



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Batch: B1 Roll No.: 16010121045

Experiment No. 8

Title: Network security and forensics using tool - Network Miner.

Objective: Working with sample real life cases related to Network security and forensics using tool - Network Miner.

CO	Outcome
CO3	Illustrate Secure software design principles and apply them for secure software development

Books/ Journals/ Websites referred:

<https://www.netresec.com/?page=Blog&month=2014-06&post=Running-NetworkMiner-on-Mac-OS-X>

<https://www.wireshark.org/>



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Abstract:-

Network security and network forensics are two critical components in ensuring the integrity, confidentiality, and availability of data within computer networks. Network security focuses on the prevention and detection of unauthorized access, misuse, modification, or denial of network resources and data. It encompasses various techniques such as firewalls, intrusion detection systems (IDS), virtual private networks (VPN), encryption, and authentication mechanisms to safeguard network infrastructure and data from malicious actors.

Network security refers to the practice of safeguarding networks from unauthorized access, misuse, modification, or denial of service. It encompasses various technologies, policies, and procedures designed to protect the integrity, confidentiality, and availability of network resources. Network forensics, on the other hand, involves the investigation and analysis of network traffic and data to uncover security breaches, malicious activities, or unauthorized access.

On the other hand, network forensics deals with the investigation and analysis of network traffic and activities to uncover evidence of security breaches, cyber attacks, or other illicit activities. It involves capturing, recording, and analyzing network packets, logs, and other digital artifacts to reconstruct events, identify perpetrators, and support legal proceedings. Network forensics tools and methodologies enable forensic analysts to trace the source of attacks, determine the extent of damage, and mitigate future risks to network security.

Related Theory: -

Attacks in computer networks can target various layers of the network stack, each serving as a potential entry point for malicious actors to exploit vulnerabilities and compromise network security. Here's an overview of common attacks targeting different layers of the network:

1. Physical Layer Attacks:

- **Wiretapping/Eavesdropping:** Attackers physically intercept network transmissions to capture sensitive information, such as passwords or confidential data, by tapping into network cables or using specialized equipment.
- **Hardware Tampering:** Attackers may physically manipulate network devices, such as routers, switches, or network interface cards (NICs), to disrupt network operations, steal data, or inject malicious code.

2. Data Link Layer Attacks:

- **MAC Address Spoofing:** Attackers forge the MAC address of a legitimate device to impersonate it on the network, allowing unauthorized access or bypassing access controls.
- **ARP Spoofing/Poisoning:** Attackers manipulate the Address Resolution Protocol (ARP) cache of network devices to associate their MAC address with the IP address of another legitimate device, enabling man-in-the-middle (MITM) attacks.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

3. Network Layer Attacks:

- **IP Spoofing:** Attackers forge the source IP address in IP packets to impersonate a trusted entity or evade detection, enabling various forms of attacks, including DDoS (Distributed Denial of Service) attacks or session hijacking.
- **ICMP Flood:** Attackers flood a target with a high volume of ICMP (Internet Control Message Protocol) packets, consuming network resources, degrading performance, or causing denial of service.

4. Transport Layer Attacks:

- **SYN Flood:** Attackers send a flood of TCP SYN (synchronization) packets to overwhelm the target's resources, preventing legitimate connections from being established and causing a denial of service.
- **UDP Flood:** Attackers flood a target with a high volume of UDP (User Datagram Protocol) packets, consuming bandwidth and network resources, leading to service disruption.

5. Session Layer Attacks:

- **Session Hijacking:** Attackers exploit vulnerabilities in session management mechanisms to intercept and take control of an ongoing session between two parties, allowing unauthorized access or data manipulation.
- **Man-in-the-Middle (MITM) Attack:** Attackers intercept communication between two parties, often by impersonating one or both parties, to eavesdrop on or alter the exchanged data.

6. Presentation Layer Attacks:

- **Code Injection:** Attackers exploit vulnerabilities in applications or protocols to inject malicious code, such as SQL injection or XSS (Cross-Site Scripting), into data exchanged between clients and servers, leading to data theft, system compromise, or unauthorized access.

7. Application Layer Attacks:

- **Buffer Overflow:** Attackers exploit vulnerabilities in software applications to overflow buffers with excessive data, causing the application to crash, execute arbitrary code, or gain unauthorized access to system resources.
- **Denial of Service (DoS) and Distributed Denial of Service (DDoS):** Attackers flood a target application or server with a high volume of requests or traffic, overwhelming its capacity and rendering it inaccessible to legitimate users.

Understanding these attacks and implementing appropriate security measures at each layer of the network stack is essential for mitigating risks and safeguarding network infrastructure and data assets against malicious threats.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Implementation:

Case 1

The screenshot shows the NetworkMiner 1.6.1 interface. The main window displays a list of network frames, with frame 167 selected. The details pane shows the message content: "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 >:-)" and its MD5 hash: d18767... The case panel on the right shows the same MD5 hash.

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 >:-)

The screenshot shows the NetworkMiner 1.6.1 interface. The main window displays a list of network frames, with frame 167 selected. The details pane shows the message content: "<HTML><BODY>thanks dude</BODY></HTML>" and its MD5 hash: d18767... The case panel on the right shows the same MD5 hash.

thanks dude

see you in hawaii!



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

NetworkMiner 1.6.1

File Tools Help

-- Select a network adapter in the list --

Hosts (14) Frames (24x) Files (3) Images Messages (4) Credentials (1) Sessions (6) DNS (3) Parameters (22) Keywords Cleartext Anomalies

Frame nr.	Source ...	Destinat...	From	To	Subject	Protocol	Timesta...
25	192.168...	64.12.2...		Sec558...	Here's the secret rec...	Oscar	13:08:2...
167	64.12.2...	192.168...	Sec558...		<HTML><BODY><F...	Oscar	13:08:2...
184	64.12.2...	192.168...	Sec558...		<HTML><BODY><F...	Oscar	13:08:2...
212	192.168...	64.12.2...		Sec558...	see you in hawaii!	Oscar	13:08:2...

