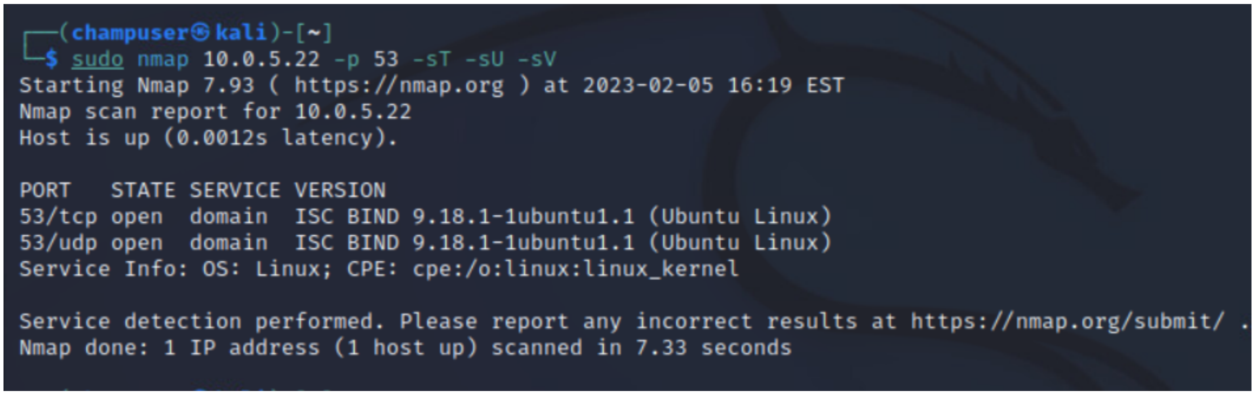
https://github.com/dthomsen116/SEC-335/wiki/Assignment-3.2---DNS-uses-TCP-and-UDP

Del 0: Provide a screenshot of your command and output similar to the screenshot below.

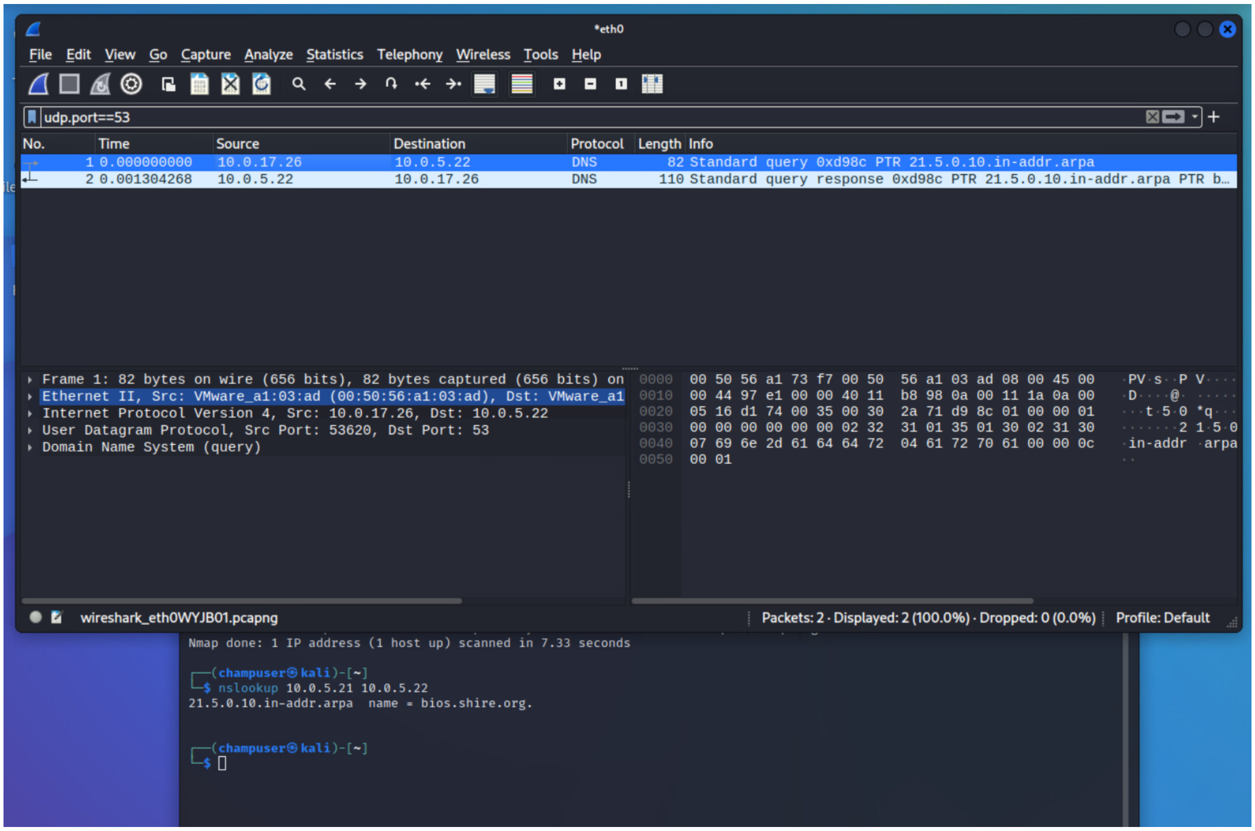


```
┌──(champuser㉿kali)-[~]
└─$ sudo nmap 10.0.5.22 -p 53 -sT -sU -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-05 16:19 EST
Nmap scan report for 10.0.5.22
Host is up (0.0012s latency).

PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND 9.18.1-1ubuntu1.1 (Ubuntu Linux)
53/udp open  domain  ISC BIND 9.18.1-1ubuntu1.1 (Ubuntu Linux)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.33 seconds
```

Deliverable 1. Run nslookup against 10.0.5.21 using the dns server 10.0.5.22. Provide a screenshot showing the traffic similar to the one below that shows your nslookup command and an indication the protocol is UDP.



udp.port==53

```
No.   Time          Source        Destination   Protocol Length Info
    1 0.000000000   10.0.17.26    10.0.5.22     DNS        82 Standard query 0xd98c PTR 21.5.0.10.in-addr.arpa
    2 0.001304268   10.0.5.22     10.0.17.26    DNS       110 Standard query response 0xd98c PTR 21.5.0.10.in-addr.arpa PTR b…
```

```
› Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on
› Ethernet II, Src: VMware_a1:03:ad (00:50:56:a1:03:ad), Dst: VMware_a1
› Internet Protocol Version 4, Src: 10.0.17.26, Dst: 10.0.5.22
› User Datagram Protocol, Src Port: 53620, Dst Port: 53
› Domain Name System (query)
```

```
0000  00 50 56 a1 73 f7 00 50  56 a1 03 ad 08 00 45 00   ·PV·s··P V·····E·
0010  00 44 97 e1 00 00 40 11  b8 98 0a 00 11 1a 0a 00   ·D····@· ········
0020  05 16 d1 74 00 35 00 30  2a 71 d9 8c 01 00 00 01   ···t·5·0 *q······
0030  00 00 00 00 00 00 02 32  31 01 35 01 30 02 31 30   ·······2 1·5·0·10
0040  07 69 6e 2d 61 64 64 72  04 61 72 70 61 00 00 0c   ·in-addr ·arpa···
0050  00 01                                              ··
```

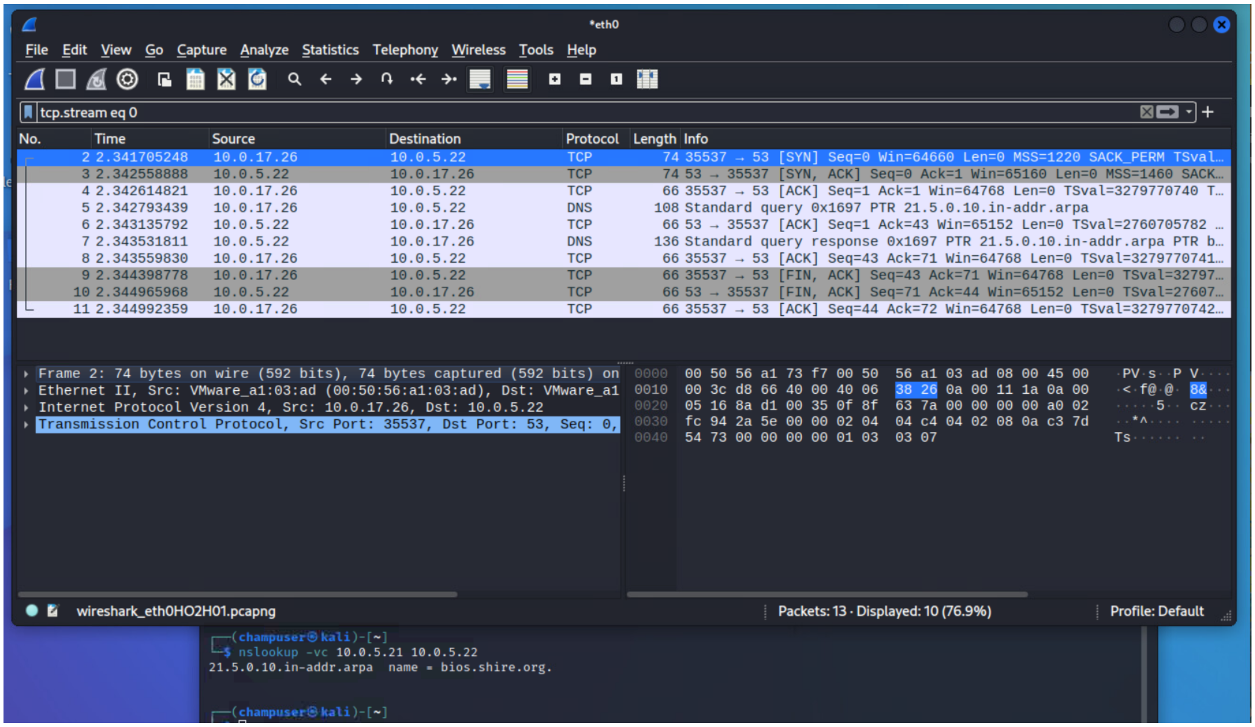
wireshark_eth0WYJB01.pcapng   Packets: 2 · Displayed: 2 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

```
Nmap done: 1 IP address (1 host up) scanned in 7.33 seconds

┌──(champuser㉿kali)-[~]
└─$ nslookup 10.0.5.21 10.0.5.22
21.5.0.10.in-addr.arpa  name = bios.shire.org.


┌──(champuser㉿kali)-[~]
└─$ 
```

Deliverable 2. Figure out how to coax nslookup to use tcp and repeat the lookup, continuing to capture packets to tcp/udp 53. Provide a screenshot similar to the one below that shows the modified nslookup command and the new packets. The illustration is also a reminder of why UDP is so efficient.



tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
2	2.341705248	10.0.17.26	10.0.5.22	TCP	74	35537 → 53 [SYN] Seq=0 Win=64660 Len=0 MSS=1220 SACK_PERM TSval…
3	2.342558888	10.0.5.22	10.0.17.26	TCP	74	53 → 35537 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK…
4	2.342614821	10.0.17.26	10.0.5.22	TCP	66	35537 → 53 [ACK] Seq=1 Ack=1 Win=64768 Len=0 TSval=3279770740 T…
5	2.342793439	10.0.17.26	10.0.5.22	DNS	108	Standard query 0x1697 PTR 21.5.0.10.in-addr.arpa
6	2.343135792	10.0.5.22	10.0.17.26	TCP	66	53 → 35537 [ACK] Seq=1 Ack=43 Win=65152 Len=0 TSval=2760705782 …
7	2.343531811	10.0.5.22	10.0.17.26	DNS	136	Standard query response 0x1697 PTR 21.5.0.10.in-addr.arpa PTR b…
8	2.343559830	10.0.17.26	10.0.5.22	TCP	66	35537 → 53 [ACK] Seq=43 Ack=71 Win=64768 Len=0 TSval=3279770741…
9	2.344398778	10.0.17.26	10.0.5.22	TCP	66	35537 → 53 [FIN, ACK] Seq=43 Ack=71 Win=64768 Len=0 TSval=32797…
10	2.344965968	10.0.5.22	10.0.17.26	TCP	66	53 → 35537 [FIN, ACK] Seq=71 Ack=44 Win=65152 Len=0 TSval=27607…
11	2.344992359	10.0.17.26	10.0.5.22	TCP	66	35537 → 53 [ACK] Seq=44 Ack=72 Win=64768 Len=0 TSval=3279770742…

```
› Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
› Ethernet II, Src: VMware_a1:03:ad (00:50:56:a1:03:ad), Dst: VMware_a1
› Internet Protocol Version 4, Src: 10.0.17.26, Dst: 10.0.5.22
› Transmission Control Protocol, Src Port: 35537, Dst Port: 53, Seq: 0,
```

