|  |
| --- |
| * This is an individual assignment, and is worth 20 points. * The due date and time is 1:00 / 5:30, Sep 19. * You should provide the answers using the accompanying outcome file. Change the file name following the naming convention: homework, underscore, last name, first initial, and extension (e.g., Lab 1\_ImG.docx). * Do not copy any of the sample screenshots provided as illustrations. * You should not scan any live servers using Nmap and hping3. For violation, you may be expelled from the school (not a joke!). |

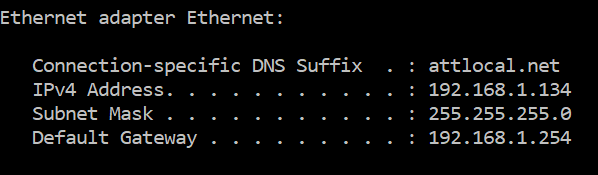
# Lab 3: Packet Analysis (Part 2)

## Task 1. Identify the IP addresses

* Task

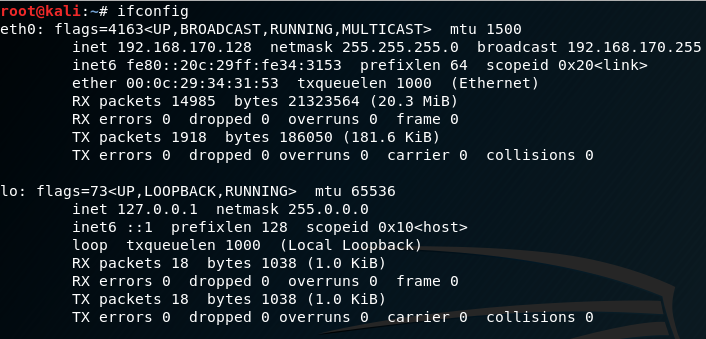
1. Idenity the IP address of your **host** and the subnet mask (use ipconfig /all). If you use wireless, the IP address of “Wireless LAN adapter Wi-Fi” is the active physical interface. Provide a screenshot for this.

