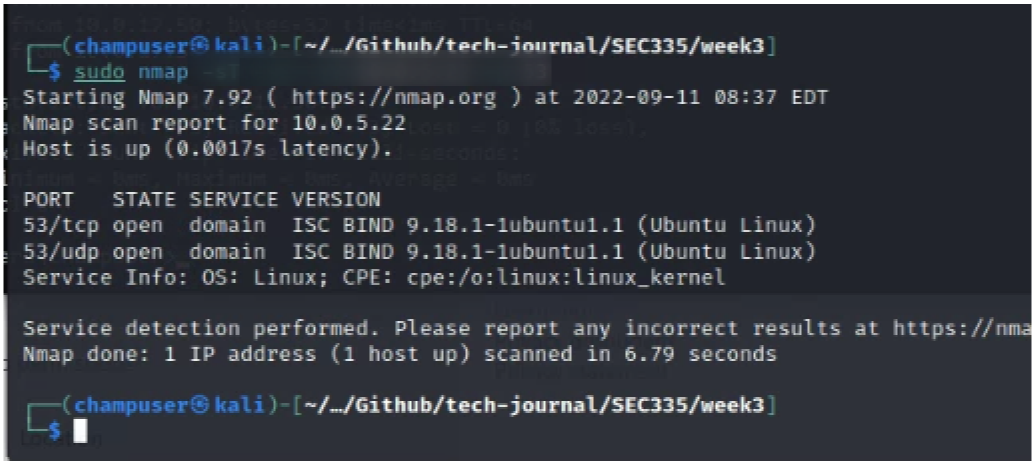
Updated: Sep 14, 2021

Assignment 3.2 - DNS Uses both UDP and TCP

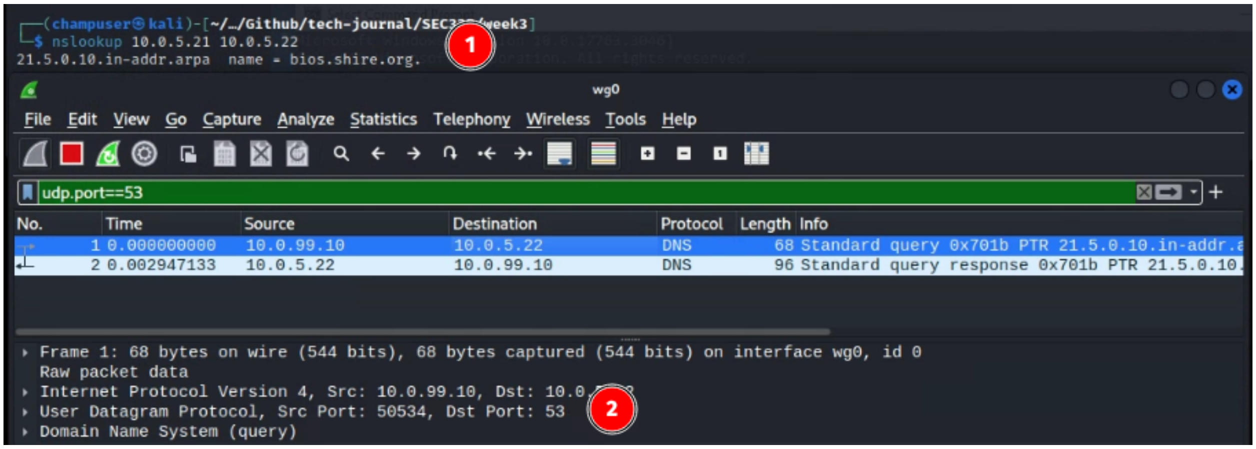
Figure out how to run nmap against 10.0.5.22 in such a way that both tcp/53 and udp/53 are checked. Provide a screenshot of your command and output similar to the screenshot below.



```
┌──(champuser㉿kali)-[~/…/Github/tech-journal/SEC335/week3]
└─$ sudo nmap [redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-11 08:37 EDT
Nmap scan report for 10.0.5.22
Host is up (0.0017s 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://nma
Nmap done: 1 IP address (1 host up) scanned in 6.79 seconds

┌──(champuser㉿kali)-[~/…/Github/tech-journal/SEC335/week3]
└─$ █
```

Using Wireshark, create a capture filter for port 53 in interface wg0 (remember this is not a display filter)

