­

Digital Forensics (CS4419-CS6419)



2021SM\_CS\_6419\_FRE1A

Assignment-01

Prepared by:  
Mohammadali Rahnama

Student number:

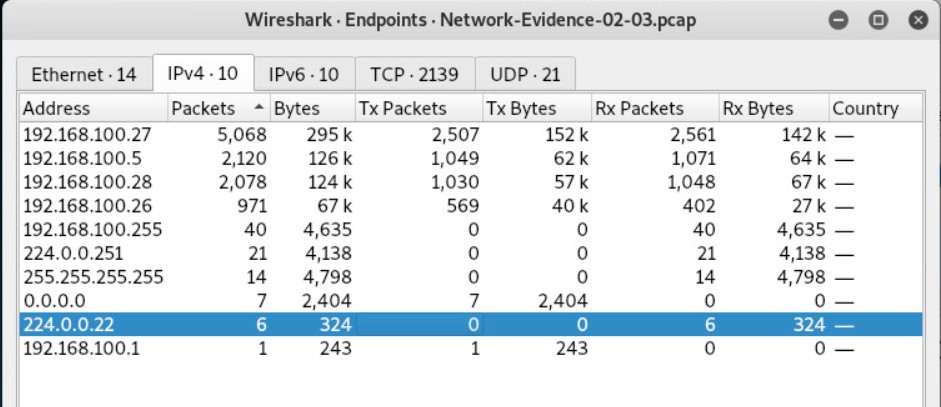
3709515

1. **What is the network address and subnet mask?**

The subnet mask is 255.255.255.0, the network address is 192.168.100

1. **For each computer:**
   1. **What is the IP of the computer?**

There are 4 computers on the network: 192.168.100.5, 192.168.100.26, 192.168.100.27, 192.168.100.28



