SHARKFEST 2014 PACKET CHALLENGE

All challenge trace files can be downloaded from **bit.ly/getchallenged**. Fill out the answer sheet and turn it in at the Wireshark University table by noon on Wednesday. The table is located at the Angelico Hall entrance on Tuesday and Sharkfest Lounge, Creekside Room on Wednesday. Good luck!

TROUBLE TICKET

Trace File: TroubleTicket.pcapng (contributed by Jasper Bongertz)

1. What is the application protocol used?
2. Are all GET requests asking for the same URI?
3. Based on where this trace was taken, do the packets get lost closer to the client or closer to the server?
4. This trace was taken inside the infrastructure. What is the Initial Round Trip Time of the connection?
5. Who owns the server?

BIG FTP

Trace File: BigFTP.pcapng

1. On which host was Wireshark running when this trace file was taken?
2. If this network does not support jumbo frames, why do we see 16,450 byte packets in the trace file?
3. What data packet is being acknowledged in frames 314-321?
4. Why can't you view the reassembled .jpg file that is uploaded in this trace file?
5. What is the true purpose of kidsatbeach.jpg?

PAID TO PLAY

Trace File: AllPlayNoWork.pcapng

1. For what server did the client try to resolve an IPv6 address?
2. What operating system do you think the client is running?
3. What is the color of the mermaid's hair?
4. What classic games did the user learn about? (Name all of them.)
5. Which Angry Birds edition did the user learn about?

BROWSING BUDDY

Trace File: BrowsingAlong.pcapng

1. What version of dumpcap was used to capture this trace file?
2. Which frame contains the 200 OK response to the GET request for /scripts/AC_OETags.js?
3. In what kind of "bar" is the client interested?
4. Which TCP stream experienced the most Retransmissions?
5. Frame 8500 is a retransmission triggered by duplicate ACKs. Why isn't it marked as a **Fast** Retransmission?

OUCH!

Trace File: AskSnopes.pcapng

1. What web server software is used by www.snopes.com?
2. About what cell phone problem is the client concerned?
3. According to Zillow, what instrument will Ryan learn to play?
4. How many web servers are running Apache?
5. What hosts (IP addresses) think that jokes are more entertaining when they are explained?

SHARKFEST 2014 PACKET CHALLENGE ANSWER SHEET

Fill out this answer sheet and turn it in at the Wireshark University table by noon on Wednesday. The table is located at the Angelico Hall entrance on Tuesday and Sharkfest Lounge, Creekside Room on Wednesday. Good luck!

TROUBLE TICKET Trace File: TroubleTicket.pcapng (contributed by Jasper Bongertz)

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

Comments:

BIG FTP Trace File: BigFTP.pcapng

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

Comments:

PAID TO PLAY Trace File: AllPlayNoWork.pcapng

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

Comments:

BROWSING BUDDY Trace File: BrowsingAlong.pcapng

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

Comments:

OUCH! Trace File: AskSnopes.pcapng

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

Comments: