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/

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:

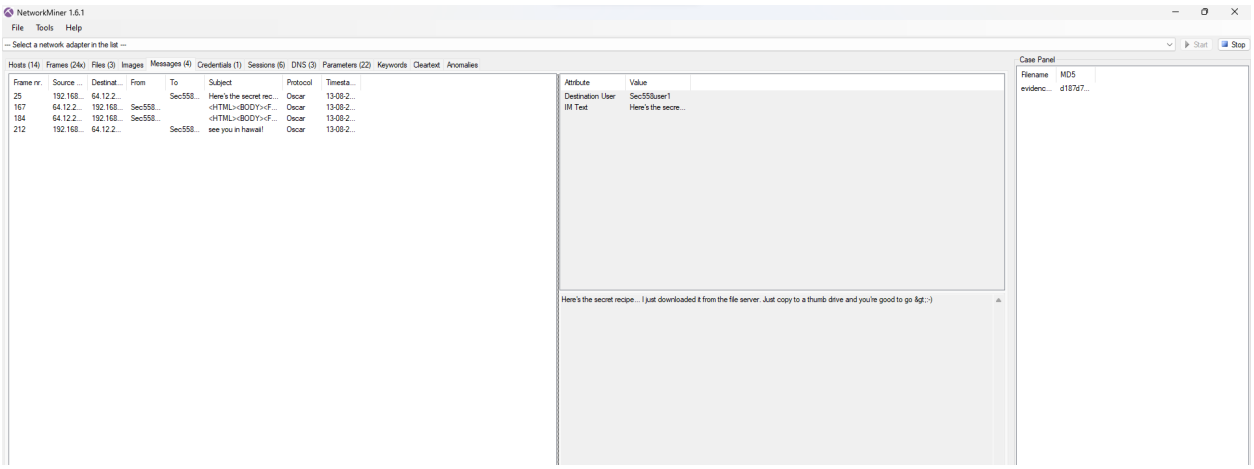
1. **Physical Layer Attacks:**
    - **Wiretapping/Eavesdropping:** Attackers physically intercept network transmissions to capture sensitive information, such as passwords or confidential data, by tapping into network cables or using specialized equipment.
    - **Hardware Tampering:** Attackers may 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.

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.

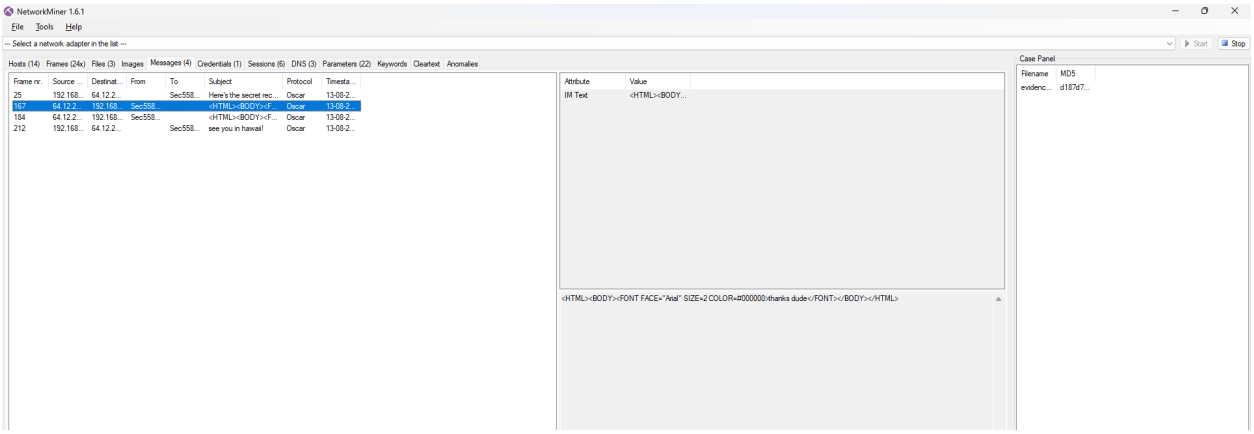
Understanding these attacks and implementing appropriate security measures at each layer of the network stack is essential for mitigating risks and safeguarding network infrastructure and data assets against malicious threats.

Implementation:

Case 1

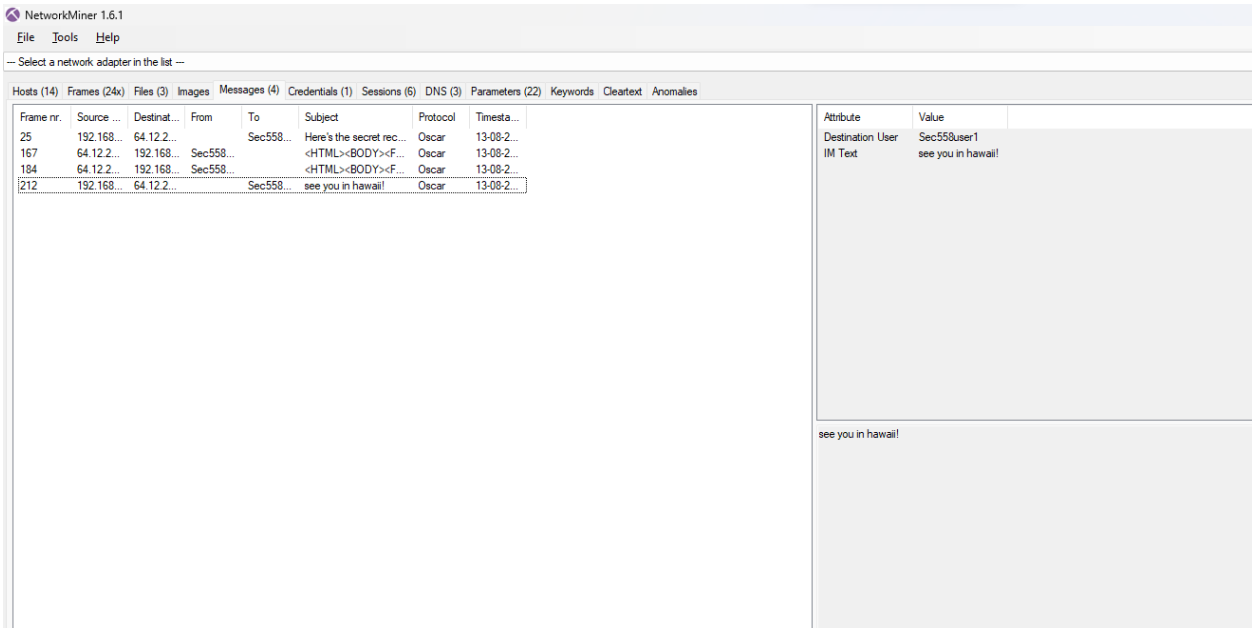


Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go >:-)



thanks dude

see you in hawaii!



Recipe for Disaster:

1 serving

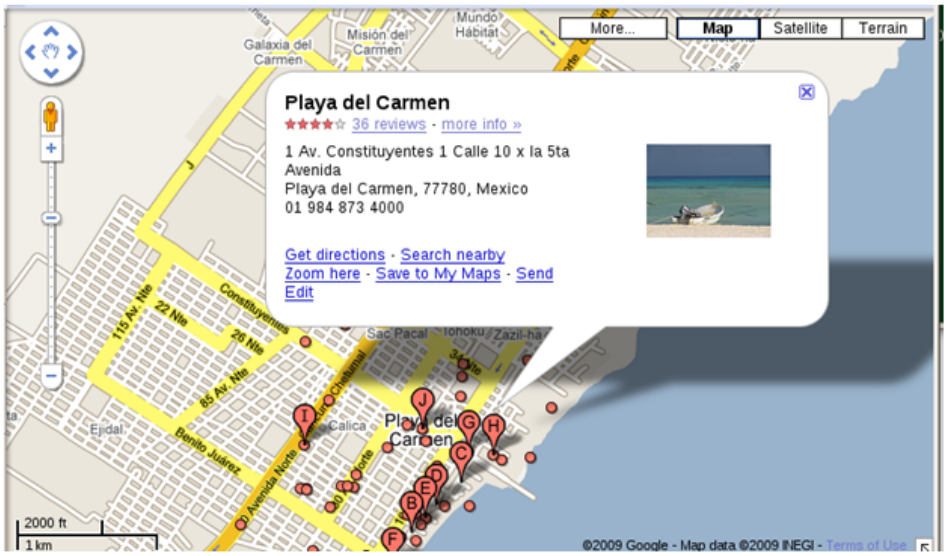
Ingredients:

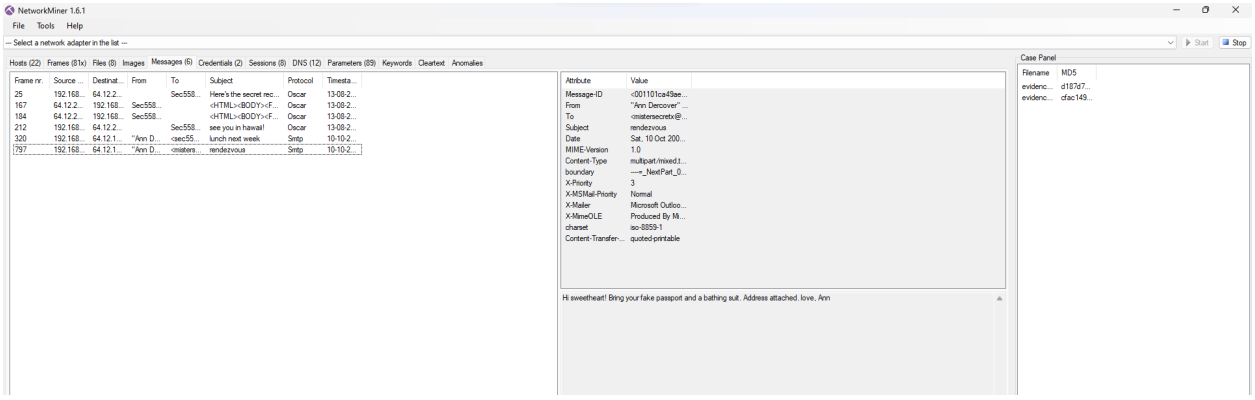
4 cups sugar

2 cups water

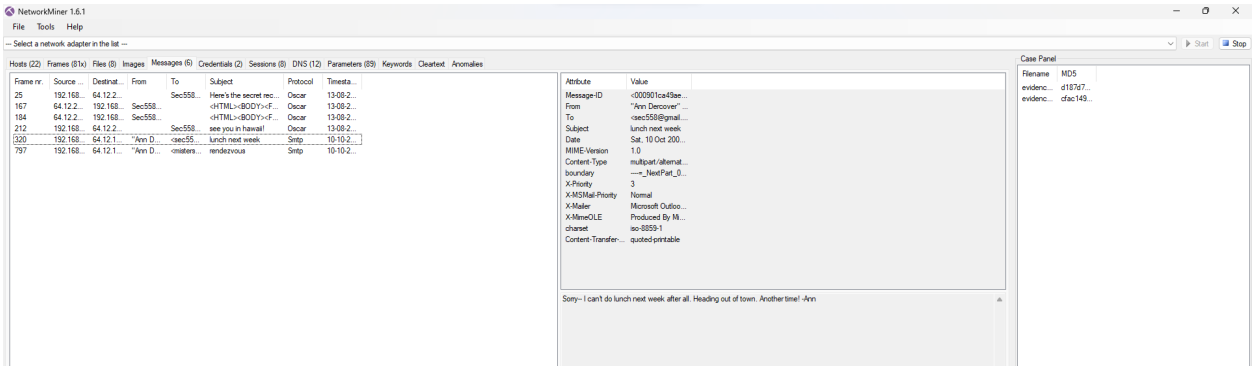
In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

