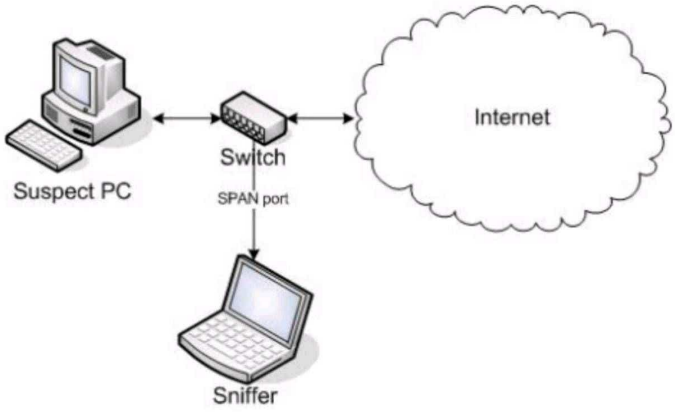
Aim :
Network forensic using Network Miner

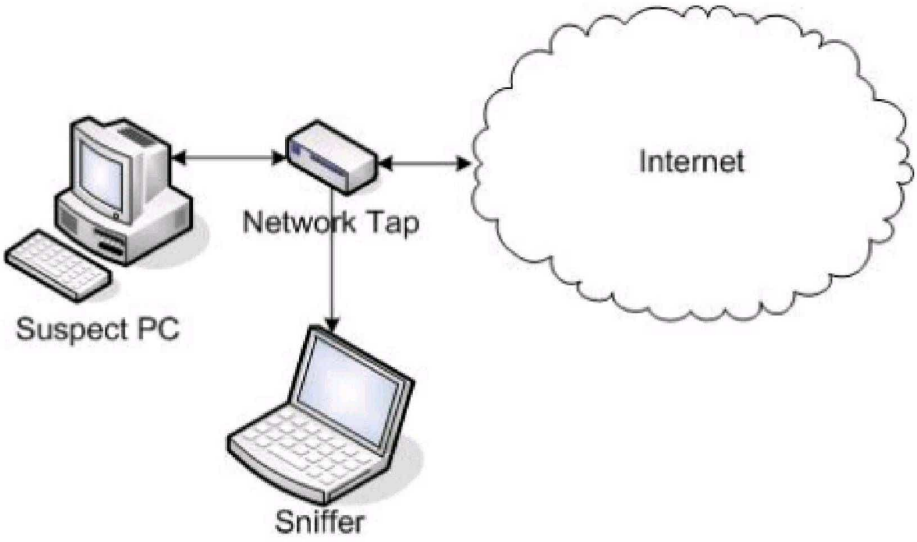
Theory :
Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information.

• When performing digital evidence collection from a stand alone computer
– Acquire data in transit (network traffic dump)
– Acquire data in use (RAM image)
– Acquire data at rest (hard drive image)
• A corporate incident response team has discovered network traffic that violates the law
Connecting a Network Sniffer
• SPAN/mirror port
– Re-configuration of switch
– Free port on switch



• Network Tap

– Special hardware
– No configuration



Capturing Network Traffic
dumpcap -i 1 -f "host 213.1.2.3" –w wiretap.pcap -b filesize:100000

Analyzing Network Traffic

- Using Wireshark

http://www.wireshark.org/

In the scope of a digital forensics-based investigation, Wireshark can be immensely helpful, especially in finding and displaying emails that could be potential evidence. For example, Wireshark can be used to catch a suspect who is stealing a victim's wireless Internet to make fraudulent online purchases. By using Wireshark as a network monitoring tool, it is possible to find the IP or MAC address of the suspect, and to see what sites he or she is visiting.

Additionally, it may be possible to recover emails and other potentially sensitive and incriminating information that the suspect is sending over the network. When used in conjunction with other forensics tools, such as aircrack_ng (a tool that concentrates on examining wireless traffic versus Ethernet), it is possible to enhance the usefulness of Wireshark to make it an effective forensic network analysis tool.

- Using NetworkMiner

http://networkminer.sourceforge.

NetworkMiner is a Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux / Mac OS X / FreeBSD). NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.

Network forensics is a branch of digital forensics that deals with the monitoring, capturing, recording, and analysis of network traffic and events in order to gather evidence for investigating and responding to cybersecurity incidents, such as attacks, intrusions, data breaches, or policy violations. Here's an overview of the key aspects of network forensics:

1. Data Collection: Network forensics involves capturing and preserving network traffic data from various sources such as network devices (routers, switches, firewalls), intrusion detection systems (IDS), network-based security appliances, and packet sniffers. Data collection can be done in real-time or from stored logs.

2. Packet Analysis: Captured network traffic is analyzed at the packet level to reconstruct events, identify patterns, and extract relevant information. Packet analysis tools like Wireshark are commonly used to examine packet headers and payloads to understand communication protocols, extract files, and uncover anomalies.

3. Log Analysis: Network devices and security systems generate logs containing valuable information about network activities, such as login attempts, firewall rules, DNS queries, and system events. Analyzing these logs can provide insights into the sequence of events leading up to a security incident.

4. Traffic Reconstruction: Network forensics specialists reconstruct the sequence of events by piecing together captured packets, logs, and other artifacts. This process helps in understanding the timeline of an attack, identifying the attacker's methods, and determining the extent of the compromise.

5. Malware Analysis: Network forensics can involve analyzing network traffic to detect and analyze malware infections. This includes identifying communication patterns associated with malware, analyzing payloads, and extracting indicators of compromise (IOCs) for further investigation.

6. Incident Response: Network forensics plays a crucial role in incident response by providing real-time visibility into ongoing security incidents, allowing security teams to detect and mitigate threats quickly. It helps in containing the damage, preserving evidence, and restoring normal operations.

7. Evidence Presentation: Findings from network forensics investigations need to be presented in a clear and concise manner, often as part of legal proceedings or internal reports. This may involve creating timelines, visualizations, and detailed reports to communicate findings effectively.

Wireshark is a popular open-source network protocol analyzer used for network troubleshooting, analysis, development, and education. Originally named Ethereal, Wireshark was created by Gerald Combs in 1998 and has since become one of the most widely used network analysis tools.

1. Packet Capture: Wireshark allows users to capture live network traffic from various network interfaces or read packets from previously captured files. It supports capturing traffic on Ethernet, Wi-Fi, Bluetooth, USB, and other network interfaces.

2. Protocol Analysis: Wireshark provides detailed protocol analysis capabilities, allowing users to inspect packet headers and payloads for a wide range of network protocols, including TCP, UDP, IP, HTTP, DNS, FTP, SSH, TLS/SSL, and many others. It decodes protocols in real-time, providing valuable insights into network communications.

