

Compsci 314 assignment 2

A. The FTP Protocol

1. What well-known port number is used? 21
2. What usercode and password are used to log in to FTP?

Usercode: anonymous, and there is no password

No.	Time	Source	Destination	Protocol	Length	SEQ/ACK analysis	Info
9	4.872010	192.168.1.1	192.168.6.1	FTP	86		Response: 220 (vsFTPd 2.3.5)
11	5.002094	192.168.1.1	192.168.1.1	FTP	82		Request: USER anonymous
13	5.002186	192.168.1.1	192.168.6.1	FTP	100		Response: 331 Please specify the p
15	5.132116	192.168.6.1	192.168.1.1	FTP	73		Request: PASS
17	5.224232	192.168.1.1	192.168.6.1	FTP	89		Response: 230 Login successful.
19	5.253697	192.168.6.1	192.168.1.1	FTP	72		Request: SYST
21	5.253770	192.168.1.1	192.168.6.1	FTP	85		Response: 215 UNIX Type: L8
23	5.384107	192.168.6.1	192.168.1.1	FTP	74		Request: TYPE I
24	5.384188	192.168.1.1	192.168.6.1	FTP	97		Response: 200 Switching to Binary
26	5.413636	192.168.6.1	192.168.1.1	FTP	91		Request: PORT 192,168,6,1,193,85
27	5.413782	192.168.1.1	192.168.6.1	FTP	117		Response: 200 PORT command success
28	5.443198	192.168.6.1	192.168.1.1	FTP	83		Request: RETR output.dat
32	5.473000	192.168.1.1	192.168.6.1	FTP	140		Response: 150 Opening BINARY mode
123...	24.644528	192.168.1.1	192.168.6.1	FTP	90		Response: 226 Transfer complete.
123...	24.774640	192.168.6.1	192.168.1.1	FTP	72		Request: QUIT
123...	24.774717	192.168.1.1	192.168.6.1	FTP	80		Response: 221 Goodbye.

Transmission Control Protocol, Src Port: 47715, Dst Port: 21, Seq: 3503516262, Ack: 2001184331, Len: 17

Source Port: 47715
Destination Port: 21
[Stream index: 1]
[TCP Segment Len: 17]
Sequence number: 3503516262
[Next sequence number: 3503516279]
Acknowledgment number: 2001184331
1000 ... = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window size value: 3
[Calculated window size: 49152]
[Window size scaling factor: 16384]
0030 00 03 28 90 00 00 01 01 08 0a 56 b1 ac ce 26 f6 ..(.....V...&
0040 84 74 52 45 54 52 20 6f 75 74 70 75 74 2e 64 61 .tRETR o utput.da