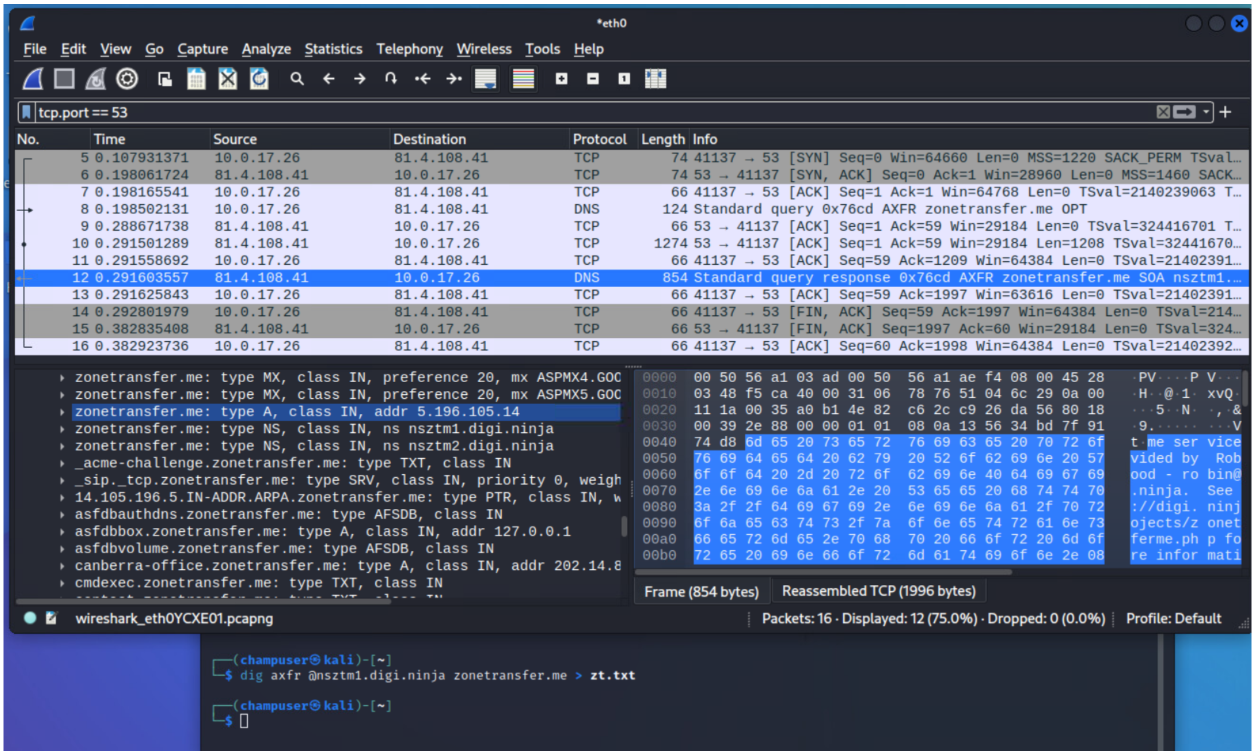
```
0000  00 50 56 a1 73 f7 00 50  56 a1 03 ad 08 00 45 00   ·PV·s··P V·····
0010  00 3c d8 66 40 00 40 06  38 26 0a 00 11 1a 0a 00   ·<·f@·@· 8&·····
0020  05 16 8a d1 00 35 0f 8f  63 7a 00 00 00 00 a0 02   ·····5·· cz·····
0030  fc 94 2a 5e 00 00 02 04  04 c4 04 02 08 0a c3 7d   ··*^···· ·······
0040  54 73 00 00 00 00 01 03  03 07                     Ts······ ··
```

wireshark_eth0HO2H01.pcapng | Packets: 13 · Displayed: 10 (76.9%) | Profile: Default

```
┌──(champuser㉿kali)-[~]
└─$ nslookup -vc 10.0.5.21 10.0.5.22
21.5.0.10.in-addr.arpa  name = bios.shire.org.

┌──(champuser㉿kali)-[~]
```

Deliverable 3. Change your capture so that you are monitoring eth0 using the same port 53 capture filter. Repeat the zone transfer from zonetransfer.me from Activity 3.1. Provide a screenshot showing the tcp stream of this transfer. (Yes, zone transfers use TCP)