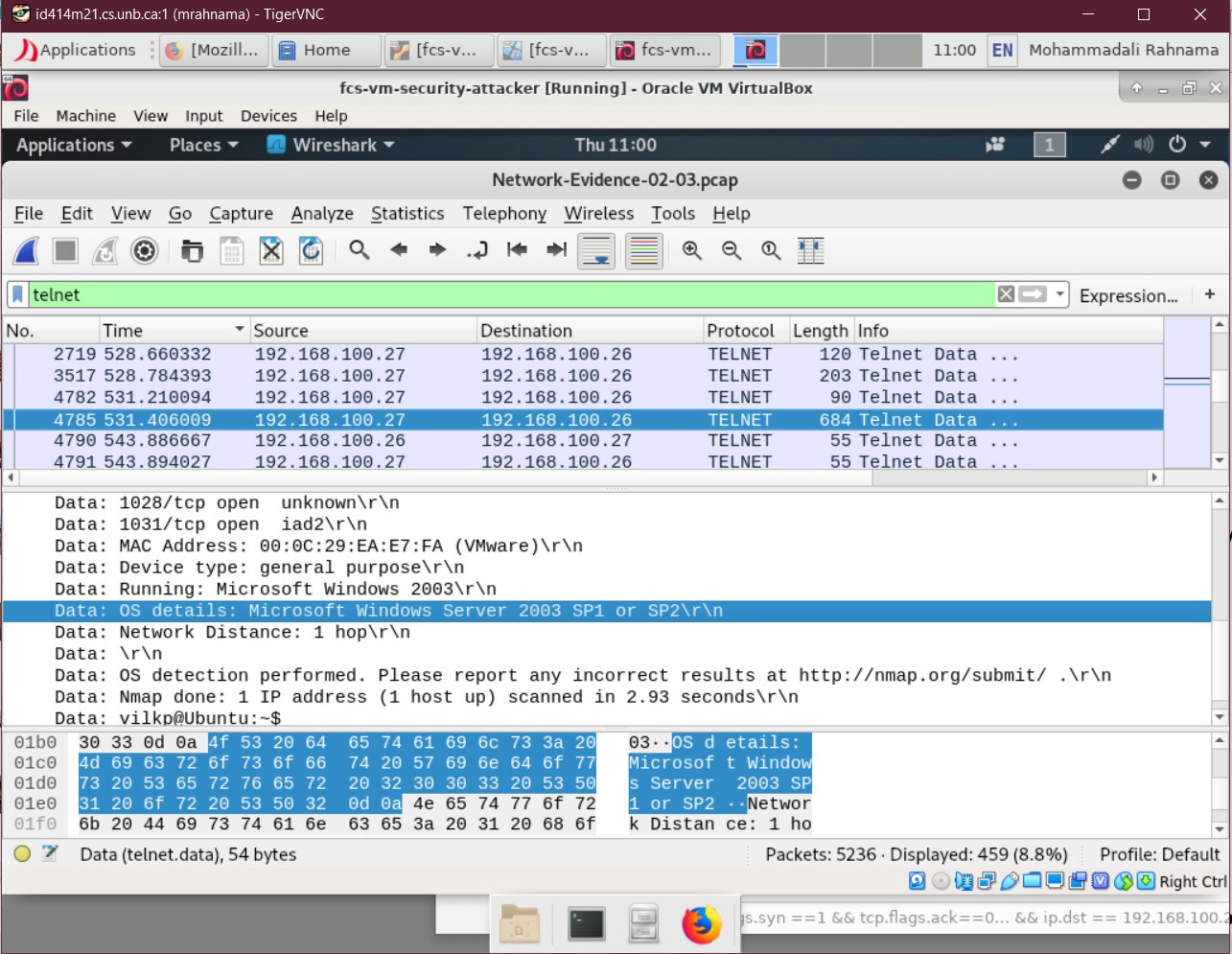
* 1. **What OS is it running?**

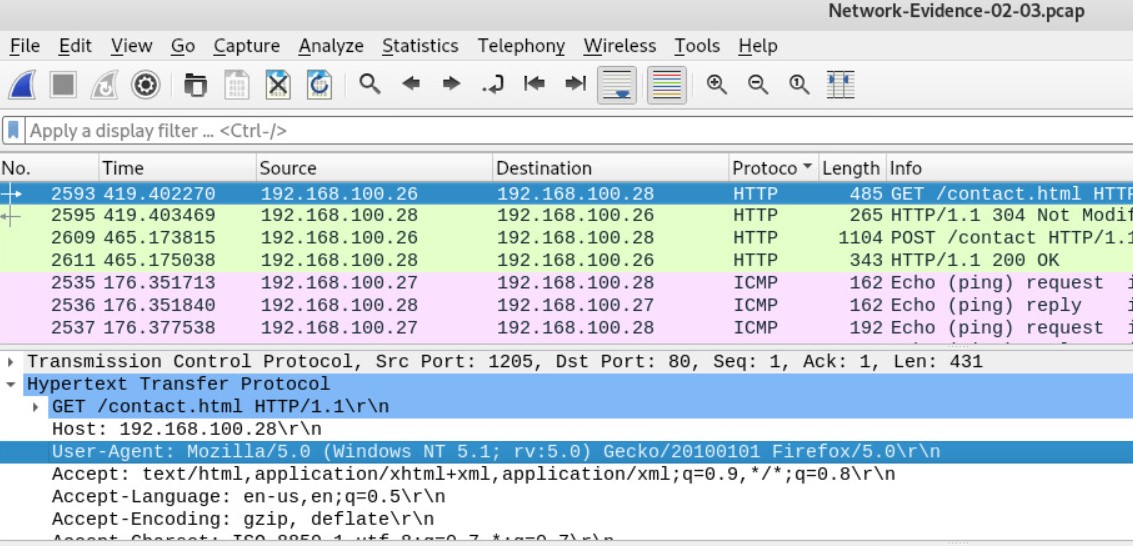
192.168.100.5 is using Microsoft Windows Server 2003.

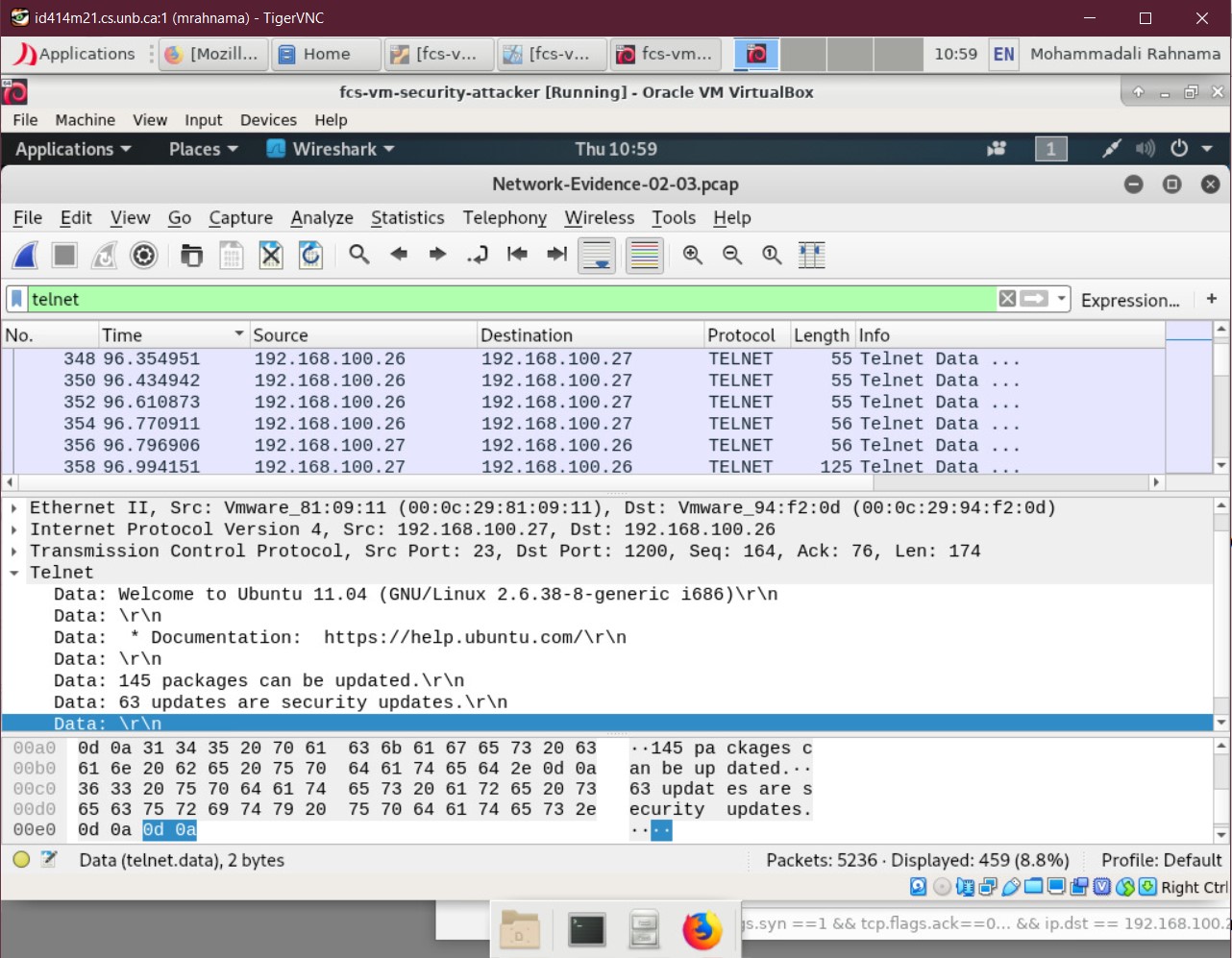
192.168.100.26 is using Microsoft Windows XP.