192.168.1.134/254



1. Identify the IP address of your **Kali** (use ifconfig). Provide a screenshot for this.

192.168.170.255

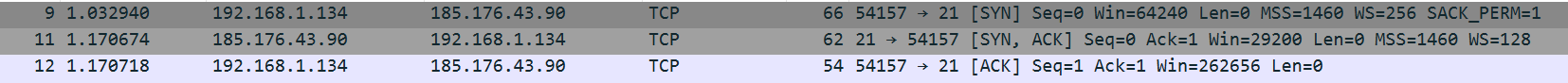


## Task 2. Analyzing FTP Signatures

* Task

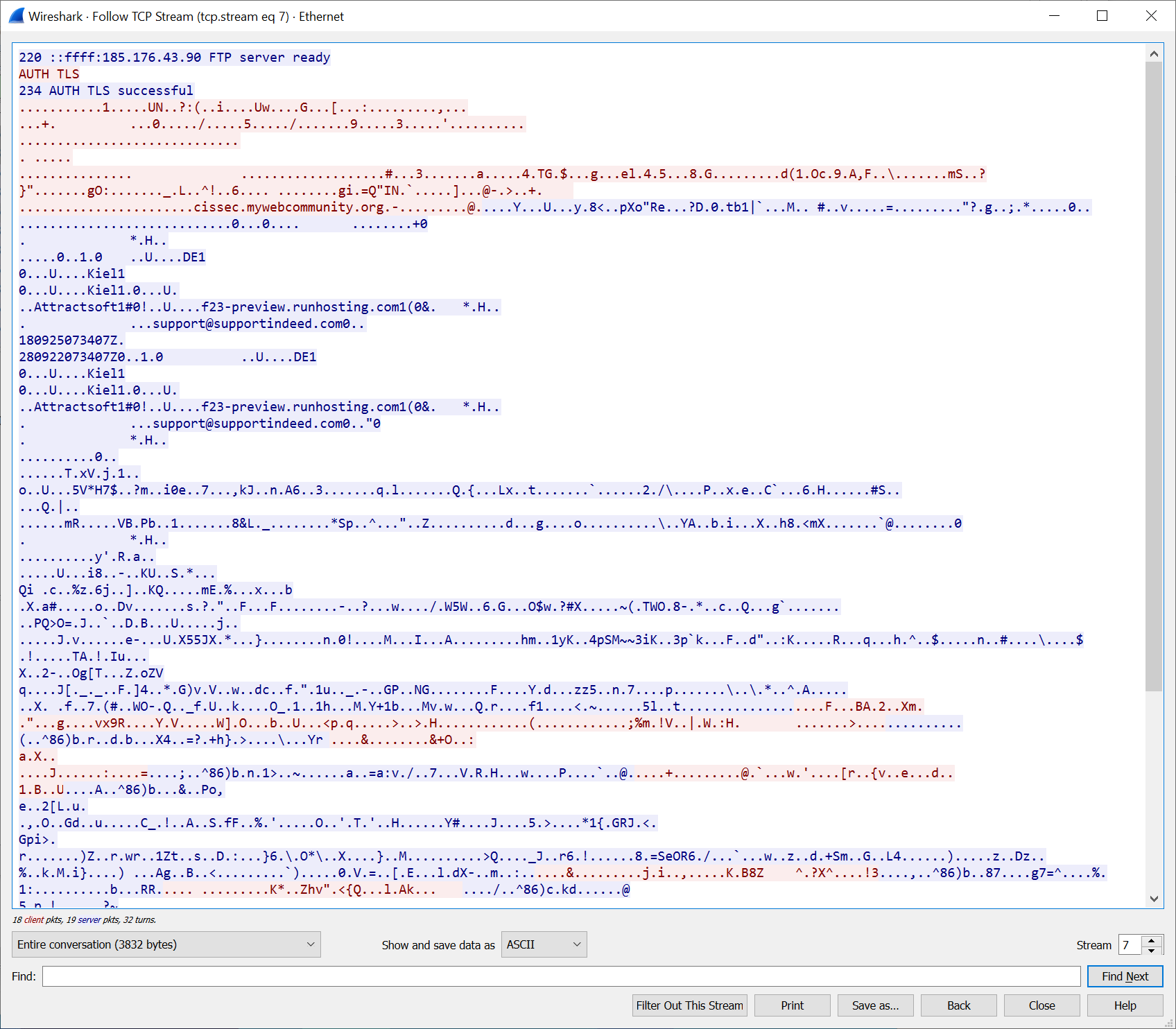
1. Identify the TCP packets used for the initial three-way handshaking. Take a screenshot of that TCP packets.

* **Hint**: These packets are placed right before ftp packets.