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

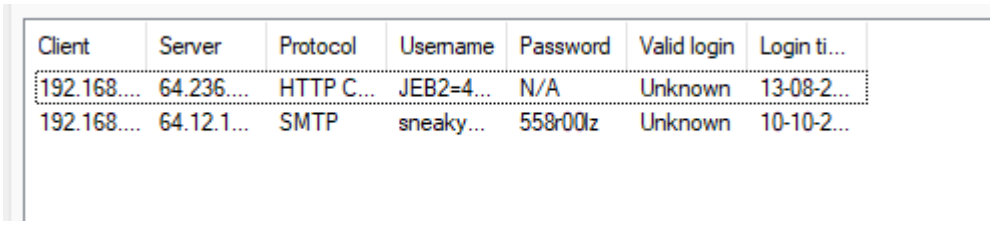




Hi sweetheart! Bring your fake passport and a bathing suit. Address attached. love, Ann

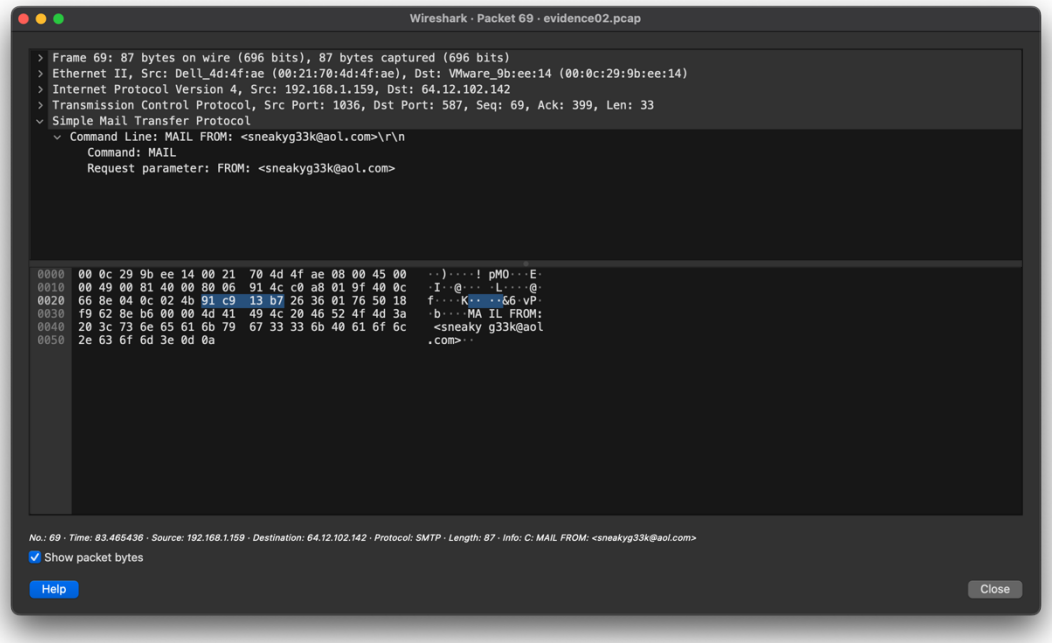


Sorry-- I can't do lunch next week after all. Heading out of town. Another time! -Ann



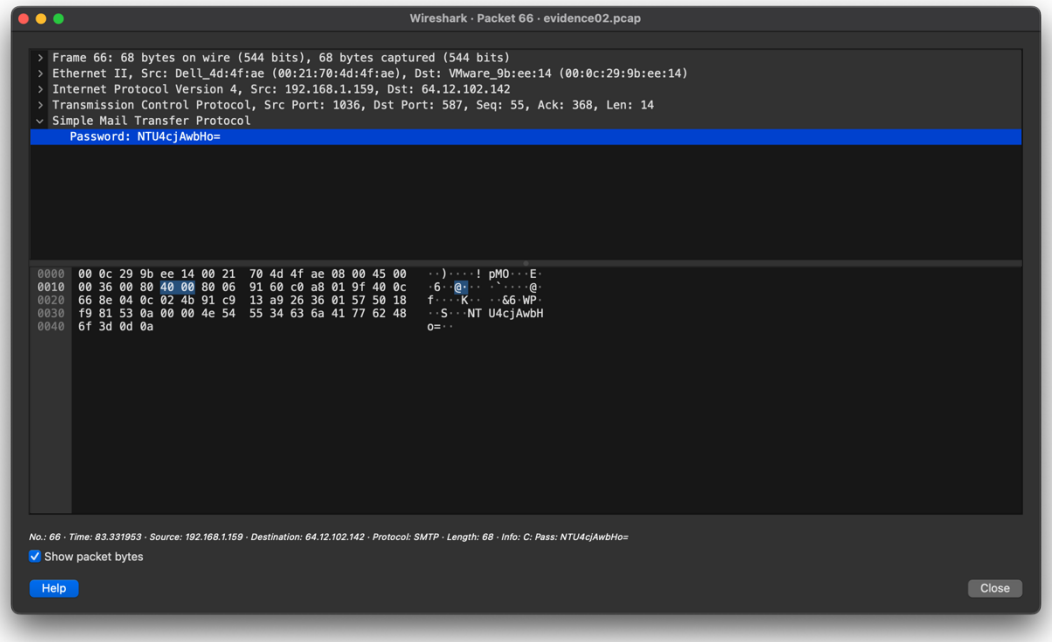
Client	Server	Protocol	Username	Password	Valid login	Login ti...
192.168....	64.236....	HTTP C...	JEB2=4...	N/A	Unknown	13-08-2...
192.168....	64.12.1...	SMTP	sneaky...	558r00lz	Unknown	10-10-2...

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



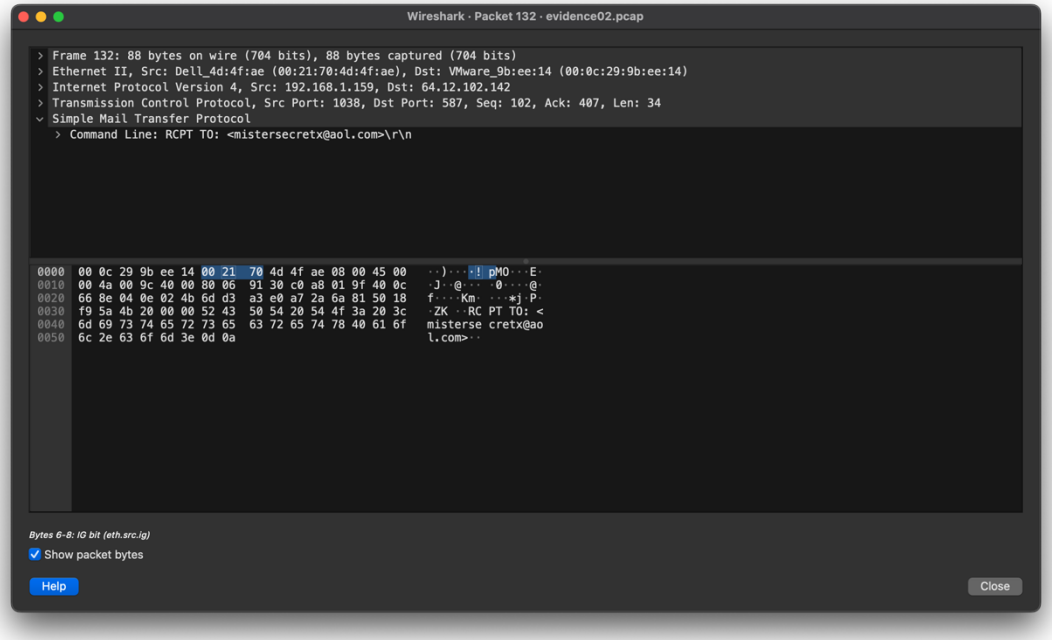
2. What is Ann's email password?

558r00lz



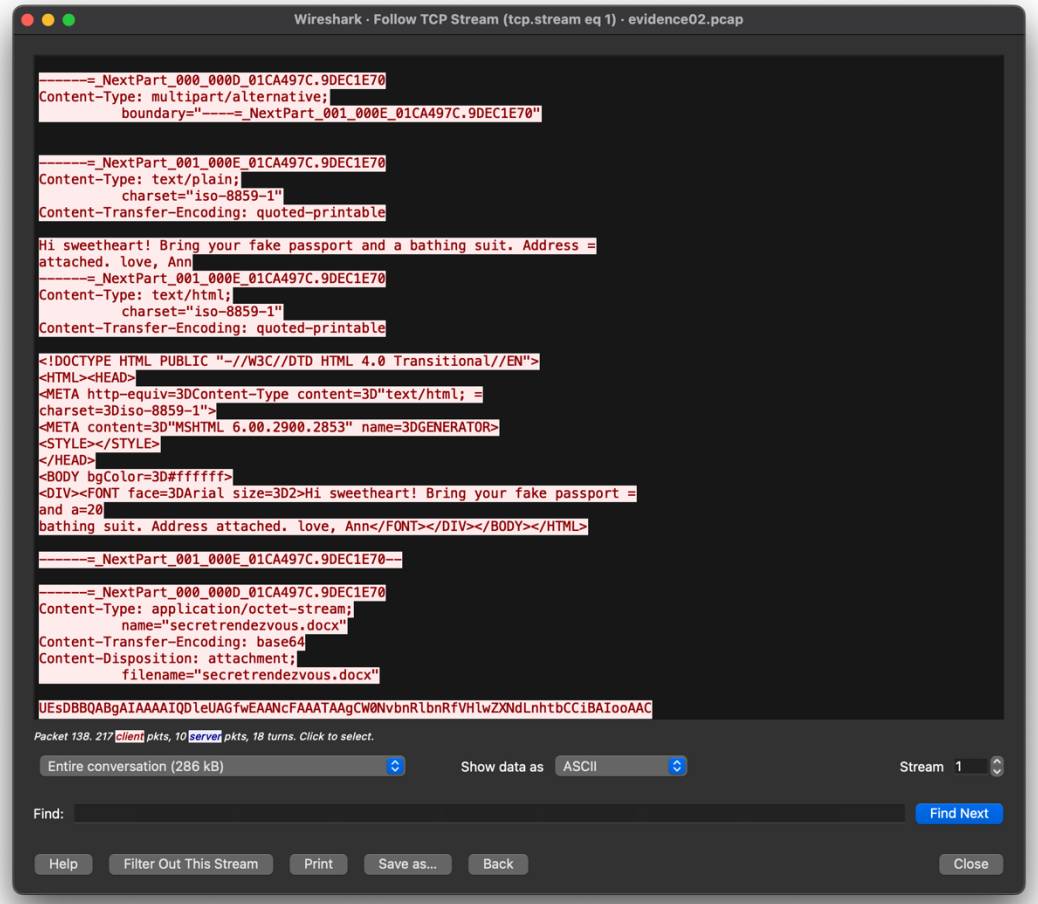
3. What is Ann's secret lover's email address?

