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.