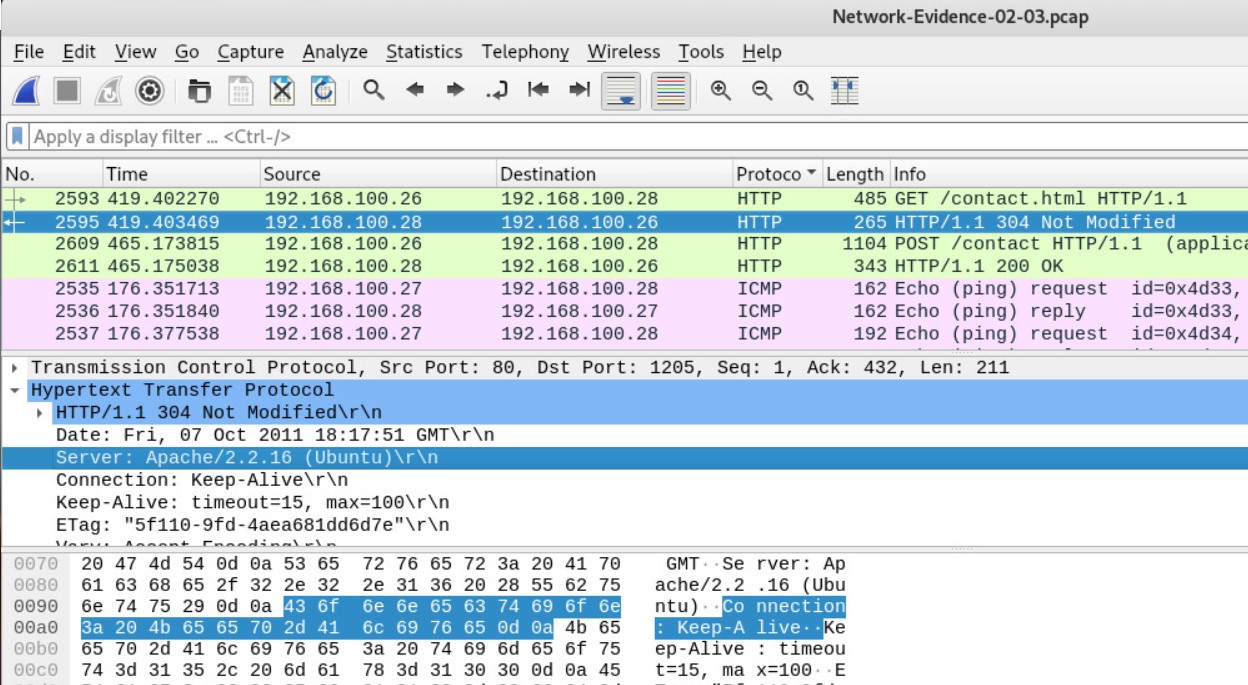
192.168.100.27 is using Ubuntu.

192.168.100.28 is using Ubuntu.









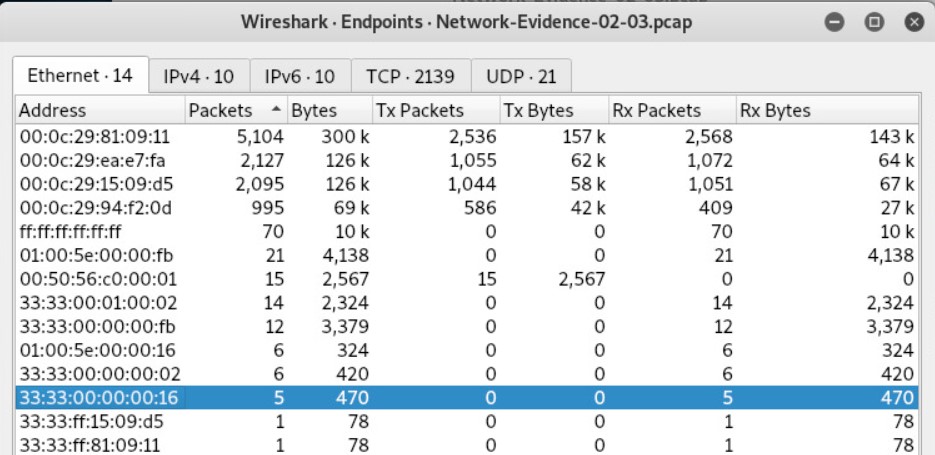
* 1. **What is the MAC address?**

192.168.100.5 is 00:0c:29:ea:e7:fa.

