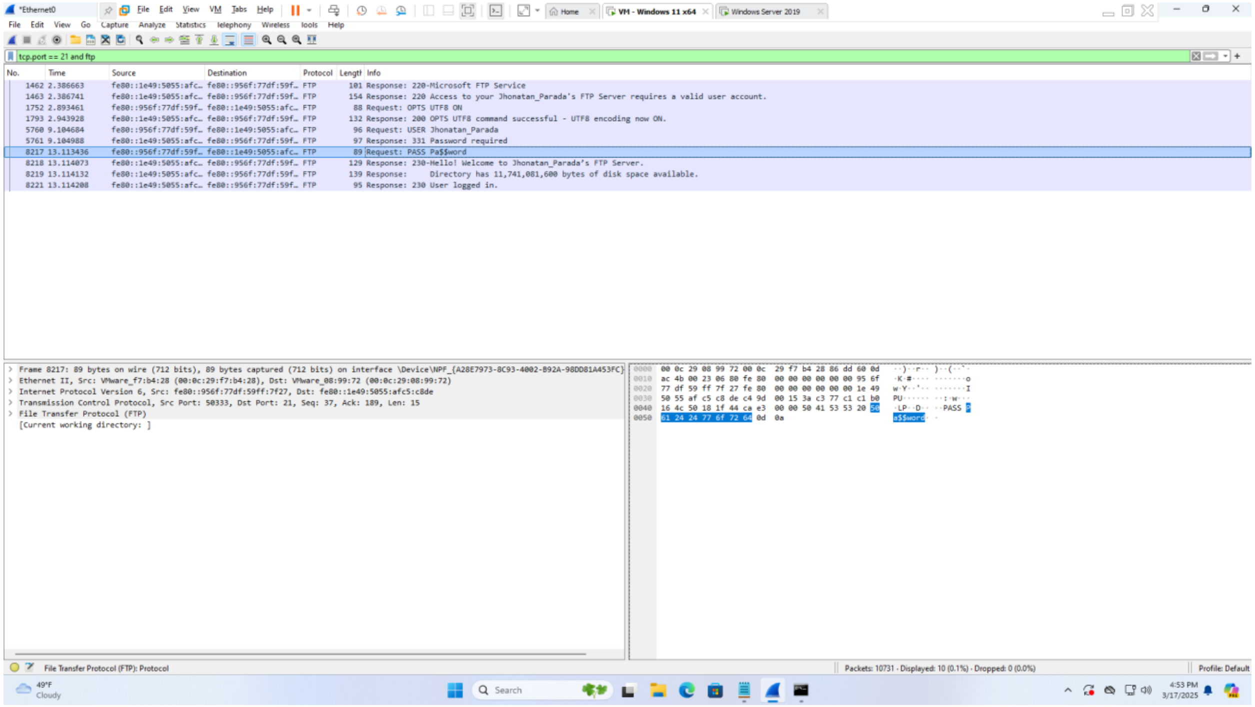
Lab 6-2

ET725

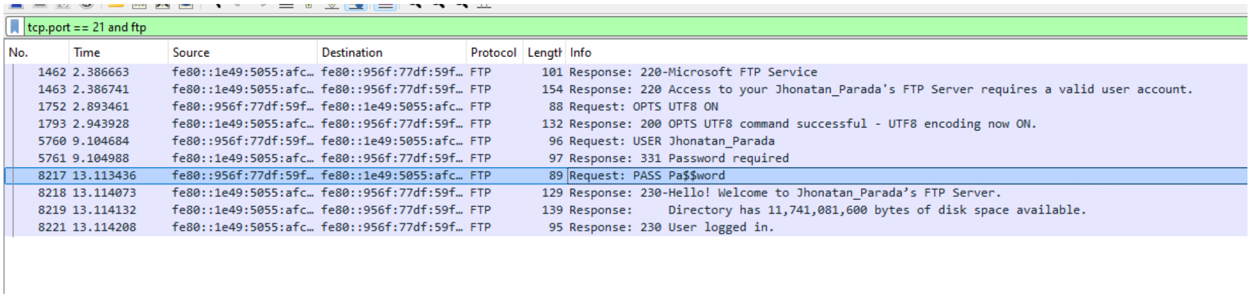
Jhonatan Parada T

Capturing FTP traffic by using the ftp and port number keywords in the packet tracer's filter bar. The traffic shown below was captured when the Jhonatan_Parada user connected and logged into the Windows FTP server. The results show the 'Pa$$word' password displayed in clear text form for the user Jhonatan_Parada.