mistersecretx@aol.com



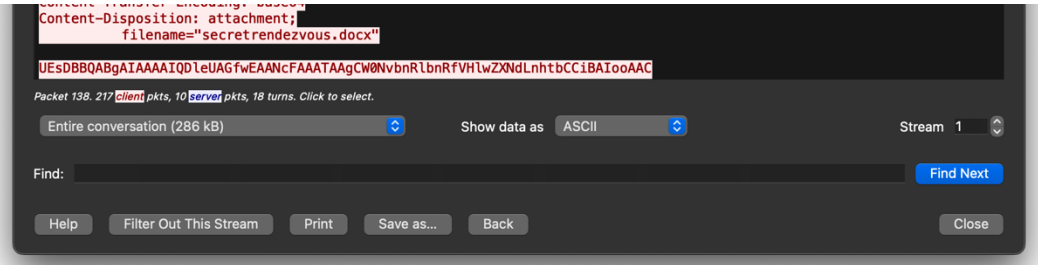
4. What two items did Ann tell her secret lover to bring?

Fake passport and bathing suit



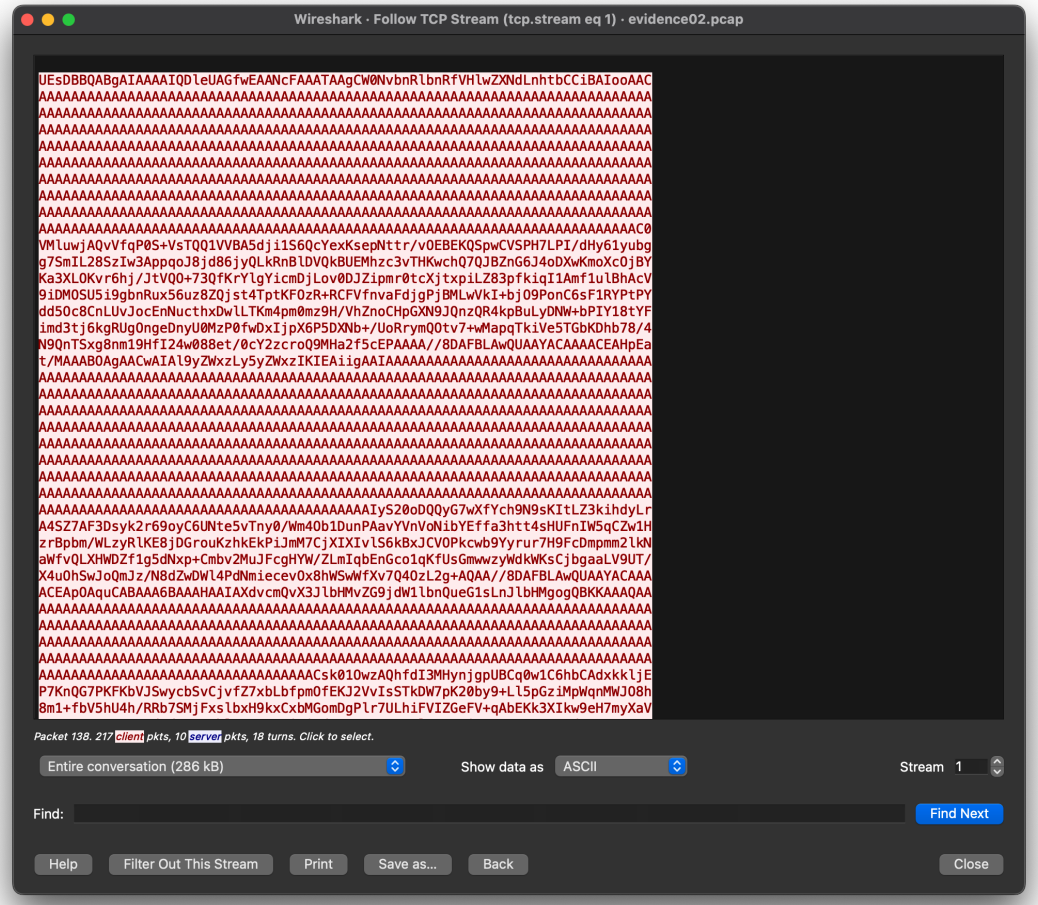
5. What is the NAME of the attachment Ann sent to her secret lover?