192.168.100.26 is 00:0c:29:94:f2:0d.

192.168.100.27 is 00:0c:29:81:09:11.

192.168.100.28 is 00:0c:29:15:09:d5.



1. **What is a port scan?**

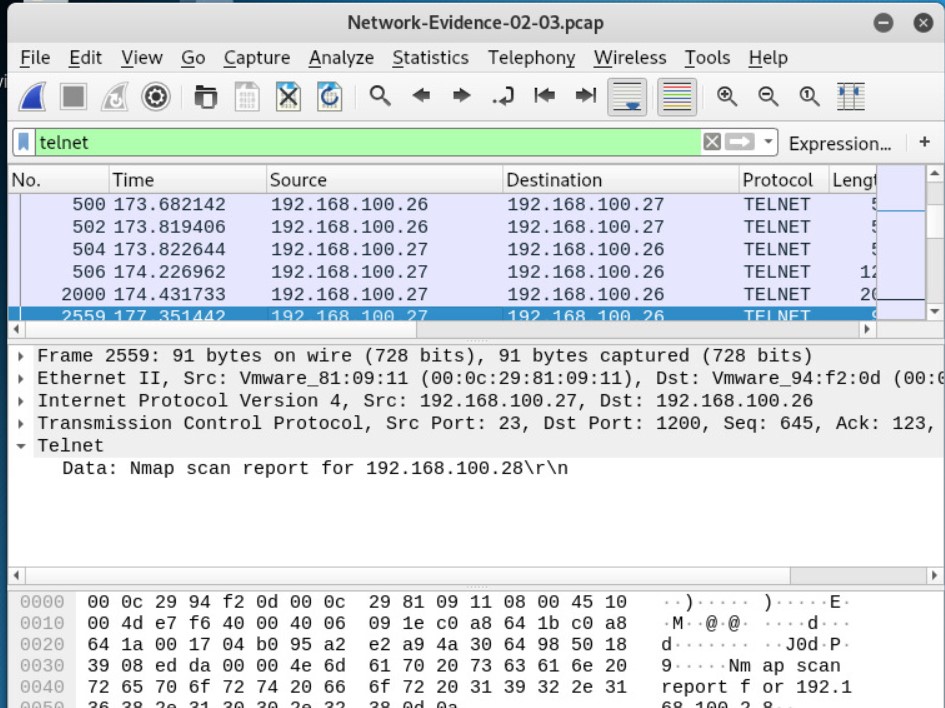
Port scanning is a technique for determining which network ports are open and potentially receiving or sending data. It is also a method of sending packets to specific ports on a host and analyzing the responses to find vulnerabilities.

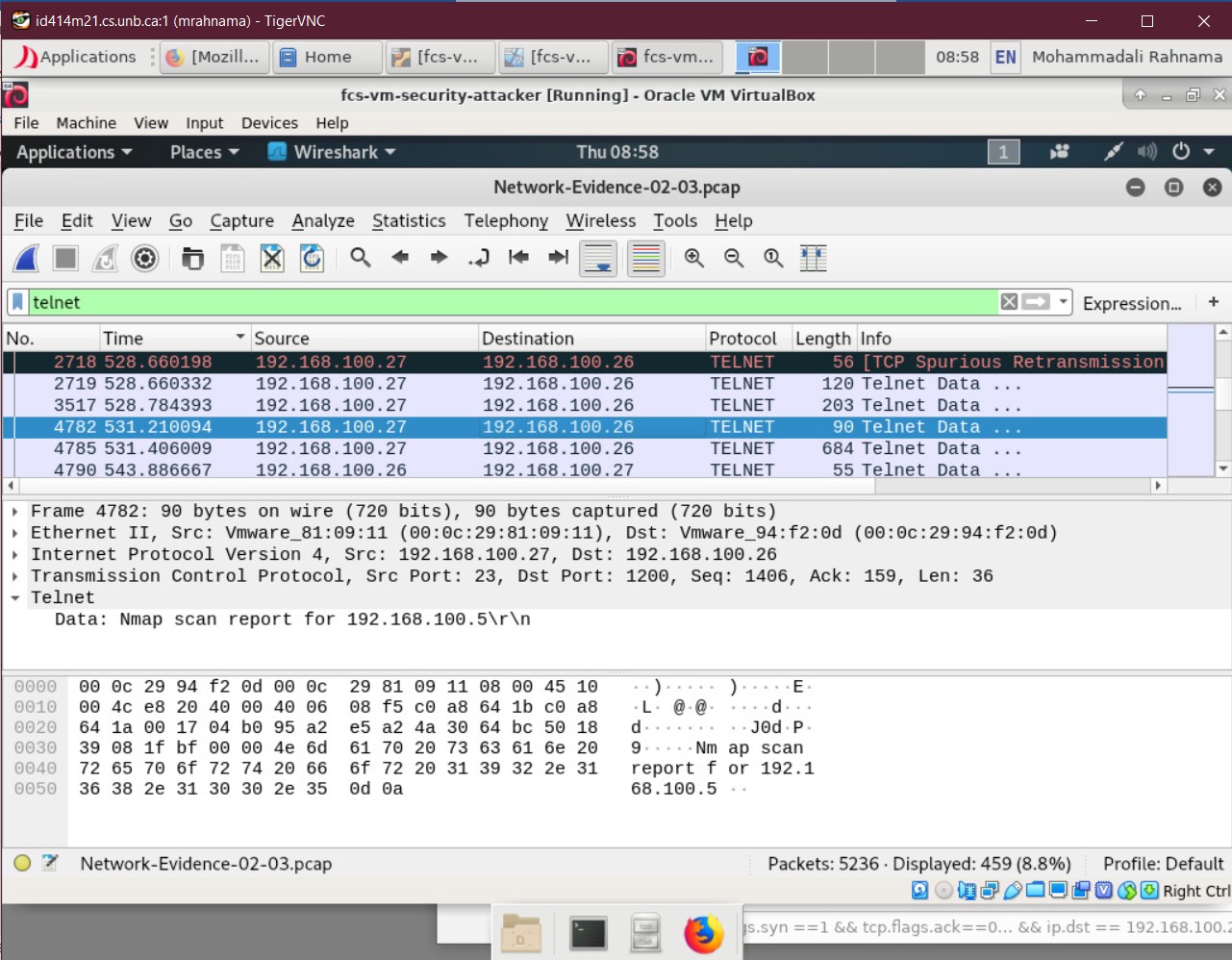
This scanning cannot take place unless a list of active hosts is identified and mapped to their IP addresses. This activity, known as host discovery, begins with a network scan.

