Sharkfest 2015 Packet Challenge

All challenge trace files can be found on the blue USB stick available at the Reef in the Grand Hall. Fill out the answer sheet and **turn it in at the Wireshark University table in the Reef by 9pm on Wednesday, June 24th**. Good luck!

PAY ME NOW

Trace File: dnsing.pcapng

1. What IP address(es) are resolved for www.paypal.com?
2. What is the largest DNS TTL value seen in the trace file?
3. Which DNS response transaction ID contained the largest number of Answer RRs?
4. What is the largest DNS response time seen in this trace file?
5. What company distributes many of PayPal's web pages?

GO GO SPEED RACER

Trace File: http-gogo.pcapng

1. What is the HTTP response time for the GET / request in packet 4? *[Fixed: had "packet 3" in 1st draft]*
2. How many packets have the SYN bit set on in this trace file?
3. What is the name of the largest HTTP object downloaded to this client?
4. How long did it take to download the browser tab icon, favicon.ico (include TCP connection setup/teardown)?
5. Frame 131 is a spurious retransmission. Which previous frame caused this to be marked "spurious"?

FTP ME, BABY

Trace File: tcp-bigftp.pcapng

1. What TCP options are supported by both client and server in this trace file?
2. What Window Size(s) are advertised in each Window Update packet?
3. What operating system must be supported to use the downloaded file?
4. How much is the largest delay preceding a Window Update packet?
5. Why does Wireshark indicate the Window Scaling factor is -1 in some of the packets?

WHATS UP?

Trace File: whatsup.pcapng

1. Why did a device send an ICMP Type 3/Code 4 packet in this trace file?
2. What was the MTU size before the drop in size?
3. What is the IP address of the router that can't forward larger sized frames?
4. What is the IP address of the host that adjusted its MTU?
5. How many more frames would be required to send a 6,000-byte file using the smaller MTU size than using the larger MTU size?

PRINTING PAIN!

Trace File: printpain.pcapng

1. What is the make and model of the target printer?
2. What file is being printed?
3. What is the maximum TCP receive buffer size advertised by the printer?
4. What three characteristics make frame 179 a "window zero probe?"
5. What is the largest delay between a Window Full indication and a Window Update?

SHARKFEST 2015 PACKET CHALLENGE ANSWER SHEET

Fill out this answer sheet and turn it in at the **Wireshark University table in the Reef by 9pm Wednesday**. Good luck!

NAME: (Required) _____

PAY ME NOW Trace File: dnsing.pcapng

1. _____
2. _____
3. _____
4. _____
5. _____

Comments:

GO GO SPEED RACER Trace File: http-gogo.pcapng

1. _____
2. _____
3. _____
4. _____
5. _____

Comments:

FTP ME, BABY Trace File: tcp-bigftp.pcapng

1. _____
2. _____
3. _____
4. _____
5. _____

Comments:

WHATS UP? Trace File: whatsup.pcapng

1. _____
2. _____
3. _____
4. _____
5. _____

Comments:

PRINTING PAIN! Trace File: printpain.pcapng

1. _____
2. _____
3. _____
4. _____
5. _____

Comments:

SHARKFEST 2015 PACKET CHALLENGE ANSWERS

PAY ME NOW Trace File: dnsing.pcapng

6. 23.13.82.234 and 23.196.228.157
7. 7,196
8. 0x9AB9
9. 0.088701 seconds
10. Akamai

Comments:

GO GO SPEED RACER Trace File: http-gogo.pcapng

6. 204 ms (includes iRTT)
7. 101 packets
8. OpenSans-Semibold.tff
9. 146 ms
10. frame 127

Comments:

#1: The GET / request is in packet 4, not 3, as many of you noted.

#5: Sender's SEQ# < receiver's last ACK #

FTP ME, BABY Trace File: tcp-bigftp.pcapng

6. MSS, Window Scaling, SACK, TCP Timestamps
7. 66608
8. Win32
9. 0.006486000 seconds
10. Window Scaling factor is unknown; no handshake seen

Comments:

WHATS UP? Trace File: whatsup.pcapng

6. Needs to fragment packet 18 which had DF bit set
7. 1500
8. Last hop before 108.160.172.65
9. Same as system named in #3 above
10. 0 extra packets

Comments:

#3: IP address appears anonymized in this trace file.

#5: 6000/1460 = 4112 = 5 packets

PRINTING PAIN! Trace File: printpain.pcapng

6. HP Officejet 6500 E710n-z
7. Installation.pdf
8. 17,520
9. (1) sequence number is the next expected one,
   (2) the window in the other direction is 0, and
   (3) the segment is exactly 1 byte
10. 25.682732 seconds

Comments:

#4: As stated in *packet-tcp.c* dissector file.