

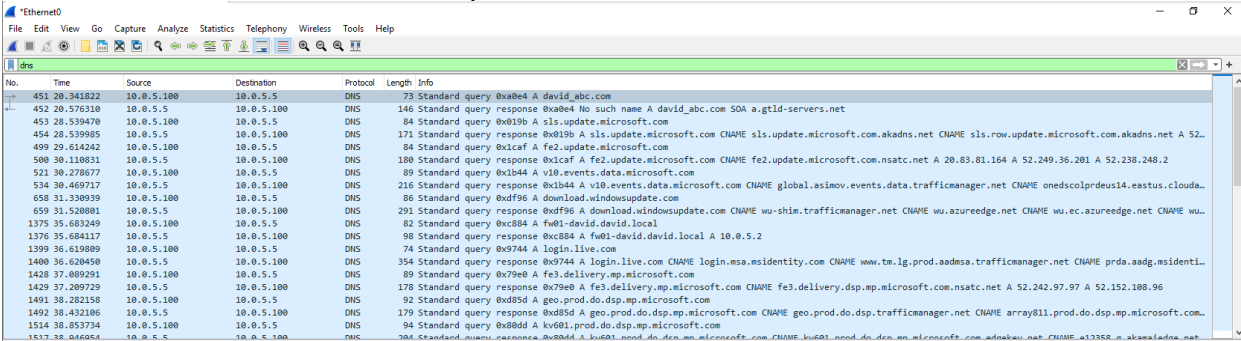
David Thomsen

SYS255

Deliverables

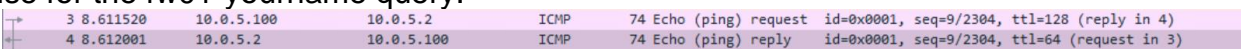
1. In your capture, what are the destination IP addresses, ports and protocols for DNS traffic?
 - a. DNS traffic flows between 10.0.5.100 and 10.0.5.5 which are the DNS server and the workstation's IPv4.
2. Perform some basic research. Does DNS ever use a protocol different than the one found in Deliverable 1? If so, why?
 - a. DNS uses many different protocols. DNS uses TCP for zone transfer and UDP for name and queries.
3. Figure out how to create a display filter showing only DNS traffic, provide a screenshot that shows at least six DNS packets.

a.



No.	Time	Source	Destination	Protocol	Length	Info
451	20.341822	10.0.5.100	10.0.5.5	DNS	73	Standard query 0xa0e4 A david_abc.com
452	20.576310	10.0.5.5	10.0.5.100	DNS	146	Standard query response 0xa0e4 No such name A david_abc.com SOA a.gtld-servers.net
453	20.539470	10.0.5.100	10.0.5.5	DNS	84	Standard query 0x019b A sls.update.microsoft.com
454	20.539985	10.0.5.5	10.0.5.100	DNS	171	Standard query response 0x019b A sls.update.microsoft.com CNAME sls.row.update.microsoft.com.akadns.net A 52...
499	29.614242	10.0.5.100	10.0.5.5	DNS	84	Standard query 0xc1af A fe2.update.microsoft.com
500	30.110831	10.0.5.5	10.0.5.100	DNS	180	Standard query response 0xc1af A fe2.update.microsoft.com CNAME fe2.update.microsoft.com.nsatc.net A 20.83.81.164 A 52.249.36.201 A 52.238.248.2
521	30.278677	10.0.5.100	10.0.5.5	DNS	89	Standard query 0x1b44 A v10.events.data.microsoft.com
534	30.469717	10.0.5.5	10.0.5.100	DNS	216	Standard query response 0x1b44 A v10.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME onedcolprdeus14.eastus.clouda...
658	31.330939	10.0.5.100	10.0.5.5	DNS	86	Standard query 0xd996 A download.windowsupdate.com
659	31.520801	10.0.5.5	10.0.5.100	DNS	291	Standard query response 0xd996 A download.windowsupdate.com CNAME wu-shim.trafficmanager.net CNAME wu.ec.azureedge.net CNAME wu...
1375	35.683249	10.0.5.100	10.0.5.5	DNS	82	Standard query 0xc884 A fw01-david.david.local
1376	35.684117	10.0.5.5	10.0.5.100	DNS	98	Standard query response 0xc884 A fw01-david.david.local A 10.0.5.2
1399	36.619889	10.0.5.100	10.0.5.5	DNS	74	Standard query 0x9744 A login.live.com
1400	36.620450	10.0.5.5	10.0.5.100	DNS	354	Standard query response 0x9744 A login.live.com CNAME login.msa.msidentity.com CNAME www.tn.lg.prod.aadmsa.trafficmanager.net CNAME prda.aadg.msidenti...
1420	37.089291	10.0.5.100	10.0.5.5	DNS	89	Standard query 0x79e0 A fe3.delivery.mp.microsoft.com
1429	37.209729	10.0.5.5	10.0.5.100	DNS	178	Standard query response 0x79e0 A fe3.delivery.mp.microsoft.com CNAME fe3.delivery.dsp.mp.microsoft.com.nsatc.net A 52.242.97.97 A 52.152.188.96
1491	38.282158	10.0.5.100	10.0.5.5	DNS	92	Standard query 0xd85d A geo.prod.do.dsp.mp.microsoft.com
1492	38.432186	10.0.5.5	10.0.5.100	DNS	179	Standard query response 0xd85d A geo.prod.do.dsp.mp.microsoft.com CNAME geo.prod.do.dsp.trafficmanager.net CNAME array811.prod.do.dsp.mp.microsoft.com...
1514	38.853734	10.0.5.100	10.0.5.5	DNS	94	Standard query 0xb0dd A kv001.prod.do.dsp.mp.microsoft.com
1517	38.866054	10.0.5.5	10.0.5.100	DNS	304	Standard query response 0xb0dd A kv001.prod.do.dsp.mp.microsoft.com CNAME kv001-nord.do.dsp.mp.microsoft.com adnabau.net CNAME m13382.a.akamaiadn.net...

4. For use case 1, what are the authoritative name servers for the .edu top level domain?
 - a. Edu: type SOA, class IN, name a.edu-servers.net.
5. For use case 1, Provide a screenshot that shows the reply code from your .edu lookup (note this will be part of the flags field)
 - a.
6. For use case 2, provide a screenshot showing the Answer's section of the DNS response for the fw01-yourname query.
 - a.
7. For use case 3, what server responds to the dns request for champlain.edu, & is it authoritative?



No.	Time	Source	Destination	Protocol	Length	Info
3	8.611520	10.0.5.100	10.0.5.2	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 4)
4	8.612001	10.0.5.2	10.0.5.100	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=64 (request in 3)

- a. IPv4 is the server and it is not authoritative.
8. What are the different types of DNS Records? Provide a brief description of each in your own words. There are dozens of DNS record types, so discuss the more common ones (< 10 of them) but more than (CNAME,A,PTR) discussed in class.
- a. A (Host Address)
 - b. AAAA (IPv6)
 - c. CNAME(domain name alias)
 - d. PTR(map IP addresses to domain names)
 - e. NS (identifies the DNS servers)
 - f. SRV (Locates a service)
 - g. TXT (Hold descriptive text)
9. Your deliverable meets the submission [guidelines](#).