secretrendezvous.docx



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

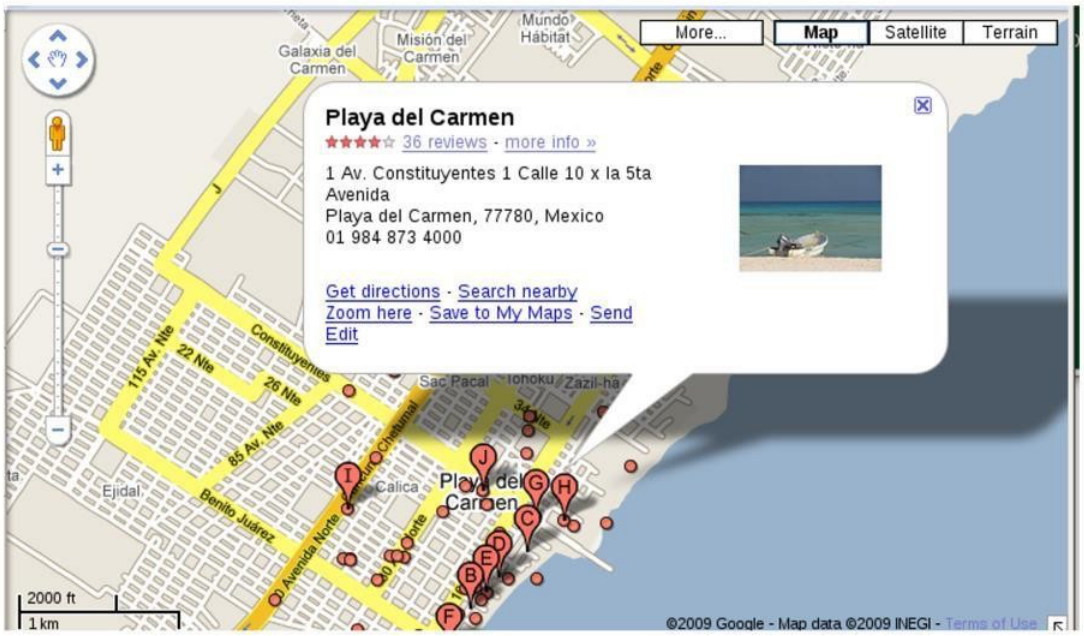
9E423E11DB88F01BBFF81172839E1923



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.



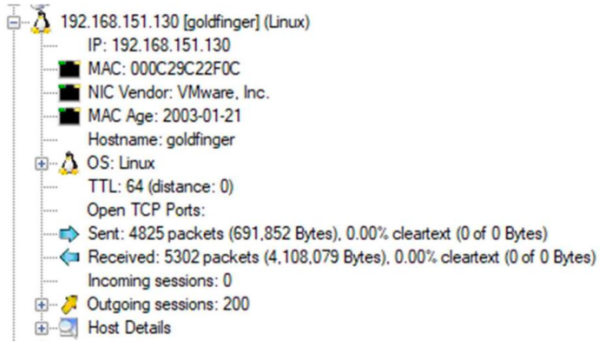
8. What is the MD5sum of the image embedded in the document?

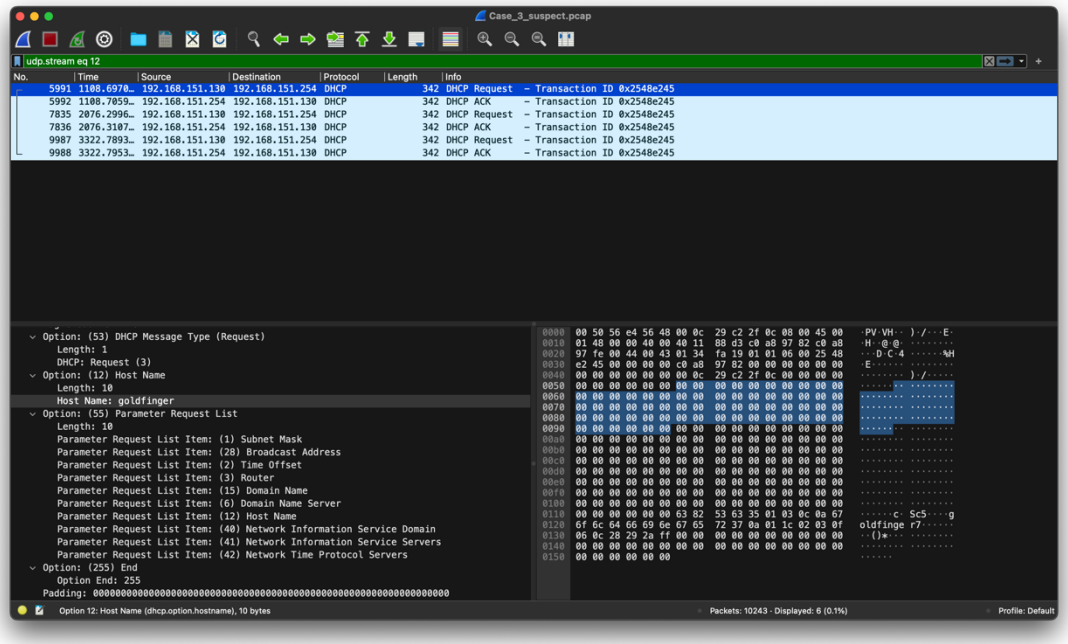
MD5: 6d3c6ed7cb0a49ede228fd045efb3792

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.

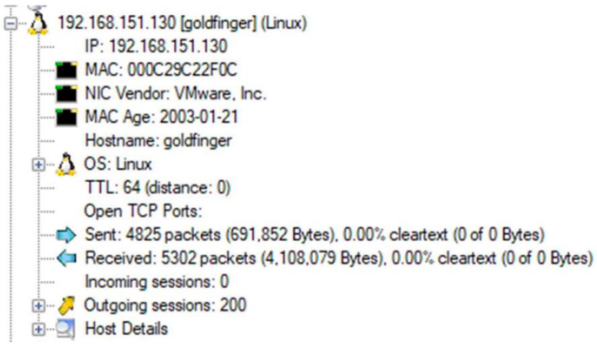
1. **What IP address and hostname does Steve Vogon's Linux computer have?**
   192.168.151.130 – goldfinger