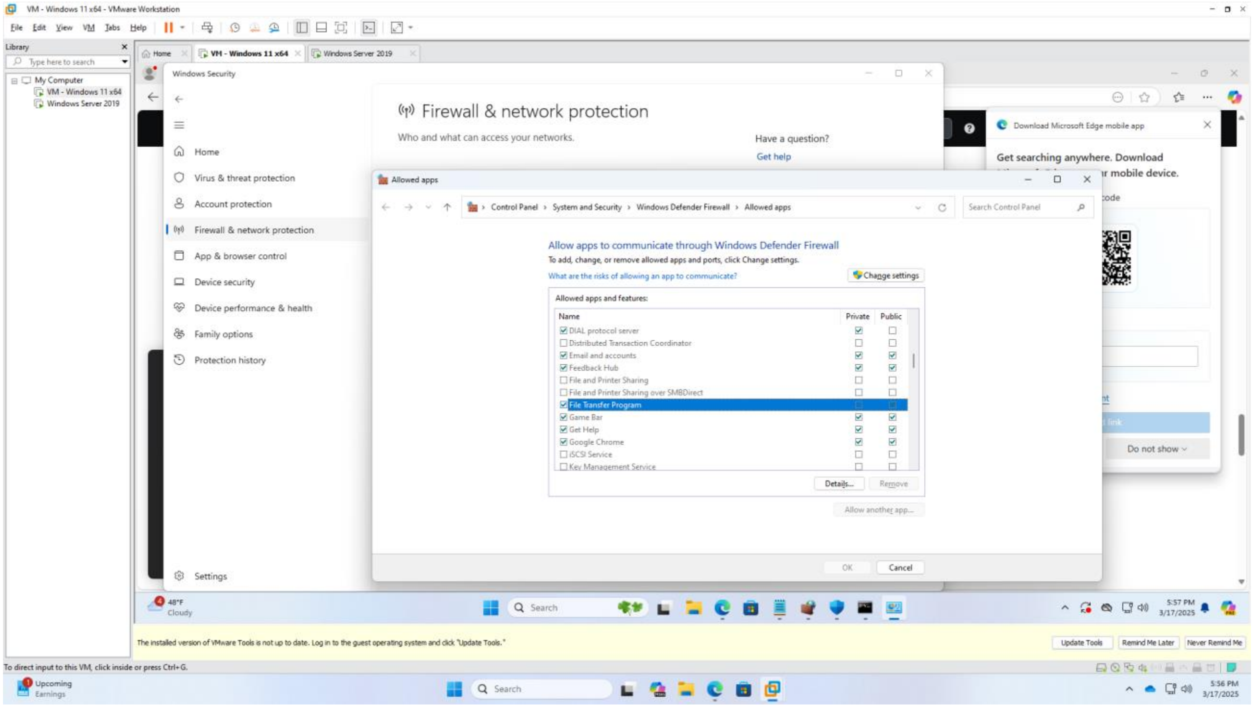
```
tcp.port == 21 and ftp

No.   Time       Source                Destination           Protocol Length Info
 1462 2.386663   fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP      101 Response: 220-Microsoft FTP Service
 1463 2.386741   fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP      154 Response: 220 Access to your Jhonatan_Parada's FTP Server requires a valid user account.
 1752 2.893461   fe80::956f:77df:59f…  fe80::1e49:5055:afc…  FTP       88 Request: OPTS UTF8 ON
 1793 2.943928   fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP      132 Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
 5760 9.104684   fe80::956f:77df:59f…  fe80::1e49:5055:afc…  FTP       96 Request: USER Jhonatan_Parada
 5761 9.104988   fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP       97 Response: 331 Password required
 8217 13.113436  fe80::956f:77df:59f…  fe80::1e49:5055:afc…  FTP       89 Request: PASS Pa$$word
 8218 13.114073  fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP      129 Response: 230-Hello! Welcome to Jhonatan_Parada's FTP Server.
 8219 13.114132  fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP      139 Response:     Directory has 11,741,081,600 bytes of disk space available.
 8221 13.114208  fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP       95 Response: 230 User logged in.

> Frame 8217: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{A28E7973-8C93-4002-B92A-98DD81A453FC}
> Ethernet II, Src: VMware_f7:b4:28 (00:0c:29:f7:b4:28), Dst: VMware_08:99:72 (00:0c:29:08:99:72)
> Internet Protocol Version 6, Src: fe80::956f:77df:59ff:7f27, Dst: fe80::1e49:5055:afc5:c8de
> Transmission Control Protocol, Src Port: 50333, Dst Port: 21, Seq: 37, Ack: 189, Len: 15
> File Transfer Protocol (FTP)
  [Current working directory: ]

0000  00 0c 29 08 99 72 00 0c  29 f7 b4 28 86 dd 60 0d   ··)··r·· )··(··`·
0010  ac 4b 00 23 06 80 fe 80  00 00 00 00 00 00 95 6f   ·K·#···· ·······o
0020  77 df 59 ff 7f 27 fe 80  00 00 00 00 00 00 1e 49   w·Y··'·· ·······I
0030  50 55 af c5 c8 de c4 9d  00 15 3a c3 77 c1 c1 b0   PU······ ··:·w···
0040  16 4c 50 18 1f 44 ca e3  00 00 50 41 53 53 20 50   ·LP··D·· ··PASS P
0050  61 24 24 77 6f 72 64 0d  0a                        a$$word··

File Transfer Protocol (FTP): Protocol    Packets: 10731 · Displayed: 10 (0.1%) · Dropped: 0 (0.0%)    Profile: Default
```

*Ethernet0
File Edit View VM Tabs Help
Home
VM - Windows 11 x64
Windows Server 2019
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
49°F
Cloudy
Search
4:53 PM
3/17/2025




```
tcp.port == 21 and ftp

No.   Time       Source                Destination           Protocol Length Info
 1462 2.386663   fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP      101 Response: 220-Microsoft FTP Service
 1463 2.386741   fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP      154 Response: 220 Access to your Jhonatan_Parada's FTP Server requires a valid user account.
 1752 2.893461   fe80::956f:77df:59f…  fe80::1e49:5055:afc…  FTP       88 Request: OPTS UTF8 ON
 1793 2.943928   fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP      132 Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
 5760 9.104684   fe80::956f:77df:59f…  fe80::1e49:5055:afc…  FTP       96 Request: USER Jhonatan_Parada
 5761 9.104988   fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP       97 Response: 331 Password required
 8217 13.113436  fe80::956f:77df:59f…  fe80::1e49:5055:afc…  FTP       89 Request: PASS Pa$$word
 8218 13.114073  fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP      129 Response: 230-Hello! Welcome to Jhonatan_Parada's FTP Server.
 8219 13.114132  fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP      139 Response:     Directory has 11,741,081,600 bytes of disk space available.
 8221 13.114208  fe80::1e49:5055:afc…  fe80::956f:77df:59f…  FTP       95 Response: 230 User logged in.
```

At this point, I was only able to able to log into the FTP server, but I was not able to read or retrieve any files from it. Every time I attempted to use the 'get' or 'dir' command, the terminal waited without any response. Initial credentials were captured, but there was a problem with file transferring. So, after doing some research on the internet, I learned that one cause the file transfer was not being successful was due to a configuration in the host firewall, more specifically, applications that were allowed to pass through it. So, I checked the File Transfer Program and enabled it in 'Allowed Applications.' After doing that, I was finally able to complete the file transfer and capture it successfull



Firewall & network protection

Who and what can access your networks.

Get searching anywhere. Download ... r mobile device.

Allowed apps

Control Panel › System and Security › Windows Defender Firewall › Allowed apps

Search Control Panel

Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Change settings

Allowed apps and features:

Name	Private	Public
☑ DIAL protocol server	☑	□
□ Distributed Transaction Coordinator	□	□
☑ Email and accounts	☑	☑
☑ Feedback Hub	☑	☑
□ File and Printer Sharing	□	□
□ File and Printer Sharing over SMBDirect	□	□
☑ File Transfer Program	□	□
☑ Game Bar	☑	☑
☑ Get Help	☑	☑
☑ Google Chrome	☑	☑
□ iSCSI Service	□	□
□ Key Management Service	□	□

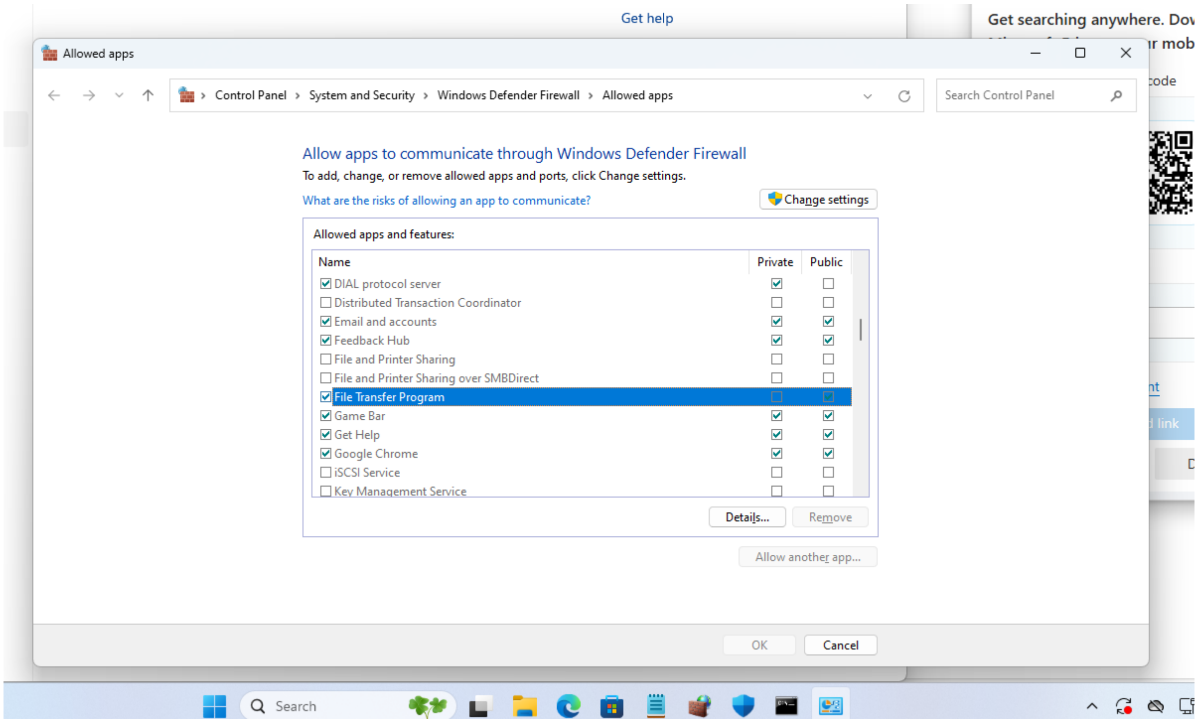
Details... Remove

Allow another app...

OK Cancel

The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

To direct input to this VM, click inside or press Ctrl+G.



Allowed apps

Control Panel › System and Security › Windows Defender Firewall › Allowed apps

Search Control Panel

Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Change settings

Allowed apps and features:

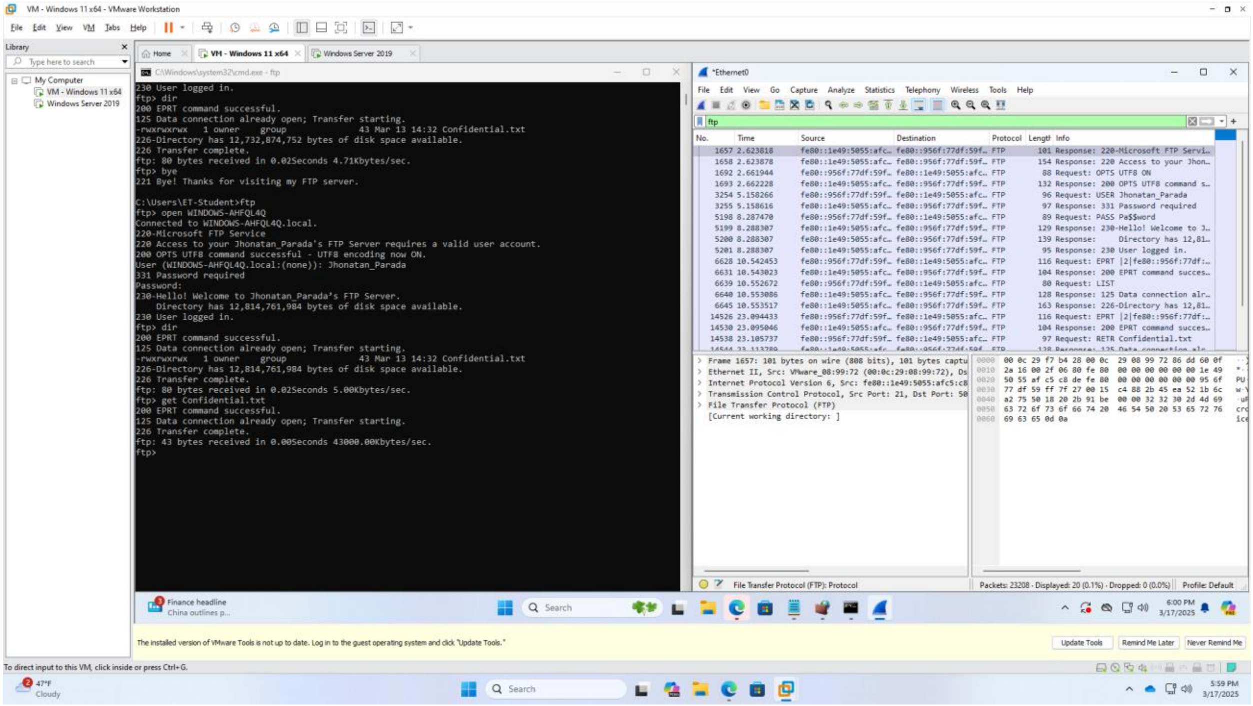
Name	Private	Public
☑ DIAL protocol server	☑	□
□ Distributed Transaction Coordinator	□	□
☑ Email and accounts	☑	☑
☑ Feedback Hub	☑	☑
□ File and Printer Sharing	□	□
□ File and Printer Sharing over SMBDirect	□	□
☑ File Transfer Program	□	□
☑ Game Bar	☑	☑
☑ Get Help	☑	☑
☑ Google Chrome	☑	☑
□ iSCSI Service	□	□
□ Key Management Service	□	□

Details... Remove

Allow another app...