tcp.port == 53

```
No.   Time         Source        Destination   Protocol Length Info
    5 0.107931371  10.0.17.26    81.4.108.41   TCP        74 41137 → 53 [SYN] Seq=0 Win=64660 Len=0 MSS=1220 SACK_PERM TSval…
    6 0.198061724  81.4.108.41   10.0.17.26    TCP        74 53 → 41137 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK…
    7 0.198165541  10.0.17.26    81.4.108.41   TCP        66 41137 → 53 [ACK] Seq=1 Ack=1 Win=64768 Len=0 TSval=2140239063 T…
    8 0.198502131  10.0.17.26    81.4.108.41   DNS       124 Standard query 0x76cd AXFR zonetransfer.me OPT
    9 0.288671738  81.4.108.41   10.0.17.26    TCP        66 53 → 41137 [ACK] Seq=1 Ack=59 Win=29184 Len=0 TSval=324416701 T…
   10 0.291501289  81.4.108.41   10.0.17.26    TCP      1274 53 → 41137 [ACK] Seq=1 Ack=59 Win=29184 Len=1208 TSval=32441670…
   11 0.291558692  10.0.17.26    81.4.108.41   TCP        66 41137 → 53 [ACK] Seq=59 Ack=1209 Win=64384 Len=0 TSval=21402391…
   12 0.291603557  81.4.108.41   10.0.17.26    DNS       854 Standard query response 0x76cd AXFR zonetransfer.me SOA nsztm1.…
   13 0.291625843  10.0.17.26    81.4.108.41   TCP        66 41137 → 53 [ACK] Seq=59 Ack=1997 Win=63616 Len=0 TSval=21402391…
   14 0.292801979  10.0.17.26    81.4.108.41   TCP        66 41137 → 53 [FIN, ACK] Seq=59 Ack=1997 Win=64384 Len=0 TSval=214…
   15 0.382835408  81.4.108.41   10.0.17.26    TCP        66 53 → 41137 [FIN, ACK] Seq=1997 Ack=60 Win=29184 Len=0 TSval=324…
   16 0.382923736  10.0.17.26    81.4.108.41   TCP        66 41137 → 53 [ACK] Seq=60 Ack=1998 Win=64384 Len=0 TSval=21402392…
```

```
    › zonetransfer.me: type MX, class IN, preference 20, mx ASPMX4.GOO
    › zonetransfer.me: type MX, class IN, preference 20, mx ASPMX5.GOO
    › zonetransfer.me: type A, class IN, addr 5.196.105.14
    › zonetransfer.me: type NS, class IN, ns nsztm1.digi.ninja
    › zonetransfer.me: type NS, class IN, ns nsztm2.digi.ninja
    › _acme-challenge.zonetransfer.me: type TXT, class IN
    › _sip._tcp.zonetransfer.me: type SRV, class IN, priority 0, weigh
    › 14.105.196.5.IN-ADDR.ARPA.zonetransfer.me: type PTR, class IN, w
    › asfdbauthdns.zonetransfer.me: type AFSDB, class IN
    › asfdbbox.zonetransfer.me: type A, class IN, addr 127.0.0.1
    › asfdbvolume.zonetransfer.me: type AFSDB, class IN
    › canberra-office.zonetransfer.me: type A, class IN, addr 202.14.8
    › cmdexec.zonetransfer.me: type TXT, class IN
```

```
0000  00 50 56 a1 03 ad 00 50  56 a1 ae f4 08 00 45 28   ·PV····P V·····E(
0010  03 48 f5 ca 40 00 31 06  78 76 51 04 6c 29 0a 00   ·H··@·1· xvQ·l)··
0020  11 1a 00 35 a0 b1 4e 82  c6 2c c9 26 da 56 80 18   ···5··N· ·,·&·V··
0030  00 39 2e 88 00 00 01 01  08 0a 13 56 34 bd 7f 91   ·9.····· ···V4···
0040  74 d8 6d 65 20 73 65 72  76 69 63 65 20 70 72 6f   t·me ser vice pro
0050  76 69 64 65 64 20 62 79  20 52 6f 62 69 6e 20 57   vided by  Robin W
0060  6f 6f 64 20 2d 20 72 6f  62 69 6e 40 64 69 67 69   ood - ro bin@digi
0070  2e 6e 69 6e 6a 61 2e 20  53 65 65 20 68 74 74 70   .ninja.  See http
0080  3a 2f 2f 64 69 67 69 2e  6e 69 6e 6a 61 2f 70 72   ://digi. ninja/pr
0090  6f 6a 65 63 74 73 2f 7a  6f 6e 65 74 72 61 6e 73   ojects/z onetrans
00a0  66 65 72 6d 65 2e 70 68  70 20 66 6f 72 20 6d 6f   ferme.ph p for mo
00b0  72 65 20 69 6e 66 6f 72  6d 61 74 69 6f 6e 2e 08   re infor mation.·
```

Frame (854 bytes) | Reassembled TCP (1996 bytes)

wireshark_eth0YCXE01.pcapng | Packets: 16 · Displayed: 12 (75.0%) · Dropped: 0 (0.0%) | Profile: Default

```
┌──(champuser㉿kali)-[~]
└─$ dig axfr @nsztm1.digi.ninja zonetransfer.me > zt.txt

┌──(champuser㉿kali)-[~]
└─$ 
```