3. Filtering and Search: Wireshark offers powerful filtering and search capabilities, enabling users to narrow down captured traffic based on specific criteria such as IP addresses, ports, protocols, packet contents, and time frames. This helps in focusing on relevant traffic and quickly identifying relevant packets.

4. Export and Reporting: Wireshark supports exporting captured packets or analysis results to various formats, including plain text, CSV, XML, and PDML (Packet Description Markup Language). It also allows users to generate detailed reports summarizing network activities and findings.

NetworkMiner is a popular network forensic analysis tool used for capturing, parsing, and analyzing network traffic. It is primarily focused on extracting artifacts and metadata from captured packets to provide insights into network communications and potential security threats. Here's an overview of NetworkMiner's key features and capabilities:

1. Packet Capture: NetworkMiner can capture live network traffic from network interfaces or import packet capture (PCAP) files generated by other tools or devices. It supports capturing traffic from Ethernet, Wi-Fi, Bluetooth, and other network interfaces.

2. Protocol Analysis: Similar to Wireshark, NetworkMiner parses and decodes various network protocols to extract information such as IP addresses, MAC addresses, ports, protocols, packet payloads, and other metadata. It automatically identifies and categorizes protocols, making it easier to analyze network traffic.

3. File Extraction: One of NetworkMiner's notable features is its ability to extract files transferred over the network, including images, documents, executables, and other types of files embedded within network traffic. This feature is particularly useful for identifying data exfiltration, malware distribution, or unauthorized file transfers.

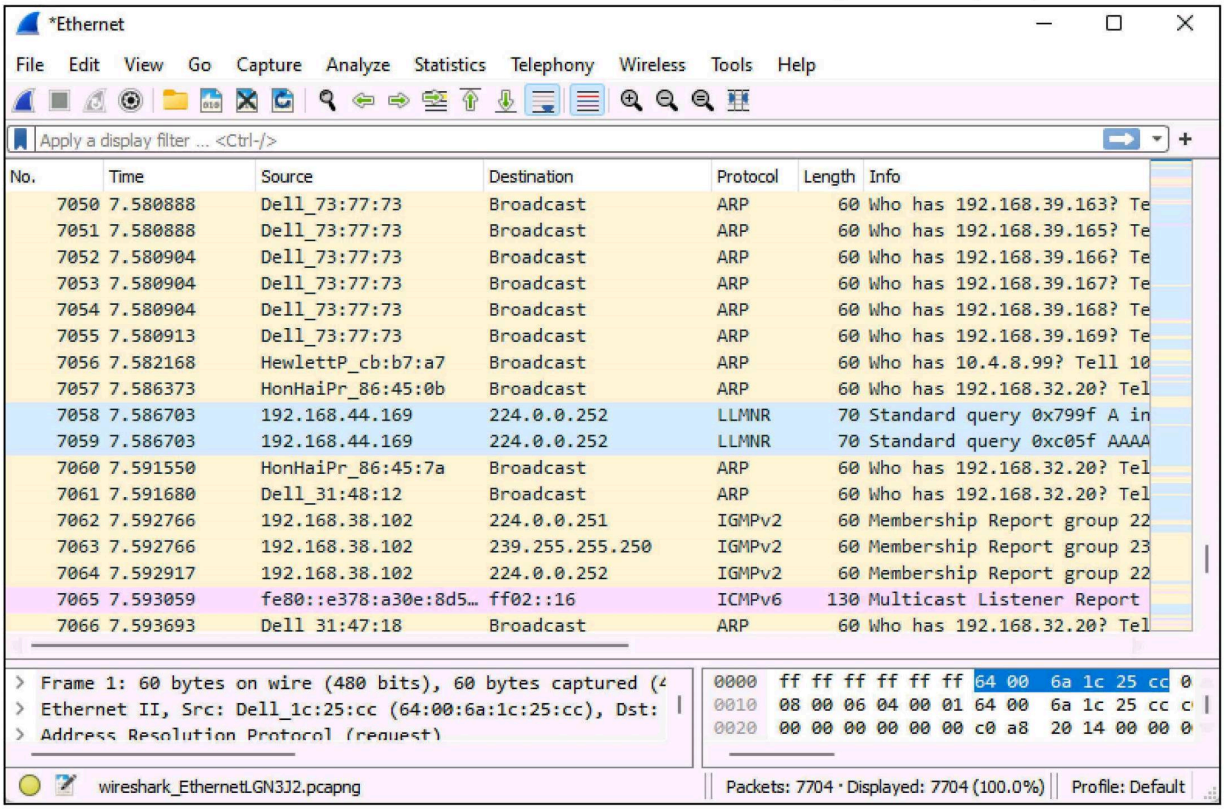
4. DNS and Host Analysis: NetworkMiner provides tools for analyzing DNS traffic and resolving hostnames associated with IP addresses. It can identify DNS queries and responses, extract domain names, and correlate IP addresses with hostnames. This helps in understanding the communication patterns and identifying potentially malicious domains.

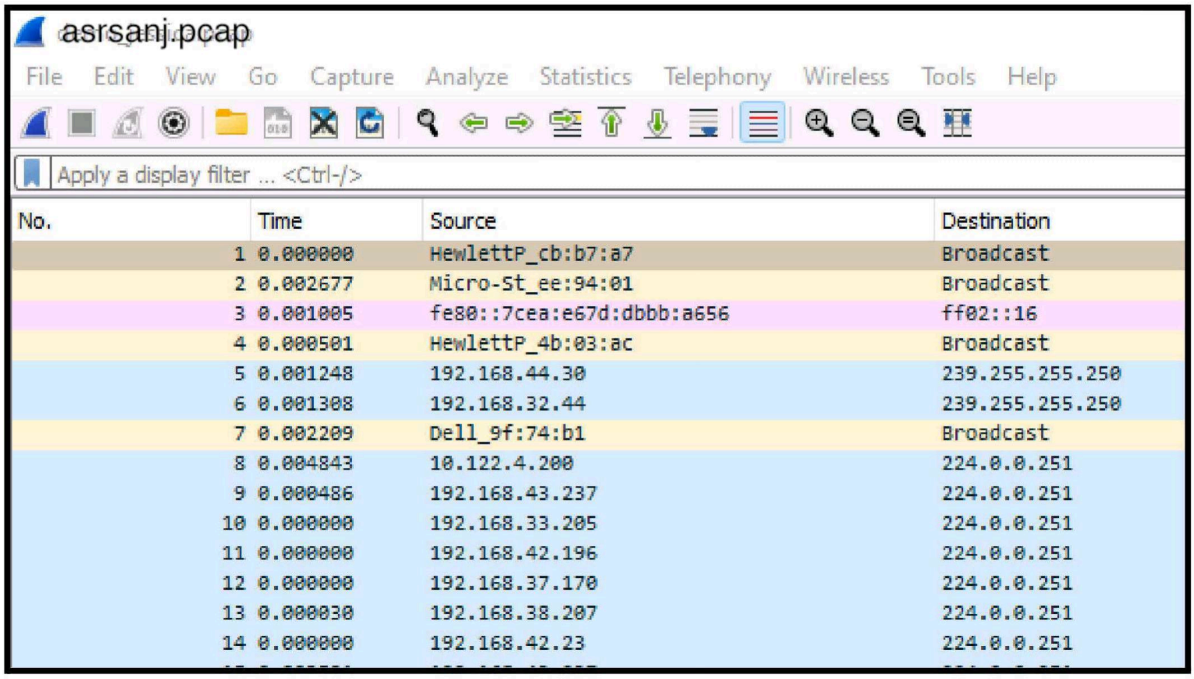
5. Timeline Analysis: NetworkMiner generates a timeline of network events based on captured packets, allowing users to visualize the sequence of network activities over time. This timeline can help in reconstructing network sessions, identifying patterns of behavior, and understanding the chronological order of events.

