

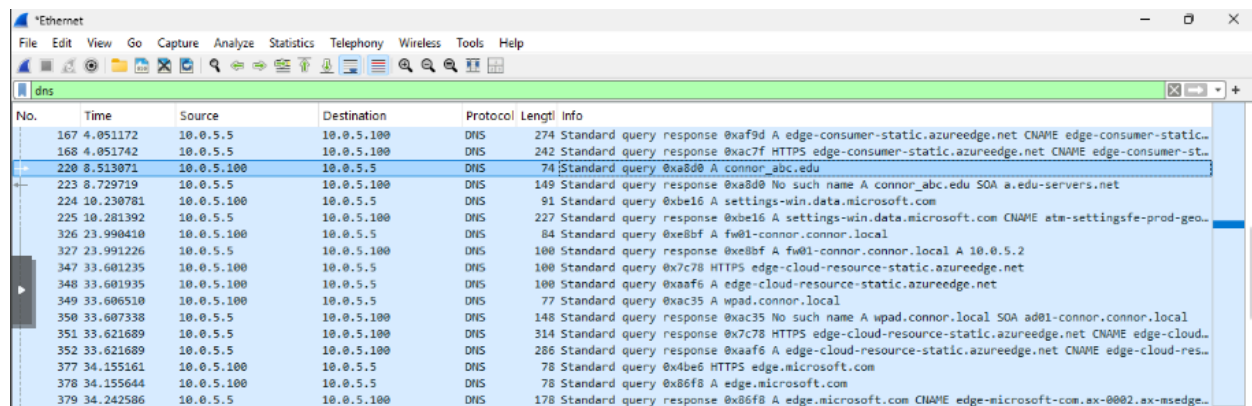
**Connor Schuler**  
**SYS-255-01**  
**STR2026**

**Deliverable 1:**

- Destination IP: 10.0.5.5
- Destination Port: 53
- Protocol: UDP or User Datagram Protocol

**Deliverable 2:** Yes, DNS sometimes uses TCP for large payloads, such as DNS server to server synchronization.

**Deliverable 3:** Simply typing “dns” into the filter bar shows only DNS traffic. The filter shows a total of 36 packets.



No.	Time	Source	Destination	Protocol	Length	Info
167	4.051172	10.0.5.5	10.0.5.100	DNS	274	Standard query response 0xaf9d A edge-consumer-static.azureedge.net CNAME edge-consumer-static...
168	4.051742	10.0.5.5	10.0.5.100	DNS	242	Standard query response 0xac7f HTTPS edge-consumer-static.azureedge.net CNAME edge-consumer-st...
220	8.513071	10.0.5.100	10.0.5.5	DNS	74	Standard query 0xa8d0 A connor_abc.edu
223	8.729719	10.0.5.5	10.0.5.100	DNS	149	Standard query response 0xa8d0 No such name A connor_abc.edu SOA a.edu-servers.net
224	10.230781	10.0.5.100	10.0.5.5	DNS	91	Standard query 0xbel6 A settings-win.data.microsoft.com
225	10.281392	10.0.5.5	10.0.5.100	DNS	227	Standard query response 0xbel6 A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo...
326	23.990410	10.0.5.100	10.0.5.5	DNS	84	Standard query 0xe8bf A fw01-connor.connor.local
327	23.991226	10.0.5.5	10.0.5.100	DNS	100	Standard query response 0xe8bf A fw01-connor.connor.local A 10.0.5.2
347	33.601235	10.0.5.100	10.0.5.5	DNS	100	Standard query 0x7c78 HTTPS edge-cloud-resource-static.azureedge.net
348	33.601935	10.0.5.100	10.0.5.5	DNS	100	Standard query 0xaa6f A edge-cloud-resource-static.azureedge.net
349	33.606510	10.0.5.100	10.0.5.5	DNS	77	Standard query 0xac35 A wpad.connor.local
350	33.607338	10.0.5.5	10.0.5.100	DNS	148	Standard query response 0xac35 No such name A wpad.connor.local SOA ad01-connor.connor.local
351	33.621609	10.0.5.5	10.0.5.100	DNS	314	Standard query response 0x7c78 HTTPS edge-cloud-resource-static.azureedge.net CNAME edge-cloud...
352	33.621609	10.0.5.5	10.0.5.100	DNS	286	Standard query response 0xaa6f A edge-cloud-resource-static.azureedge.net CNAME edge-cloud-res...
377	34.155161	10.0.5.100	10.0.5.5	DNS	78	Standard query 0x4be6 HTTPS edge.microsoft.com
378	34.155644	10.0.5.100	10.0.5.5	DNS	78	Standard query 0x86f8 A edge.microsoft.com
379	34.242586	10.0.5.5	10.0.5.100	DNS	178	Standard query response 0x86f8 A edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-msedge...