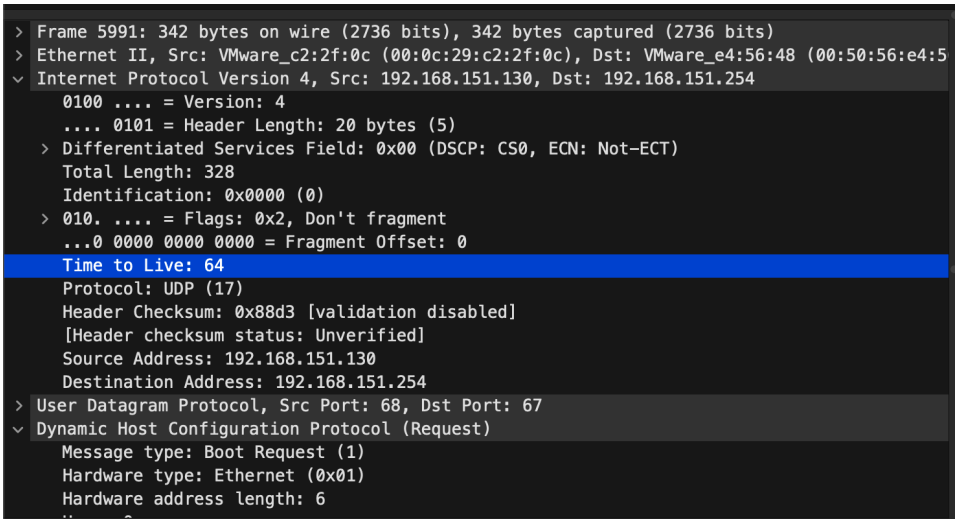




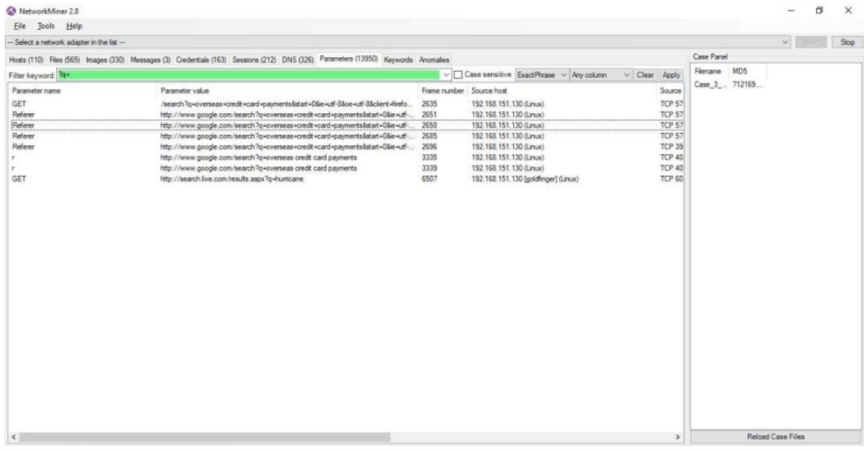
2. What evidence do you have to assume that this computer is running Linux?

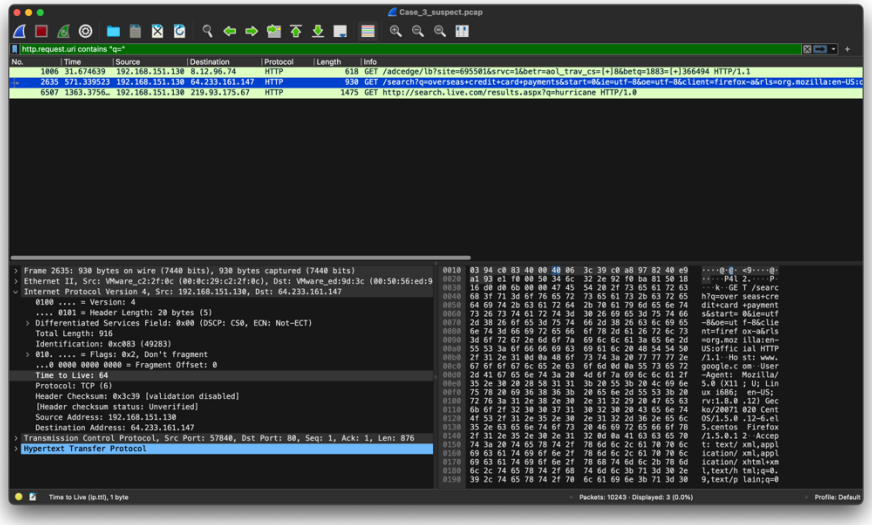
Proof: TTL for Linux - 64





3. **What Google searches did Steve Vogon perform?**
   - overseas credit card payments
   - hurricane





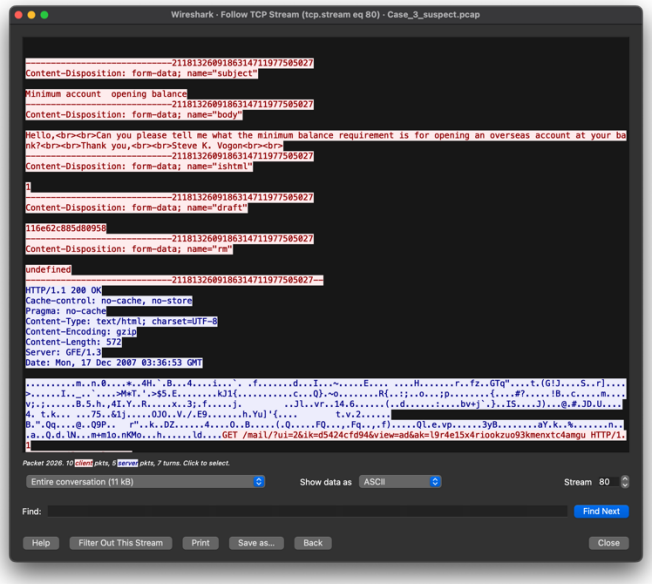
4. **What message did the email contain that Steve Vogon sentfrom his Gmail account?**