Attribute	Value
Destination User	Sec558user1
IM Text	see you in hawaii!

see you in hawaii!

Recipe for Disaster:

1 serving

Ingredients:

4 cups sugar

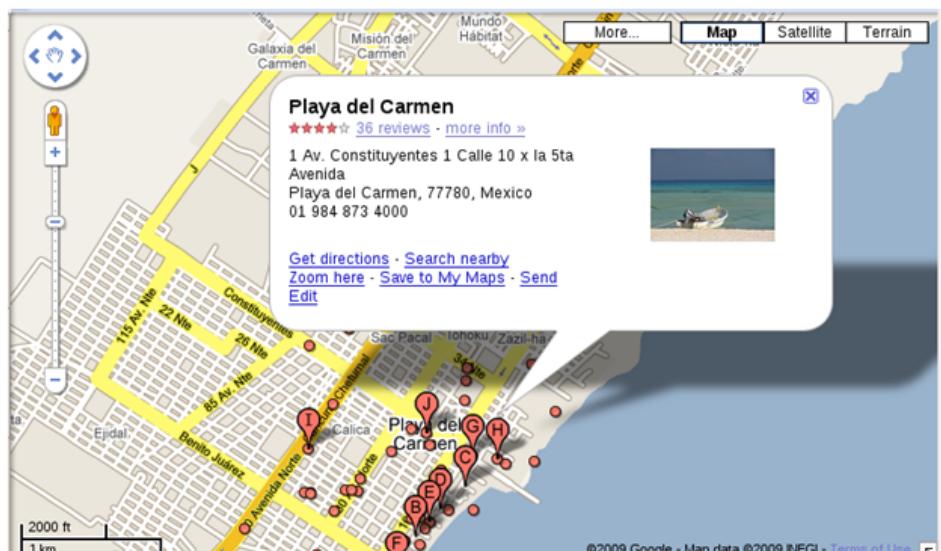
2 cups water

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.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.



NetworkMiner 1.6.1

File Tools Help

Select a network adapter in the list --

Hosts (22) Frames (81) Files (8) Images Messages (6) Credentials (2) Sessions (8) DNS (12) Parameters (83) Keywords Clearfirst Anomalies

Frame nr.	Source	Destnat.	From	To	Subject	Protocol	Timestamp
25	192.168.64.12.2	192.168.64.12.2	Se558..	Oscar	He's the secret rec...	Http	13:08:2...
167	64.12.2	192.168.64.12.2	Se558..	Oscar	<HTML><BODY>-F-	Http	13:08:2...
184	64.12.2	192.168.64.12.2	Se558..	Oscar	<HTML><BODY>-F-	Http	13:08:2...
212	192.168.64.12.2	192.168.64.12.2	Se558..	Oscar	see you in Hawaii!	Http	13:08:2...
320	192.168.64.12.1	"Ann D...@csc55...	csc55...	Oscar	Lunch next week	Http	13:10:2...
797	192.168.64.12.1	"Ann D...@csc55...	csc55...	Oscar	rendezvous	Http	13:10:2...

Attribute Value

Message-ID <001101ca63ae...

From <Ann Devover>...

To <anndevover@...

Subject rendezvous

Date Sat, 10 Oct 200...

MIME-Version 1.0

Content-Type multipart/mixed...

X-Priority --_NextPart_...

X-MSMail-Priority 3

X-Mailer Normal

X-MimeOLE Microsoft Outlook...

X-Header Produced By M...

Content-Transfer quoted-printable

Case Panel

Renam... MD5 evidenc... d18767... evidenc... cfac149...

H sweetheart! Bring your fake passport and a bathing suit. Address attached. love, Ann

Hi sweetheart! Bring your fake passport and a bathing suit. Address attached.
love, Ann



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

The screenshot shows a NetworkMiner 1.6.1 interface. The top menu bar includes File, Tools, Help, and a dropdown for selecting a network adapter. Below the menu is a toolbar with icons for Hosts, Frames, Files, Images, Messages, Credentials, Sessions, DNS, Parameters, Keywords, Cleartext, and Anomalies. The main window displays a list of captured frames. Frame 25 shows a message from '64.12.2.' to '64.12.1.' with subject 'See558...'. Frame 167 shows a response from '64.12.1.' to '64.12.2.' with subject 'Re: See558...'. Frame 184 shows another message from '64.12.1.' to '64.12.2.' with subject 'lunch next week'. Frame 212 shows a response from '64.12.2.' to '64.12.1.' with subject 'Re: lunch next week'. Frame 320 shows a message from '64.12.1.' to '64.12.2.' with subject 'Ann D... cse55... lunch next week'. Frame 797 shows a response from '64.12.2.' to '64.12.1.' with subject 'Ann D... cse55... rendezvous'. To the right of the frame list is a detailed view of the selected frame's attributes, including Message-ID, From, To, Subject, Date, MIME-Version, Content-Type, Boundary, X-Priority, X-MSMail-Protocol, X-Mailer, and Content-Transfer. Below the frame list is a text area containing the message body: "Sorry-- I can't do lunch next week after all. Heading out of town. Another time! - Ann". A 'Case Panel' on the right lists file names: M05, d18767, evidenc., dfa149.

Sorry-- I can't do lunch next week after all. Heading out of town. Another time! - Ann

Client	Server	Protocol	Username	Password	Valid login	Login ti...
192.168...	64.236...	HTTP C...	JEB2=4...	N/A	Unknown	13-08-2...
192.168....	64.12.1...	SMTP	sneaky...	558r001z	Unknown	10-10-2...

- What is Ann's email address?
sneakyg33k@aol.com

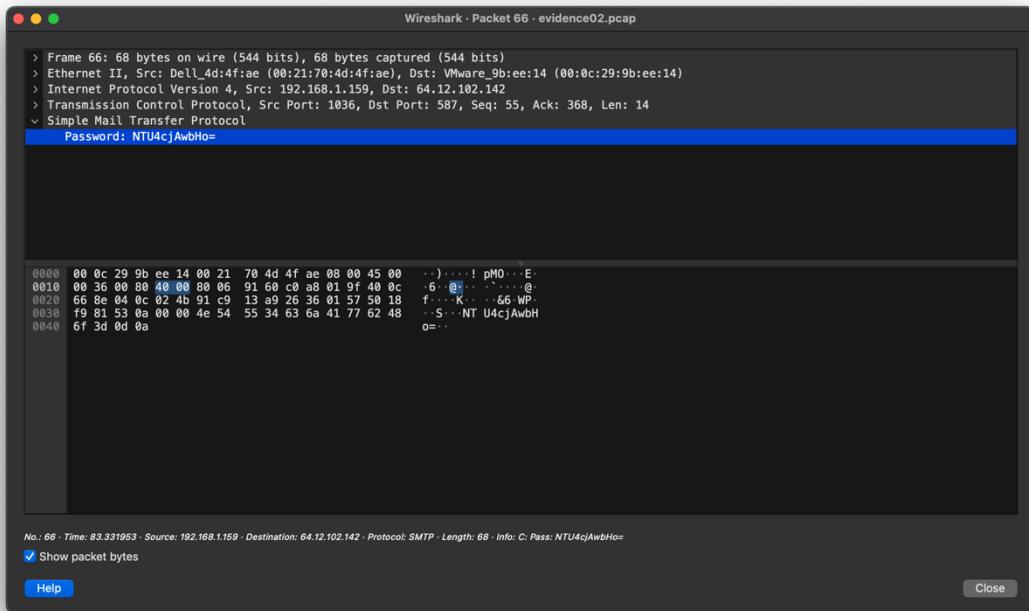
The screenshot shows a Wireshark window titled 'Wireshark - Packet 69 - evidence02.pcap'. The packet details pane shows a Simple Mail Transfer Protocol (SMTPL) command: 'MAIL FROM: <sneakyg33k@aol.com>\r\n'. The bytes pane shows the raw hex and ASCII data of the packet. The status bar at the bottom indicates: 'No.: 69 · Time: 83.465436 · Source: 192.168.1.159 · Destination: 64.12.102.142 · Protocol: SMTP · Length: 87 · Info: C: MAIL FROM: <sneakyg33k@aol.com>'. At the bottom left, there is a checked checkbox for 'Show packet bytes'. At the bottom right, there are 'Help' and 'Close' buttons.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

2. What is Ann's email password?

558r00lz



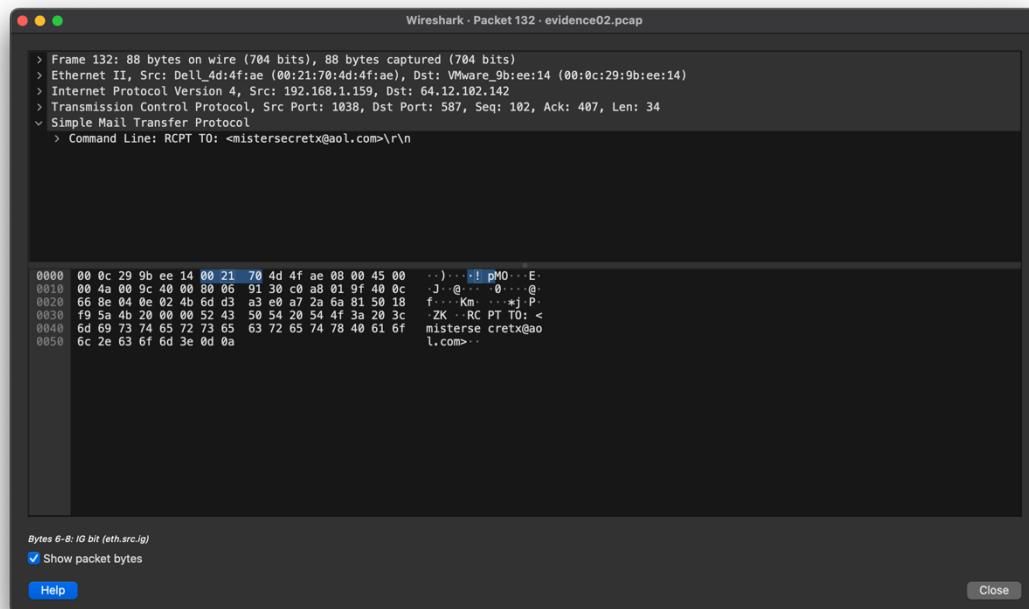
Wireshark - Packet 66 · evidence02.pcap

> Frame 66: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: Dell_4d:4f:ae (00:21:70:4d:4f:ae), Dst: VMware_9b:ee:14 (00:0c:29:9b:ee:14)
> Internet Protocol Version 4, Src: 192.168.1.159, Dst: 64.12.102.142
> Transmission Control Protocol, Src Port: 1036, Dst Port: 587, Seq: 55, Ack: 368, Len: 14
Simple Mail Transfer Protocol
Password: NTU4cjAwbHo=

No.: 66 · Time: 83.331953 · Source: 192.168.1.159 · Destination: 64.12.102.142 · Protocol: SMTP · Length: 68 · Info: C-Pass: NTU4cjAwbHo=
 Show packet bytes
Help Close

3. What is Ann's secret lover's email address?

mistersecretx@aol.com



Wireshark - Packet 132 · evidence02.pcap

> Frame 132: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
> Ethernet II, Src: Dell_4d:4f:ae (00:21:70:4d:4f:ae), Dst: VMware_9b:ee:14 (00:0c:29:9b:ee:14)
> Internet Protocol Version 4, Src: 192.168.1.159, Dst: 64.12.102.142
> Transmission Control Protocol, Src Port: 1038, Dst Port: 587, Seq: 102, Ack: 407, Len: 34
Simple Mail Transfer Protocol
> Command Line: RCPT TO: <mistersecretx@aol.com>\r\n