`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.`



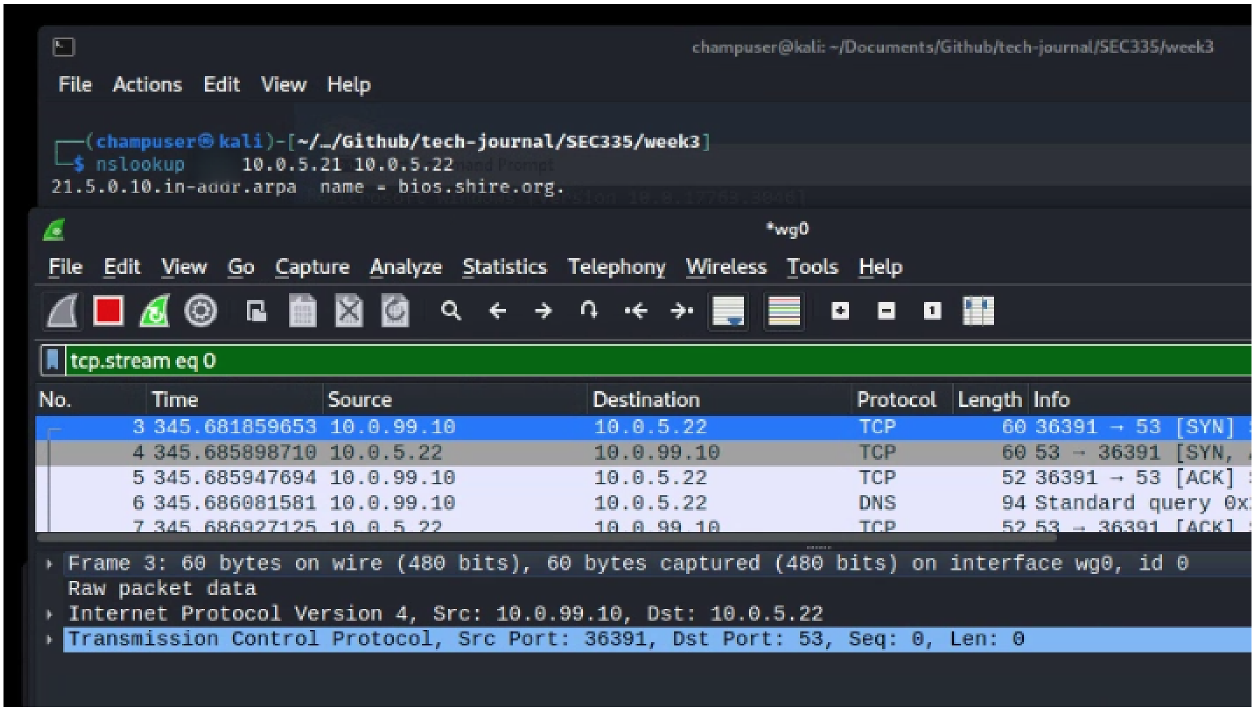
```
┌──(champuser㉿kali)-[~/…/Github/tech-journal/SEC335/week3]
└─$ nslookup 10.0.5.21 10.0.5.22
21.5.0.10.in-addr.arpa  name = bios.shire.org.
```

1
wg0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp.port==53

No.  Time          Source       Destination  Protocol Length Info
   1 0.000000000   10.0.99.10   10.0.5.22    DNS        68 Standard query 0x701b PTR 21.5.0.10.in-addr.a
   2 0.002947133   10.0.5.22    10.0.99.10   DNS        96 Standard query response 0x701b PTR 21.5.0.10.

› Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface wg0, id 0
  Raw packet data
› Internet Protocol Version 4, Src: 10.0.99.10, Dst: 10.0.
› User Datagram Protocol, Src Port: 50534, Dst Port: 53
› Domain Name System (query)
```

Updated: Sep 14, 2021

`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.`


champuser@kali: ~/Documents/Github/tech-journal/SEC335/week3
File Actions Edit View Help
*wg0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
┌──(champuser㉿kali)-[~/…/Github/tech-journal/SEC335/week3]
└─$ nslookup      10.0.5.21 10.0.5.22
21.5.0.10.in-addr.arpa  name = bios.shire.org.
```