   Hello,

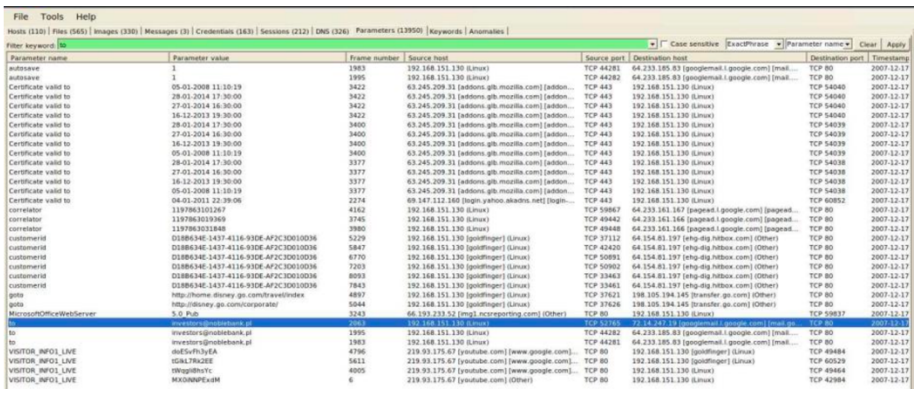
Can you please tell me what the minimum balance requirement is for opening an
   overseas account at your bank?

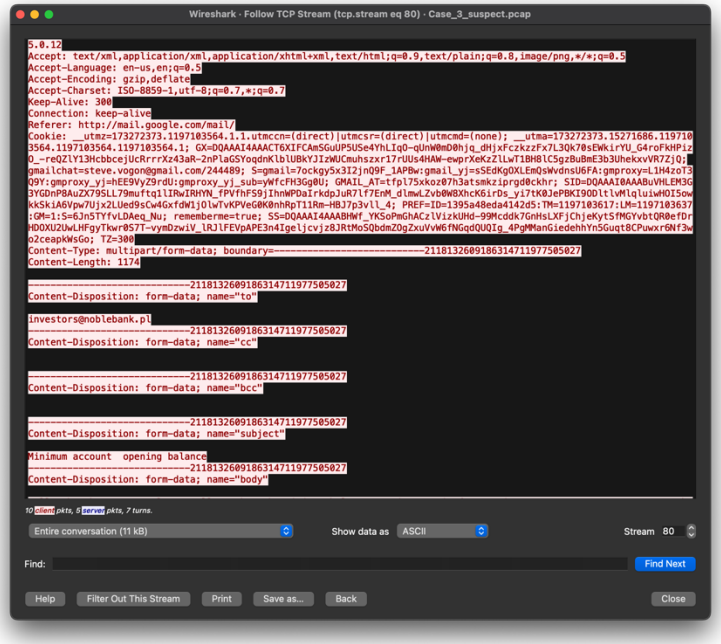
Thank you,

Steve K. Vogon



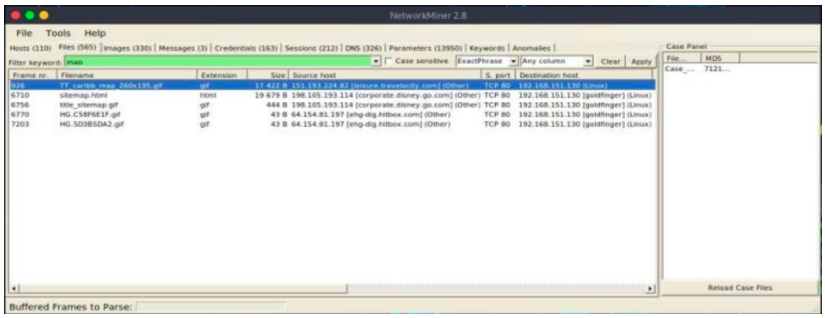
5. **How did Steve find the email address to which he sent his email?**
   Website: www.noblebank.pl Email:investors@noblebank.pl

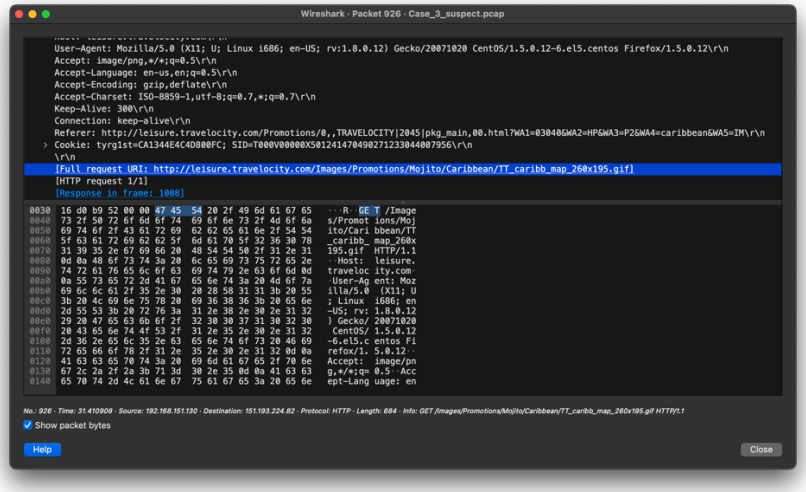




6. **One web page opened by Steve contains a map, what region does the map show?**

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





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.

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 sniffers) 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.