The scaled window size (if scaling has been used) (tcp.window.size), 2 bytes

Packets: 12326 · Displayed: 16 (0.1%) · Load time: 0:0.198

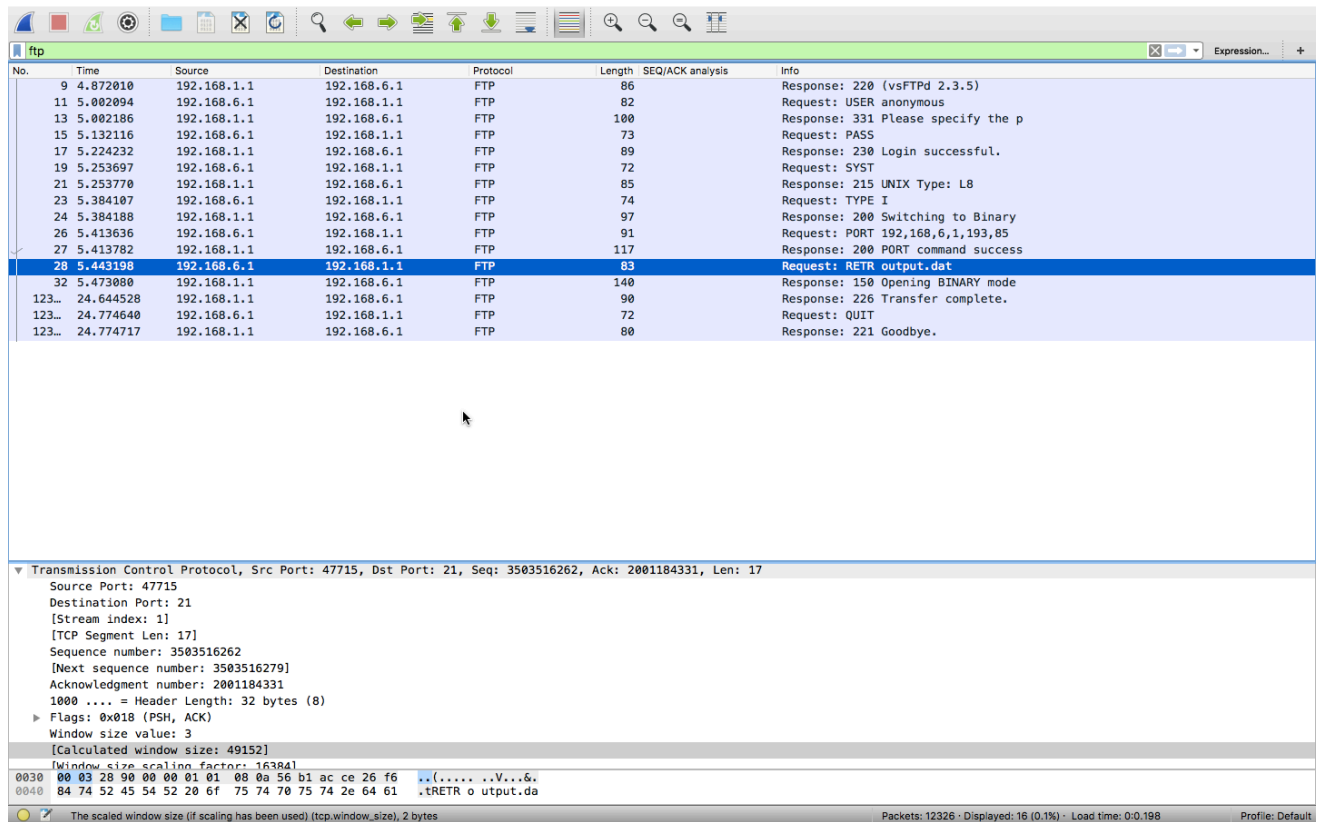
Profile: Default

3. Why is FTP mode switched to binary?

Binary transmits raw bytes of the file being transferred. Hence the file could be transferred in its exact original form

4. What FTP command is used to download the test file?

RETR output.dat



No.	Time	Source	Destination	Protocol	Length	SEQ/ACK analysis	Info
9	4.872818	192.168.1.1	192.168.6.1	FTP	86		Response: 220 (vsFTPd 2.3.5)
11	5.002094	192.168.6.1	192.168.1.1	FTP	82		Request: USER anonymous
13	5.002186	192.168.1.1	192.168.6.1	FTP	100		Response: 331 Please specify the p
15	5.132116	192.168.6.1	192.168.1.1	FTP	73		Request: PASS
17	5.224232	192.168.1.1	192.168.6.1	FTP	89		Response: 230 Login successful.
19	5.253697	192.168.6.1	192.168.1.1	FTP	72		Request: SYST
21	5.253770	192.168.1.1	192.168.6.1	FTP	85		Response: 215 UNIX Type: L8
23	5.384107	192.168.6.1	192.168.1.1	FTP	74		Request: TYPE I
24	5.384188	192.168.1.1	192.168.6.1	FTP	97		Response: 200 Switching to Binary
26	5.413636	192.168.6.1	192.168.1.1	FTP	91		Request: PORT 192,168,6,1,193,85
27	5.413782	192.168.1.1	192.168.6.1	FTP	117		Response: 200 PORT command success
28	5.443198	192.168.6.1	192.168.1.1	FTP	83		Request: RETR output.dat
32	5.473888	192.168.1.1	192.168.6.1	FTP	140		Response: 150 Opening BINARY mode
123...	24.644528	192.168.1.1	192.168.6.1	FTP	90		Response: 226 Transfer complete.
123...	24.774640	192.168.6.1	192.168.1.1	FTP	72		Request: QUIT
123...	24.774717	192.168.1.1	192.168.6.1	FTP	80		Response: 221 Goodbye.