6. Export and Reporting: NetworkMiner allows users to export extracted files, metadata, and analysis results to various formats, including CSV, XML, and HTML. It also provides built-in reporting features for generating detailed reports summarizing network activities and findings.

Practical:

1. Using Wireshark to capture the network traffic and saving it as a .pcap file

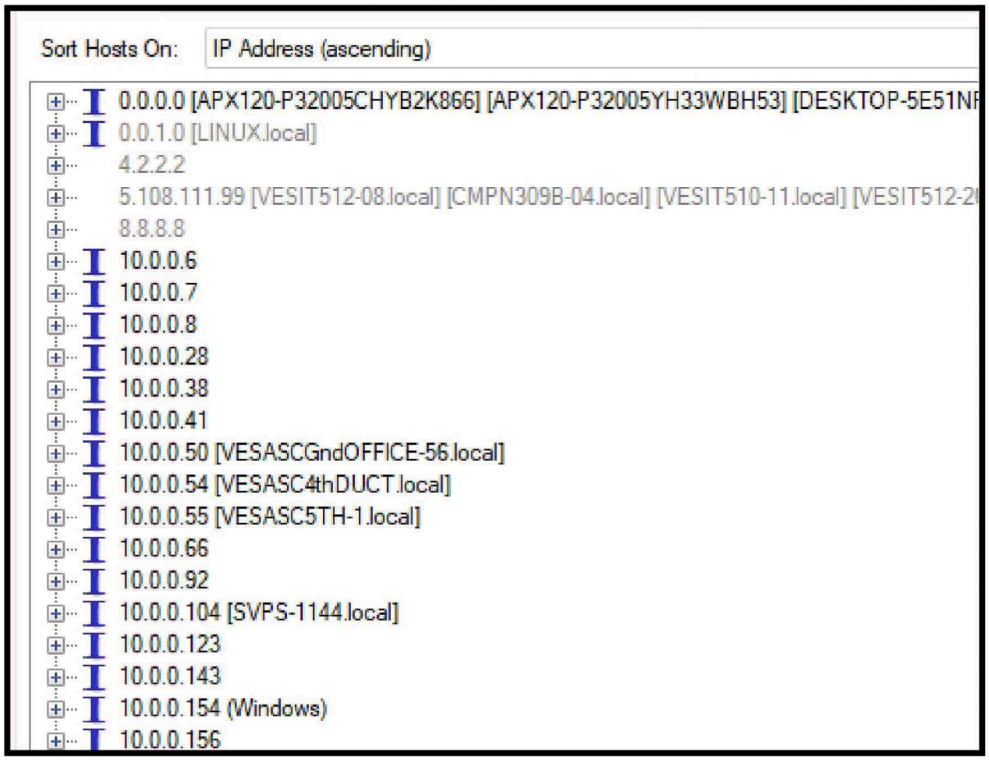




No.	Time	Source	Destination
1	0.000000	HewlettP_cb:b7:a7	Broadcast
2	0.002677	Micro-St_ee:94:01	Broadcast
3	0.001005	fe80::7cea:e67d:dbbb:a656	ff02::16
4	0.000501	HewlettP_4b:03:ac	Broadcast
5	0.001248	192.168.44.30	239.255.255.250
6	0.001308	192.168.32.44	239.255.255.250
7	0.002209	Dell_9f:74:b1	Broadcast
8	0.004843	10.122.4.200	224.0.0.251
9	0.000486	192.168.43.237	224.0.0.251
10	0.000000	192.168.33.205	224.0.0.251
11	0.000000	192.168.42.196	224.0.0.251
12	0.000000	192.168.37.170	224.0.0.251
13	0.000030	192.168.38.207	224.0.0.251
14	0.000000	192.168.42.23	224.0.0.251

