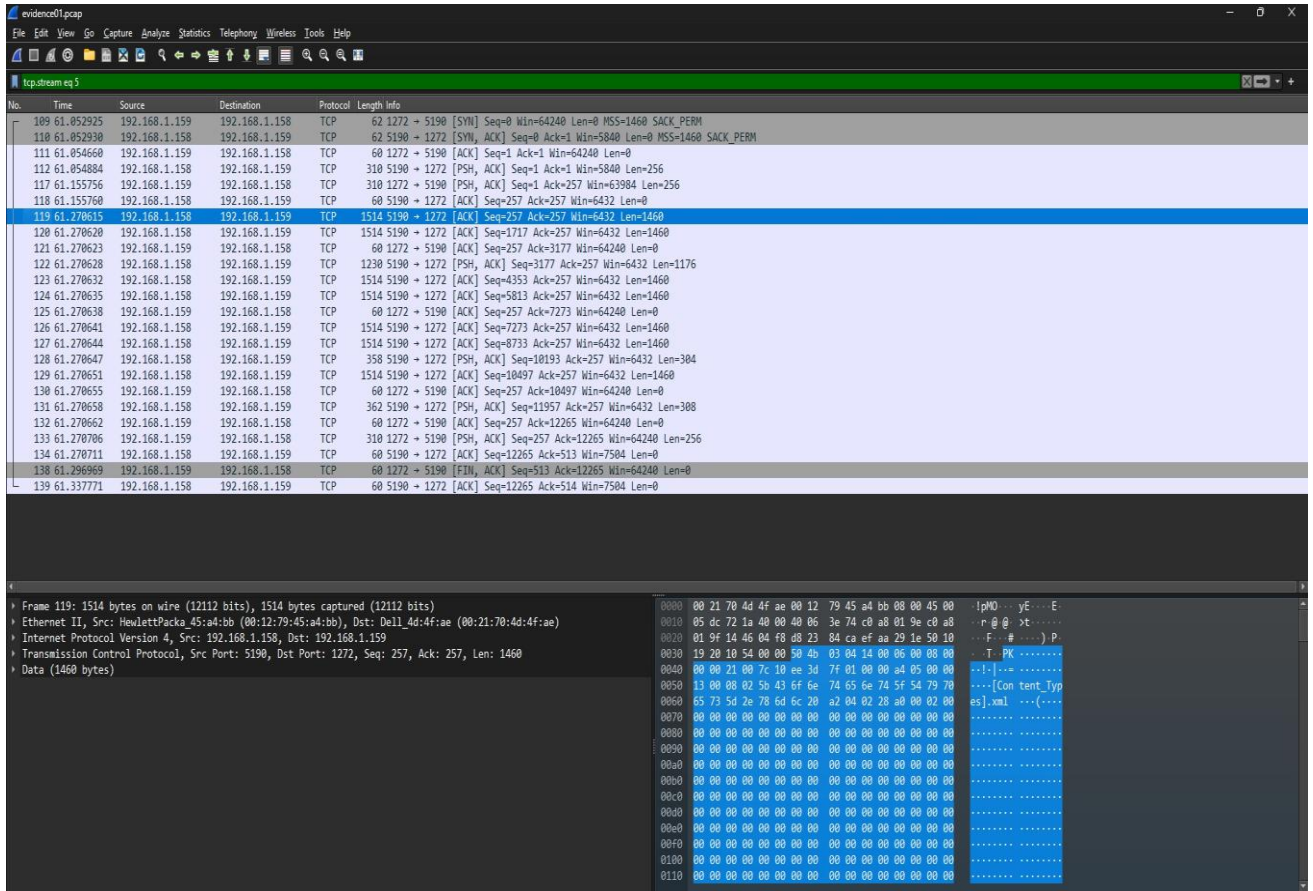
0FT2.....recipe.docx.....Cool FileXfer.....
.....recipe.docx.....Cool FileXfer.....
.....[Content_Types].xml .....
.....Ik.0.....k.P3.C.c.h.....
.....8..4..NbJ.6.b.f...H..d.!*gs.z,+).$g...%...v.r.....'1gSD.y.S0*f...?..F...{!...m.w....S.....JHF"...0...3.Fs.`F.....uum g.{.0.....N)U) ...3C
.Y.y.PA.....<A%f...%Y[...m.....w)t.qv(...%o.....$.Hs7:k.F(.M...+.....
.....Xs...g...l).'_B.R.;q.u@.....~.Hw.x=-.4.....pv.{3o.'M,....b..w.i.O...0..E]]'.x...?.....PK.....!.....N.....rels/.rels ...(.