Transmission Control Protocol, Src Port: 47715, Dst Port: 21, Seq: 3503516262, Ack: 2001184331, Len: 17	
Source Port:	47715
Destination Port:	21
[Stream index: 1]	
[TCP Segment Len: 17]	
Sequence number:	3503516262
[Next sequence number: 3503516279]	
Acknowledgment number:	2001184331
1000 = Header Length: 32 bytes (8)	
Flags: 0x018 (PSH, ACK)	
Window size value:	3
[Calculated window size: 49152]	
Window size scaling factor: 163841	
0030 00 03 28 90 00 00 01 01 08 0a 56 b1 ac ce 26 f6	..(.....V...&
0040 84 74 52 45 54 52 20 6f 75 74 70 75 74 2e 64 61	.tRETR o utput.da

The scaled window size (if scaling has been used) (tcp.window.size), 2 bytes

Packets: 12326 · Displayed: 16 (0.1%) · Load time: 0:0.198 Profile: Default

B: Data bytes transmitted by TCP [8 marks]

Set a Wireshark filter to look at all packets sent through the ftp-data flow:

5a. What well-known port number is used for FTP data? [1 mark]

20

No.	Time	Source	Destination	Protocol	Length	SEQ/ACK analysis	Info
33	5.473100	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
34	5.473103	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
35	5.473106	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
36	5.473109	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
37	5.473110	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
38	5.473113	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
39	5.473115	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
40	5.473116	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
41	5.473118	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
42	5.473120	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
44	5.502391	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
46	5.502399	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
47	5.502402	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
48	5.502403	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
49	5.502405	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
50	5.502406	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
51	5.502408	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
52	5.502409	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
53	5.502410	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
54	5.502412	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
56	5.531671	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
57	5.531674	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
58	5.531675	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
59	5.531677	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
60	5.531678	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
61	5.531679	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
62	5.531682	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
63	5.531683	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
64	5.531684	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
65	5.531685	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.6.1							
Transmission Control Protocol, Src Port: 20, Dst Port: 49493, Seq: 2666475027, Ack: 335683545, Len: 1448							
Source Port: 20							
Destination Port: 49493							
[Stream index: 2]							
[TCP Segment Len: 1448]							
Sequence number: 2666475027							
[Next sequence number: 2666476475]							
Acknowledgment number: 335683545							
1000 = Header Length: 32 bytes (8)							
Flags: 0x010 (ACK)							
Window size value: 9							
[Calculated window size: 18432]							
0030	00 09	0e 21 00 00 01 01	08 0a 26 f6 84 83 56 b1&...V.	
0040	ac d5 00 00 00 00 00	00 00 00 00 00 00 00	00 00 00 00 00 00 00	

5b. What are the packet and sequence numbers for the file transfer's opening SYN? [2 marks]

