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

Batch: B1 Roll No.: 16010121045

Experiment No. 4

Title: Wireshark

Objective:
Wireshark Case Study

CO	Outcome
CO2	Perform Penetration testing and vulnerability assessment on various systems

Books/ Journals/ Websites referred:

- Web Penetration Testing with Kali Linux, Joseph Muniz, Aamir Lakhani, Packt Publishing, 2013.

Introduction:

Wireshark is a powerful open-source packet analyzer used for network troubleshooting, analysis, software and communication protocol development, and education. It allows users to capture and interactively browse the traffic running on a computer network in real time, or to analyze saved capture files offline. Wireshark provides detailed information about network protocols, packet contents, and can even reconstruct entire sessions for analysis.

Now, diving into key theories related to network security and forensics, several fundamental concepts underpin these fields:

1. **Defense in Depth**: This principle advocates for multiple layers of security controls to protect a network. It means that even if one layer of defense fails, there are other layers to prevent attackers from compromising the system. These layers can include firewalls, intrusion detection systems, antivirus software, and user training.
2. **Least Privilege**: This theory emphasizes restricting access rights for users, accounts, and computing processes to only those resources absolutely necessary to perform their job or function. By limiting access, organizations can minimize the potential damage caused by insider threats or external attackers who gain unauthorized access.
3. **Vulnerability Management**: Network security involves identifying, classifying, prioritizing, and mitigating vulnerabilities. This theory emphasizes the importance of regularly scanning systems for vulnerabilities, applying patches and updates promptly, and implementing security controls to protect against known vulnerabilities.
4. **Encryption**: Encryption plays a vital role in securing data transmitted over networks. It involves encoding data in such a way that only authorized parties can access it. Encryption ensures confidentiality, integrity, and authenticity of data, preventing eavesdropping and tampering by unauthorized entities.
5. **Incident Response**: This theory focuses on the processes and procedures for responding to security incidents effectively. It involves detecting, analyzing, and containing security breaches in a timely manner to minimize damage and recover normal operations as quickly as possible. Incident response plans typically include steps for identification, containment, eradication, recovery, and lessons learned.
6. **Chain of Custody**: In digital forensics, the chain of custody refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical and electronic evidence. It ensures that evidence is admissible in legal proceedings by maintaining its integrity and authenticity.
7. **Network Forensics**: This field involves the capture, recording, and analysis of network events to discover the source of security attacks or other problem incidents. Network forensics tools like Wireshark enable investigators to reconstruct network activity, identify suspicious behavior, and determine the root cause of security incidents.

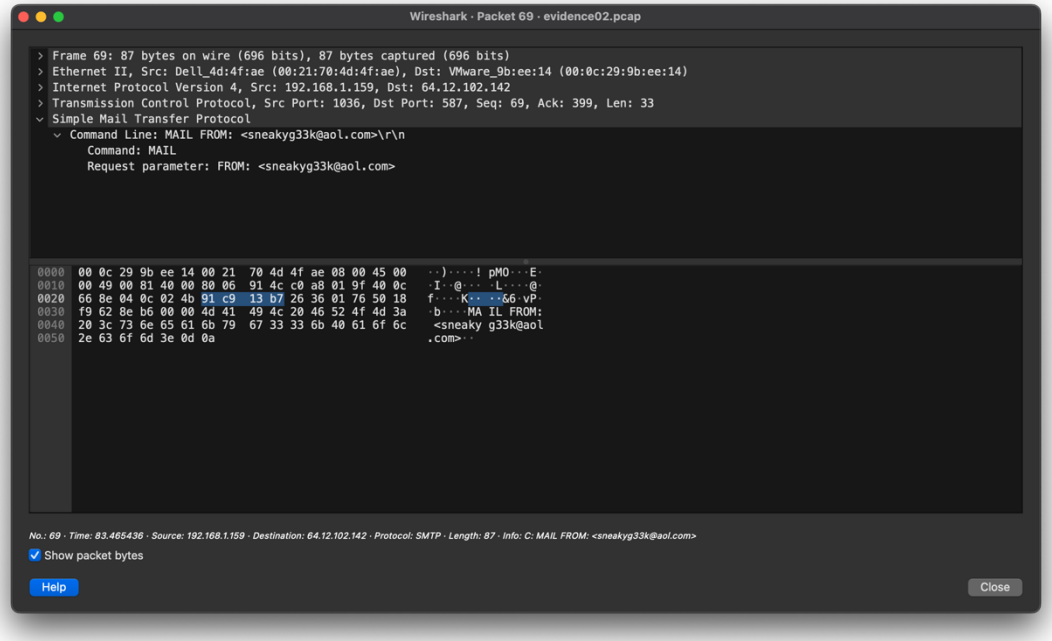
Implementation details:

After being released on bail, Ann Dercover disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town.

"We believe Ann may have communicated with her secret lover, Mr. X, before she left," says the police chief. "The packet capture may contain clues to her whereabouts."

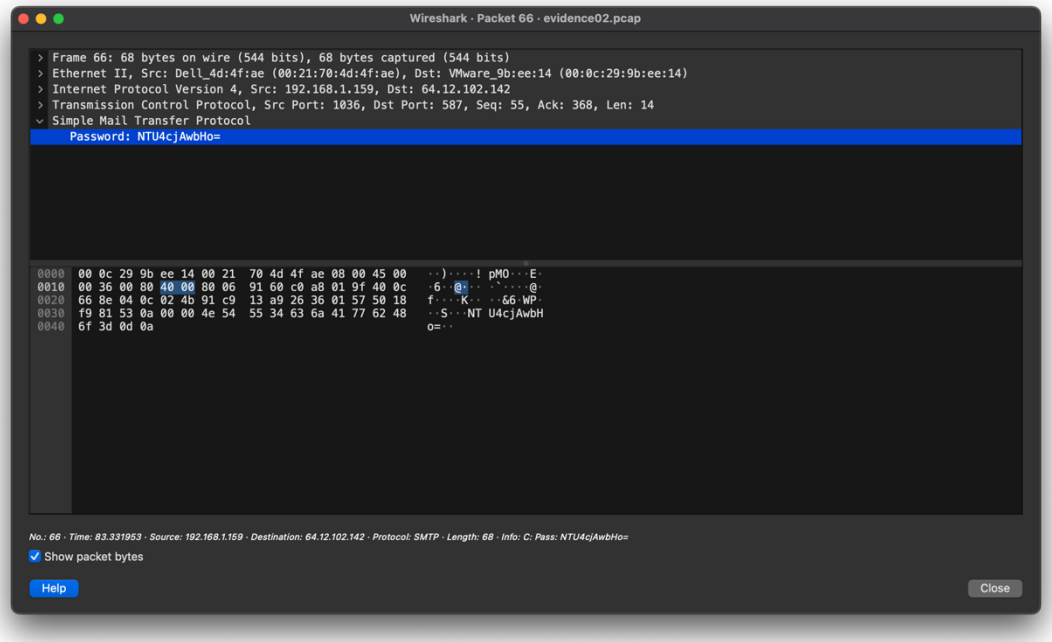
You are the forensic investigator. Your mission is to figure out what Ann emailed, where she went, and recover evidence including:

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



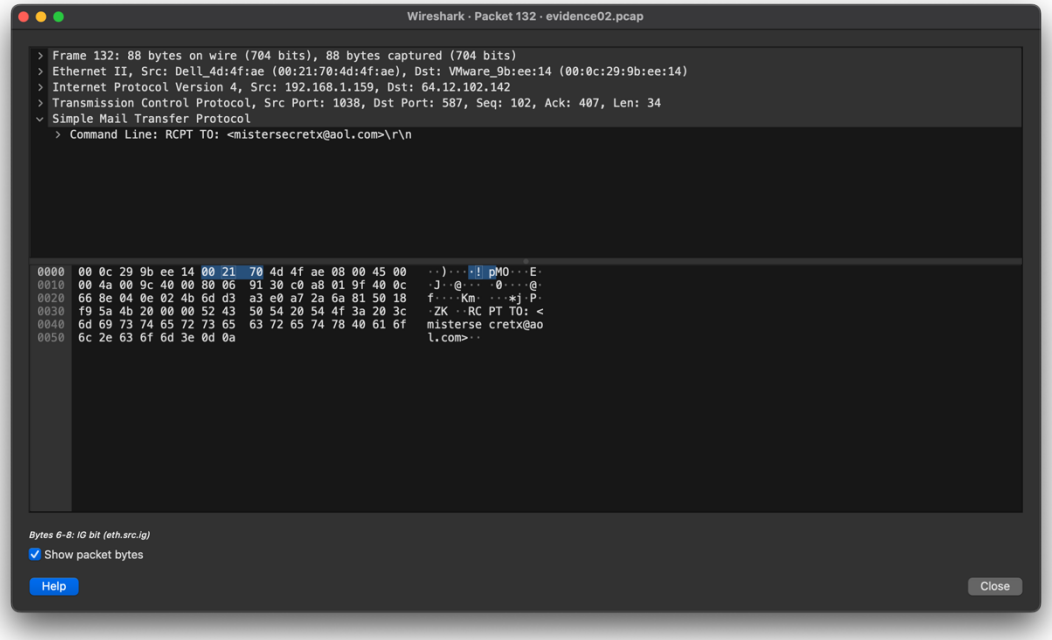
2. What is Ann's email password?

558r00lz



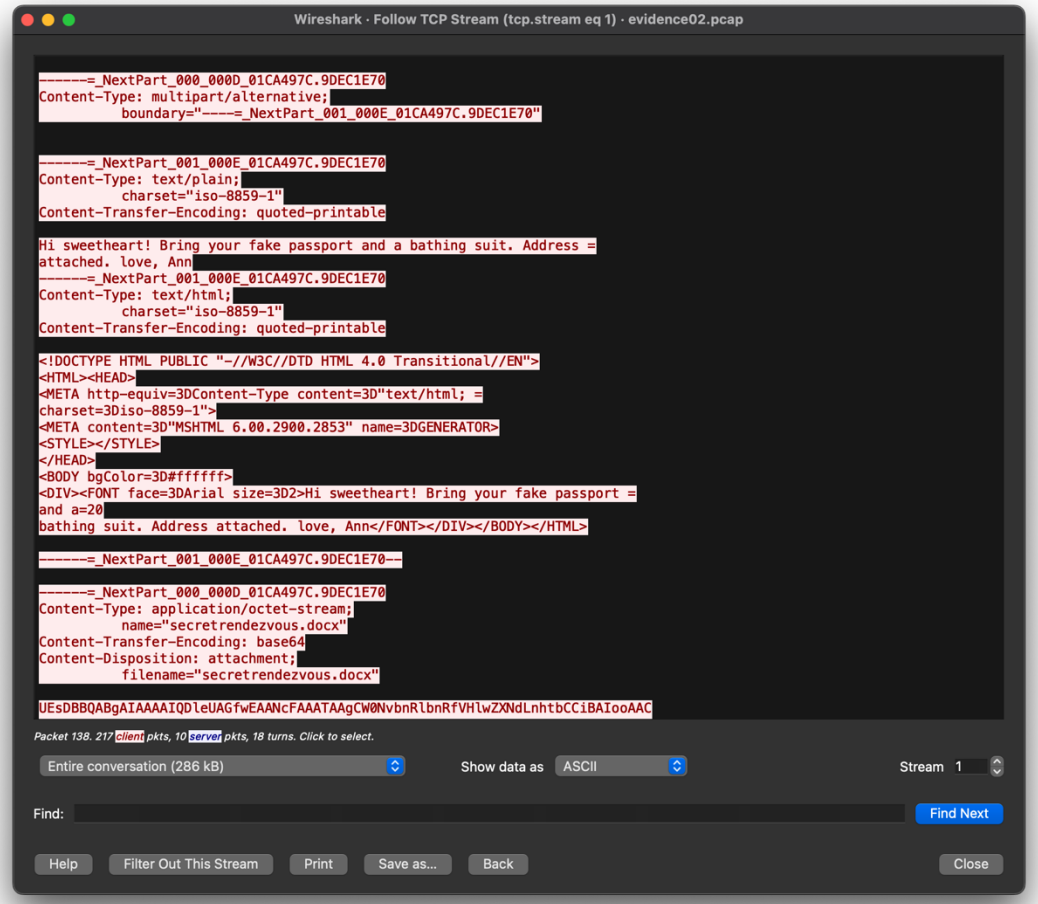
3. What is Ann's secret lover's email address?

mistersecretx@aol.com



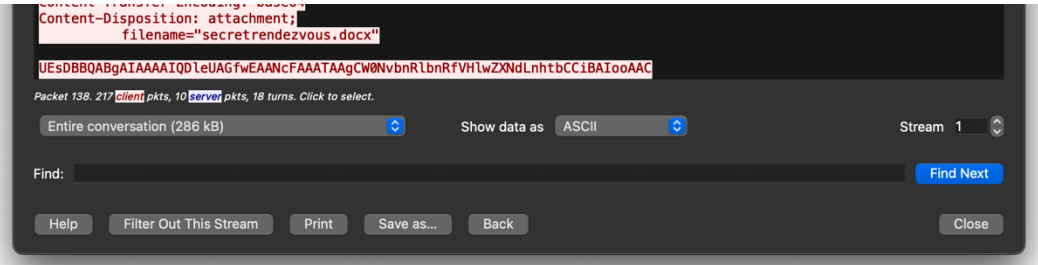
4. What two items did Ann tell her secret lover to bring?

Fake passport and bathing suit



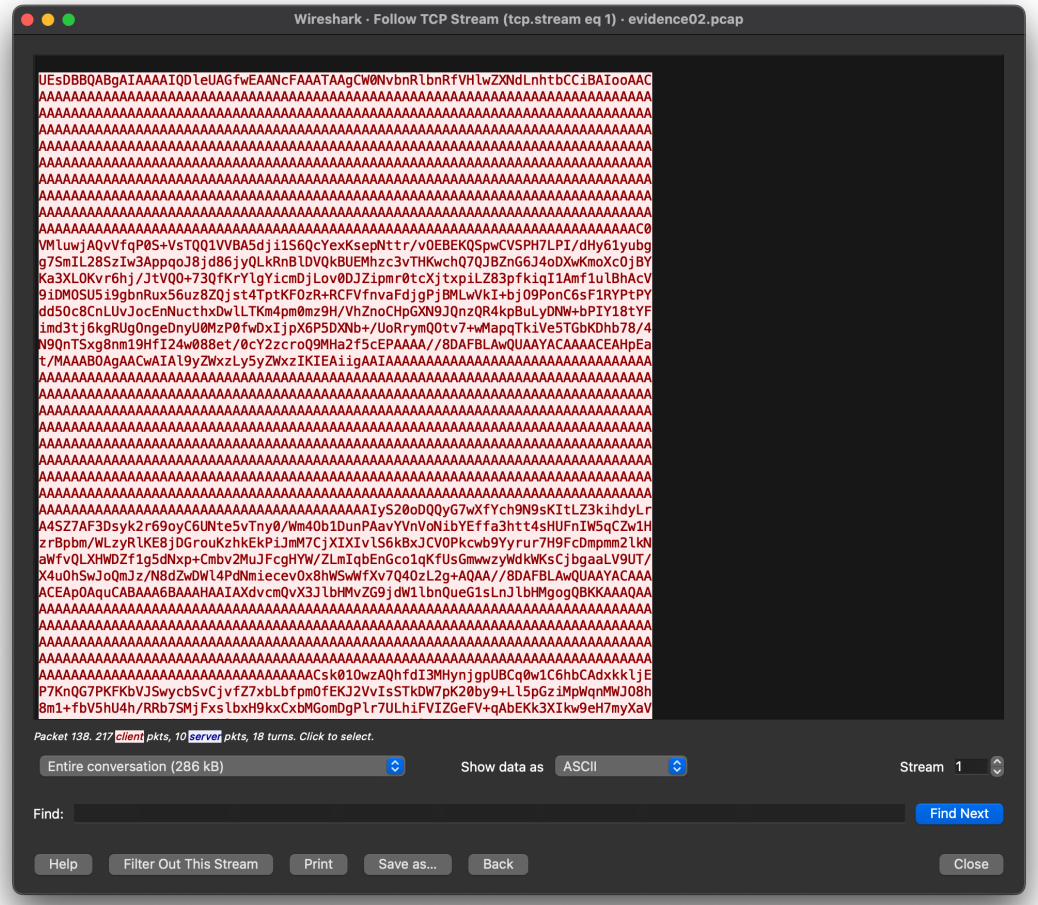
5. What is the NAME of the attachment Ann sent to her secret lover?