.....
....."..H.w".....w.....P.^...o.....j.<.aY...`G.kxm...PY.[...g
G.ino./<...<1...A$>*f3...T...I S.....W.....Y
lg.@.X6...7..
f.....ao..b*1I.r.j)...10.%..b.
6.i..D...
...|u.Z^t.y.j.!Y,}{.C./h>.....PK.....!.....L.....word/_rels/document.xml.rels ...(.
.....
.....OK.0.....!...|u.e...W.5.N.'..dV.7.....^z ...y.7.d..1-.B..g%<.V..... X e...z...no...*.B.t.E..$.D.F...k4*p...7..FQ,}%:
.PU.b.$k...j.x.}!...{y...Y6...>.t%B.$...|$. ...:jQ...8.3.P...K..c g>b.#..bTECh.9...4...$C).s.qI.Y...p...q...PK.....!E.e.P...
word/document.xml.Vmo.0...>i...+...*Tui.}...'.&q.U.v...IX.2.n...~...}.X...<...T.d9....."s.....@mt.x...Ns.U.J...!m.G..9...vT.;R.34...pj.X.P..L M..2
!.$Q...Q..22ml...p.H..e...%w...r...V.....a..d...Z...[nH...]+k.2j...-q...
!.'$Ba.c".G..O..L...7.c.+..b..U.....k1_..$.M.)..._D'.8.n..%..H.].V.....#B. G..(.xk..U..W.S.1n!p..-I2..W...fLS.{.Kf.u...k(.....^!W...b....<K...y5.^
...3b...|H/6.[.^...~B...d...?..|y...../.1. +/3%..ZM2...P...@...K..j"...(.j...*.Gp...#..0>...c.J!?...^..\...=E.z.&.ro.t...2<...G.9.V.=.
.E...*/<w..ci..8b\..j.%...0...7...Q^7...^JLO...9u..F.R..&T...F...E.K..i.q@.dE.k...w...<...@4s..e.Bm..+...B...2.L.Nw...%o..IH...;6[.tw..M..9.
.sZ.X.9..3...B)...iY.0m.e.v...>$. ...h.L.s...].1X1.M..1o...u.T...PK.....!P.....word/theme1.xml.Y0o.6...w toc'v...u...-M..n..i..P.@.I)...
a..m.a[...4.1...GR..X^..6...>$... ..!O^..r.C$.y@.../yH*... ..).....UDb..)"q..J...X^.)I'n.E...p)...li.V[.]1Mk...O.P..6r...=...z.gb.I.g...u.S
e..b..0...R.D...qu
g..Z...o...lAp.lx.pt0...+{..}j.....zA.....V.2.F...i@.q.v..5\].....N..le.X.d.s...jcs...7..f...
.W..+...7...g...J...j...|..h(K..D...
dX...iJ...x$S...<...>...!.._T..S..1.....?E...?..?ZB..m..U/.....?..~...xY...'.y5..g&./.....>..G..M.Ge..D.....3Vq%'#q.....$.8..K.....)f.w.9:
...
x)r..x...w...r.:TZaG*.y8I.j.br.c|X.....I
u3.KG.nd.1..N..IB...
.R..u..K>V..E.L+M2.#'.f..i..V..v1.{.u8..z...H.
.*.....(W...
~...J..T.e\0*.tH.G..HY...KN.P.*.....T...9/#..A7.qZ...$*c?.....qU...n..w..N...%..0..i..4..=3...P..
...1.P.m.\9.....M...2a.D.].;Yt.\...[x.....].Wr...|.].g-...
eW.
j6-r..C.S..j..
i.d
.D..A...IqbJ#x...6k...#.A.Sh...&...t(Q.%..p%..&].ca5..l=X.....\P.1.Mh..9..M...V.dDA..av.B..[.fJ..P..8.....A..V^..f
...H...n...>...z...n...>...>...b...&...2...v...Ky...D...AGm..n..z...i...z...n...Y..C..6.OMf..3o.r..$.5...N.H.T[Xf64.T...M0.E)'#5.XY.'...%.1.U
...m;...R>QD...D.cp..U..'&LE./p...m...%]...8fi..r.S4.d.7y\.'J.n...I..R...3U..w.7+...#..m..q.BiD...i*.L6..9..m.Y.&...i...HE..=(K&N!V...K.e.LD,
{D. ....v.E...de..N...e.(.MN9...R..6...&3(.a..)/D..U.z.<{...Y.....V...).9.Z[.4^n...5...!J...?..Q.3.eBo.C.....M.....m<...vp...IY.f..Z.Y p.[=a!
