Dom Moore
10/19/20
Wireshark

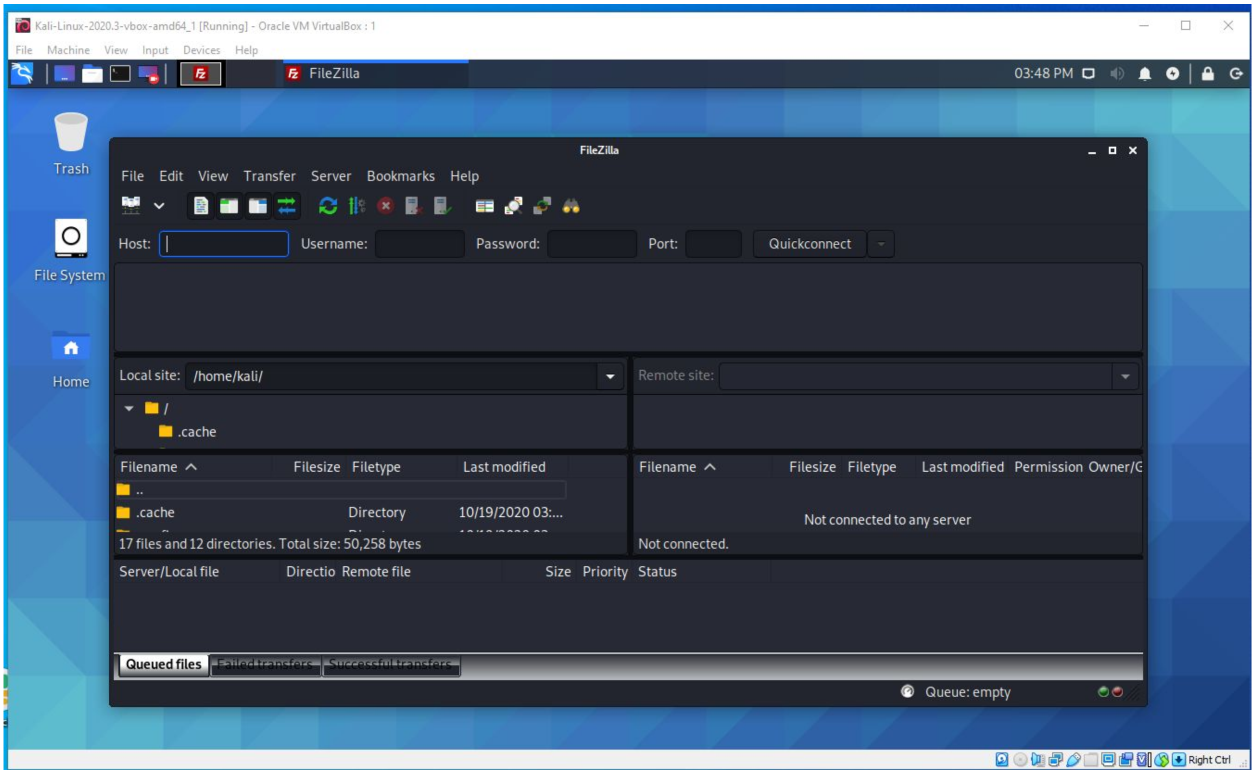
Overview

Perform network packet analysis using Wireshark.

Part 1: Staging

- Install Filezilla on your Kali Linux

Filezilla Install


Kali-Linux-2020.3-vbox-amd64_1 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
FileZilla
03:48 PM
Trash
File System
Home
FileZilla
File Edit View Transfer Server Bookmarks Help
Host:
Username:
Password:
Port:
Quickconnect
Remote site:
Filename Filesize Filetype Last modified
Filename Filesize Filetype Last modified Permission Owner/G
Server/Local file Directio Remote file Size Priority Status
Queued files
Failed transfers
Successful transfers
Right Ctrl

Local site: /home/kali/

/
.cache

Filename	Filesize	Filetype	Last modified
..			
.cache		Directory	10/19/2020 03:...

17 files and 12 directories. Total size: 50,258 bytes

Not connected to any server

Not connected.

Queue: empty

Part 2: Analyzing web server traffic with Wireshark

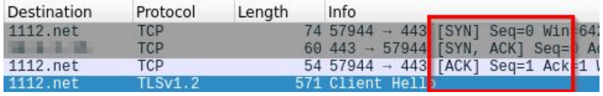
Step 1- Perform an HTTP GET request

Step 2- Sniff the packets with Wireshark.

Step 3- Analyze the packets to locate the HTML text and tag contents of the page.

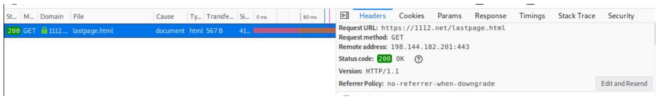
When I first performed a GET request for the specified URL I did not receive an HTTP OK packet I received a TLS packet, I did not receive an HTTP ok packet until navigating to another URL with more activity, my assumption was that because the first page was a static site that Wireshark did not detect or have anything to fetch for the GET although it did provide an ok status in the inspection tool.

Handshake



```
Destination   Protocol  Length  Info
1112.net      TCP           74 57944 → 443 [SYN] Seq=0 Win=642
[redacted]    TCP           60 443 → 57944 [SYN, ACK] Seq=0 Ac
1112.net      TCP           54 57944 → 443 [ACK] Seq=1 Ack=1 W
1112.net      TLSv1.2      571 Client Hello
```

HTTP ok

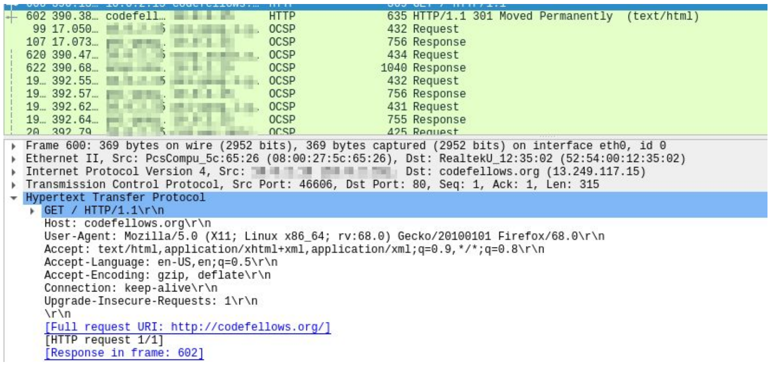


St… M… Domain File Cause Ty… Transfe… Si… 0 ms 80 ms
Headers Cookies Params Response Timings Stack Trace Security
Edit and Resend

```
200 GET 1112.… lastpage.html document html 567 B 41…
```

```
Request URL: https://1112.net/lastpage.html
Request method: GET
Remote address: 198.144.182.201:443
Status code: 200 OK
Version: HTTP/1.1
Referrer Policy: no-referrer-when-downgrade
```

Html



```
600 390.13… 10.0.2.15 codefellows.… HTTP       369 GET / HTTP/1.1
602 390.38… codefell… [redacted]    HTTP       635 HTTP/1.1 301 Moved Permanently  (text/html)
 99 17.050… [redacted]              OCSP       432 Request
107 17.073… [redacted]              OCSP       756 Response
620 390.47… [redacted]              OCSP       434 Request
622 390.68… [redacted]              OCSP      1040 Response
19… 392.55… [redacted]              OCSP       432 Request
19… 392.57… [redacted]              OCSP       756 Response
19… 392.62… [redacted]              OCSP       431 Request
19… 392.64… [redacted]              OCSP       755 Response
20… 392.79… [redacted]              OCSP       425 Request
```

```
▸ Frame 600: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_5c:65:26 (08:00:27:5c:65:26), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: [redacted] Dst: codefellows.org (13.249.117.15)
▸ Transmission Control Protocol, Src Port: 46606, Dst Port: 80, Seq: 1, Ack: 1, Len: 315
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: codefellows.org\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://codefellows.org/]
    [HTTP request 1/1]
    [Response in frame: 602]
```