secretrendezvous.docx



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

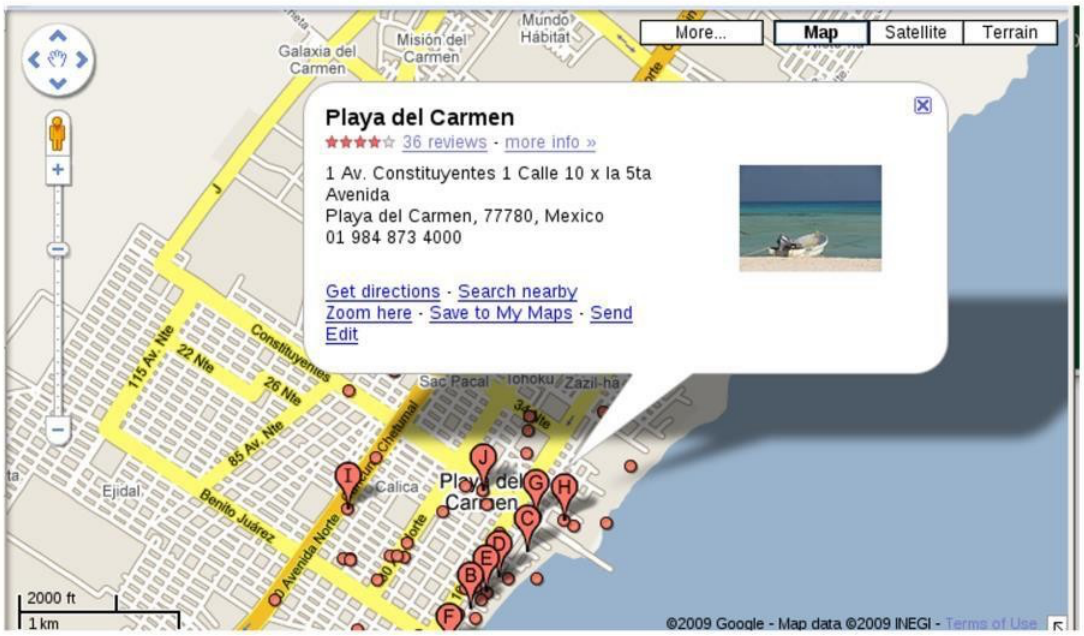
9E423E11DB88F01BBFF81172839E1923



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

Conclusion:

Successfully completed the give task activity in wireshark.