-Y.)Nc.....4vfa.v1...S'..A.8.|.*.u.{...-0%0.7%...<.....PK.....!..?
a.....word/settings.xml.U.n.@.}G.,?..N..Xu.^..J...$Y7...6.Bk...d...t.z.Xi...Q..~(%6.h**(<I..'(Z.....m5r.
M.....(Im..g...L{.kUS...xj...i...Q.m...;..].&...$S.....6.Bk...d...t.z.Xi...Q..~(%6.h**(<I..'(Z.....m5r.
A..([.m...j|C...S..v@ ..f.d...CSh.H.JIg..v...$hx48..h.....X\~X.^5..m6z...R..I..2..Cxcvd...\.0...b..0^gB..1.6d~....."D.....0....}D
V..K&,"..>g..d..V..K*t h.z.fv...w'6.r.l..WQj.../5?&h>..^..5.odMp...n.D.m.S..K.(>..Y.../8..f.^..Z...|+.."Xwa...w...p.jf+...y...o...x.M..m...j0..G..
...s.T..d..A..$.0b...j..y..#v...;{.N..G.X8z|.8W-...@}...4R..r.J...m...Z'}.J.ZS...5...W...%i.....K..X1..b/-8...5=N..r...PK...
.....!..t?9z...((.....customXml/_rels/item1.xml.rels ...(.
.....1.....;X...XY.....t23.i
S..(..0+..1..?..S4.T5(.z.G.?.....)'2...=..1.....D60...&..+J..d...2..Yw.#.u]ot.m@.a.Co .....J..6
.w.E..0...X(\..|...6.(..`X...k.....PK.....!.....Tc..U...(.customXml/itemProps1.xml..$. (.....j.0.....=..8e%-...:..u...[.v.
.....u..."..j.aGvE..9 ..Z.C..5...v>f%...k.H.%8..].z.mUT!.SD.R..|j$[5...S..Y.Y.E...!;...XB.t&H.b...=UaM..4..[...=..3...E... \ o.....R..2...
O.u...}.PK.....!..q.;...i...word/styles.xml..QS.8..o.....e.vZz.P..0...
.r.R.>.I+{...}"...jW.5 ..p.M.<SB...(.x.X...fyv.&.fi...y..U...;Q.!.*0.Ru...C.m..W..Sso...kv{(k...2.oY...0... ..6b.....]&#...v.8{[&...q/..g.f.D
+5...7.q&S..."!..q.V.2..1U^4w8S...|.Kw...7..H..0^".....qq...:Z.z...O.n.eg..?..+{ie.....!DZ..E.{.....Xd..ak.M.MJ..D..g...>1..^.....1..|.L.I.I
```

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

```
Wireshark · Follow TCP Stream (tcp.stream eq 2) · evidence01.pcap

*..`..*.a.....E4628778....Sec558user1.....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 &gt;:-)....*.b.".....F.....Sec558user1..*.V.....
*..A.....E.....P.....p..p.....P.....p..
p.&.'.....U4.....h.....p...@.&.'.....
...|.h.....p...@.&.'*.V.....E4628778....Sec558user1*..c.z.....G717464
7....Sec558user1.....R..7174647.F.CL...."DEST.....F.
.....'.....recipe.docx*.V.....
*..c.....G.....P.....p..p.._w.....P.....p..
p.&a.....U.....h.....p...@.&a
.....h.....p...@.&a.....*.V.....G7174647....Sec558user1*.V..{.....*..
7174647....Sec558user1.....J.H.....+.1n....+.O.....J.....71746
47.      F.CL...."DEST.....*.V..".....*.1.....Sec558user1..*.V.....*.y..
N....w....Sec558user1.....J.H.....+.1n....+.O.....J.....a.....X
...<HTML><BODY><FONT FACE="Arial" SIZE=2 COLOR=#000000>thanks dude</FONT></BODY></HTML>.
.....+.1n....+.O.....*.V..".....*.....Sec558user1..*.V.....+
Q....L....Sec558user1.....J.H.....+.1n....+.O.....J.....s.....
..j....<HTML><BODY><FONT FACE="Arial" SIZE=2 COLOR=#000000>can't wait to sell it on ebay<
/FONT></BODY></HTML>.
.....+.1n....+.O.....*.V..".....+
.....Sec558user1..*.V..".....+.....Sec558user1..*.d.".....H.....
...Sec558user1..*.e.J.....I5088496....Sec558user1...".....see you in hawa
ii!....*.f.".....J.....Sec558user1..*.V.....