OK Cancel

Here I am capturing my local traffic with Wireshark while logging into the FTP server and downloading the Confidential.txt file.



```
230 User logged in.
ftp> dir
200 EPRT command successful.
125 Data connection already open; Transfer starting.
-rwxrwxrwx   1 owner    group              43 Mar 13 14:32 Confidential.txt
226-Directory has 12,732,874,752 bytes of disk space available.
226 Transfer complete.
ftp: 80 bytes received in 0.02Seconds 4.71Kbytes/sec.
ftp> bye
221 Bye! Thanks for visiting my FTP server.

C:\Users\ET-Student>ftp
ftp> open WINDOWS-AHFQL4Q
Connected to WINDOWS-AHFQL4Q.local.
220-Microsoft FTP Service
220 Access to your Jhonatan_Parada's FTP Server requires a valid user account.
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (WINDOWS-AHFQL4Q.local:(none)): Jhonatan_Parada
331 Password required
Password:
230-Hello! Welcome to Jhonatan_Parada’s FTP Server.
    Directory has 12,814,761,984 bytes of disk space available.
230 User logged in.
ftp> dir
200 EPRT command successful.
125 Data connection already open; Transfer starting.
-rwxrwxrwx   1 owner    group              43 Mar 13 14:32 Confidential.txt
226-Directory has 12,814,761,984 bytes of disk space available.
226 Transfer complete.
ftp: 80 bytes received in 0.02Seconds 5.00Kbytes/sec.
ftp> get Confidential.txt
200 EPRT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp: 43 bytes received in 0.00Seconds 43000.00Kbytes/sec.
ftp>
```

*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

```
No.    Time       Source                 Destination            Protocol Length Info
 1657  2.623818   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      101 Response: 220-Microsoft FTP Servi…
 1658  2.623878   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      154 Response: 220 Access to your Jhon…
 1692  2.661944   fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP       88 Request: OPTS UTF8 ON
 1693  2.662228   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      132 Response: 200 OPTS UTF8 command s…
 3254  5.158266   fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP       96 Request: USER Jhonatan_Parada
 3255  5.158616   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP       97 Response: 331 Password required
 5198  8.287470   fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP       89 Request: PASS Pa$$word
 5199  8.288307   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      129 Response: 230-Hello! Welcome to J…
 5200  8.288307   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      139 Response:     Directory has 12,81…
 5201  8.288307   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP       95 Response: 230 User logged in.
 6628 10.542453   fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP      116 Request: EPRT |2|fe80::956f:77df:…
 6631 10.543023   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      104 Response: 200 EPRT command succes…
 6639 10.552672   fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP       80 Request: LIST
 6640 10.553086   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      128 Response: 125 Data connection alr…
 6645 10.553517   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      163 Response: 226-Directory has 12,81…
14526 23.094433   fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP      116 Request: EPRT |2|fe80::956f:77df:…
14530 23.095046   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      104 Response: 200 EPRT command succes…
14538 23.105737   fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP       97 Request: RETR Confidential.txt
```

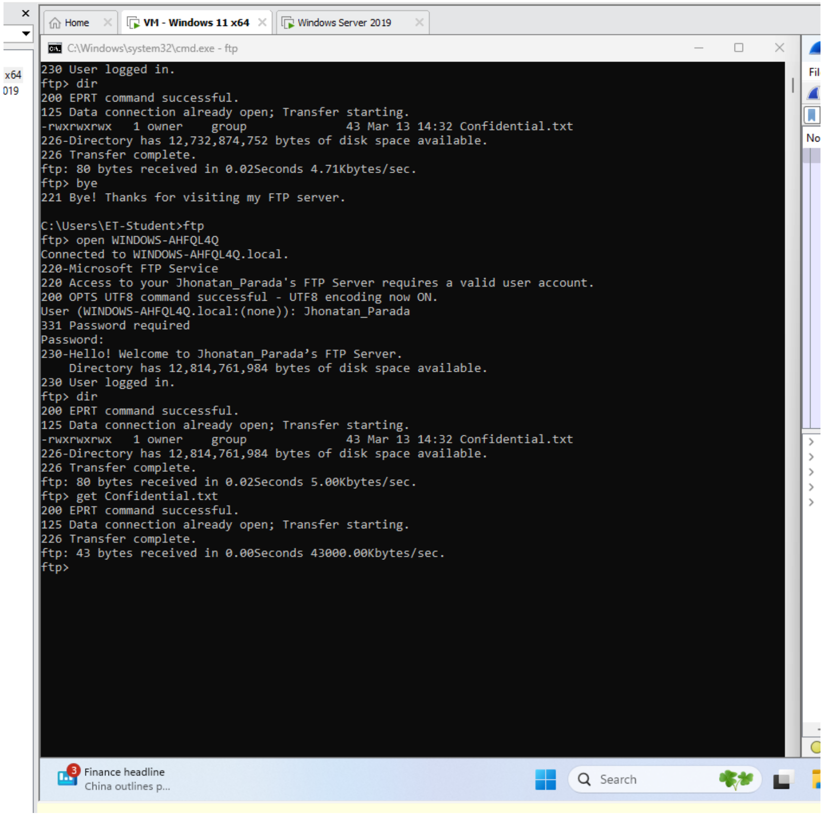
```
> Frame 1657: 101 bytes on wire (808 bits), 101 bytes captu
> Ethernet II, Src: VMware_08:99:72 (00:0c:29:08:99:72), Ds
> Internet Protocol Version 6, Src: fe80::1e49:5055:afc5:c8
> Transmission Control Protocol, Src Port: 21, Dst Port: 50
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  00 0c 29 f7 b4 28 00 0c  29 08 99 72 86 dd 60 0f
0010  2a 16 00 2f 06 80 fe 80  00 00 00 00 00 00 1e 49
0020  50 55 af c5 c8 de fe 80  00 00 00 00 00 00 95 6f
0030  77 df 59 ff 7f 27 00 15  c4 88 2b 45 ea 52 1b 6c
0040  a2 75 50 18 20 2b 91 be  00 00 32 32 30 2d 4d 69
0050  63 72 6f 73 6f 66 74 20  46 54 50 20 53 65 72 76
0060  69 63 65 0d 0a
```

File Transfer Protocol (FTP): Protocol | Packets: 23208 · Displayed: 20 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