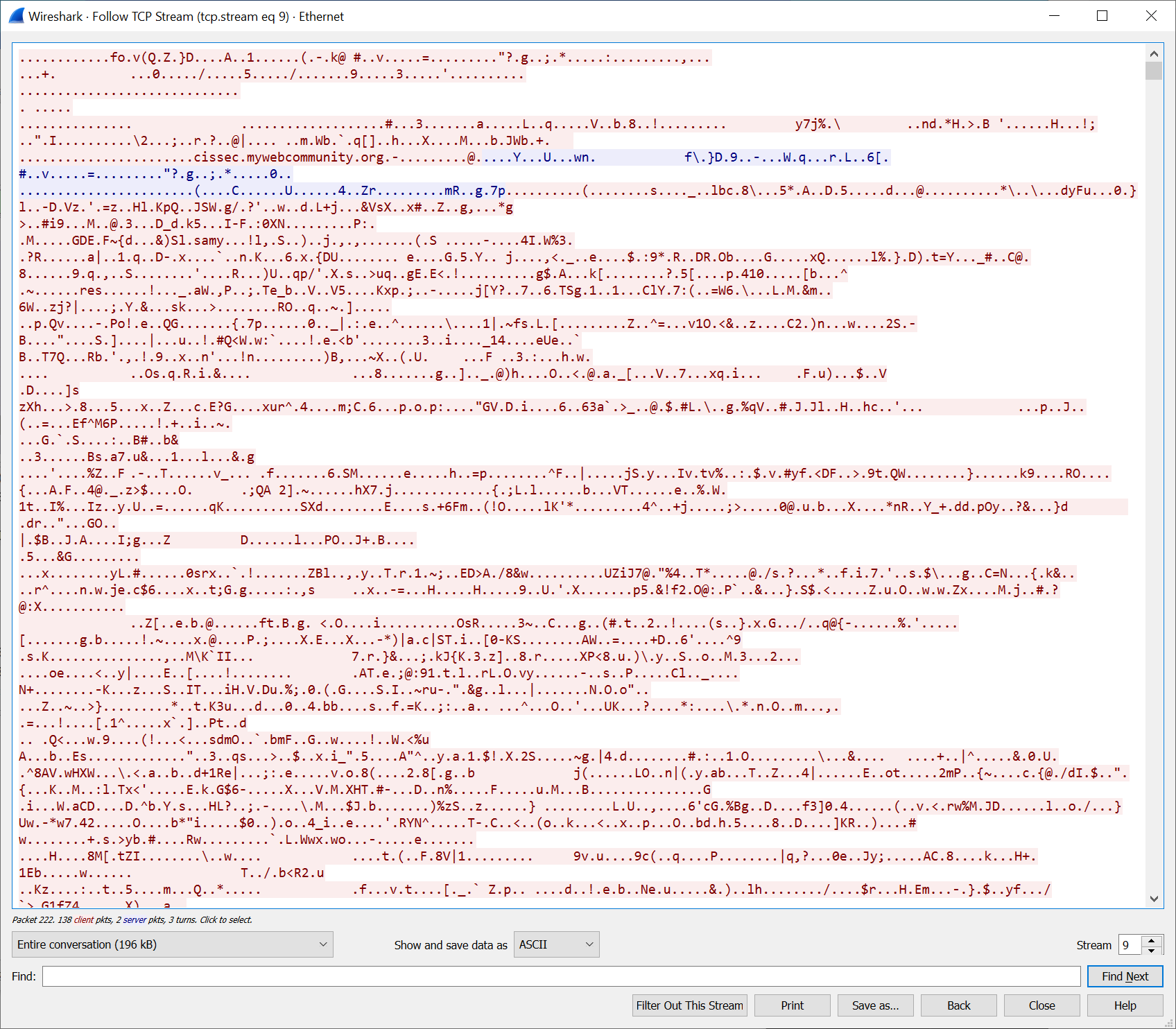


1. Identify the TCP stream used for authentication to the FTP server. The packets are encrypted and so we should guess. Take a screenshot of the TCP stream.

* **Hint**: Use the IP address of the ftp server to recognize the relevant TCP stream. Use the display filter “tcp.stream eq 7” as necessary.

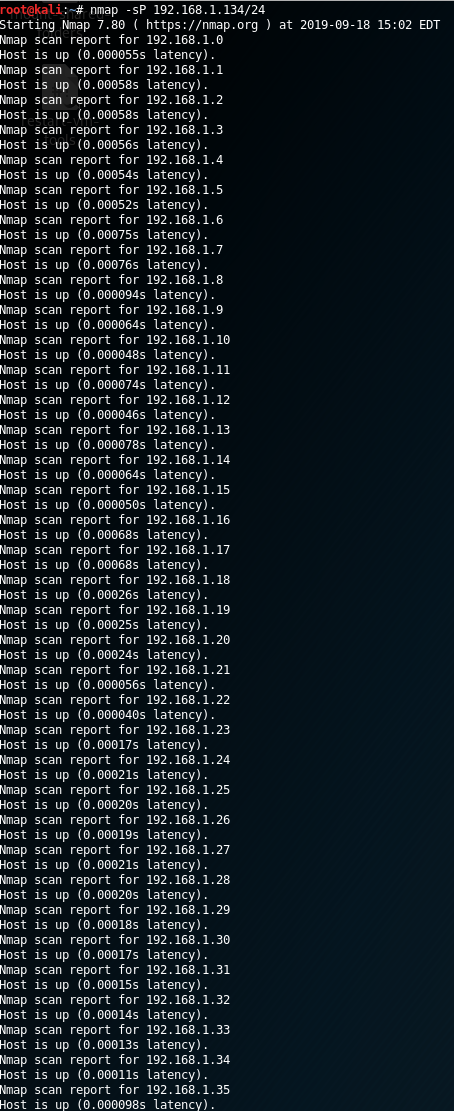


1. Identify the TCP stream used for the uploading. Take a screenshot of that TCP stream.



## Task 3. Ping Sweeping

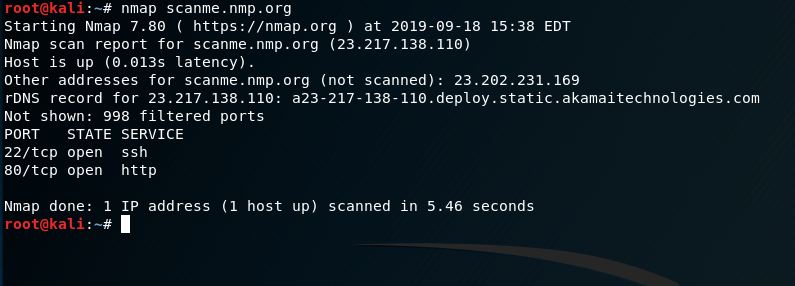
* Report the result with a screenshot.



k

## Task 4. Port Scanning

* Report the result with a screenshot.



## Task 5. SYN Flooding Attack

* Task

1. Report your Wireshark result in a screenshot.