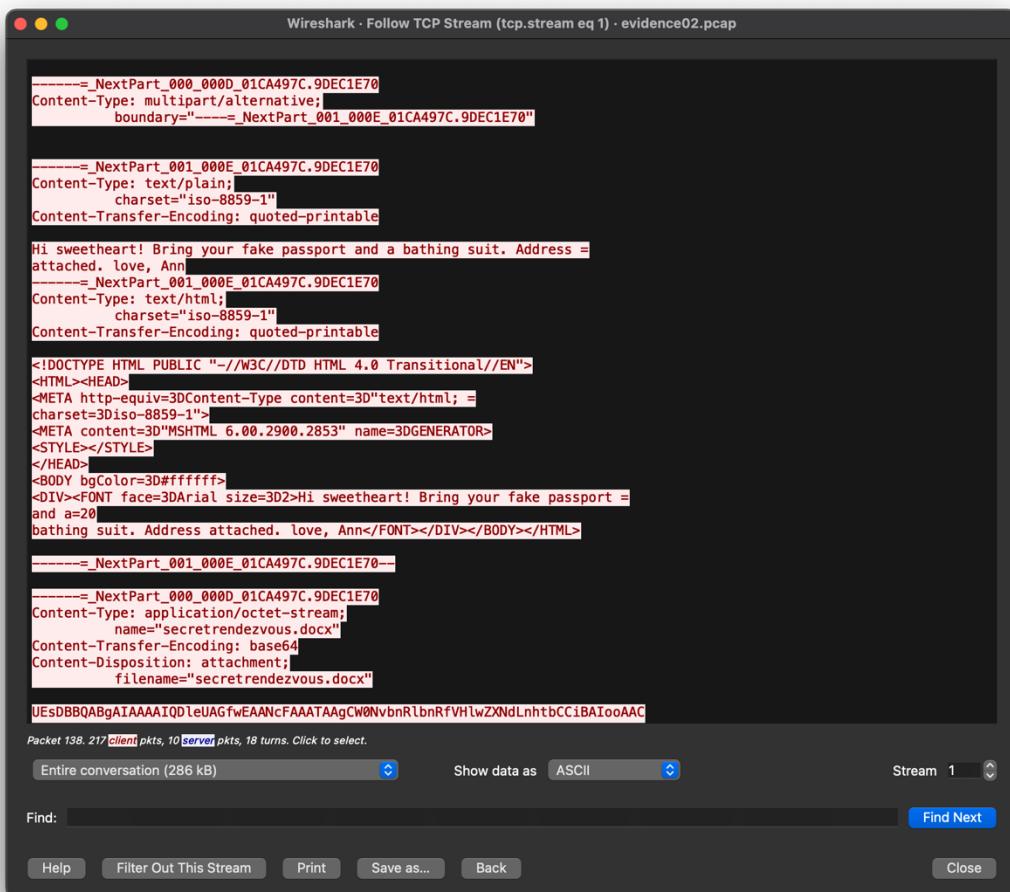
Bytes 6-8: IQ bit (eth.src.g)
 Show packet bytes
Help Close



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

4. What two items did Ann tell her secret lover to bring?

Fake passport and bathing suit



The screenshot shows the Wireshark interface with the TCP Stream 1 selected. The message content is displayed in ASCII format:

```
-----=_NextPart_000_000D_01CA497C.9DEC1E70
Content-Type: multipart/alternative;
boundary="-----=_NextPart_001_000E_01CA497C.9DEC1E70"

-----=_NextPart_001_000E_01CA497C.9DEC1E70
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Hi sweetheart! Bring your fake passport and a bathing suit. Address =
attached. love, Ann
-----=_NextPart_001_000E_01CA497C.9DEC1E70
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; =
charset=3Diso-8859-1">
<META content=3D"MSHTML 6.00.2900.2853" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV><FONT face=3Darial size=3D2>Hi sweetheart! Bring your fake passport =
and a=20
bathing suit. Address attached. love, Ann</FONT></DIV></BODY></HTML>

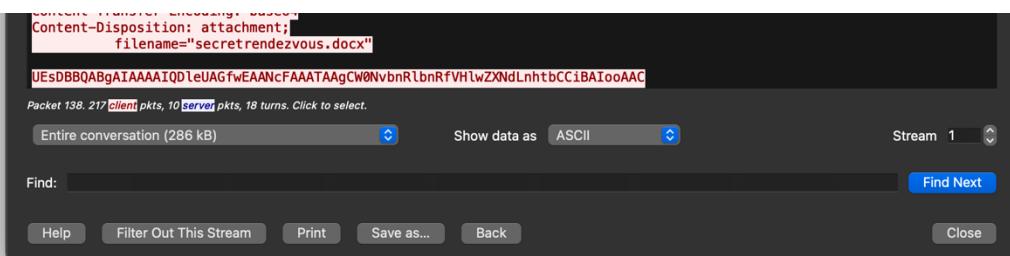
-----=_NextPart_001_000E_01CA497C.9DEC1E70--

-----=_NextPart_000_000D_01CA497C.9DEC1E70
Content-Type: application/octet-stream;
name="secretrendezvous.docx"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="secretrendezvous.docx"

UEsDBBQABgAIAAAIIQDleUAGfwEAANcFAAATAAgCW0NvbnnRlbnRfVHlwZXNdlnhbtCCiBAIooAAC
```