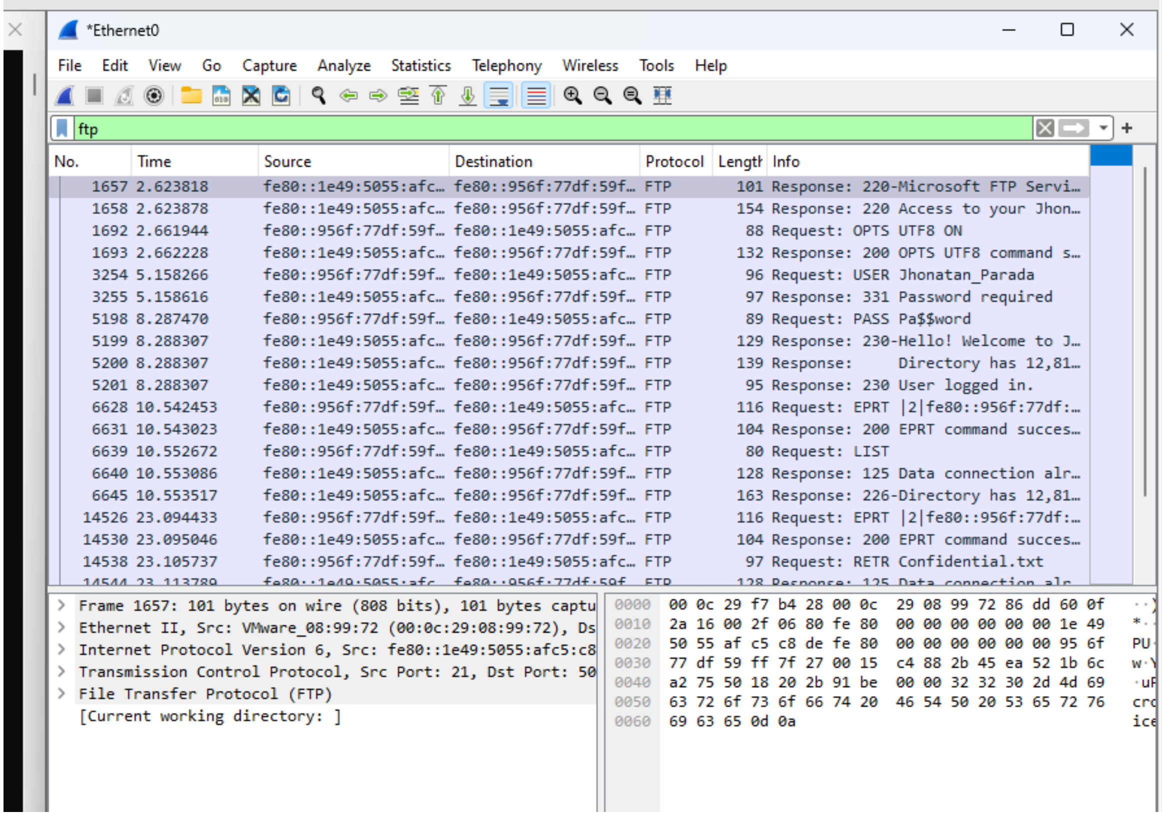
The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

Here is a closer view of the terminal and the commands. First, I log in with the Jhonatan_Parada user, then I display the contents of the current directory with the ‘dir’ command. Finally, I download the confidential.txt file by using the get command, everything while running the Wireshark protocol analyzer.



```
230 User logged in.
ftp> dir
200 EPRT command successful.
125 Data connection already open; Transfer starting.
-rwxrwxrwx   1 owner    group              43 Mar 13 14:32 Confidential.txt
226-Directory has 12,732,874,752 bytes of disk space available.
226 Transfer complete.
ftp: 80 bytes received in 0.02Seconds 4.71Kbytes/sec.
ftp> bye
221 Bye! Thanks for visiting my FTP server.

C:\Users\ET-Student>ftp
ftp> open WINDOWS-AHFQL4Q
Connected to WINDOWS-AHFQL4Q.local.
220-Microsoft FTP Service
220 Access to your Jhonatan_Parada's FTP Server requires a valid user account.
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (WINDOWS-AHFQL4Q.local:(none)): Jhonatan_Parada
331 Password required
Password:
230-Hello! Welcome to Jhonatan_Parada’s FTP Server.
    Directory has 12,814,761,984 bytes of disk space available.
230 User logged in.
ftp> dir
200 EPRT command successful.
125 Data connection already open; Transfer starting.
-rwxrwxrwx   1 owner    group              43 Mar 13 14:32 Confidential.txt
226-Directory has 12,814,761,984 bytes of disk space available.
226 Transfer complete.
ftp: 80 bytes received in 0.02Seconds 5.00Kbytes/sec.
ftp> get Confidential.txt
200 EPRT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp: 43 bytes received in 0.00Seconds 43000.00Kbytes/sec.
ftp>
```

Here I stopped the traffic capturing, the FTP filter is applied, but it will only display credential information, because the transfer of the Confidential.txt file was done using the TCP protocol. Nonetheless, this picture shows valuable information such as my username and password denoted by the ‘PASS’ keyword.