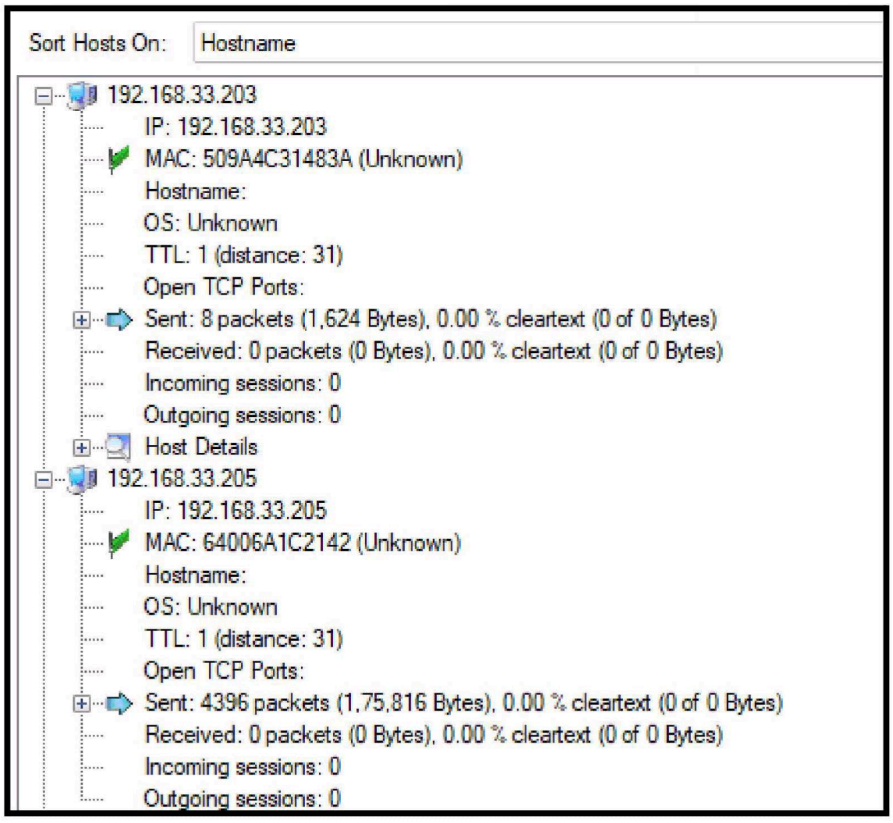
- **Analyzing it using Networkminer**

1. **IP Address**

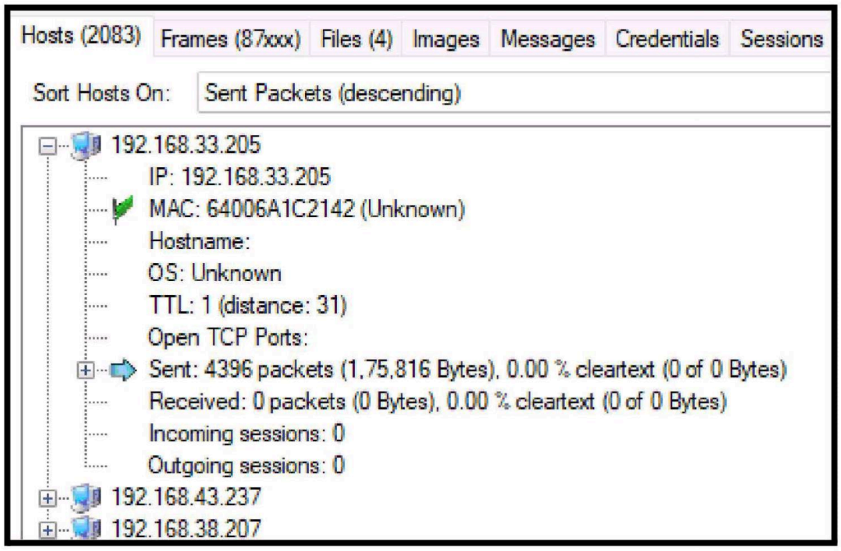


2. **MAC Address**

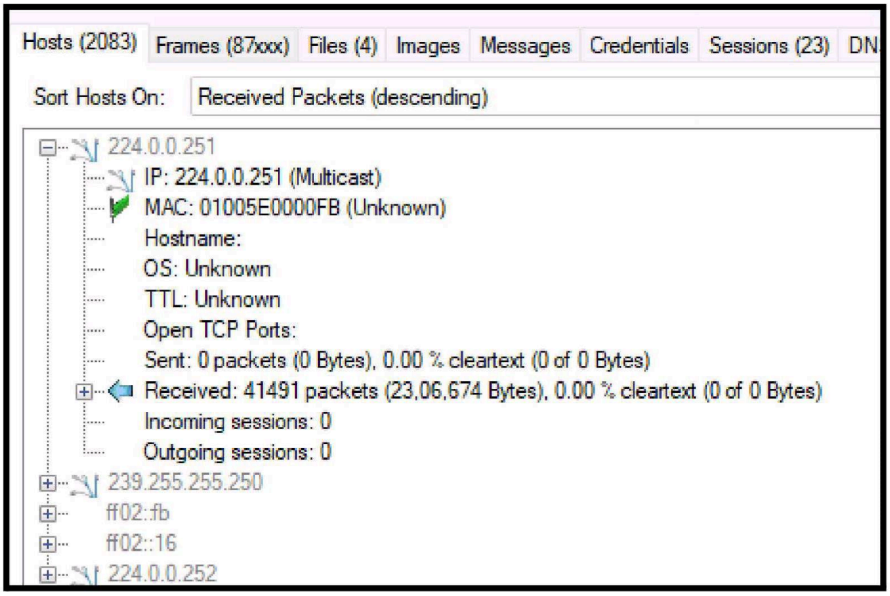
3. **Host names**



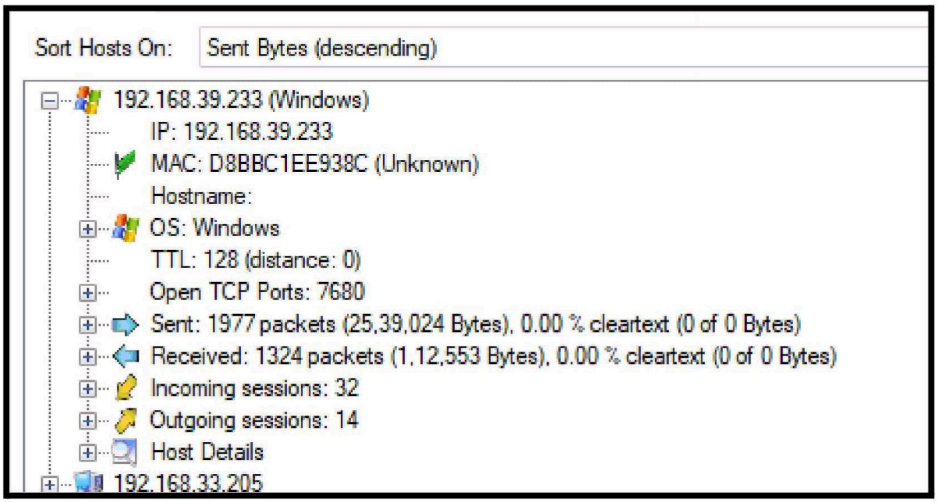
4. **Sent packets**



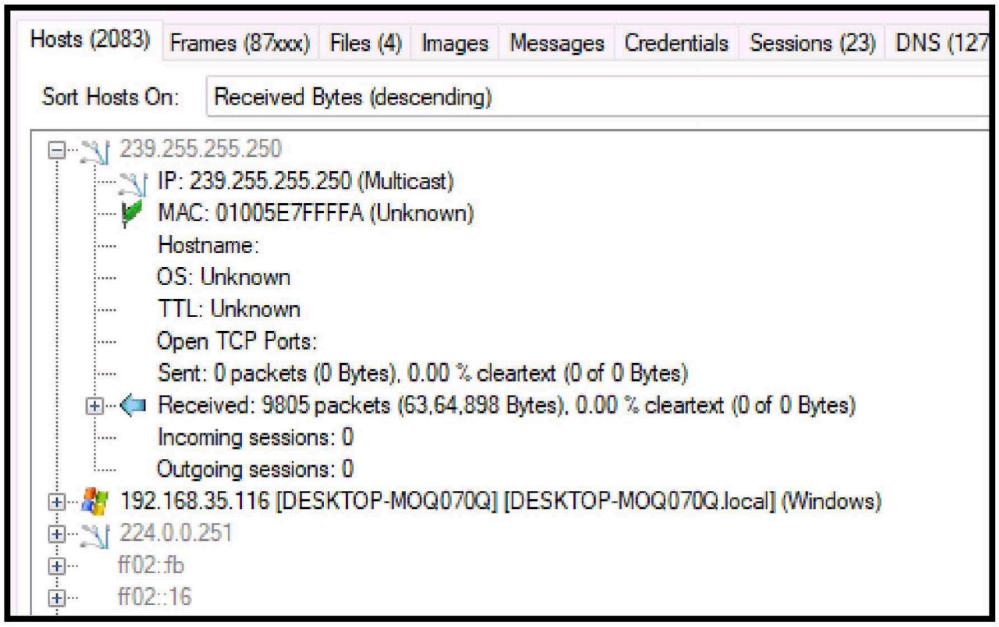
5. **Received packets**



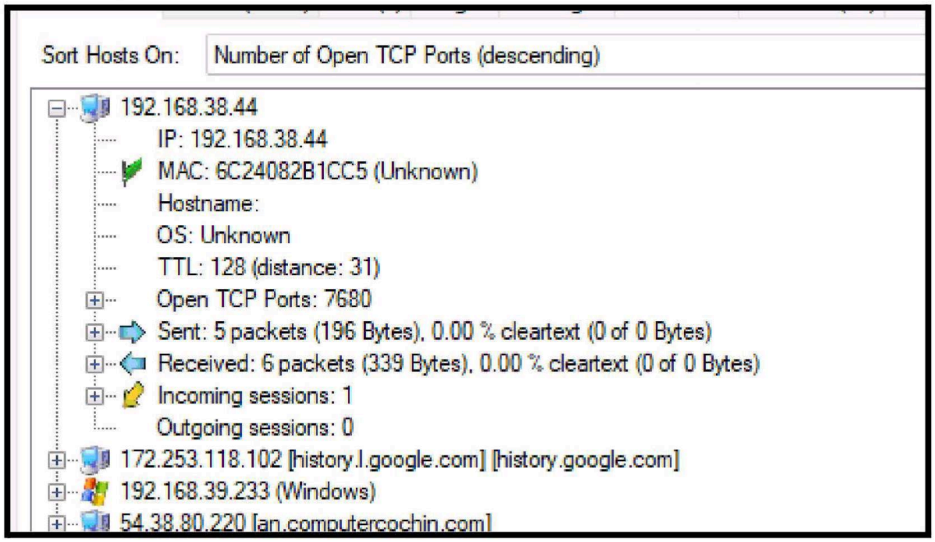