Packet number 29, sequence number: 2666475026

No.	Time	Source	Destination	Protocol	Length	SEQ/ACK analysis	Info
3	0.291282	QuantaCo_6d56a1af	Spanning-tree-(for...	STP	119		HST. Root = 32768/0/04:7d:7b:6d:6a:af Cost = 0 Port = 0x8034[Packet
4	2.291079	QuantaCo_6d56a1af	Spanning-tree-(for...	STP	119		HST. Root = 32768/0/04:7d:7b:6d:6a:af Cost = 0 Port = 0x8034[Packet
5	4.291276	QuantaCo_6d56a1af	Spanning-tree-(for...	STP	119		HST. Root = 32768/0/04:7d:7b:6d:6a:af Cost = 0 Port = 0x8034[Packet
6	4.840637	192.168.6.1	192.168.1.1	TCP	74		47715 → 21 [SYN] Seq=3503516199 Win=42340 Len=0 MSS=1460 SACK_PERM=1
7	4.840673	192.168.1.1	192.168.6.1	TCP	74		21 → 47715 [SYN, ACK] Seq=2001184152 Ack=3503516200 Win=17896 Len=0 M
8	4.870088	192.168.6.1	192.168.1.1	TCP	66		47715 → 21 [ACK] Seq=3503516200 Ack=2001184153 Win=49152 Len=0 TSval=
9	4.872010	192.168.1.1	192.168.6.1	FTP	86		Response: 220 (vsFTPd 2.3.5)
10	4.901437	192.168.6.1	192.168.1.1	TCP	66		47715 → 21 [ACK] Seq=3503516200 Ack=2001184173 Win=49152 Len=0 TSval=
11	5.002094	192.168.6.1	192.168.1.1	FTP	82		Request: USER anonymous
12	5.002123	192.168.1.1	192.168.6.1	TCP	66		21 → 47715 [ACK] Seq=2001184173 Ack=3503516216 Win=18432 Len=0 TSval=
13	5.002186	192.168.1.1	192.168.6.1	FTP	100		Response: 331 Please specify the p
14	5.031523	192.168.6.1	192.168.1.1	TCP	66		47715 → 21 [ACK] Seq=3503516216 Ack=2001184207 Win=49152 Len=0 TSval=
15	5.132116	192.168.6.1	192.168.1.1	FTP	73		Request: PASS
16	5.170442	192.168.1.1	192.168.6.1	TCP	66		21 → 47715 [ACK] Seq=2001184207 Ack=3503516223 Win=18432 Len=0 TSval=
17	5.224232	192.168.1.1	192.168.6.1	FTP	89		Response: 230 Login successful.
18	5.253665	192.168.6.1	192.168.1.1	TCP	66		47715 → 21 [ACK] Seq=3503516229 Ack=2001184230 Win=49152 Len=0 TSval=
19	5.253697	192.168.6.1	192.168.1.1	FTP	72		Request: SYST
20	5.253702	192.168.1.1	192.168.6.1	TCP	66		21 → 47715 [ACK] Seq=2001184230 Ack=3503516229 Win=18432 Len=0 TSval=
21	5.327770	192.168.1.1	192.168.6.1	FTP	85		Response: 215 UNIX Type: L8
22	5.327267	192.168.6.1	192.168.1.1	TCP	66		47715 → 21 [ACK] Seq=3503516229 Ack=2001184249 Win=49152 Len=0 TSval=
23	5.384107	192.168.6.1	192.168.1.1	FTP	74		Request: TYPE I
24	5.384188	192.168.1.1	192.168.6.1	FTP	97		Response: 200 Switching to Binary
25	5.413607	192.168.6.1	192.168.1.1	TCP	66		47715 → 21 [ACK] Seq=3503516237 Ack=2001184280 Win=49152 Len=0 TSval=
26	5.413636	192.168.6.1	192.168.1.1	FTP	91		Request: PORT 192,168,6,1,193,85
27	5.413782	192.168.1.1	192.168.6.1	FTP	117		Response: 200 PORT command success
28	5.443198	192.168.6.1	192.168.1.1	FTP	83		Request: RETR output.dat
29	5.443519	192.168.1.1	192.168.6.1	TCP	74		20 → 49493 [SYN] Seq=2666475026 Win=17920 Len=0 MSS=8960 SACK_PERM=1
30	5.472942	192.168.6.1	192.168.1.1	TCP	74		49493 → 20 [SYN, ACK] Seq=335683544 Ack=2666475027 Win=43440 Len=0 MS
31	5.472977	192.168.1.1	192.168.6.1	TCP	66		20 → 49493 [ACK] Seq=2666475027 Ack=335683545 Win=18432 Len=0 TSval=6
Frame 29: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)							
Ethernet II, Src: Broadcom_e8:31:c0 (00:10:18:e8:31:c0), Dst: IntelCor_2f:5b:c0 (a0:36:9f:2f:5b:c0)							
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.6.1							
Transmission Control Protocol, Src Port: 20, Dst Port: 49493, Seq: 2666475026, Len: 0							
Source Port: 20							
Destination Port: 49493							
[Stream index: 2]							
[TCP Segment Len: 0]							
Sequence number: 2666475026							
Acknowledgment number: 0							
1010 = Header Length: 40 bytes (10)							
Flags: 0x002 (SYN)							
Window size value: 17920							
0020	06 01 00 14 c1 55 9e ef	2e 12 00 00 00 00 00 02U..	
0030	46 00 88 81 00 00 02 04	23 00 04 02 08 0a 26 f6	F.....	#.....6.	