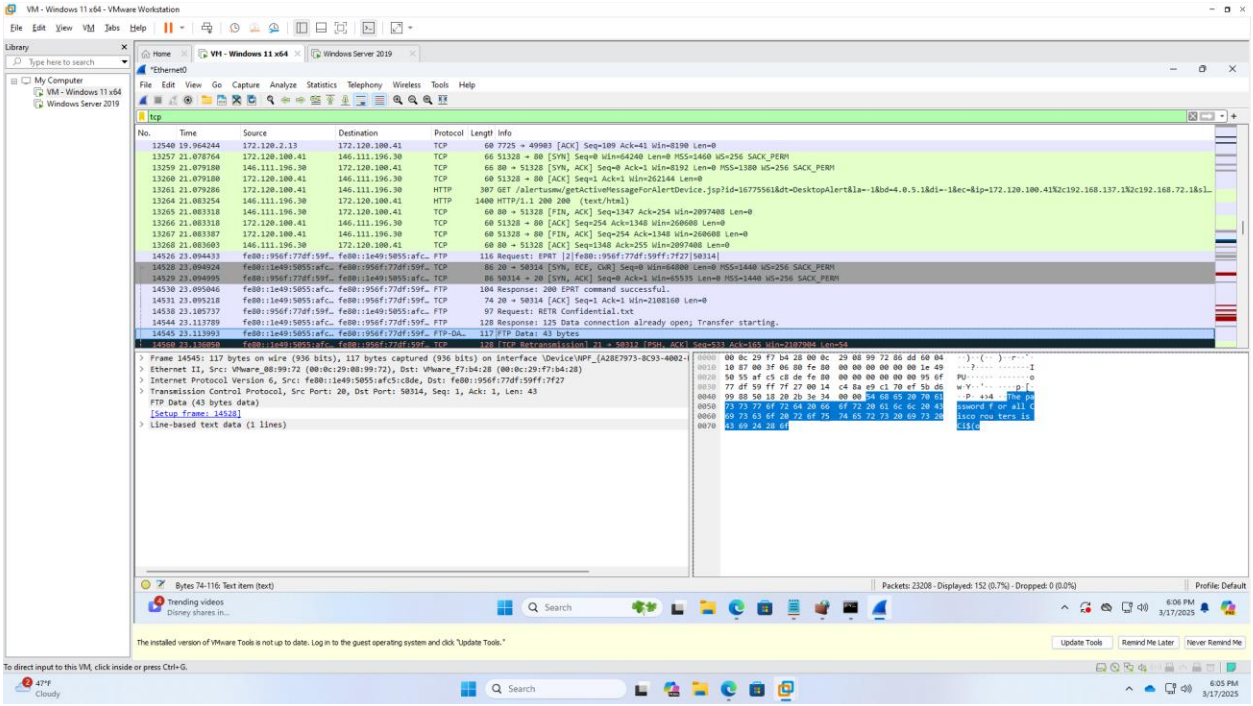


```
No.     Time       Source                 Destination            Protocol Length Info
   1657 2.623818   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      101 Response: 220-Microsoft FTP Servi…
   1658 2.623878   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      154 Response: 220 Access to your Jhon…
   1692 2.661944   fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP       88 Request: OPTS UTF8 ON
   1693 2.662228   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      132 Response: 200 OPTS UTF8 command s…
   3254 5.158266   fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP       96 Request: USER Jhonatan_Parada
   3255 5.158616   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP       97 Response: 331 Password required
   5198 8.287470   fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP       89 Request: PASS Pa$$word
   5199 8.288307   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      129 Response: 230-Hello! Welcome to J…
   5200 8.288307   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      139 Response:     Directory has 12,81…
   5201 8.288307   fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP       95 Response: 230 User logged in.
   6628 10.542453  fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP      116 Request: EPRT |2|fe80::956f:77df:…
   6631 10.543023  fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      104 Response: 200 EPRT command succes…
   6639 10.552672  fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP       80 Request: LIST
   6640 10.553086  fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      128 Response: 125 Data connection alr…
   6645 10.553517  fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      163 Response: 226-Directory has 12,81…
  14526 23.094433  fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP      116 Request: EPRT |2|fe80::956f:77df:…
  14530 23.095046  fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      104 Response: 200 EPRT command succes…
  14538 23.105737  fe80::956f:77df:59f…   fe80::1e49:5055:afc…   FTP       97 Request: RETR Confidential.txt
  14544 23.113789  fe80::1e49:5055:afc…   fe80::956f:77df:59f…   FTP      128 Response: 125 Data connection alr…
```

```
> Frame 1657: 101 bytes on wire (808 bits), 101 bytes captu
> Ethernet II, Src: VMware_08:99:72 (00:0c:29:08:99:72), Ds
> Internet Protocol Version 6, Src: fe80::1e49:5055:afc5:c8
> Transmission Control Protocol, Src Port: 21, Dst Port: 50
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  00 0c 29 f7 b4 28 00 0c  29 08 99 72 86 dd 60 0f   ··)
0010  2a 16 00 2f 06 80 fe 80  00 00 00 00 00 00 1e 49   *··
0020  50 55 af c5 c8 de fe 80  00 00 00 00 00 00 95 6f   PU·
0030  77 df 59 ff 7f 27 00 15  c4 88 2b 45 ea 52 1b 6c   w·Y
0040  a2 75 50 18 20 2b 91 be  00 00 32 32 30 2d 4d 69   ·uP
0050  63 72 6f 73 6f 66 74 20  46 54 50 20 53 65 72 76   cro
0060  69 63 65 0d 0a                                     ice
```

Here, I changed the filter to display TCP traffic only because the target now is the file named Confidential.txt. Right after the Request and Response FTP packets, we can read the content or payload of the file. The content of Confidential.txt is highlighted below.



VM - Windows 11 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
VM - Windows 11 x64
Windows Server 2019
Home
VM - Windows 11 x64
Windows Server 2019
*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.    Time      Source             Destination        Protocol Length Info
 12540 19.964244 172.120.2.13       172.120.100.41     TCP        60 7725 → 49903 [ACK] Seq=109 Ack=41 Win=8190 Len=0
 13257 21.078764 172.120.100.41     146.111.196.30     TCP        66 51328 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 13259 21.079180 146.111.196.30     172.120.100.41     TCP        66 80 → 51328 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM
 13260 21.079180 172.120.100.41     146.111.196.30     TCP        60 51328 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 13261 21.079286 172.120.100.41     146.111.196.30     HTTP      307 GET /alertusmw/getActiveMessageForAlertDevice.jsp?id=16775561&dt=DesktopAlert&la=-1&bd=4.0.5.1&di=-1&ec=&ip=172.120.100.41%2c192.168.137.1%2c192.168.72.1&sl…
 13264 21.083254 146.111.196.30     172.120.100.41     HTTP     1400 HTTP/1.1 200 200  (text/html)
 13265 21.083318 146.111.196.30     172.120.100.41     TCP        60 80 → 51328 [FIN, ACK] Seq=1347 Ack=254 Win=2097408 Len=0
 13266 21.083318 172.120.100.41     146.111.196.30     TCP        60 51328 → 80 [ACK] Seq=254 Ack=1348 Win=260608 Len=0
 13267 21.083387 172.120.100.41     146.111.196.30     TCP        60 51328 → 80 [FIN, ACK] Seq=254 Ack=1348 Win=260608 Len=0
 13268 21.083603 146.111.196.30     172.120.100.41     TCP        60 80 → 51328 [ACK] Seq=1348 Ack=255 Win=2097408 Len=0
 14526 23.094433 fe80::956f:77df:59f… fe80::1e49:5055:afc… FTP     116 Request: EPRT |2|fe80::956f:77df:59ff:7f27|50314|
 14528 23.094924 fe80::1e49:5055:afc… fe80::956f:77df:59f… TCP      86 20 → 50314 [SYN, ECE, CWR] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
 14529 23.094995 fe80::956f:77df:59f… fe80::1e49:5055:afc… TCP      86 50314 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
 14530 23.095046 fe80::1e49:5055:afc… fe80::956f:77df:59f… FTP     104 Response: 200 EPRT command successful.
 14531 23.095218 fe80::1e49:5055:afc… fe80::956f:77df:59f… TCP      74 20 → 50314 [ACK] Seq=1 Ack=1 Win=2108160 Len=0
 14538 23.105737 fe80::956f:77df:59f… fe80::1e49:5055:afc… FTP      97 Request: RETR Confidential.txt
 14544 23.113789 fe80::1e49:5055:afc… fe80::956f:77df:59f… FTP     128 Response: 125 Data connection already open; Transfer starting.
 14545 23.113993 fe80::1e49:5055:afc… fe80::956f:77df:59f… FTP-DA… 117 FTP Data: 43 bytes
 14560 23.136050 fe80::1e49:5055:afc… fe80::956f:77df:59f… TCP     128 [TCP Retransmission] 21 → 50312 [PSH, ACK] Seq=533 Ack=165 Win=2107904 Len=54
```