..+ @.....I.....P.....p..p..a.....P.....p..
p.&.....V.....h.....p...@.&.....
...|.h.....p...@.&...*.V.....I5088496....Sec558user1
```

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



The image shows a Wireshark packet capture analysis of an HTTP GET request. The top pane displays a list of network packets. The selected packet (No. 119) is an HTTP GET request from 192.168.1.158 to 192.168.1.158. The bottom pane shows the packet details and the raw data in hexadecimal and ASCII.

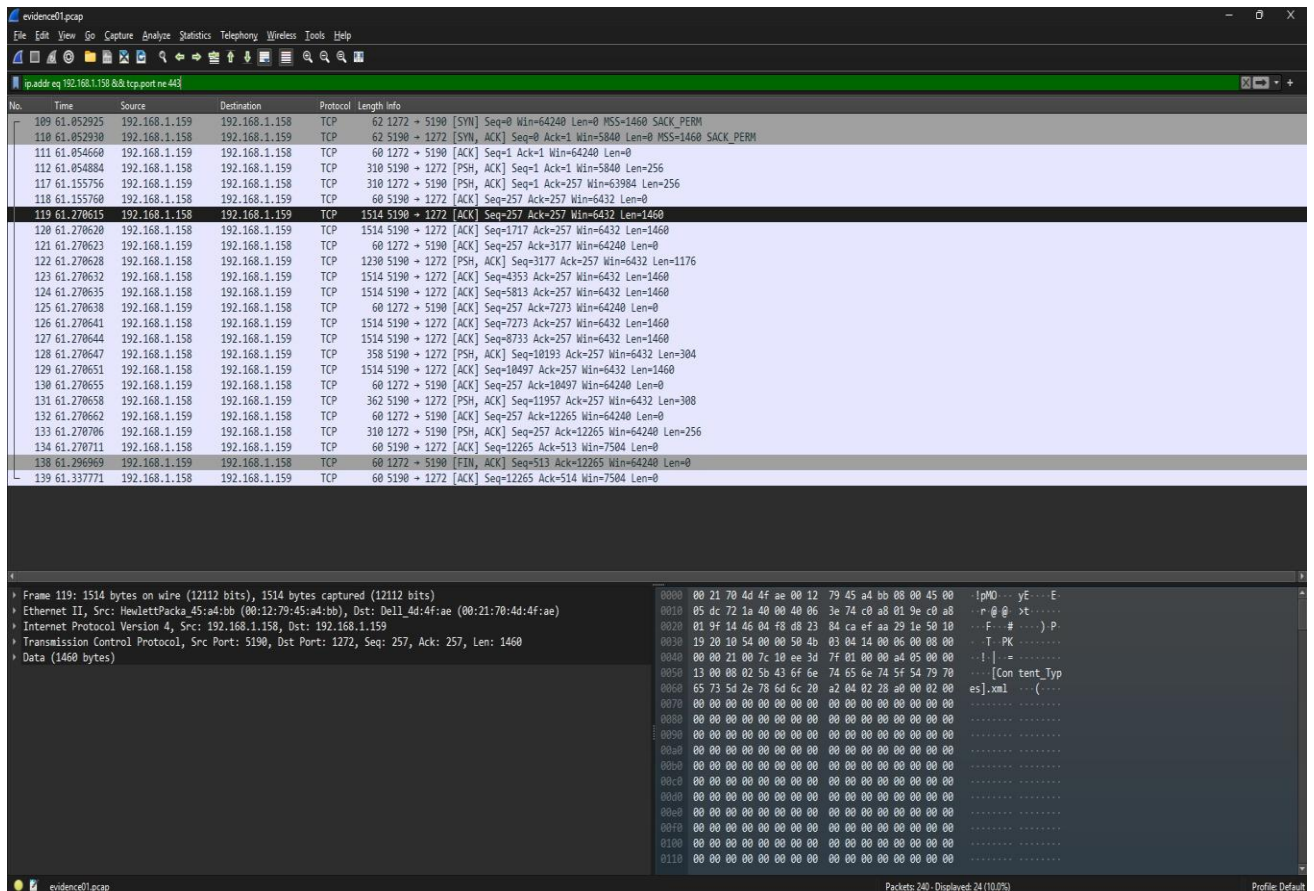
No.	Time	Source	Destination	Protocol	Length	Info
109	61.852925	192.168.1.158	192.168.1.158	TCP	62	1272 → 5190 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
110	61.852930	192.168.1.158	192.168.1.158	TCP	62	5190 → 1272 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
111	61.854660	192.168.1.158	192.168.1.158	TCP	60	1272 → 5190 [ACK] Seq=1 Ack=1 Win=64240 Len=0
112	61.854884	192.168.1.158	192.168.1.158	TCP	310	5190 → 1272 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=256
117	61.155756	192.168.1.158	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	192.168.1.158	TCP	60	5190 → 1272 [ACK] Seq=257 Ack=257 Win=6432 Len=0
119	61.270615	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=257 Ack=257 Win=6432 Len=1460
120	61.270620	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=1717 Ack=257 Win=6432 Len=1460
121	61.270623	192.168.1.158	192.168.1.158	TCP	60	1272 → 5190 [ACK] Seq=257 Ack=3177 Win=64240 Len=0
122	61.270628	192.168.1.158	192.168.1.158	TCP	1230	5190 → 1272 [PSH, ACK] Seq=3177 Ack=257 Win=6432 Len=1176
123	61.270632	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=4353 Ack=257 Win=6432 Len=1460
124	61.270635	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=5813 Ack=257 Win=6432 Len=1460
125	61.270638	192.168.1.158	192.168.1.158	TCP	60	1272 → 5190 [ACK] Seq=257 Ack=7273 Win=64240 Len=0
126	61.270641	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=7273 Ack=257 Win=6432 Len=1460
127	61.270644	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=8733 Ack=257 Win=6432 Len=1460
128	61.270647	192.168.1.158	192.168.1.158	TCP	358	5190 → 1272 [PSH, ACK] Seq=10193 Ack=257 Win=6432 Len=304
129	61.270651	192.168.1.158	192.168.1.158	TCP	1514	5190 → 1272 [ACK] Seq=10497 Ack=257 Win=6432 Len=1460
130	61.270655	192.168.1.158	192.168.1.158	TCP	60	1272 → 5190 [ACK] Seq=257 Ack=10497 Win=64240 Len=0
131	61.270658	192.168.1.158	192.168.1.158	TCP	362	5190 → 1272 [PSH, ACK] Seq=11957 Ack=257 Win=6432 Len=308