**Deliverable 4:** The authoritative name server is a.edu-servers.net.

```
Domain Name System (response)
  Transaction ID: 0xa8d0
  > Flags: 0x8183 Standard query response, No such name
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 0
  > Queries
  > Authoritative nameservers
    > edu: type SOA, class IN, #name a.edu-servers.net
    [Request In: 220]
    [Time: 216.648000 milliseconds]
```

**Deliverable 5:** Image shows a reply code of “no such name”

223	8.729719	10.0.5.5	10.0.5.100	DNS	149 Standard query response	@xa8d0 No such name A connor_abc.edu SOA a.edu-servers.net
224	10.230781	10.0.5.100	10.0.5.5	DNS	91 Standard query	@xbe16 A settings-win.data.microsoft.com
225	10.281392	10.0.5.5	10.0.5.100	DNS	227 Standard query response	@xbe16 A settings-win.data.microsoft.com CNAME atm-settingsfe-prod.geo.
326	23.990410	10.0.5.100	10.0.5.5	DNS	84 Standard query	@xe8bf A fw01-connor.connor.local
327	23.991226	10.0.5.5	10.0.5.100	DNS	100 Standard query response	@xe8bf A fw01-connor.connor.local A 10.0.5.2

> User Datagram Protocol, Src Port: 53, Dst Port: 56213 > Domain Name System (response) Transaction ID: 0xa8d0 > Flags: 0x8183 Standard query response, No such name 1... .. = Response: Message is a response .000 0... .. = Opcode: Standard query (0) ....0... .. = Authoritative: Server is not an authority for domain ....0... .. = Truncated: Message is not truncated ....1... .. = Recursion desired: Do query recursively ....1... .. = Recursion available: Server can do recursive queries ....0... .. = Z: reserved (0) ....0... .. = Answer authenticated: Answer/authority portion was not au ....0... .. = Non-authenticated data: Unacceptable ....0011 = Reply code: No such name (3) Questions: 1 Answer RRs: 0 Authority RRs: 1 Additional RRs: 0		0000 bc 24 11 12 c3 84 bc 24 11 1f b4 7e 08 00 45 00 -.\$-E- 0010 00 87 b4 3a 00 00 00 11 67 c3 0a 00 05 05 0a 00 -V?g- 0020 05 64 00 35 db 95 00 73 6a 84 a8 d0 81 83 00 01 -d5-sj- 0030 00 00 00 01 00 00 0a 63 6f 6e 6e 6f 72 5f 61 62 -c-connor_ab 0040 63 03 65 64 75 00 00 01 00 01 c0 17 00 06 00 01 -c-edu- 0050 00 00 03 83 00 3f 01 61 0b 65 64 75 2d 73 65 72 -?-a-edu-ser 0060 76 65 72 73 03 6e 65 74 00 05 6e 73 74 6c 64 0c -vers-net-nsld- 0070 76 65 72 69 73 69 67 6e 2d 67 72 73 03 63 6f 6d -verisign-grs-com 0080 00 69 7a db 2b 00 00 07 08 00 00 03 84 00 09 3a -iz+- 0090 00 00 00 03 84 .....
--	--	---