5. What is the NAME of the attachment Ann sent to her secret lover?

secretrendezvous.docx



The screenshot shows the Wireshark interface with the TCP Stream 1 selected. The attachment details are displayed in ASCII format:

```
Content-Type: application/octet-stream;
Content-Disposition: attachment;
filename="secretrendezvous.docx"

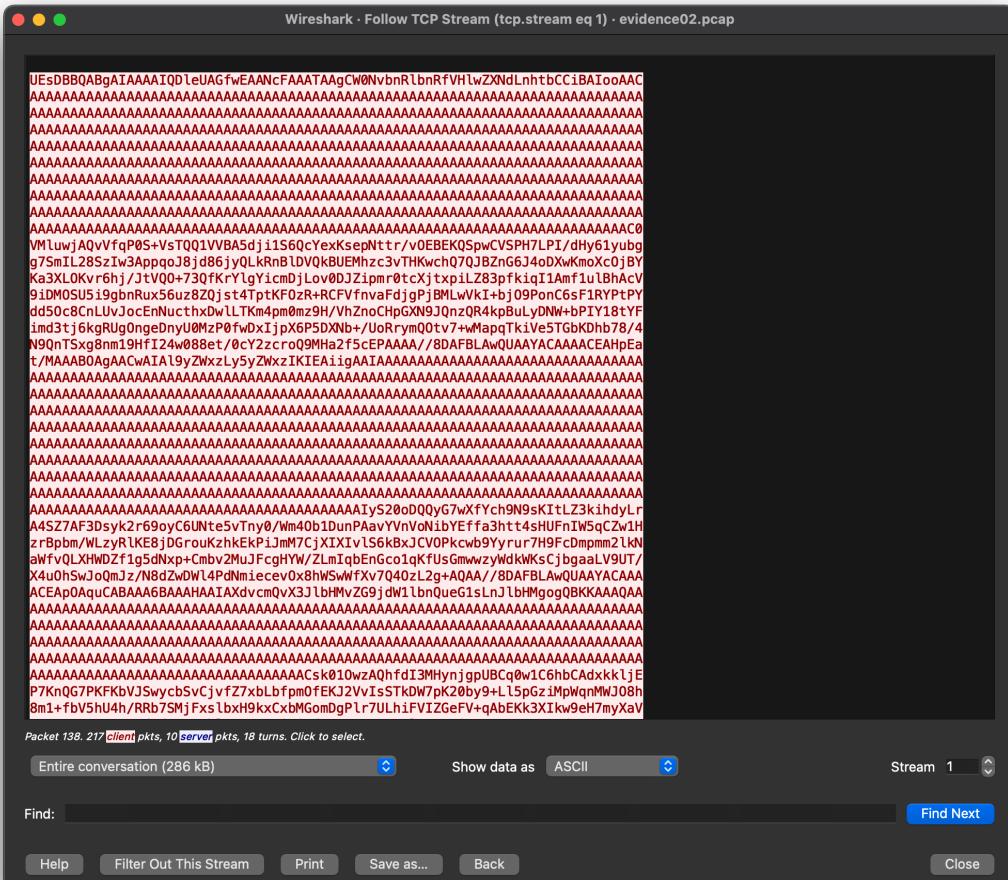
UEsDBBQABgAIAAAIIQDleUAGfwEAANcFAAATAAgCW0NvbnnRlbnRfVHlwZXNdlnhbtCCiBAIooAAC
```



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

6. What is the MD5sum of the attachment Ann sent to her secret lover?

9E423E11DB88F01BBFF81172839E1923



The screenshot shows a Wireshark window with the title "Wireshark - Follow TCP Stream (tcp.stream eq 1) · evidence02.pcap". The main pane displays a single TCP stream. The first few bytes of the payload are the MD5 hash: "9E423E11DB88F01BBFF81172839E1923". The rest of the payload consists of a large amount of binary data, which appears as a series of 'A' characters in the ASCII dump view.

Packet 138. 217 client pkts, 10 server pkts, 18 turns. Click to select.

Entire conversation (286 kB) Show data as ASCII Stream 1

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

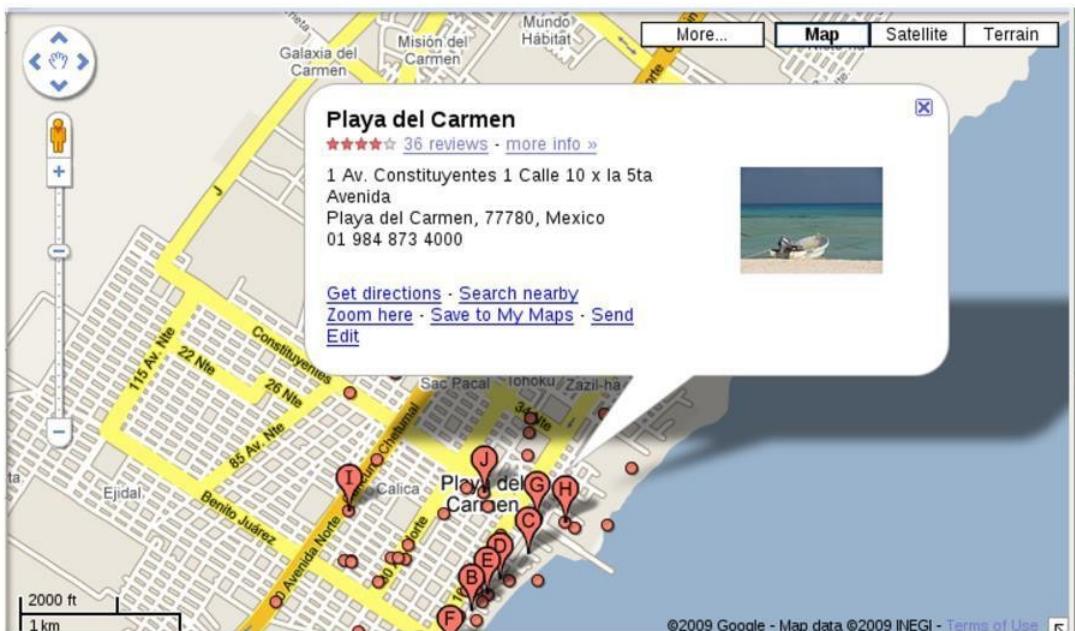


Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

7. In what CITY and COUNTRY is their rendez-vous point?

Location: Playa del Carmen, Mexico

Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.



