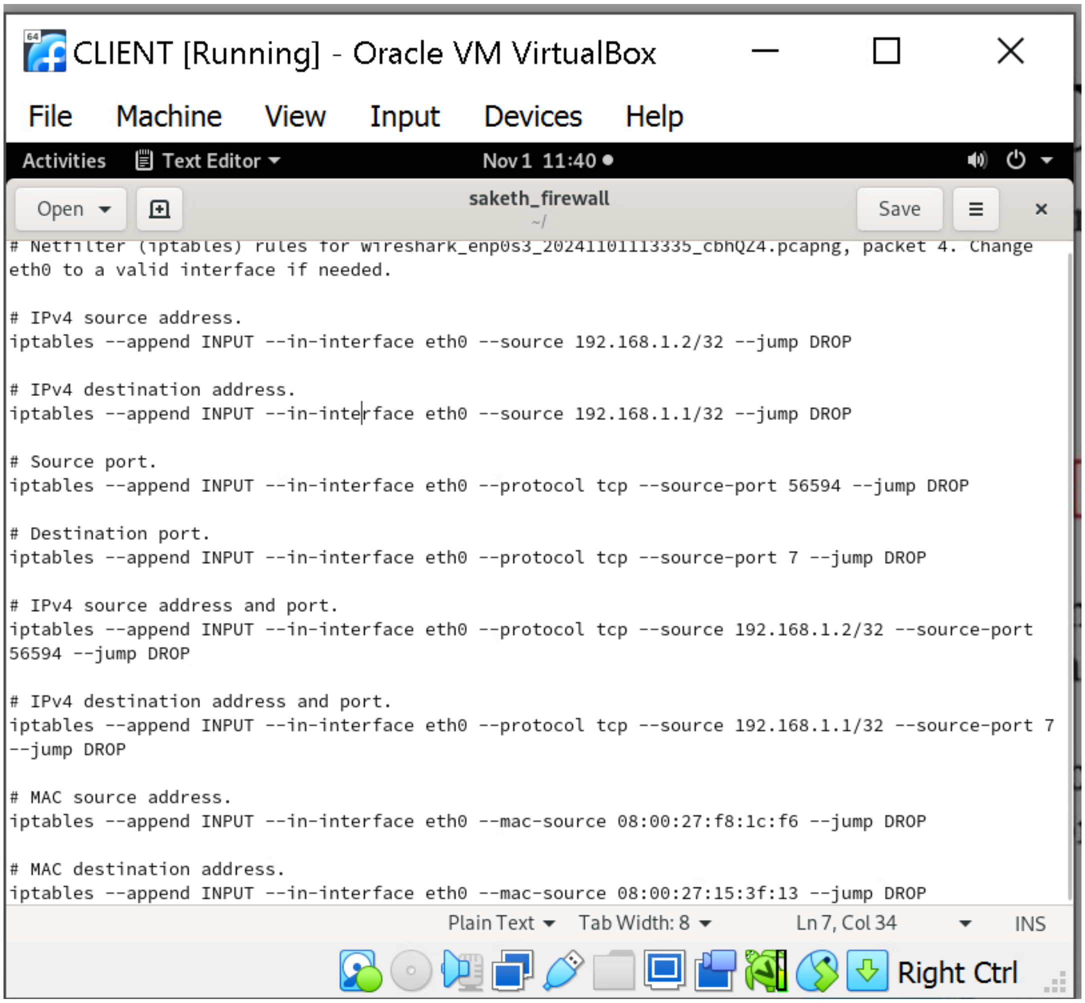
CSCI 530: Security Systems
Lab Assignment 5: Wireshark, Due: November 1st, 2024
Name: Anne Sai Venkata Naga Saketh
USC Email: annes@usc.edu
USC ID: 3725520208

Assignment Questions:

1. The number of bytes in the echo protocol exchange in section 4 above, according to the "Follow TCP Stream" window, is ***14 bytes***

2. The number of bytes in the echo protocol exchange in section 4 above, according to the Statistics/Conversation List/TCP window, is ***888 Bytes***