Part 3: Capturing FTP packets with Wireshark

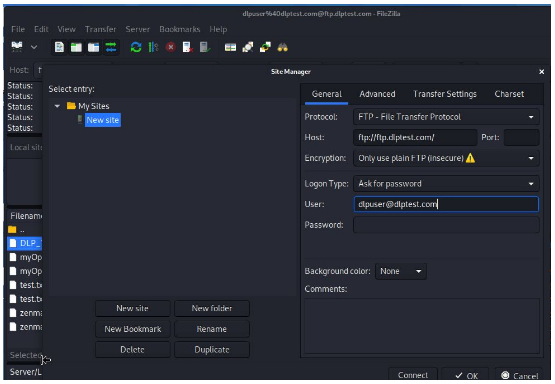
Step 1- Use Filezilla on your Kali Linux VM to access an FTP server

Step 2- Capture packets sent to and from the FTP server

Step 3- Using Wireshark, demonstrate why FTP is not a secure protocol

During the FTP test, I received some mixed results the first time accessing and transferring the XML document from host to Filezilla server the information was encrypted and showed only minor details, but after making some configuration to the Filezilla setting and resending files across the network using FTP Wireshark was able to obtain username and passwords indicating that FTP protocol is not a secure way to transfer data.

FTP setup



dlpuser%40dlptest.com@ftp.dlptest.com - FileZilla

Site Manager

Select entry:
My Sites
New site

Protocol: FTP - File Transfer Protocol

Host: ftp://ftp.dlptest.com/ Port:

Encryption: Only use plain FTP (insecure) ⚠

Logon Type: Ask for password

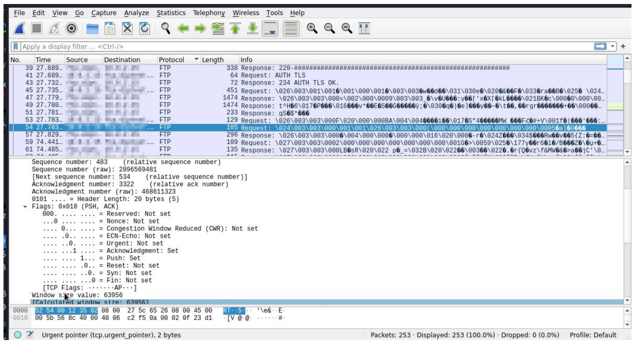
User: dlpuser@dlptest.com

Password:

Background color: None

Comments:

FTP packets



```
No.  Time       Source     Destination  Protocol  Length Info
  39 27.689…   [redacted] [redacted]   FTP          338 Response: 220-##########################################################
  41 27.689…   [redacted] [redacted]…  FTP           64 Request: AUTH TLS
  43 27.732…   [redacted] [redacted]   FTP           72 Response: 234 AUTH TLS OK.
  45 27.735…   [redacted] [redacted]…  FTP          451 Request: \026\003\001\001�\001\000\001�\003\003�w��d��\031\030e�\020�&��F�\033�ra��B�\025� \024…
  47 27.779…   [redacted] [redacted]   FTP         1474 Response: \026\003\003\000=\002\000\0009\003\003_�\v�U���:y��['x�X[�kL���\021BK�c\000�0\000\00…
  49 27.780…   [redacted] [redacted]   FTP         1474 Response: t^H�6\017�P���\016���v*��E�S��G�����ÿ;�\030�q�)�e]���y��~�\t��,��rgr�������+��\000��…
  51 27.781…   [redacted] [redacted]   FTP          233 Response: gS�S*���
  53 27.783…   [redacted] [redacted]…  FTP          129 Request: \026\003\003\000F\020\000\000BA\004\004����i��\017�S"4�����MW ���F<�#+V\001f�|���'���:…
  54 27.783…   [redacted] [redacted]…  FTP          105 Request: \024\003\003\000\001\001\026\003\003\000(\000\000\000\000\000\000\000\0005�a]�����
  57 27.829…   [redacted] [redacted]   FTP          296 Response: \026\003\003\000�\004\000\000�\000\000\016\020\000�-r�\024Z���\034S���Rw��v��5{Z:�=��…
  59 74.441…   [redacted] [redacted]…  FTP          109 Request: \027\003\003\0002\000\000\000\000\000\000\000\001G�>\0059\025�\177y��r6�l�/B���Z�\�y+�…
  61 74.485…   [redacted] [redacted]   FTP          135 Response: \027\003\003\000LB�sR\020\022 p�_=\032B\020\022��\003��\022�.�r{Q�vz\fdMW�&�>a��jC'\0…
```

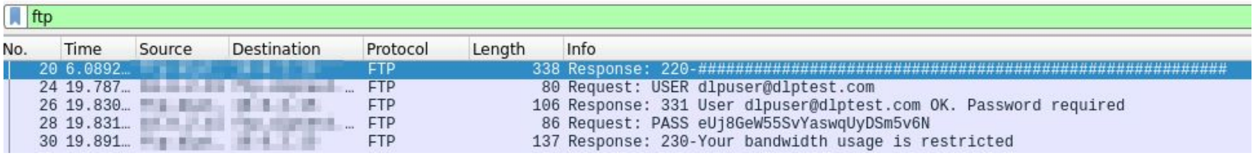
```
   Sequence number: 483    (relative sequence number)
   Sequence number (raw): 2896569481
   [Next sequence number: 534    (relative sequence number)]
   Acknowledgment number: 3322    (relative ack number)
   Acknowledgment number (raw): 468611323
   0101 .... = Header Length: 20 bytes (5)
 ▾ Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······AP···]
   Window size value: 63956
   [Calculated window size: 63956]

0000  52 54 00 12 35 02 08 00  27 5c 65 26 08 00 45 00   RT··5···'\e&··E·
0010  00 5b 56 8c 40 00 40 06  c2 f5 0a 00 02 0f 23 d1   ·[V·@·@·······#·
```

Urgent pointer (tcp.urgent_pointer), 2 bytes

Packets: 253 · Displayed: 253 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

FTP non- secure



ftp

```
No.  Time      Source      Destination   Protocol  Length Info
  20 6.0892…   [redacted]  [redacted]    FTP          338 Response: 220-#############################################################
  24 19.787…   [redacted]  [redacted]…   FTP           80 Request: USER dlpuser@dlptest.com
  26 19.830…   [redacted]  [redacted]    FTP          106 Response: 331 User dlpuser@dlptest.com OK. Password required
  28 19.831…   [redacted]  [redacted]…   FTP           86 Request: PASS eUj8GeW55SvYaswqUyDSm5v6N
  30 19.891…   [redacted]  [redacted]    FTP          137 Response: 230-Your bandwidth usage is restricted
```

Part 4: Sniffing hub traffic with Wireshark

Hubs behave a lot differently than switches! Now that we're getting hands-on with a network traffic sniffer, let's take a look at the difference between hubs and switches. In either GNS3, cloud, or physical lab:

Step 1- Deploy a hub, computer with Wireshark (A), and two other computers (B & C).

All computers are powered on and connected to the hub.

Step 2- Activate Wireshark sniffing on computer A.

Step 3 - On computer B, ping computer C.

Step 4 - Did you capture the ICMP packets? If so, include a screenshot.