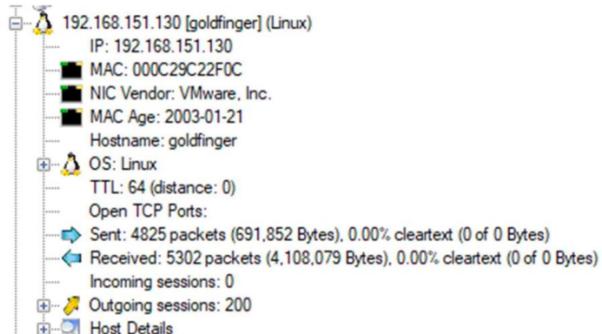
8. What is the MD5sum of the image embedded in the document?

MD5: 6d3c6ed7cb0a49ede228fd045efb3792

Case 2

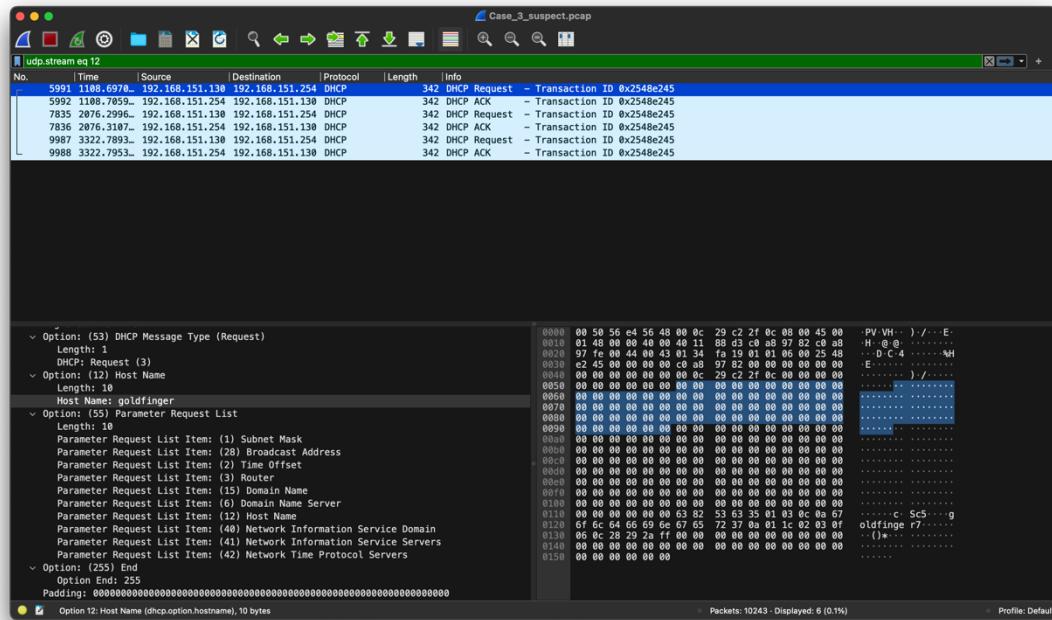
An employee named Steve Vogon is suspected of having illegal contacts with external parties. Steve is believed to have used his personal Linux laptop on the corporate network for his suspicious activity.

1. What IP address and hostname does Steve Vogon's Linux computer have?
192.168.151.130 – goldfinger



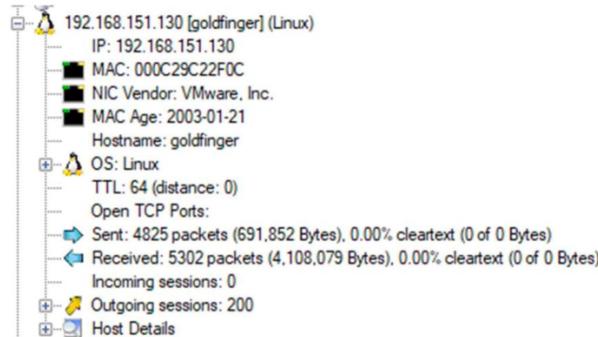


Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering



2. What evidence do you have to assume that this computer is running Linux?

Proof: TTL for Linux - 64



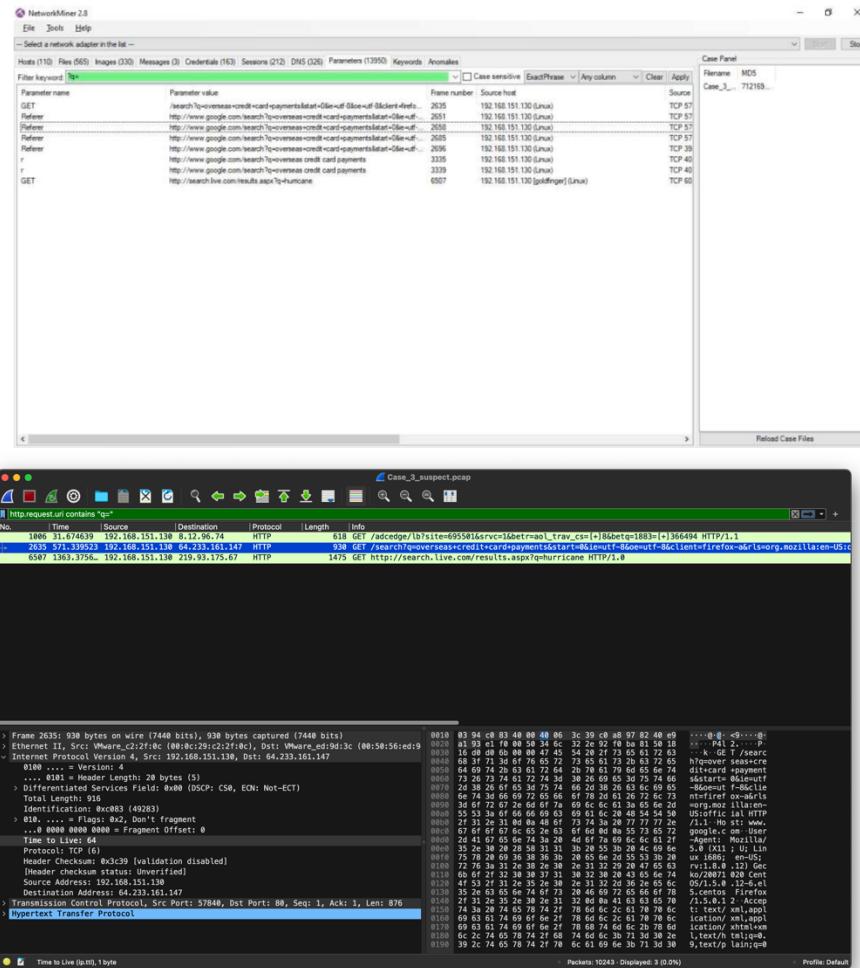
```
> Frame 5991: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: VMware_c2:2f:0c (00:0c:29:c2:2f:0c), Dst: VMware_e4:56:48 (00:50:56:e4:5
< Internet Protocol Version 4, Src: 192.168.151.130, Dst: 192.168.151.254
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x88d3 [validation disabled]
      [Header checksum status: Unverified]
    Source Address: 192.168.151.130
    Destination Address: 192.168.151.254
  > User Datagram Protocol, Src Port: 68, Dst Port: 67
  < Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
```