**Deliverable 6:** Image shows a DNS response of 10.0.5.2 for fw01-connor.connor.local

327	23.991226	10.0.5.5	10.0.5.100	DNS	100 Standard query response	@xe8bf A fw01-connor.connor.local A 10.0.5.2
347	33.601235	10.0.5.100	10.0.5.5	DNS	100 Standard query	@x7c70 HTTPS edge-cloud-resource-static.azureedge.net
348	33.601935	10.0.5.100	10.0.5.5	DNS	100 Standard query	@xae6 A edge-cloud-resource-static.azureedge.net
349	33.606510	10.0.5.100	10.0.5.5	DNS	77 Standard query	@xac35 A wpad.connor.local

> Frame 327: Packet, 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on inter > Ethernet II, Src: ProxmoxServe1f:b4:7e (bc:24:11:1f:b4:7e), Dst: ProxmoxServe12:c3:84 > Internet Protocol Version 4, Src: 10.0.5.5, Dst: 10.0.5.100 > User Datagram Protocol, Src Port: 53, Dst Port: 56213 > Domain Name System (response) Transaction ID: 0xe8bf > Flags: 0x8580 Standard query response, No error Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0 > Queries > Answers > fw01-connor.connor.local: type A, class IN, addr 10.0.5.2 [Request ID: 326] [Time: 816.000 microseconds]		0000 bc 24 11 12 c3 84 bc 24 11 1f b4 7e 08 00 45 00 -.\$-E- 0010 00 56 b4 3f 00 00 00 11 67 ef 0a 00 05 05 0a 00 -V?g- 0020 05 64 00 35 db 95 00 42 32 a2 e8 bf 85 80 00 01 -d5-sj- 0030 00 01 00 00 00 00 0b 66 77 30 31 2d 63 6f 6e 6e -c-fw01-conn 0040 6f 72 06 63 6f 6e 6e 6f 72 05 6c 6f 63 61 6c 00 -or-connor-local- 0050 00 01 00 01 c0 0c 00 01 00 01 00 00 0e 10 00 04 ..... 0060 0a 00 05 02 .....
--	--	---

**Deliverable 7:** Server 10.0.5.5 responds to the request, it is not authoritative.

459	40.003845	10.0.5.5	10.0.5.100	DNS	89 Standard query response	@xd1dd A champion.edu A 23.105.0.3
517	45.935752	10.0.5.100	10.0.5.5	DNS	74 Standard query	@x04f2 A assets.msn.com

UDP payload (47 bytes) > Domain Name System (response) Transaction ID: 0xd1dd > Flags: 0x8180 Standard query response, No error 1... .. = Response: Message is a response .000 0... .. = Opcode: Standard query (0) ....0... .. = Authoritative: Server is not an authority for domain ....0... .. = Truncated: Message is not truncated ....1... .. = Recursion desired: Do query recursively ....1... .. = Recursion available: Server can do recursive queries ....0... .. = Z: reserved (0) ....0... .. = Answer authenticated: Answer/authority portion was not au ....0... .. = Non-authenticated data: Unacceptable ....0000 = Reply code: No error (0) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0		0000 bc 24 11 12 c3 84 bc 24 11 1f b4 7e 08 00 45 00 -.\$-E- 0010 00 4b b4 4c 00 00 00 11 67 eb 0a 00 05 05 0a 00 -K-N-g- 0020 05 64 00 35 c1 1b 00 37 b3 ae d1 dd 81 80 00 01 -d5-7- 0030 00 01 00 00 00 00 09 63 68 61 6d 70 6c 61 69 6e -c-champain 0040 03 65 64 75 00 00 01 00 01 c0 0c 00 01 00 01 00 -edu- 0050 00 01 2b 00 04 17 b9 00 03 -+-
---	--	--

**Deliverable 8:**

- A: maps a domain to an IPv4 address
- AAAA: maps a domain to an IPv6 address
- CNAME: Forwards one domain to another
- MX: Directs email traffic to a specific server
- TXT: basic text, often used for domain ownership verification or sender policy framework data
- NS: specifies the authoritative name server that manages the DNS records for domain or zone

## **Deliverable 9:** Document formatting