5c. What are the packet and sequence numbers for the ACK to the file transfer's closing FIN (i.e. the FIN from the FTP data sender)? [2 marks]

Packet number: 12316, sequence number: 335683545

No.	Time	Source	Destination	Protocol	Length	SEQ/ACK analysis	Info
12297	24.582696	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12298	24.582698	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12299	24.582699	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12300	24.582700	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12301	24.612018	192.168.6.1	192.168.1.1	TCP	66		49493 → 20 [ACK] Seq=335683545 Ack=2682171163 Win=114688 Le
12302	24.612052	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12303	24.612055	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12304	24.612057	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12305	24.612058	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12306	24.612059	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12307	24.612061	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12308	24.612063	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12309	24.612065	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12310	24.612066	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12311	24.612067	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12312	24.612068	192.168.1.1	192.168.6.1	FTP-DATA	1514		FTP Data: 1448 bytes
12313	24.612070	192.168.1.1	192.168.6.1	FTP-DATA	714		FTP Data: 648 bytes
12314	24.612072	192.168.6.1	192.168.1.1	TCP	66		49493 → 20 [ACK] Seq=335683545 Ack=2682187091 Win=114688 Le
12315	24.641413	192.168.6.1	192.168.1.1	TCP	66		49493 → 20 [ACK] Seq=335683545 Ack=2682203019 Win=114688 Le
12316	24.644369	192.168.6.1	192.168.1.1	TCP	66		49493 → 20 [FIN, ACK] Seq=335683545 Ack=2682203668 Win=1146
12317	24.644402	192.168.1.1	192.168.6.1	TCP	66		20 → 49493 [ACK] Seq=2682203668 Ack=335683546 Win=18432 Len
12318	24.644528	192.168.1.1	192.168.6.1	FTP	90		Response: 226 Transfer complete.
12319	24.673904	192.168.6.1	192.168.1.1	TCP	66		47715 → 21 [ACK] Seq=3503516279 Ack=2001184429 Win=49152 Le
12320	24.774640	192.168.6.1	192.168.1.1	FTP	72		Request: QUIT
12321	24.774717	192.168.1.1	192.168.6.1	FTP	80		Response: 221 Goodbye.
12322	24.774725	192.168.1.1	192.168.6.1	TCP	66		21 → 47715 [FIN, ACK] Seq=2001184443 Ack=3503516285 Win=184
12323	24.804159	192.168.6.1	192.168.1.1	TCP	66		47715 → 21 [ACK] Seq=3503516285 Ack=2001184443 Win=49152 Le
12324	24.804317	192.168.6.1	192.168.1.1	TCP	66		47715 → 21 [FIN, ACK] Seq=3503516285 Ack=2001184444 Win=491
12325	24.804349	192.168.1.1	192.168.6.1	TCP	66		21 → 47715 [ACK] Seq=2001184444 Ack=3503516286 Win=18432 Le
12326	24.854792	192.168.6.1	192.168.1.1	SSH	102		Encrypted packet (len=36) [Packet size limited during captur

Frame 12316: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Ethernet II, Src: IntelCor_2f:5b:c0 (a0:36:9f:2f:5b:c0), Dst: Broadcom_e8:31:c0 (08:10:18:e8:31:c0)
 Internet Protocol Version 4, Src: 192.168.6.1, Dst: 192.168.1.1
 Transmission Control Protocol, Src Port: 49493, Dst Port: 20, Seq: 335683545, Ack: 2682203668, Len: 0
 Source Port: 49493
 Destination Port: 20
 [Stream index: 2]
 [TCP Segment Len: 0]
 Sequence number: 335683545
 Acknowledgment number: 2682203668
 1000 = Header Length: 32 bytes (8)
 Flags: 0x011 (FIN, ACK)
 Window size value: 7

5d. How many actual data bytes were sent by the file transfer? [2 marks]

Ack – seq

$$= (2682203668 - 2666475026) - 2 = 15728640 \text{ bytes}$$

5e. What was the size of the transferred file? [1 marks]

15728640 bytes

C: Packets retransmitted by TCP [7 marks]

Set a Wireshark filter to look at packets with TCP source port FTP-DATA.