3. The iptables command syntax to create a firewall rule prohibiting use of the standard echo protocol (Section 6 above) is:



```
# Netfilter (iptables) rules for wireshark_enp0s3_20241101113335_cbhQZ4.pcapng, packet 4. Change
eth0 to a valid interface if needed.

# IPv4 source address.
iptables --append INPUT --in-interface eth0 --source 192.168.1.2/32 --jump DROP

# IPv4 destination address.
iptables --append INPUT --in-interface eth0 --source 192.168.1.1/32 --jump DROP

# Source port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source-port 56594 --jump DROP

# Destination port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source-port 7 --jump DROP

# IPv4 source address and port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source 192.168.1.2/32 --source-port
56594 --jump DROP

# IPv4 destination address and port.
iptables --append INPUT --in-interface eth0 --protocol tcp --source 192.168.1.1/32 --source-port 7
--jump DROP

# MAC source address.
iptables --append INPUT --in-interface eth0 --mac-source 08:00:27:f8:1c:f6 --jump DROP

# MAC destination address.
iptables --append INPUT --in-interface eth0 --mac-source 08:00:27:15:3f:13 --jump DROP
```

4. ***OMITTED - Do not answer this question.***

5. The number of frames in section 9's data stream was ___***1350***___

6. The average length/size (in bytes) of the frames in section 9's DataStream was ___***1012.45***___

7. The most common frame size among the frames in section 9's DataStream was __***1513.96 (~1514 bytes)***__

8. The maximum frame size among the frames in section 9's DataStream was ___***1513.96 (~1514 bytes)***___

9. For any of those max-sized frames, the size of its ethernet payload portion was ____***1500***____

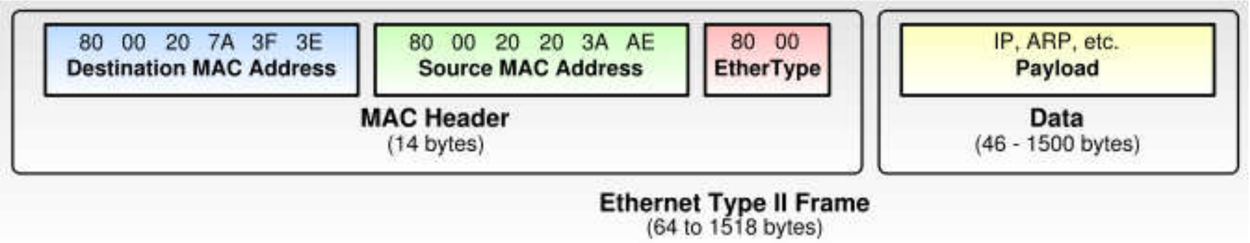
10. For that frame, the size of the remainder of the packet (i.e., its header) was ___***14***___

11. For that frame (and all the others like it) Wireshark names its highest-level payload (see the packet details pane). It's _____***FTP***_____

12. The observed value of the maximum frame size is interesting. It could not be any larger because (consider the reference graphic that follows):