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

3. What Google searches did Steve Vogon perform?

- overseas credit card payments
- hurricane



4. What message did the email contain that Steve Vogon sent from his Gmail account?

Hello,

Can you please tell me what the minimum balance requirement is for opening an
overseas account at your bank?

Thank you,

Steve K.
Vogon



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Parameter name	Parameter value
TLS Handshake ServerHello Supported Version	3.1 (0x301)
TLS Handshake ServerHello Supported Version	3.1 (0x303)
TLS Handshake ServerHello Supported Version	3.1 (0x301)
TLS Handshake ServerHello Supported Version	3.1 (0x301)
[A]35 Signature	769,4
[A]35 Signature	769,4
[A]35 Signature	769,4
[A]35 Signature	769,53
[A]35 Hash	53611273a714cb4789c8222932ef15a7
[A]35 Hash	53611273a714cb4789c8222932ef15a7
[A]35 Hash	53611273a714cb4789c8222932ef15a7
[A]35 Hash	able32eaf70ee94:0a0f08bd126891
body	Hello, Can you please tell me what the minimum balance requirement is for opening an overseas account at your bank? The
body	Hello, Can you please tell me what the minimum balance requirement is for opening an overseas account at your bank
body	Hello, Can you please tell me what the minimum balance requirement is for opening an overseas account at your bank

5. How did Steve find the email address to which he sent his email?

Website: www.noblebank.pl Email:investors@noblebank.pl

File	Tools	Help										
Hosts (110) Files (545) Images (330) Messages (3) Credentials (163) Sessions (212) DNS (326) Parameters (13950) Keywords Anomalies												
Filter keyword												
Parameter name	Parameter value	Frame number	Source host	Source port	Destination host	Protocol	Case sensitive	ExactPhrase	Parameter name	Clear	App	
autovisit	1	2401	192.168.151.130 (Linux)	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	autovisit			
Certificate valid to	05-01-2018 11:10:19	3422	63.249.209.31 (addons.glib.mobilla.com)[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
Certificate valid to	29-01-2014 16:30:00	3422	63.249.209.31 (addons.glib.mobilla.com)[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
Certificate valid to	27-01-2014 16:30:00	3422	63.249.209.31 (addons.glib.mobilla.com)[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
Certificate valid to	16-12-2013 19:30:00	3422	63.249.209.31 (addons.glib.mobilla.com)[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
Certificate valid to	28-01-2014 16:30:00	3400	63.249.209.31 (addons.glib.mobilla.com)[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
Certificate valid to	28-01-2014 16:30:00	3400	63.249.209.31 (addons.glib.mobilla.com)[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
Certificate valid to	16-12-2013 19:30:00	3400	63.249.209.31 (addons.glib.mobilla.com)[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
Certificate valid to	05-01-2009 11:10:19	3400	63.249.209.31 (addons.glib.mobilla.com)[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
Certificate valid to	28-01-2014 16:30:00	3377	63.249.209.31 (addons.glib.mobilla.com)[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
Certificate valid to	27-01-2014 16:30:00	3377	63.249.209.31 (addons.glib.mobilla.com)[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
Certificate valid to	16-12-2013 19:30:00	3377	63.249.209.31 (addons.glib.mobilla.com)[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
Certificate valid to	05-01-2009 11:10:19	3377	63.249.209.31 (addons.glib.mobilla.com)[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
Certificate valid to	04-01-2011 22:39:06	2276	69.147.112.160 ([logon.yahoo.akamai.net])[...]	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	Certificate valid to			
correlation	11978983012617	4162	192.168.151.130 (Linux)	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	correlation			
customerid	11978983012617	4162	192.168.151.130 (Linux)	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	customerid			
customerid	11978983012617	3986	192.168.151.130 (Linux)	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	customerid			
customerid	D1B8634C-1471-4116-91DE-AFC100D010004	5229	192.168.151.130 (postfix)[...]	443	TCP ACK[4] > 192.168.151.130 (postfix)[...]	TCP ACK[4]	0	0	customerid			
customerid	D1B8634C-1471-4116-91DE-AFC100D010005	6770	192.168.151.130 (postfix)[...]	443	TCP ACK[4] > 192.168.151.130 (postfix)[...]	TCP ACK[4]	0	0	customerid			
customerid	D1B8634C-1471-4116-91DE-AFC100D010006	8070	192.168.151.130 (postfix)[...]	443	TCP ACK[4] > 192.168.151.130 (postfix)[...]	TCP ACK[4]	0	0	customerid			
customerid	D1B8634C-1471-4116-91DE-AFC100D010007	7843	192.168.151.130 (postfix)[...]	443	TCP ACK[4] > 192.168.151.130 (postfix)[...]	TCP ACK[4]	0	0	customerid			
customerid	D1B8634C-1471-4116-91DE-AFC100D010008	4897	192.168.151.130 (postfix)[...]	443	TCP ACK[4] > 192.168.151.130 (postfix)[...]	TCP ACK[4]	0	0	customerid			
gata	http://home.diney.go.th/tranfer/index.php	1000	192.168.151.130 (postfix)[...]	443	TCP ACK[4] > 192.168.151.130 (postfix)[...]	TCP ACK[4]	0	0	gata			
MicrosoftOfficeWebServer	http://doseey.go.th/conncporate/	5044	192.168.151.130 (postfix)[...]	443	TCP ACK[4] > 192.168.151.130 (postfix)[...]	TCP ACK[4]	0	0	MicrosoftOfficeWebServer			
MicrosoftOfficeWebServer	http://investorstdinternat.../index.php	5203	192.168.151.130 (Linux)	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	MicrosoftOfficeWebServer			
MicrosoftOfficeWebServer	http://investorstdinternat.../index.php	5203	192.168.151.130 (Linux)	443	TCP ACK[4] > 192.168.151.130 (Linux)	TCP ACK[4]	0	0	MicrosoftOfficeWebServer			
VISITOR_INFO1_LIVE	d0e5fb9f7eA	4796	219.93.175.67 (youtube)[...]	443	TCP ACK[4] > 219.93.175.67 (youtube)[...]	TCP ACK[4]	0	0	VISITOR_INFO1_LIVE			
VISITOR_INFO1_LIVE	DGALKTRE2E	5412	219.93.175.67 (youtube)[...]	443	TCP ACK[4] > 219.93.175.67 (youtube)[...]	TCP ACK[4]	0	0	VISITOR_INFO1_LIVE			
VISITOR_INFO1_LIVE	MDXONPvF4H	4000	219.93.175.67 (youtube)[...]	443	TCP ACK[4] > 219.93.175.67 (youtube)[...]	TCP ACK[4]	0	0	VISITOR_INFO1_LIVE			
VISITOR_INFO1_LIVE	MDXONPvF4H	6	219.93.175.67 (youtube)[...]	443	TCP ACK[4] > 219.93.175.67 (youtube)[...]	TCP ACK[4]	0	0	VISITOR_INFO1_LIVE			