6a. How many packets are displayed using this filter? [1 mark] Hint: Try Wireshark's Statistics | Summary Set a Wireshark filter to look at packets with TCP source port FTP-DATA that were retransmitted.

10921

Details

File

Name: /Users/rahulissar/Downloads/Wireshark314-588382864.pcap
 Length: 1273 kB
 Format: Wireshark/tcpdump/... - pcap
 Encapsulation: Ethernet
 Snapshot length: 90

Time

First packet: 2015-07-10 14:28:03
 Last packet: 2015-07-10 14:28:28
 Elapsed: 00:00:24

Capture

Hardware: Unknown
 OS: Unknown
 Application: Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Unknown	Unknown	Unknown	Ethernet	90 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	12326	10921 (88.6%)	—
Time span, s	24.855	19.201	—
Average pps	495.9	568.8	—
Average packet size, B	1347.5	1512.5	—
Bytes	16610372	16516042 (99.4%)	0
Average bytes/s	668 k	860 k	—
Average bits/s	5346 k	6881 k	—

Capture file comments

Help Refresh Copy To Clipboard Close Save Comments

6b. How many retransmitted packets does Wireshark display? [1 mark]

26.

Details

File

Name: /Users/rahulissar/Downloads/Wireshark314-588382864.pcap
 Length: 1273 kB
 Format: Wireshark/tcpdump/... - pcap
 Encapsulation: Ethernet
 Snapshot length: 90

Time

First packet: 2015-07-10 14:28:03
 Last packet: 2015-07-10 14:28:28
 Elapsed: 00:00:24

Capture

Hardware: Unknown
 OS: Unknown
 Application: Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Unknown	Unknown	Unknown	Ethernet	90 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	12326	26 (0.2%)	—
Time span, s	24.855	12.821	—
Average pps	495.9	2.0	—
Average packet size, B	1347.5	1514.5	—
Bytes	16610372	39364 (0.2%)	0
Average bytes/s	668 k	3070	—
Average bits/s	5346 k	24 k	—

Capture file comments

Help Refresh Copy To Clipboard Close Save Comments

6c. How does Wireshark recognise a packet retransmission? Hint: Use a search engine to find out about this. [3 marks]

Regardless of the sequence and acknowledge numbers, dropping packets are not possible in Wireshark. Wireshark shows any packet which is captured. It does not consider using checksum or IP id in recognising a packet transmission. It recognises a packet retransmission with a comparison that shows the difference between the sequence numbers and the expected sequence number from the last packet of the conversation into the same direction. The packets are placed in order.

6d. What is the observed packet loss percentage for this trace file? [2 marks]

$(10921 - 26) / 10921 * 100 = 99.76\%$. This is the successfully transmitted packets. Therefore, the packet loss is $100 - 99.76 = 0.24\%$

D: Protocol overhead [8 marks]

Set a Wireshark filter to look at packets with TCP source port FTP-DATA.

7a. In question 5e you determined the number of data bytes transferred. How many bytes were actually sent during that transfer? [2 marks]

16516042 bytes

7b. What was the percentage of “protocol overhead” for that file transfer? [2 marks]

$16516042 - 15728640 = 787402$, this equals the total overhead. Therefore, $(787402 / 16516042) * 100 = 4.77\%$ (2dp) this gives the percentage protocol overhead for the file transfer.

7c. What parts of the packets contributed to that overhead? Note: your answer to this question must be a proper English sentence. An answer that is not a sentence will score zero marks. Hint: “overhead” means everything except the actual data. [4 marks]

Overhead is everything except the actual data. Frame length is 1514 bytes whereas actual data is 1448 bytes ($1514 - 1448 = 66$). The 66 bytes is therefore the overhead. 32 bytes from these 66 bytes is from the TCP header length, 20 bytes from the IP header length and the rest of it is from the Ethernet layer (resent packets).

E: Round-trip time [4 marks]

8. What is the most common Round-Trip Time (RTT) for packets from sender and receiver and back? [4 marks] Hint: Try Wireshark's Statistics | TCPStreamGraph | Round Trip Time Graph You can drag the mouse to form a rectangle over any section of interest on that graph.

According to the Round-Trip time graphs shown below, the most common RTT for packets is 29.50 ms.