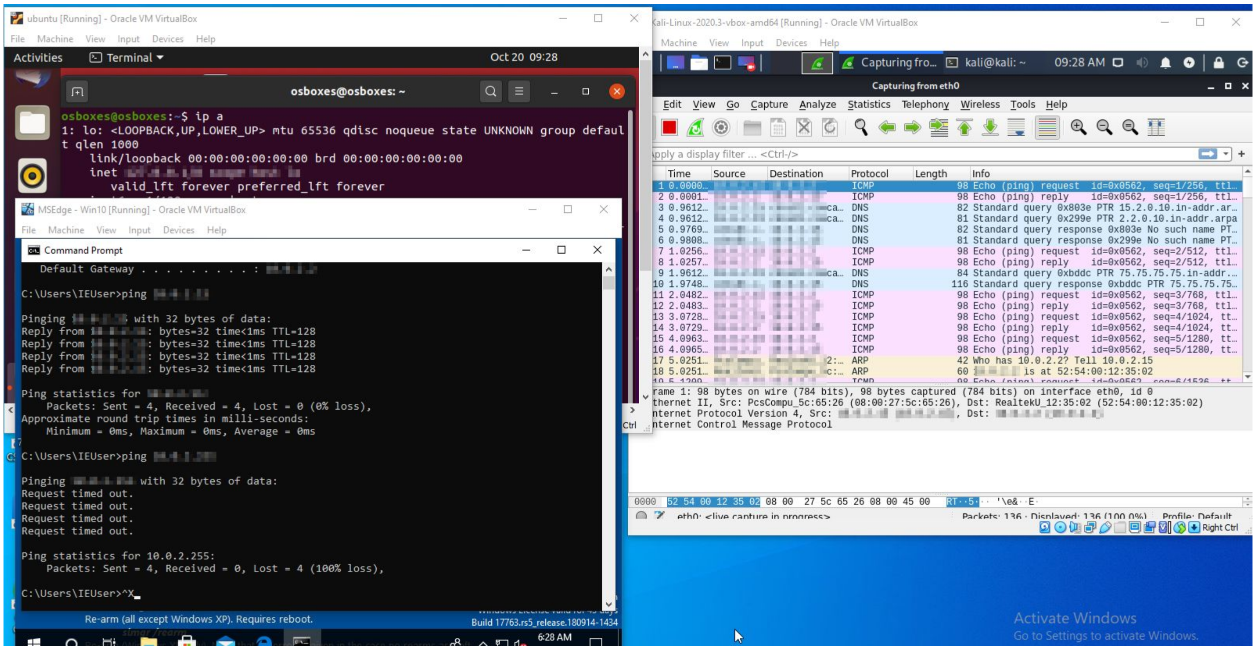
Step 5- Halt and clear Wireshark. Replace the hub with a switch.

Step - Activate Wireshark sniffing on computer A.

Step 6- On computer B, ping computer C.

During testing of the ability for hubs to keep ICMP undetected from Wireshark it failed until I input a switch, the hub allows Wireshark to detect traffic although they were two other devices, that is because the network is the same and hubs act as dummy devices and to do not prevent packet collision.

Ping ICMP packets



ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 20 09:28
osboxes@osboxes: ~

```
osboxes@osboxes:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet [redacted]
       valid_lft forever preferred_lft forever
```

MSEdge - Win10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt

```
   Default Gateway . . . . . . . . . : [redacted]

C:\Users\IEUser>ping [redacted]

Pinging [redacted] with 32 bytes of data:
Reply from [redacted]: bytes=32 time<1ms TTL=128
Reply from [redacted]: bytes=32 time<1ms TTL=128
Reply from [redacted]: bytes=32 time<1ms TTL=128
Reply from [redacted]: bytes=32 time<1ms TTL=128

Ping statistics for [redacted]
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\IEUser>ping [redacted]

Pinging [redacted] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.2.255:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\IEUser>^X_
```