132	61.270662	192.168.1.158	192.168.1.158	TCP	60	1272 → 5190 [ACK] Seq=257 Ack=12265 Win=64240 Len=0
133	61.270706	192.168.1.158	192.168.1.158	TCP	310	1272 → 5190 [PSH, ACK] Seq=257 Ack=12265 Win=64240 Len=256
134	61.270711	192.168.1.158	192.168.1.158	TCP	60	5190 → 1272 [ACK] Seq=12265 Ack=513 Win=7504 Len=0
138	61.296969	192.168.1.158	192.168.1.158	TCP	60	1272 → 5190 [FIN, ACK] Seq=513 Ack=12265 Win=64240 Len=0
139	61.337771	192.168.1.158	192.168.1.158	TCP	60	5190 → 1272 [ACK] Seq=12265 Ack=514 Win=7504 Len=0

Frame 119: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
 Ethernet II, Src: HewlettPacka_45:a4:bb (00:12:79:45:a4:bb), Dst: Dell_4d:4f:ae (00:21:70:4d: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: 257, Ack: 257, Len: 1460
 Data (1460 bytes)

```

0000  00 21 70 4d 4f ae 00 12 79 45 a4 bb 00 00 45 00  :IpV4...yE...E
0010  05 dc 72 1a 40 00 40 06 3e 74 c0 a8 01 9e c0 a8  :...@ @ >E...
0020  01 9f 14 46 04 f8 d8 23 84 ca ef aa 29 1e 50 10  :...F...#...).P
0030  19 20 10 54 00 00 50 4b 03 04 14 00 06 00 00 00  :...T.PK.....
0040  00 00 21 00 7c 10 ee 3d 7f 01 00 00 a4 05 00 00  :...!...=...
0050  13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70  :...[Con tent_Typ
0060  65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00  :es].xml...{(
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  :.....
0080  00 00 00 00 00 00 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  :.....
00a0  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  :.....
00c0  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  :.....
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  :.....
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  :.....
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  :.....
0110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  :.....
  
```


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



HashMyFiles					
File Edit View Options Help					
Filename	MD5	SHA1	CRC32	SHA-256	SHA-512
recipe.docx	8350582774e1d4dbe1d61d64c89e0ea1	11745854a7f8cd0c513dbaa695e84fde9fa0e581	d6d12650	f0f74a902a814640aeddaf5fd6542ac010e8c5e...	1181921b99946512f6807ad30086a62e40e23c...

Post Lab Questions:

81 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.

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

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

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

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.

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

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.