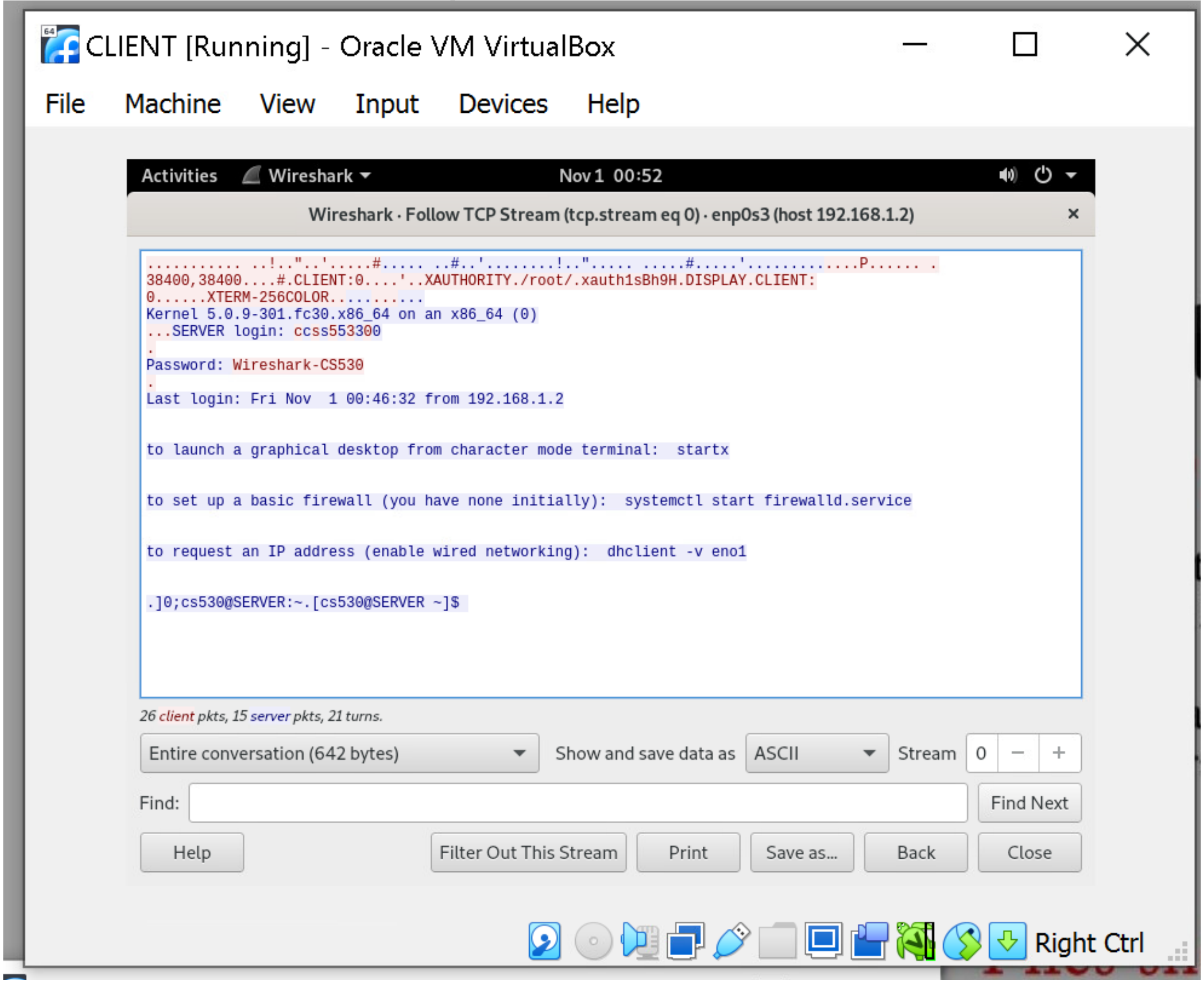
Answer: ***The standard maximum transmission unit (MTU) for Ethernet frames, which is 1500 bytes for the payload + 14 bytes for the Ethernet header, is represented by the observed maximum frame size of 1514 bytes, making it noteworthy. Because it complies with the Ethernet MTU, the frame size limit specified by the Ethernet standard, this maximum frame size could not be greater.***

For reference, question 12:



13. At the bottom of your file, insert two screen captures you made:
- the one you generated in section 7 above (telnet login showing cleartext password)
- the one you generated in section 10 ("snakeoil" tls decrypt)

Section 7 Screenshot with the password:



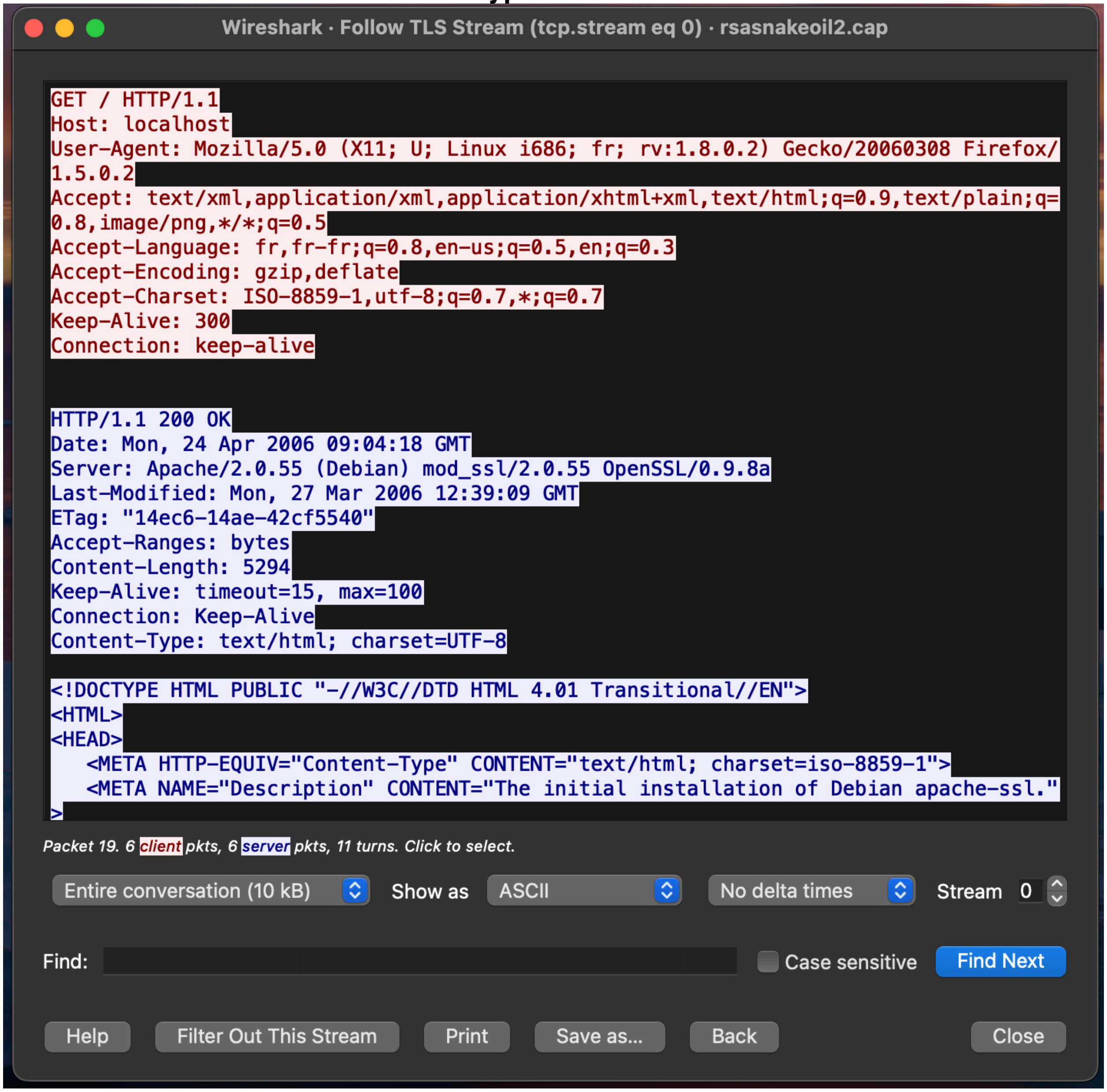
CLIENT [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Wireshark
Nov 1 00:52
Wireshark · Follow TCP Stream (tcp.stream eq 0) · enp0s3 (host 192.168.1.2)

```
........... ..!.."..'.....#..... ..#..'........!..".... .....#.....'.............P...... .
38400,38400....#.CLIENT:0....'..XAUTHORITY./root/.xauth1sBh9H.DISPLAY.CLIENT:
0......XTERM-256COLOR...........
Kernel 5.0.9-301.fc30.x86_64 on an x86_64 (0)
...SERVER login: ccss553300
.
Password: Wireshark-CS530
.
Last login: Fri Nov  1 00:46:32 from 192.168.1.2


to launch a graphical desktop from character mode terminal:  startx


to set up a basic firewall (you have none initially):  systemctl start firewalld.service


to request an IP address (enable wired networking):  dhclient -v eno1


.]0;cs530@SERVER:~.[cs530@SERVER ~]$ 
```

26 client pkts, 15 server pkts, 21 turns.

Entire conversation (642 bytes) Show and save data as ASCII Stream 0

Section 10 Screenshot with the decrypted TLS Stream:



Wireshark · Follow TLS Stream (tcp.stream eq 0) · rsasnakeoil2.cap

```
GET / HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.8.0.2) Gecko/20060308 Firefox/
1.5.0.2
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=
0.8,image/png,*/*;q=0.5
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive


HTTP/1.1 200 OK
Date: Mon, 24 Apr 2006 09:04:18 GMT
Server: Apache/2.0.55 (Debian) mod_ssl/2.0.55 OpenSSL/0.9.8a
Last-Modified: Mon, 27 Mar 2006 12:39:09 GMT
ETag: "14ec6-14ae-42cf5540"
Accept-Ranges: bytes
Content-Length: 5294
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<HTML>
<HEAD>
   <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
   <META NAME="Description" CONTENT="The initial installation of Debian apache-ssl."
>
```

Packet 19. 6 client pkts, 6 server pkts, 11 turns. Click to select.

Entire conversation (10 kB) Show as ASCII No delta times Stream 0

Find: □ Case sensitive