6. **Sent bytes**



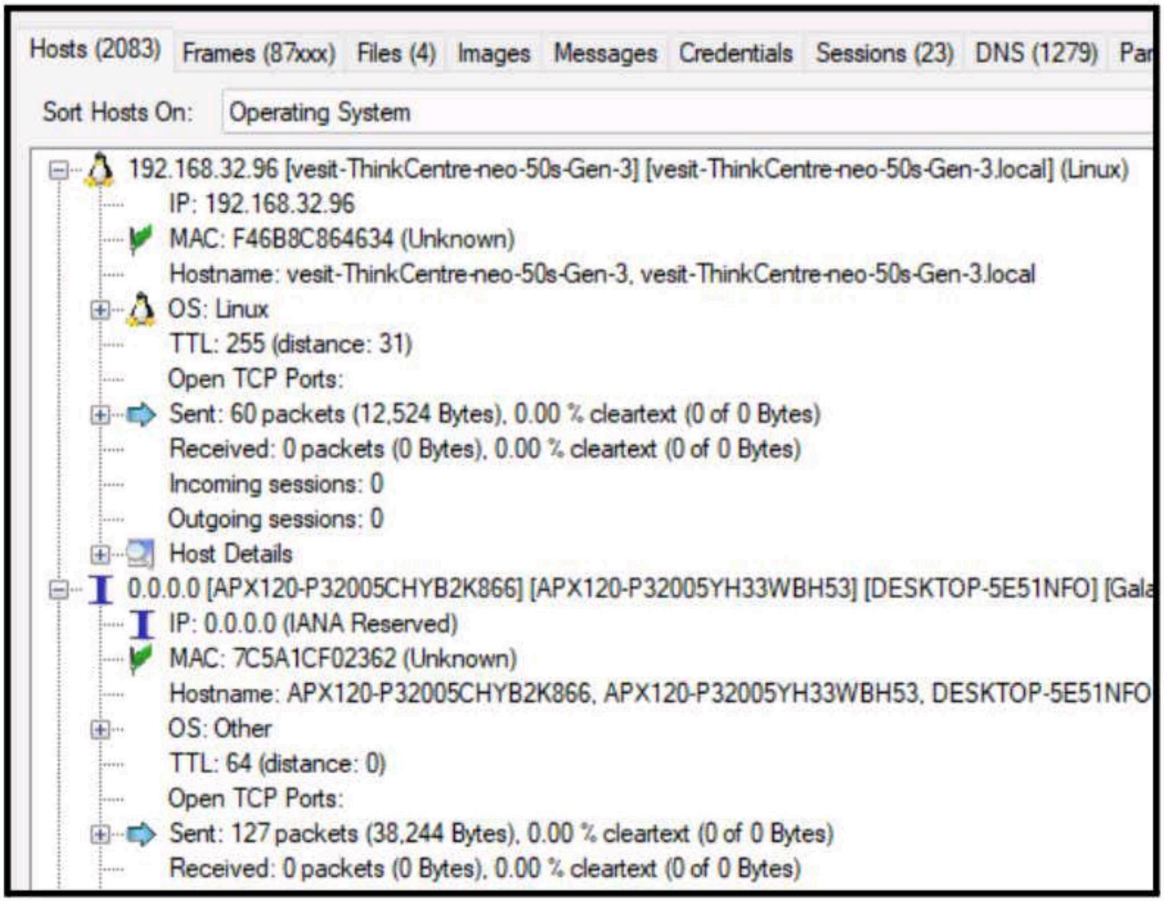
7. **Received bytes**



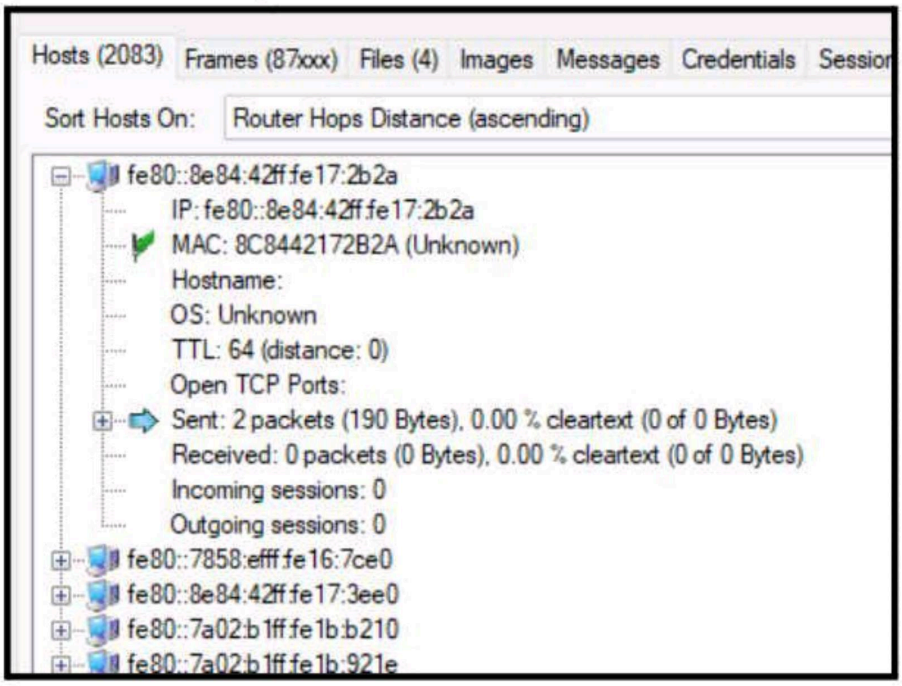
8. Open TCP Ports



9. Operating system



10. Router Hops distance

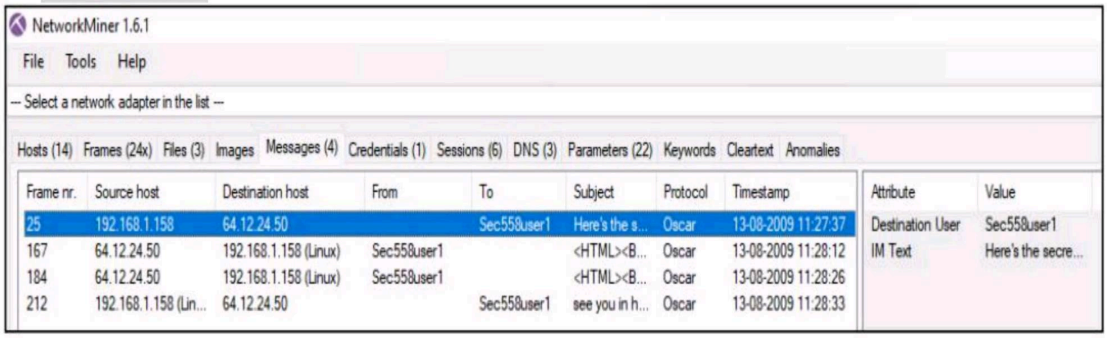


D17B1 SANJANA ASRANI DF-NETWORK MINER

1. Case 1: evidence01.pcap

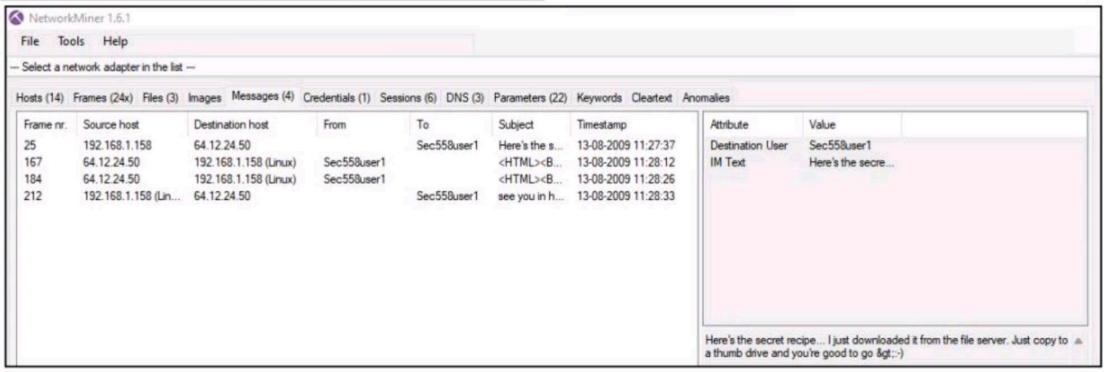