```
> Frame 14545: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface \Device\NPF_{A28E7973-8C93-4002-
> Ethernet II, Src: VMware_08:99:72 (00:0c:29:08:99:72), Dst: VMware_f7:b4:28 (00:0c:29:f7:b4:28)
> Internet Protocol Version 6, Src: fe80::1e49:5055:afc5:c8de, Dst: fe80::956f:77df:59ff:7f27
> Transmission Control Protocol, Src Port: 20, Dst Port: 50314, Seq: 1, Ack: 1, Len: 43
  FTP Data (43 bytes data)
  [Setup frame: 14528]
> Line-based text data (1 lines)
```

```
0000  00 0c 29 f7 b4 28 00 0c  29 08 99 72 86 dd 60 04   ··)··(·· )··r··`·
0010  10 87 00 3f 06 80 fe 80  00 00 00 00 00 00 1e 49   ···?···· ·······I
0020  50 55 af c5 c8 de fe 80  00 00 00 00 00 00 95 6f   PU······ ·······o
0030  77 df 59 ff 7f 27 00 14  c4 8a e9 c1 70 ef 5b d6   w·Y··'·· ····p·[·
0040  99 88 50 18 20 2b 3e 34  00 00 54 68 65 20 70 61   ··P· +>4 ··The pa
0050  73 73 77 6f 72 64 20 66  6f 72 20 61 6c 6c 20 43   ssword f or all C
0060  69 73 63 6f 20 72 6f 75  74 65 72 73 20 69 73 20   isco rou ters is 
0070  43 69 24 28 6f                                     Ci$(o
```

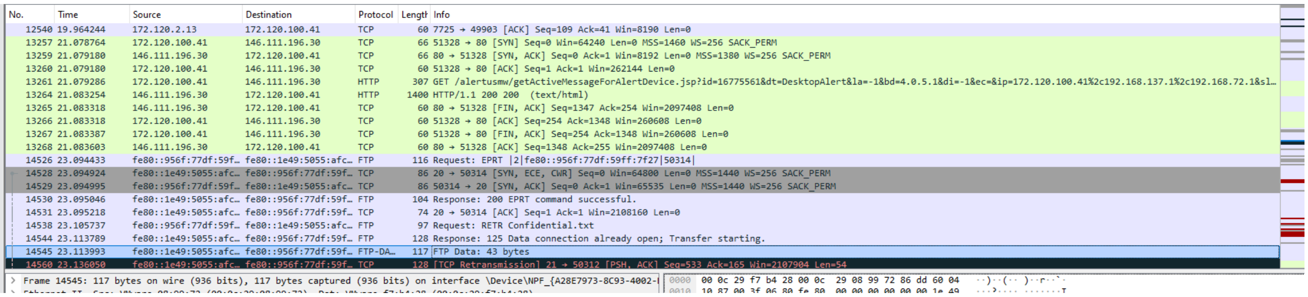
Bytes 74-116: Text item (text)

Packets: 23208 · Displayed: 152 (0.7%) · Dropped: 0 (0.0%)

Profile: Default

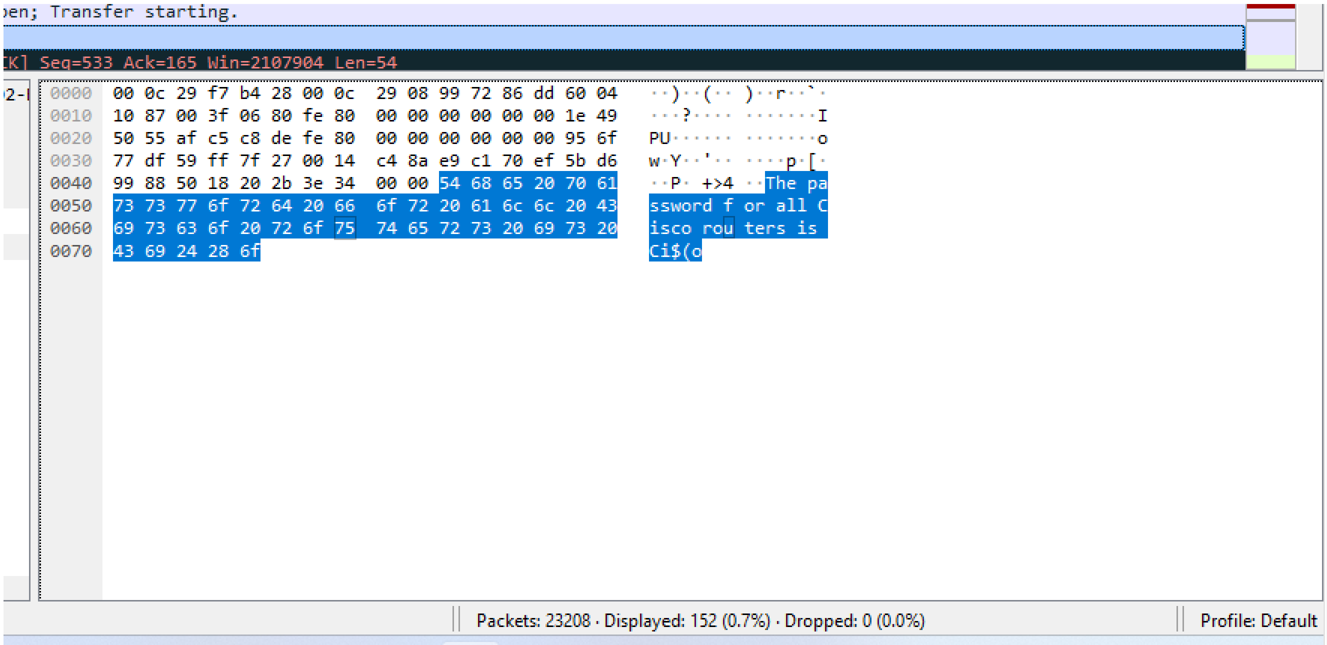
The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

To direct input to this VM, click inside or press Ctrl+G.