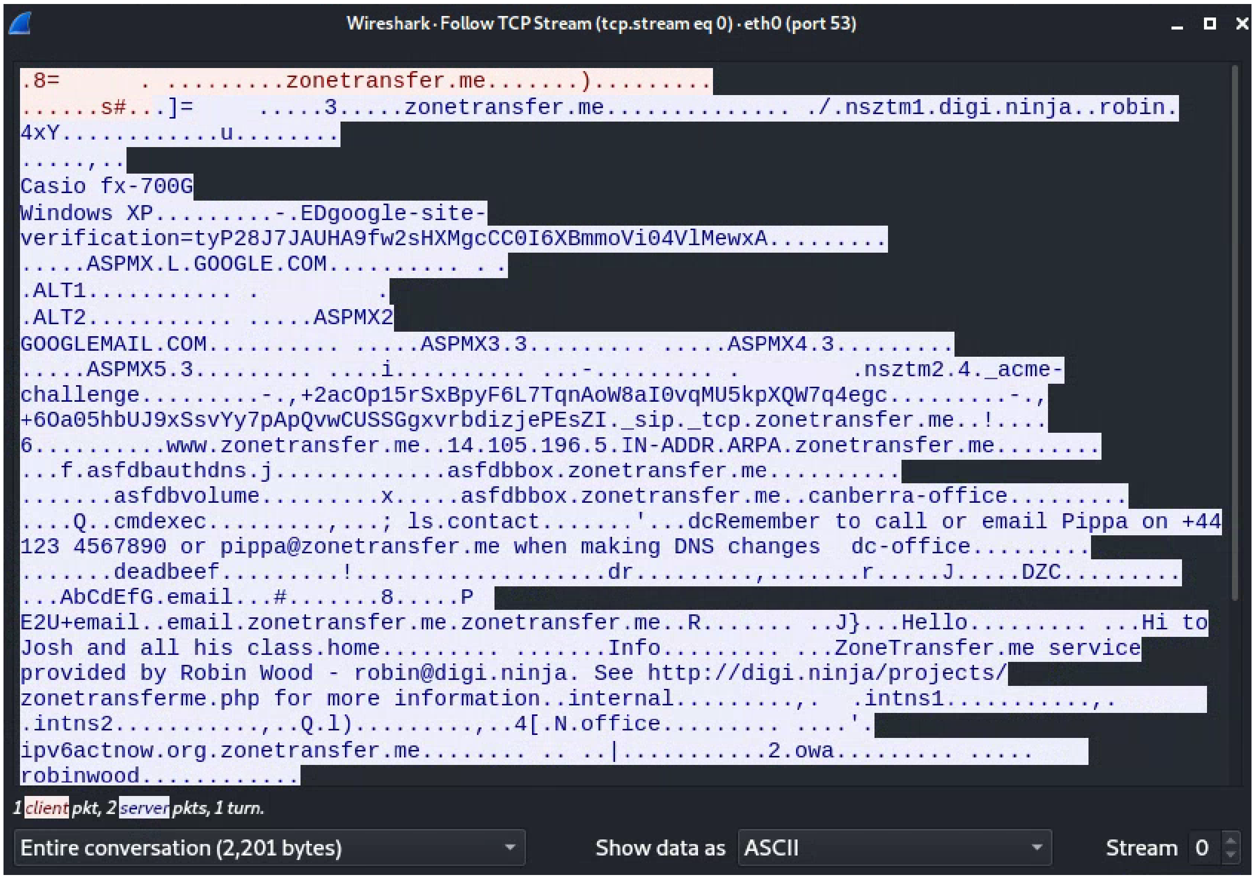
tcp.stream eq 0

```
No.   Time           Source       Destination  Protocol Length Info
    3 345.681859653  10.0.99.10   10.0.5.22    TCP          60 36391 → 53 [SYN]
    4 345.685898710  10.0.5.22    10.0.99.10   TCP          60 53 → 36391 [SYN,
    5 345.685947694  10.0.99.10   10.0.5.22    TCP          52 36391 → 53 [ACK]
    6 345.686081581  10.0.99.10   10.0.5.22    DNS          94 Standard query 0x
    7 345.686927125  10.0.5.22    10.0.99.10   TCP          52 53 → 36391 [ACK]
```

```
› Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface wg0, id 0
  Raw packet data
› Internet Protocol Version 4, Src: 10.0.99.10, Dst: 10.0.5.22
› Transmission Control Protocol, Src Port: 36391, Dst Port: 53, Seq: 0, Len: 0
```

Updated: Sep 14, 2021

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)


Wireshark · Follow TCP Stream (tcp.stream eq 0) · eth0 (port 53)

```
.8=       . .........zonetransfer.me.......).........
......s#...]=     .....3.....zonetransfer.me.............. ./.nsztm1.digi.ninja..robin.
4xY............u........
.....,..
Casio fx-700G
Windows XP.........-.EDgoogle-site-
verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA.........
.....ASPMX.L.GOOGLE.COM.......... . .
.ALT1........... .         .
.ALT2........... .....ASPMX2
GOOGLEMAIL.COM.......... .....ASPMX3.3......... .....ASPMX4.3.........
.....ASPMX5.3......... ....i.......... ...-......... .         .nsztm2.4._acme-
challenge.........-.,+2acOp15rSxBpyF6L7TqnAoW8aI0vqMU5kpXQW7q4egc.........-.,
+6Oa05hbUJ9xSsvYy7pApQvwCUSSGgxvrbdizjePEsZI._sip._tcp.zonetransfer.me..!....
6..........www.zonetransfer.me..14.105.196.5.IN-ADDR.ARPA.zonetransfer.me........
...f.asfdbauthdns.j.............asfdbbox.zonetransfer.me.........
.......asfdbvolume.........x.....asfdbbox.zonetransfer.me..canberra-office.........
....Q..cmdexec.........,...; ls.contact.......'...dcRemember to call or email Pippa on +44
123 4567890 or pippa@zonetransfer.me when making DNS changes  dc-office.........
.......deadbeef.........!...................dr.........,.......r.....J.....DZC.........
...AbCdEfG.email...#.......8.....P
E2U+email..email.zonetransfer.me.zonetransfer.me..R....... ..J}...Hello......... ...Hi to
Josh and all his class.home......... .......Info......... ...ZoneTransfer.me service
provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/projects/
zonetransferme.php for more information..internal.........,.  .intns1...........,.
.intns2...........,..Q.l).........,..4[.N.office......... ....'.
ipv6actnow.org.zonetransfer.me........ .. ..|..........2.owa......... .....
robinwood...........
```

1 client pkt, 2 server pkts, 1 turn.