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

- 6. One web page opened by Steve contains a map, what region does the map show?**

/Images/Promotions/Mojito/Caribbean/TT_caribb_map_260x195.gif
Caribbean map

Frame nr.	Filename	Extension	Size	Source host	Destination host	S. port
6249	TT_captch-260x195.gpt	gpt	17,432 B	192.168.151.130	192.168.151.130	443
6710	index.html	html	19 B	192.168.151.130	192.168.151.130	(corporate disney go.com) [Other]
6736	site_imapmap.gpt	gpt	444 B	198.105.193.114	192.168.151.130	(corporate disney go.com) [Other]
6770	HG.C5BF6E17.gpt	gpt	43 B	64.154.81.197	192.168.151.130	[httpd-fcgi] [Linux]
7203	HG.D03B5D042.gpt	gpt	43 B	64.154.81.197	192.168.151.130	[gastfinger] [Linux]



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Conclusion:- Hence all the evidences were scanned properly to answer the questions which were verified successfully.

Postlab Questions:

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

Handling network-based incidents presents several challenges, including:

1. **Detection:** Identifying and detecting malicious activities or security breaches within the vast volume of network traffic can be challenging, especially with increasingly sophisticated attack techniques.
 2. **Visibility:** Lack of comprehensive visibility into network traffic, especially encrypted traffic, hampers the detection and analysis of suspicious behavior or anomalies.
 3. **Complexity:** Networks are becoming more complex with diverse architectures, cloud services, and IoT devices, making it difficult to monitor, analyze, and respond to security incidents effectively.
 4. **Data Volume:** The sheer volume of network data generated by modern networks can overwhelm security tools and personnel, leading to difficulties in timely detection and response to security incidents.
 5. **False Positives:** Security tools may generate false positive alerts, overwhelming security teams with irrelevant or inaccurate information and diverting resources from genuine security incidents.
 6. **Privacy Concerns:** Balancing the need for network monitoring with privacy regulations and individual privacy rights presents a challenge, especially when capturing and analyzing sensitive user data.

8.2 Discuss the tools used for monitoring network traffic.

Several tools are used for monitoring network traffic, including:

1. **Wireshark:** A widely used network protocol analyzer that captures and displays network packets in real-time. It allows users to inspect packet details, analyze protocols, and troubleshoot network issues.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

2. **Tcpdump:** A command-line packet analyzer for capturing and analyzing network packets. It offers similar functionality to Wireshark but is primarily used in terminal environments.
3. **NetworkMiner:** A network forensic analysis tool that captures and parses network packets to extract metadata, files, and artifacts exchanged over the network. It provides insights into network activities and facilitates forensic investigations.
4. **Ntopng:** A network traffic monitoring tool that provides real-time visibility into network traffic flows, protocols, and bandwidth usage. It offers detailed network statistics and graphical representations for network analysis.
5. **Snort:** An open-source intrusion detection system (IDS) that analyzes network traffic for signs of malicious activity or security breaches. It uses rule-based detection to identify and alert on suspicious network events.
6. **Suricata:** Another open-source IDS and intrusion prevention system (IPS) that monitors network traffic for suspicious behavior, including intrusion attempts, malware infections, and denial-of-service attacks. It offers high-performance network security monitoring and threat detection capabilities.

8.3 What do you understand by packet sniffing?

Packet sniffing refers to the process of capturing and analyzing network packets as they traverse a network interface. Packet sniffers (or network sniffer) intercept and log network traffic passing through a network segment, allowing users to inspect packet contents, analyze protocols, and troubleshoot network issues.

Packet sniffing can be performed using specialized software tools like Wireshark, Tcpdump, or NetworkMiner, which capture packets in real-time or from packet capture files. By analyzing packet headers and payloads, packet sniffers can provide insights into network activities, including communication between devices, protocol usage, application behavior, and potential security threats.

Packet sniffing is commonly used for network troubleshooting, performance monitoring, security analysis, and network forensics. However, it can also raise privacy concerns if used to capture sensitive information, highlighting the importance of ethical considerations and legal compliance when performing packet sniffing activities.