Re-arm (all except Windows XP). Requires reboot.
Build 17763.rs5_release.180914-1434
6:28 AM
Kali-Linux-2020.3-vbox-amd64 [Running] - Oracle VM VirtualBox
Machine View Input Devices Help
Capturing fro...
kali@kali: ~
09:28 AM
Capturing from eth0
Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
   Time      Source      Destination    Protocol  Length  Info
 1 0.0000…  [redacted]  [redacted]     ICMP        98 Echo (ping) request  id=0x0562, seq=1/256, ttl…
 2 0.0001…  [redacted]  [redacted]     ICMP        98 Echo (ping) reply    id=0x0562, seq=1/256, ttl…
 3 0.9612…  [redacted]  [redacted]ca…  DNS         82 Standard query 0x803e PTR 15.2.0.10.in-addr.ar…
 4 0.9612…  [redacted]  [redacted]ca…  DNS         81 Standard query 0x299e PTR 2.2.0.10.in-addr.arpa
 5 0.9769…  [redacted]  [redacted]     DNS         82 Standard query response 0x803e No such name PT…
 6 0.9808…  [redacted]  [redacted]     DNS         81 Standard query response 0x299e No such name PT…
 7 1.0256…  [redacted]  [redacted]     ICMP        98 Echo (ping) request  id=0x0562, seq=2/512, ttl…
 8 1.0257…  [redacted]  [redacted]     ICMP        98 Echo (ping) reply    id=0x0562, seq=2/512, ttl…
 9 1.9612…  [redacted]  [redacted]ca…  DNS         84 Standard query 0xbddc PTR 75.75.75.75.in-addr.…
10 1.9748…  [redacted]  [redacted]     DNS        116 Standard query response 0xbddc PTR 75.75.75.75…
11 2.0482…  [redacted]  [redacted]     ICMP        98 Echo (ping) request  id=0x0562, seq=3/768, ttl…
12 2.0483…  [redacted]  [redacted]     ICMP        98 Echo (ping) reply    id=0x0562, seq=3/768, ttl…
13 3.0728…  [redacted]  [redacted]     ICMP        98 Echo (ping) request  id=0x0562, seq=4/1024, tt…
14 3.0729…  [redacted]  [redacted]     ICMP        98 Echo (ping) reply    id=0x0562, seq=4/1024, tt…
15 4.0963…  [redacted]  [redacted]     ICMP        98 Echo (ping) request  id=0x0562, seq=5/1280, tt…
16 4.0965…  [redacted]  [redacted]     ICMP        98 Echo (ping) reply    id=0x0562, seq=5/1280, tt…
17 5.0251…  [redacted]  [redacted]2:…  ARP         42 Who has 10.0.2.2? Tell 10.0.2.15
18 5.0251…  [redacted]  [redacted]c:…  ARP         60 [redacted] is at 52:54:00:12:35:02
19 5.1200…                             ICMP        98 Echo (ping) request  id=0x0562, seq=6/1536, tt…
rame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
thernet II, Src: PcsCompu_5c:65:26 (08:00:27:5c:65:26), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
nternet Protocol Version 4, Src: [redacted], Dst: [redacted]
nternet Control Message Protocol

0000  52 54 00 12 35 02 08 00  27 5c 65 26 08 00 45 00   RT··5···'\e&··E·
```

eth0: <live capture in progress>
Packets: 136 · Displayed: 136 (100.0%)
Profile: Default
Right Ctrl
Activate Windows
Go to Settings to activate Windows.

Part 5: Reporting

Answer the below discussion prompts in your own words as thoroughly as you can articulate:

- What kind of tool is Wireshark and what does it do?
    - Wireshark is a network sniffer, more specifically a protocol analyzer that can detect traffic over networks and provide insight on the traffic it detects.
- What other HTTP request methods can Wireshark capture and why would this be relevant to web app security?
    - Just to name a few, FTP, UDP. Smtp, tls this would be relevant to app security because depending on what methods are being used to send the traffic if a person knows what they are looking for Wireshark and provide details and bout the traffic that could lead to vulnerabilities to an application.
- How can Wireshark help a cyber defender detect how a threat actor is abusing the three-way handshake?
    - Wireshark can read live data that has traveled across the network and allows you to monitor this information to detect patterns of traffic therefore being able to detect patterns in traffic that mimic threats.
- What are some ways to avoid the security flaws of FTP? Include examples of data at rest and data in motion.
    - Ensure that you are using sftp as well as https or other secure protocols when transmitting data. Ensure that firewalls are in place as well as the network that the host device is using a secure or private connection.
- How can Wireshark be used offensively against a network topology that uses hubs?
    - This can take advantage of the limitation that comes with the hub as they are dummy devices they allow packets to be sent to other devices that are connected to that hub if a bad actor is able to gain access to a device on the hub they can see the traffic that is traveling on the network and gain access to that information using some feature of Wireshark that accepts all packets.
- What is the most technically correct term for the thing that hub ports share, but switch ports do not?
    - Hub ports share packets causing packet collision but switches do not share packets; they also function on layer two of the OSI model while hubs operate on the physical layer of the OSI model.