The goal of port and network scanning is to identify the organization of IP addresses, hosts, and ports so that open or vulnerable server locations can be determined, and security levels can be diagnosed.

1. **How many port scans were run?**

Once Using TCP, and twice using Telnet.

****

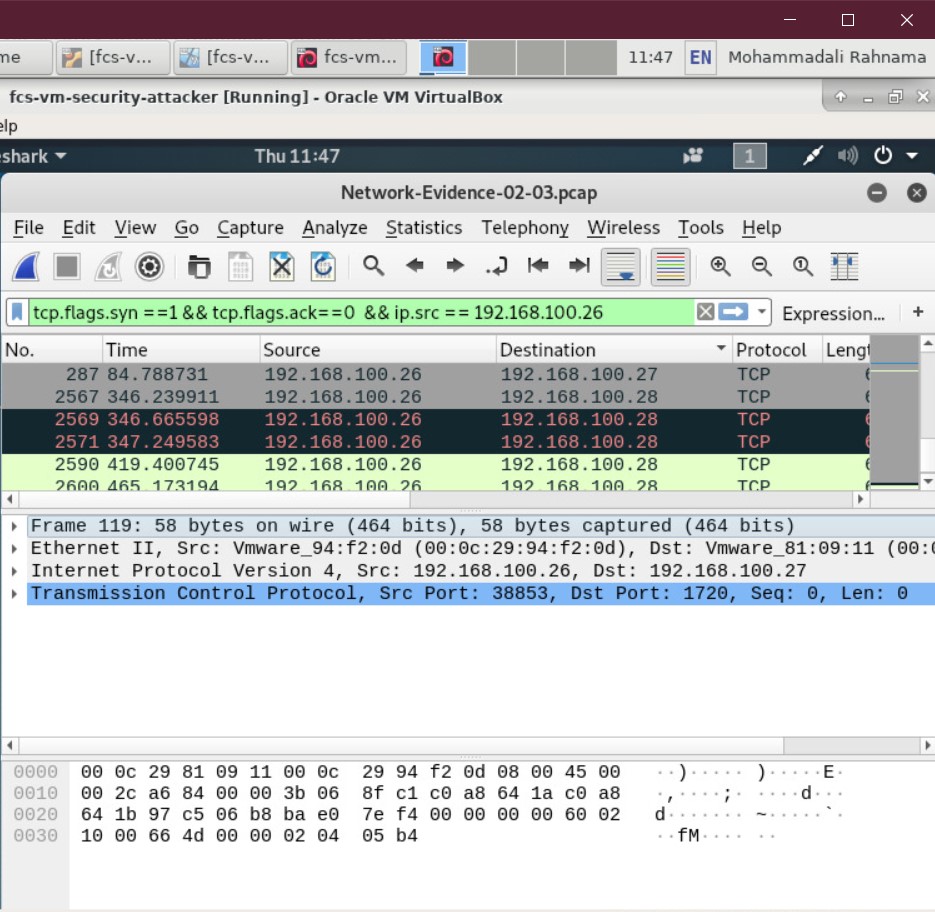
****

**b. What computer initiated the port scan(s)? What were the target computers?**

192.168.100.26 initiated the port scans and 192.168.100.5, 192.168.100.27 and 192.168.100.28 were the targets.

**c. What type of port scan(s) did the attacker use (refer to the Nmap)?**

They used TCP Half-Open Scan. The TCP half-open port scan, also known as a SYN scan, is one of the more common and popular port scanning techniques. Unlike TCP Connect, Half-Open leaves the target hanging rather than completing the TCP connection.