```
No.    Time      Source             Destination        Protocol Length Info
 12540 19.964244 172.120.2.13       172.120.100.41     TCP        60 7725 → 49903 [ACK] Seq=109 Ack=41 Win=8190 Len=0
 13257 21.078764 172.120.100.41     146.111.196.30     TCP        66 51328 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 13259 21.079180 146.111.196.30     172.120.100.41     TCP        66 80 → 51328 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM
 13260 21.079180 172.120.100.41     146.111.196.30     TCP        60 51328 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 13261 21.079286 172.120.100.41     146.111.196.30     HTTP      307 GET /alertusmw/getActiveMessageForAlertDevice.jsp?id=16775561&dt=DesktopAlert&la=-1&bd=4.0.5.1&di=-1&ec=&ip=172.120.100.41%2c192.168.137.1%2c192.168.72.1&sl…
 13264 21.083254 146.111.196.30     172.120.100.41     HTTP     1400 HTTP/1.1 200 200  (text/html)
 13265 21.083318 146.111.196.30     172.120.100.41     TCP        60 80 → 51328 [FIN, ACK] Seq=1347 Ack=254 Win=2097408 Len=0
 13266 21.083318 172.120.100.41     146.111.196.30     TCP        60 51328 → 80 [ACK] Seq=254 Ack=1348 Win=260608 Len=0
 13267 21.083387 172.120.100.41     146.111.196.30     TCP        60 51328 → 80 [FIN, ACK] Seq=254 Ack=1348 Win=260608 Len=0
 13268 21.083603 146.111.196.30     172.120.100.41     TCP        60 80 → 51328 [ACK] Seq=1348 Ack=255 Win=2097408 Len=0
 14526 23.094433 fe80::956f:77df:59f… fe80::1e49:5055:afc… FTP     116 Request: EPRT |2|fe80::956f:77df:59ff:7f27|50314|
 14528 23.094924 fe80::1e49:5055:afc… fe80::956f:77df:59f… TCP      86 20 → 50314 [SYN, ECE, CWR] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
 14529 23.094995 fe80::956f:77df:59f… fe80::1e49:5055:afc… TCP      86 50314 → 20 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
 14530 23.095046 fe80::1e49:5055:afc… fe80::956f:77df:59f… FTP     104 Response: 200 EPRT command successful.
 14531 23.095218 fe80::1e49:5055:afc… fe80::956f:77df:59f… TCP      74 20 → 50314 [ACK] Seq=1 Ack=1 Win=2108160 Len=0
 14538 23.105737 fe80::956f:77df:59f… fe80::1e49:5055:afc… FTP      97 Request: RETR Confidential.txt
 14544 23.113789 fe80::1e49:5055:afc… fe80::956f:77df:59f… FTP     128 Response: 125 Data connection already open; Transfer starting.
 14545 23.113993 fe80::1e49:5055:afc… fe80::956f:77df:59f… FTP-DA… 117 FTP Data: 43 bytes
 14560 23.136050 fe80::1e49:5055:afc… fe80::956f:77df:59f… TCP     128 [TCP Retransmission] 21 → 50312 [PSH, ACK] Seq=533 Ack=165 Win=2107904 Len=54
> Frame 14545: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface \Device\NPF_{A28E7973-8C93-4002-
0000  00 0c 29 f7 b4 28 00 0c  29 08 99 72 86 dd 60 04   ··)··(·· )··r··`·
```

Here is a closer look at the raw data of the packet and the ASCII translation. It clearly displays ‘The password for all Cisco routers is Ci$(o.’



```
pen; Transfer starting.
[K] Seq=533 Ack=165 Win=2107904 Len=54
2-|  0000  00 0c 29 f7 b4 28 00 0c  29 08 99 72 86 dd 60 04   ··)··(·· )··r··`·
     0010  10 87 00 3f 06 80 fe 80  00 00 00 00 00 00 1e 49   ···?···· ·······I
     0020  50 55 af c5 c8 de fe 80  00 00 00 00 00 00 95 6f   PU······ ·······o
     0030  77 df 59 ff 7f 27 00 14  c4 8a e9 c1 70 ef 5b d6   w·Y··'·· ····p·[·
     0040  99 88 50 18 20 2b 3e 34  00 00 54 68 65 20 70 61   ··P· +>4 ··The pa
     0050  73 73 77 6f 72 64 20 66  6f 72 20 61 6c 6c 20 43   ssword f or all C
     0060  69 73 63 6f 20 72 6f 75  74 65 72 73 20 69 73 20   isco rou ters is 
     0070  43 69 24 28 6f                                     Ci$(o
```

Packets: 23208 · Displayed: 152 (0.7%) · Dropped: 0 (0.0%)   Profile: Default

Review Questions

1. You have been asked to install an FTP server on the company’s internal network to be used only by an employee committee that will be working on an advertising campaign to encourage employees to donate to a charity. Which of the following would be the most secure configuration of the FTP server?

a. Require users to authenticate using their domain account.

b. Require users to authenticate using a local account.

c. Require users to use anonymous authentication.

d. Allow users to share a single username and password.

Answer: a.) Require users to authenticate using their domain account.

2. In this lab, what is listed in the Info column of the frame in which the content of the file Confidential.txt is visible?

a. FTP Data

b. Response

c. Request

d. get-request

Answer: a.) FTP Data

3. Which of the following statements is the most accurate description of the communication between Client and the FTP server in this lab?

a. Client initiated the connection by sending to the FTP server a packet with TCP flags SYN and ACK set.

b. Client initiated the connection by sending to the FTP server a packet with TCP flag ACK set.

c. Client initiated the connection by sending to the FTP server a packet with TCP flag SYN set.

d. The FTP server initiated the connection by sending a packet to Client with TCP flag SYN set.

Answer: c.) Client initiated the connection by sending to the FTP server a packet with TCP flag SYN set

4. Which of the following statements is the most accurate description of the communication between the Client system and the FTP server in this lab?

a. Once the FTP server was contacted by Client, it sent a packet with the TCP flags SYN and ACK set.

b. Once the FTP server was contacted by Client, it sent a packet with the TCP flag ACK set.
c. Once the FTP server was contacted by Client, it sent a packet with the TCP flag SYN set.
d. The FTP server was not first contacted by Client; it advertised its FTP service, and Seven responded

Answer: a.) Once the FTP server was contacted by Client, it sent a packet with the TCP flags SYN and ACK set.

5. Which of the following statements is the most accurate description of the communication between the Client system and the FTP server in this lab?

a. The teardown of the TCP session began when the FTP server sent a packet to Client with the TCP flag FIN set.

b. The teardown of the TCP session began when Client sent a FIN packet to the FTP server.
c. The teardown of the TCP session began when the FTP server sent a packet to Client with the TCP flags FIN and ACK set.

d. The teardown of the TCP session began when Client sent a packet to the FTP server with the TCP flags FIN and ACK set

Answer: b.) The teardown of the TCP session began when Client sent a FIN packet to the FTP server.