Q1. what is the name of Ann's IM buddy?

➔ **Sec558user1**



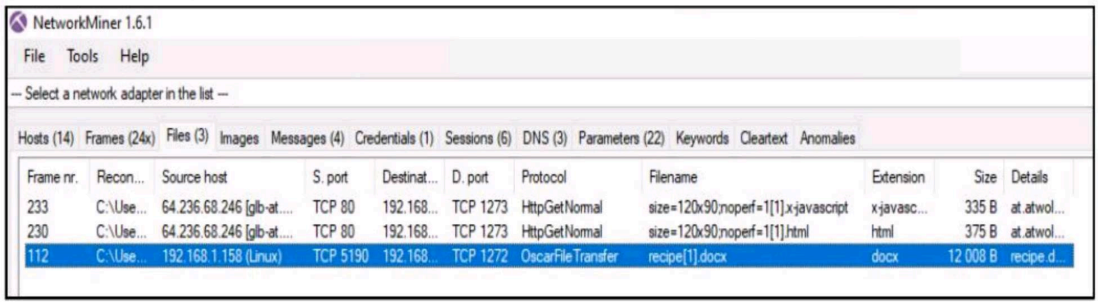
Q2. What was the first comment in the captured IM conversatioN?

➔ **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 >:-)**



Q3. What is the name of the file Ann Transferred?

➔ **recipe.docx**



Q4. What is the magic number of the file you want to extract (first four bytes)? Number ?