****

1. **What computer (refer by OS name and last octet of the IP address) is running the telnet service?**

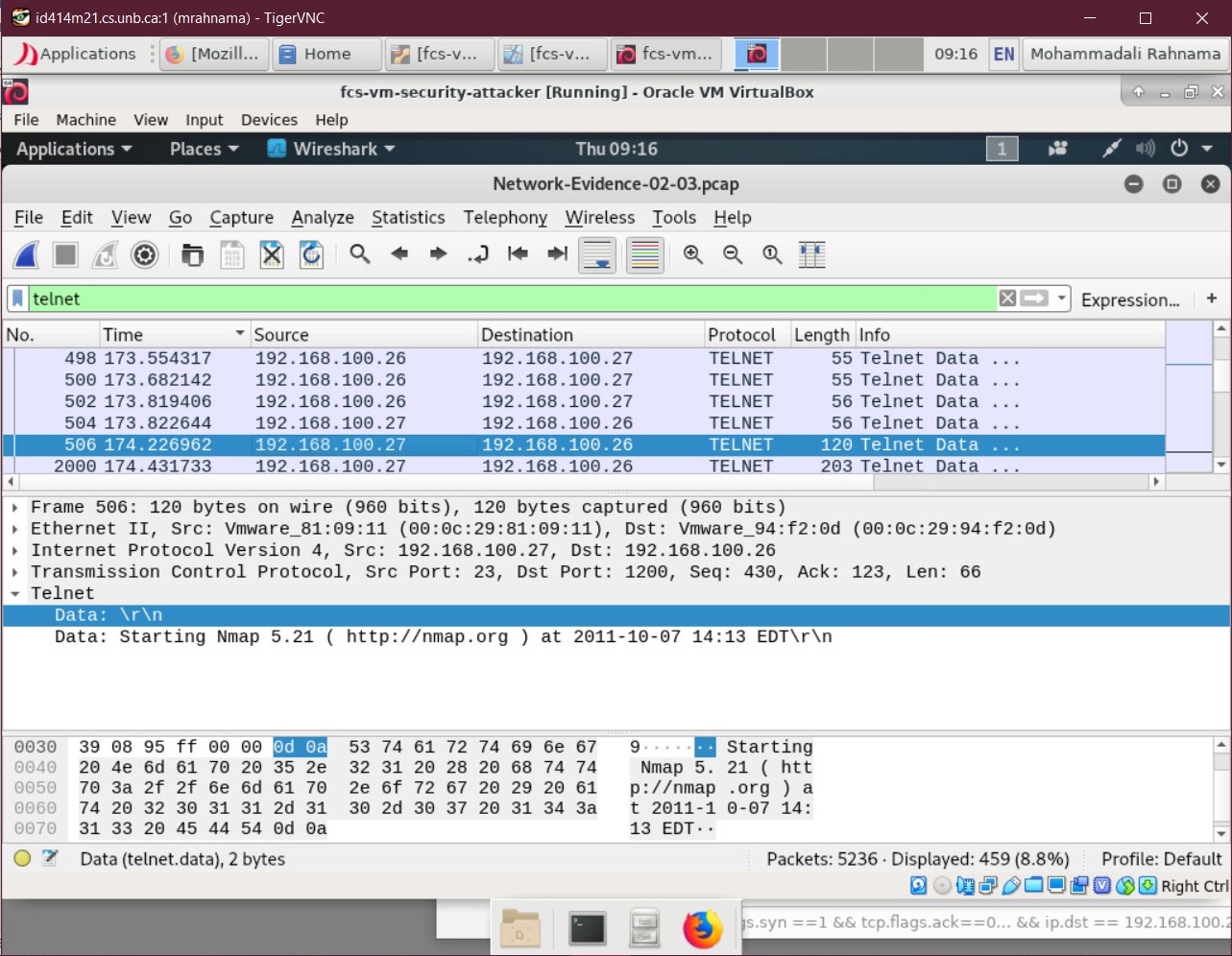
192.168.100.27, Ubuntu

**a. Which computer(s) accessed the telnet server?**

192.168.100.26, Microsoft Windows XP

