Sharkfest 2016 (US/Europe) Packet Challenge

Laura Chappell created this Packet Challenge for SharkFest 2016 (US and Europe). Questions? info@wiresharktraining.com.

THE CEILING IS THE LIMIT (Use Wireshark v2.x for all challenges)

Trace File: sf2016-a.pcapng

1. What IP addresses are used by Laura's iPad?
2. What is the IPv4 address of the host that is attempting to discover a Cannon printer/scanner?
3. Which DNS response transaction IDs contained the largest number of Answer RRs?
4. What is the largest DNS response time seen in this trace file?
5. What website is the user browsing for ceiling fans?

BINGING (Use Wireshark v2.x for all challenges)

Trace File: sf2016-b.pcapng

1. How many cipher suites are offered to the www.bing.com server?
2. Which cipher suite did the www.bing.com server select to use for the connection?
3. What host name query is generating DNS errors?
4. Who owns the iPad detected in this trace file?
5. What server is the client connecting to in TCP stream 8?

HOT, HOT, HOT (Use Wireshark v2.x for all challenges)

Trace File: sf2016-c.pcapng

1. How many days are covered by the Money Back Guarantee for HotAlarmClock?
2. Which content delivery network (CDN) is used by Microsoft?
3. What caused the DNS client to send an ICMP message to a DNS response? [Be specific.]
4. How many complete TCP handshakes are seen in this trace file?
5. What is the host name of the system that offers the largest TCP window scale multiplier?

TOUCH UP (Use Wireshark v2.x for all challenges)

Trace File: sf2016-d.pcapng

1. Who owns an iPod Touch?
2. Why did Wireshark mark Frame 11 as a Spurious Retransmission?
3. How many Gratuitous ARPs are in this trace file?
4. What is getting "hairy"?
5. Why was a user redirected when connecting to www.wireshark.org?

REMEMBER WHAT YOU TOLD ME… YOU ARE AWESOME! (Use Wireshark v2.x for all challenges)

Trace File: sf2016-e.pcapng

1. Who or what is "awesome"?
2. What is the IP address of the DHCP Relay Agent?
3. How many TCP FIN packets are marked as spurious retransmissions?
4. What manufacturer's products are looking for 169.254.255.255?
5. How many IP hosts advertise a window scaling factor of 128?

SHARKFEST 2016 (US/Europe) PACKET CHALLENGE ANSWER SHEET

Laura Chappell created this Packet Challenge for SharkFest 2016 (US and Europe). Questions? info@wiresharktraining.com.

THE CEILING IS THE LIMIT Trace File: sf2016-a.pcapng

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

Comments:

BINGING Trace File: sf2016-b.pcapng

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

Comments:

HOT, HOT, HOT Trace File: sf2016-c.pcapng

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

Comments:

TOUCH UP Trace File: sf2016-d.pcapng

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

Comments:

REMEMBER WHAT YOU TOLD ME… YOU ARE AWESOME! Trace File: sf2016-e.pcapng

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

Comments:

SHARKFEST EUROPE 2016 PACKET CHALLENGE ANSWERS

Laura Chappell created this Packet Challenge for SharkFest 2016 (US and Europe). Questions? info@wiresharktraining.com.

THE CEILING IS THE LIMIT Trace File: sf2016-a.pcapng

1. 0.0.0.0, 192.168.1.66, 2602:301:7786:9aa0:452:a774:5191:841a, ::, fe80::8f5:de86:f16e:a500
2. 192.168.1.70
3. 0x99c9, 0x5813
4. 1.104968
5. www.wayfair.com

Comments: 1) 5 addresses used by the iPad (filter on the iPad's source MAC address)

BINGING Trace File: sf2016-b.pcapng

1. 26
2. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
3. wpad.attlocal.net
4. Pat
5. acrobat.com (files.acrobat.com)

Comments:

HOT, HOT, HOT Trace File: sf2016-c.pcapng

1. 30 days
2. Akamai
3. got DNS response already in frame 1171; socket closed
4. 23
5. aus5.mozilla.org (from trace file)

Comments: 1) This answer is in a reassembled graphic image. 2) Yes, Microsoft uses Akamai – just do a filter for "frame contains "Microsoft" and you'll see the CNAME info in DNS responses.

TOUCH UP Trace File: sf2016-d.pcapng

1. Jason
2. Seq 132 already ACKed in frame 10
3. 12
4. Sharks series blues getting hairy
5. Redirected to https for a secure communication

Comments:

REMEMBER WHAT YOU TOLD ME… YOU ARE AWESOME! Trace File: sf2016-e.pcapng

1. Tejas (Texas)
2. 172.19.134.2
3. 447
4. Apple (key: "looking for" – in an ARP)
5. 88

Comments: 5) This caught a lot of people – if you filter on the Window Scaling Factor of 128 and then open the Endpoints window, watch for 172.19.131.144 – lots of folks put 89 in this answer because of that one host.