➔ **4f 46 54 32**

PROCESS TO FIND:

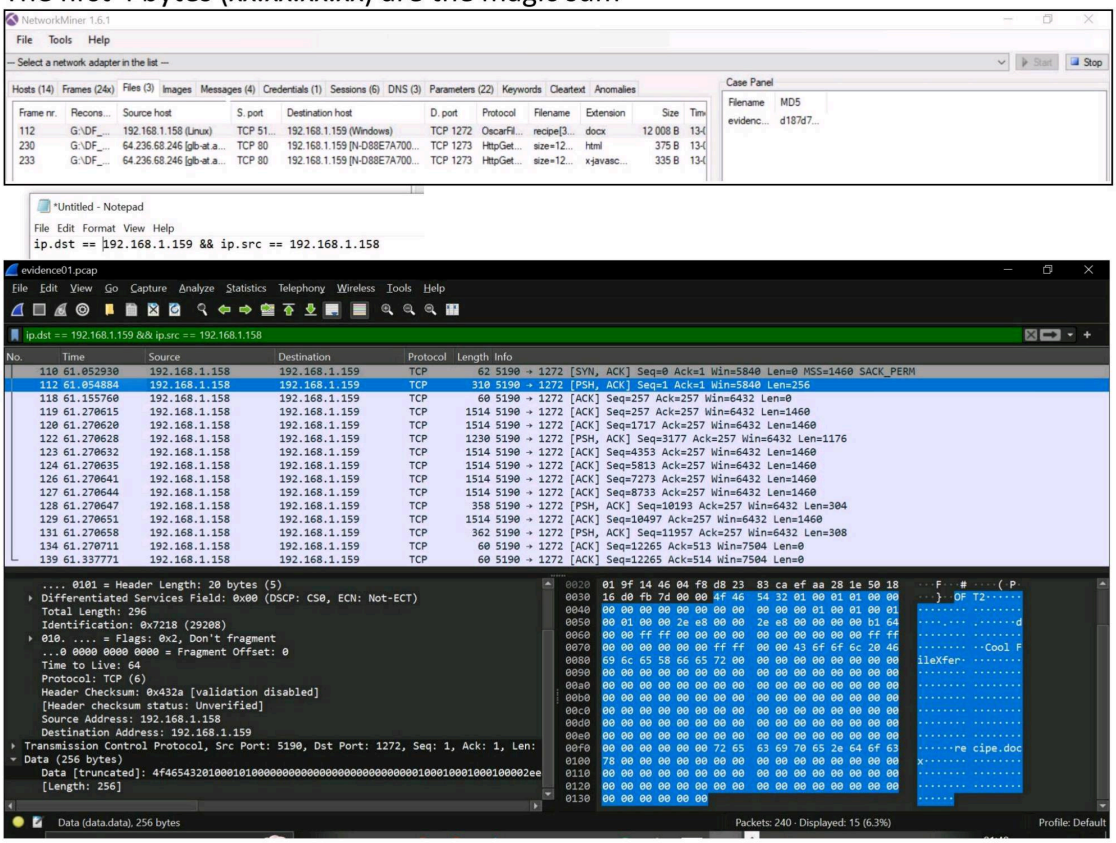
Create a filter query

Find the source and dest ip using Network Miner

filter the packets with those ips in Wireshark

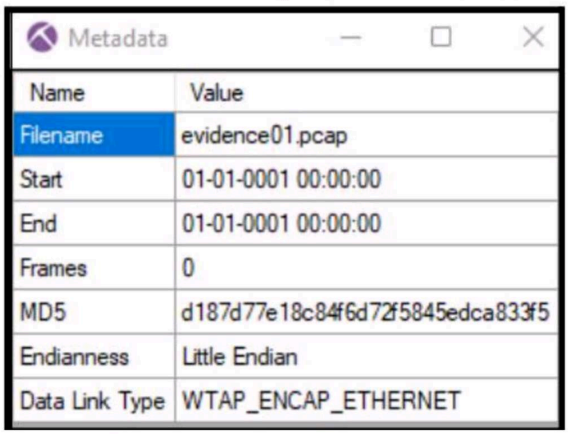
Find the tuples with the 'data field', click on the first tuple

The first 4 bytes (xx.xx.xx.xx) are the magic sum



Q5. What was the MD5 sum of the file?

➔ MD5 of evidence1.pcap: in metadata:



HASH of the attached file sent: recipe.docx:

STEPS: SAVE THE FILE OR OPEN CMD IN ITS DIR.

RUN THE CMD in windows : ***certutil -hashfile recipe.docx*** for SHA1 HASH

RUN THE CMD in windows : ***certutil -hashfile recipe.docx MD5*** for MD5HASH

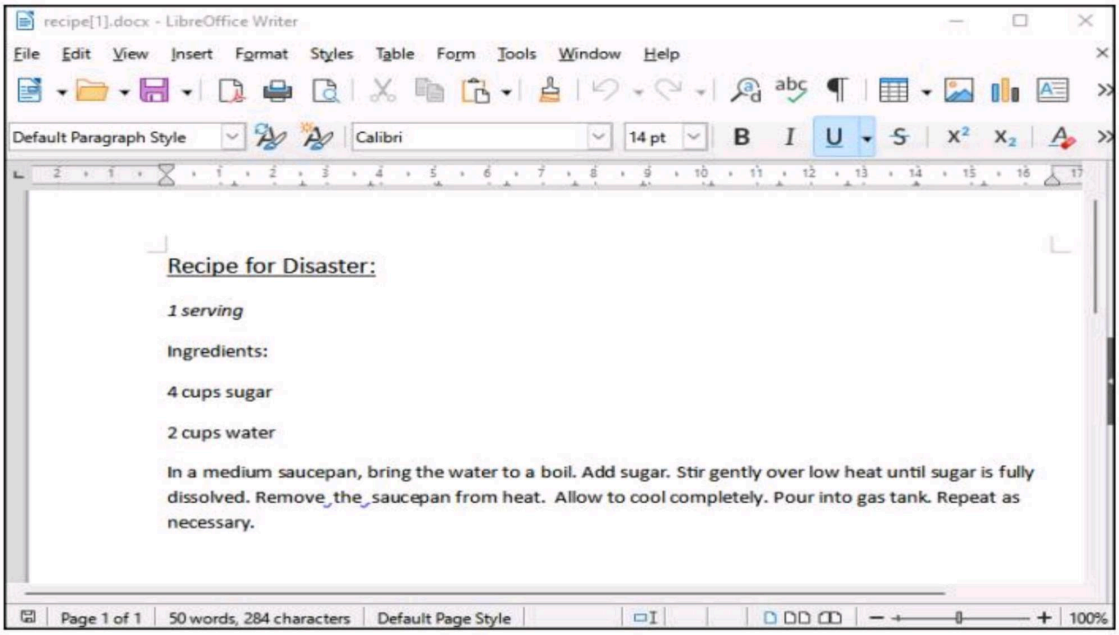
```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

G:\DF_TOOLS\secret-files-pcap\evidence-01>certutil -hashfile recipe.docx MD5
MD5 hash of recipe.docx:
8350582774e1d4dbe1d61d64c89e0ea1
CertUtil: -hashfile command completed successfully.

G:\DF_TOOLS\secret-files-pcap\evidence-01>certutil -hashfile recipe.docx
SHA1 hash of recipe.docx:
11745854a7f8cd0c513dbaa695e84fde9fa0e581
CertUtil: -hashfile command completed successfully.

G:\DF_TOOLS\secret-files-pcap\evidence-01>
```

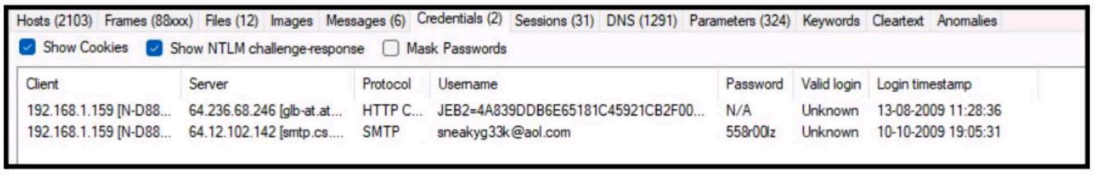
Q6. What is the secret recipe?



2. CASE 02: evidence02.pcap

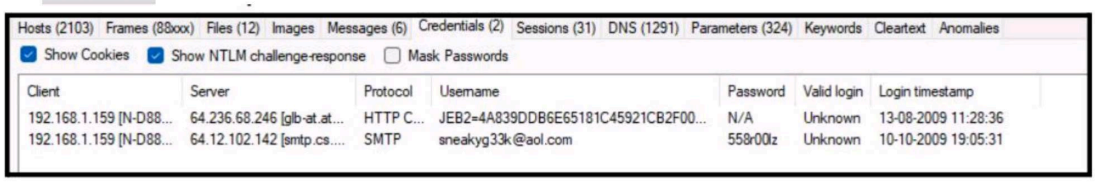
Q1. **What is Ann's email address?**

➔ **sneaky33k@aol.com**



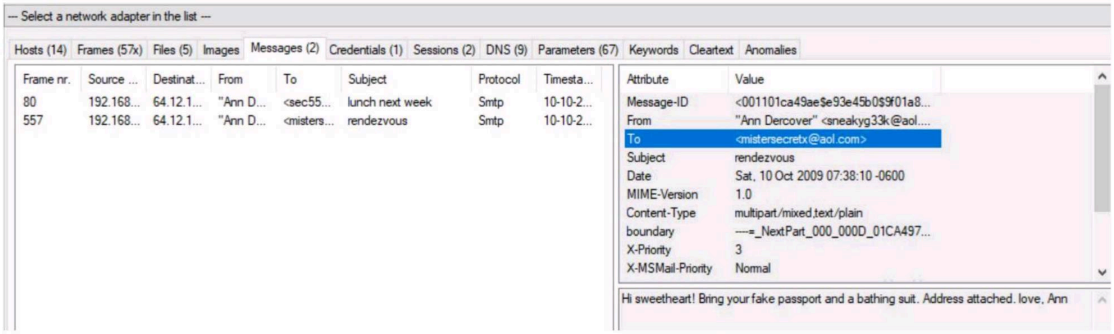
Q2. **What is Ann's email password?**

➔ **558r00lz**



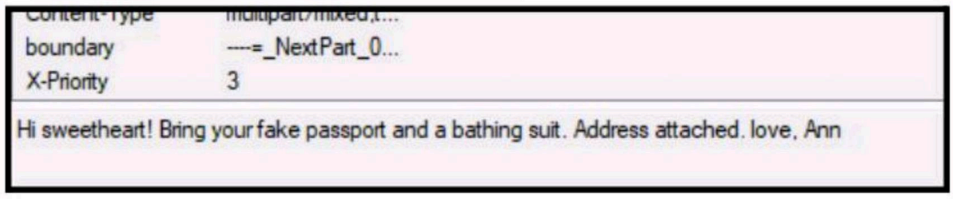
Q3. **What is Ann's secret lover's email address?**

➔ **mistersecretx@aol.com**



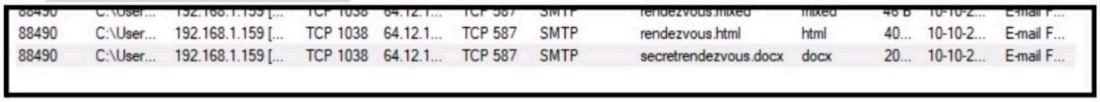
Q4. What two items did Ann tell her secret lover to bring?

➔ **Her fake passport and a bathing suit.**



Q5. What is the NAME of the attachment Ann sent to her secret lover?

➔ **secretrendezvous.docx**



Q6. What is the MD5sum of the attachment Ann sent to her secret lover?

HASH OF THE ATTACHED FILE: ***secretrendezvous.docx:***

```
G:\DF_TOOLS\secret-files-pcap\evidence-02>certutil -hashfile secretrendezvous.docx
SHA1 hash of secretrendezvous.docx:
21499db49b9a9a4f8d755cc359ed152b4fcc9c66
CertUtil: -hashfile command completed successfully.

G:\DF_TOOLS\secret-files-pcap\evidence-02>certutil -hashfile secretrendezvous.docx MD5
MD5 hash of secretrendezvous.docx:
f130c813f8483449fd7d127648cd7320
CertUtil: -hashfile command completed successfully.

G:\DF_TOOLS\secret-files-pcap\evidence-02>
```

Q7. In what CITY and COUNTRY is their rendez-vous point?

Q8. What is the MD5sum of the image embedded in the document?

MD5 OF THE evidence02.pcap file:

Metadata

Name	Value
Filename	evidence02.pcap
Start	01-01-0001 12.00.00 AM
End	01-01-0001 12.00.00 AM
Frames	0
MD5	cfac149a49175ac8e89d5b5b5d69bad3
Endianness	Little Endian
Data Link Type	WTAP_ENCAP_ETHERNET

HASH OF THE IMAGE INSIDE THE ATTACHED FILE ***secretrendezvous.docx:***

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

G:\DF_TOOLS\secret-files-pcap\evidence-02>certutil -hashfile evi2-img.png MD5
MD5 hash of evi2-img.png:
aadeace50997b1ba24b09ac2ef1940b7
CertUtil: -hashfile command completed successfully.

G:\DF_TOOLS\secret-files-pcap\evidence-02>certutil -hashfile evi2-img.png
SHA1 hash of evi2-img.png:
23260cf2c8614cd6e2834adc78cd2563c3c38b0a
CertUtil: -hashfile command completed successfully.

G:\DF_TOOLS\secret-files-pcap\evidence-02>
```