**b. At what time(s)/date did this access occur?**

at 2011-10-07 14:13 EDT

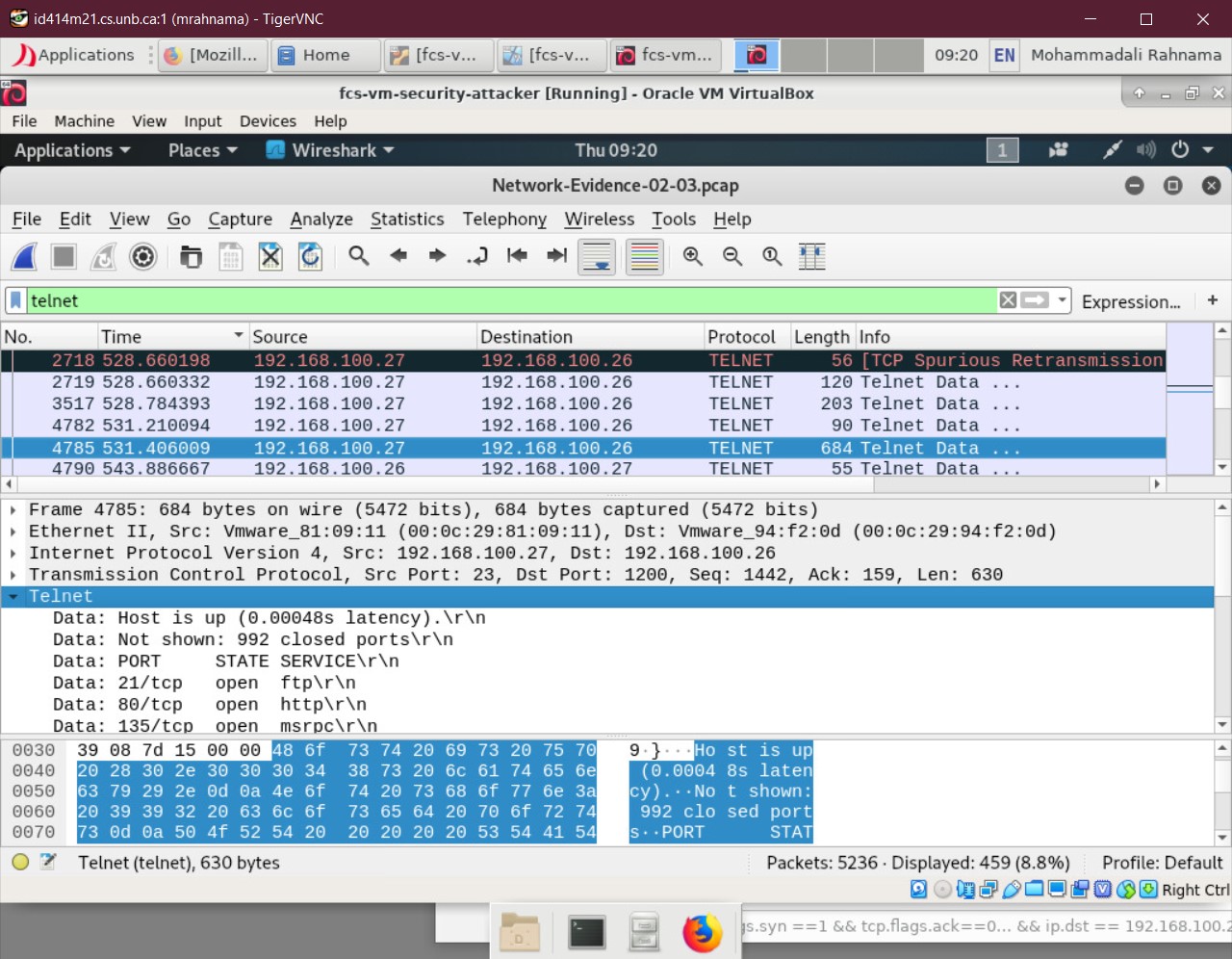
****

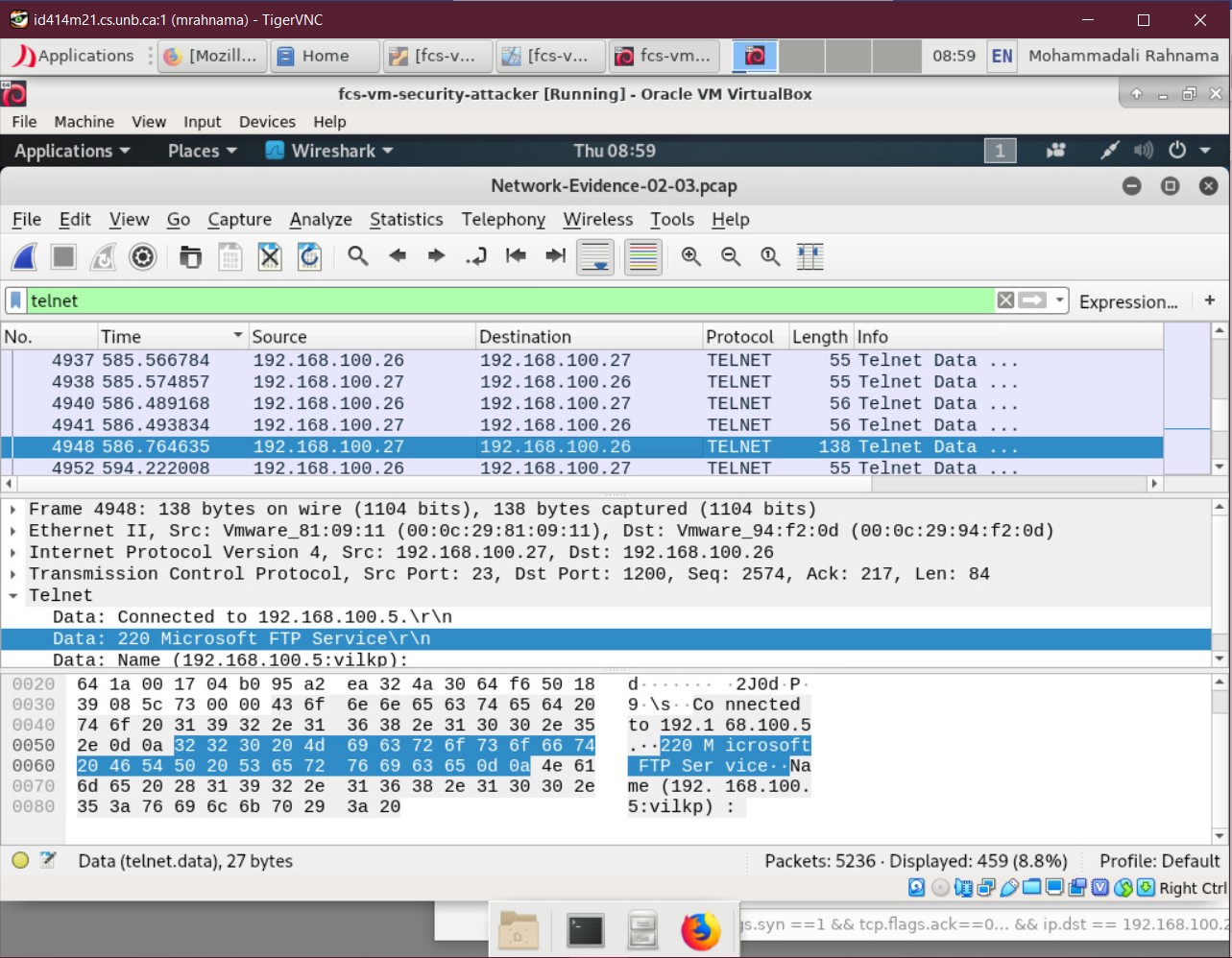
**5. What usernames/passwords were used to access the telnet server?**

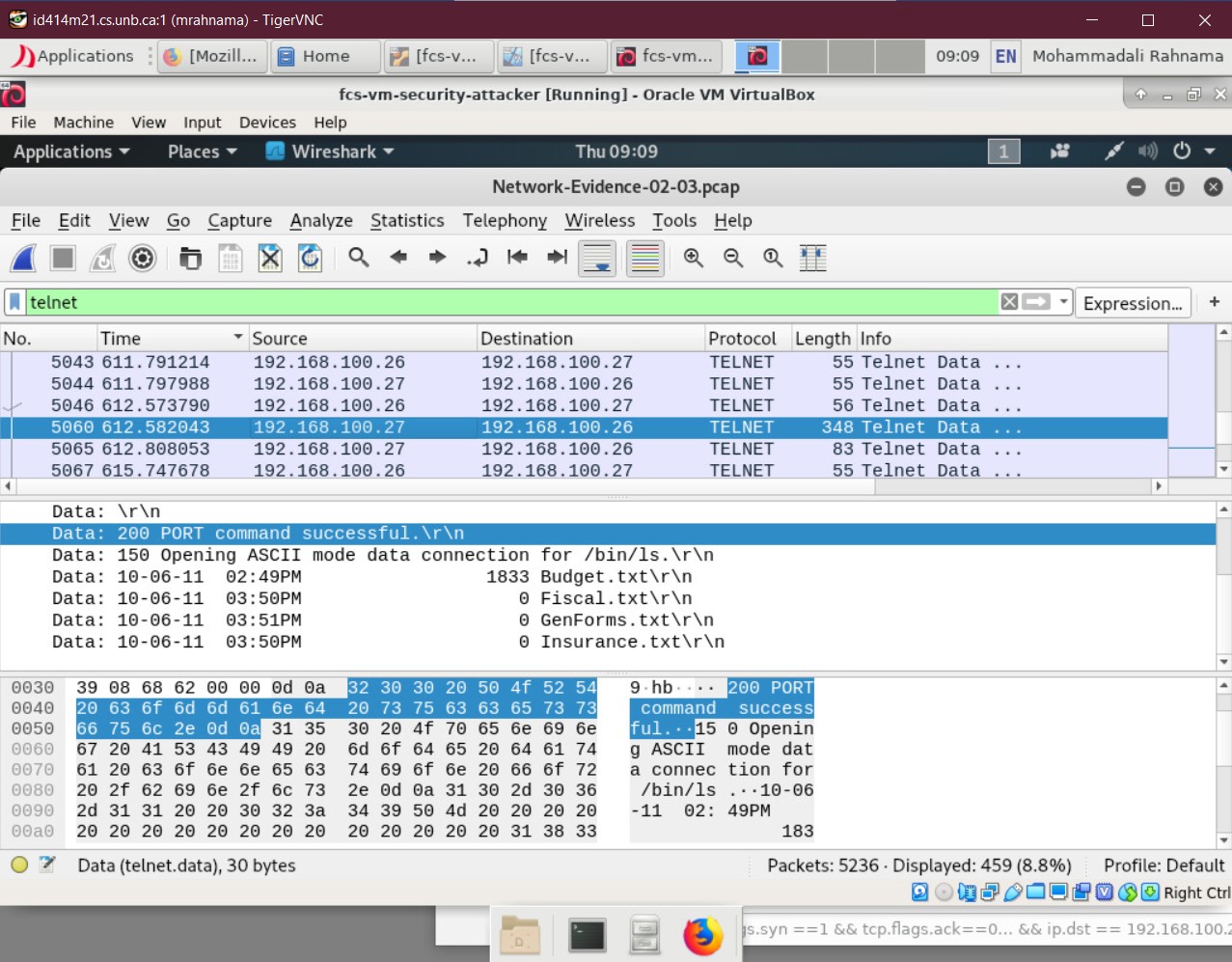
Username: Vilkp, Password: Password, email: [yeah@right.com](mailto:yeah@right.com)

1. **What did the attacker do, if anything, from the telnet server?**
2. **Explain why the attacker might have done this.**

They usen Nmap to check the ports of the computers on the network (192.168.100.5,192.168.100.28) and when they realized that an FTP port is open they used the FTP protocol to retrieve a sensitive file called Budget.txt







**6. What is the IP address of the attacker?**

192.168.100.26