Lab 2

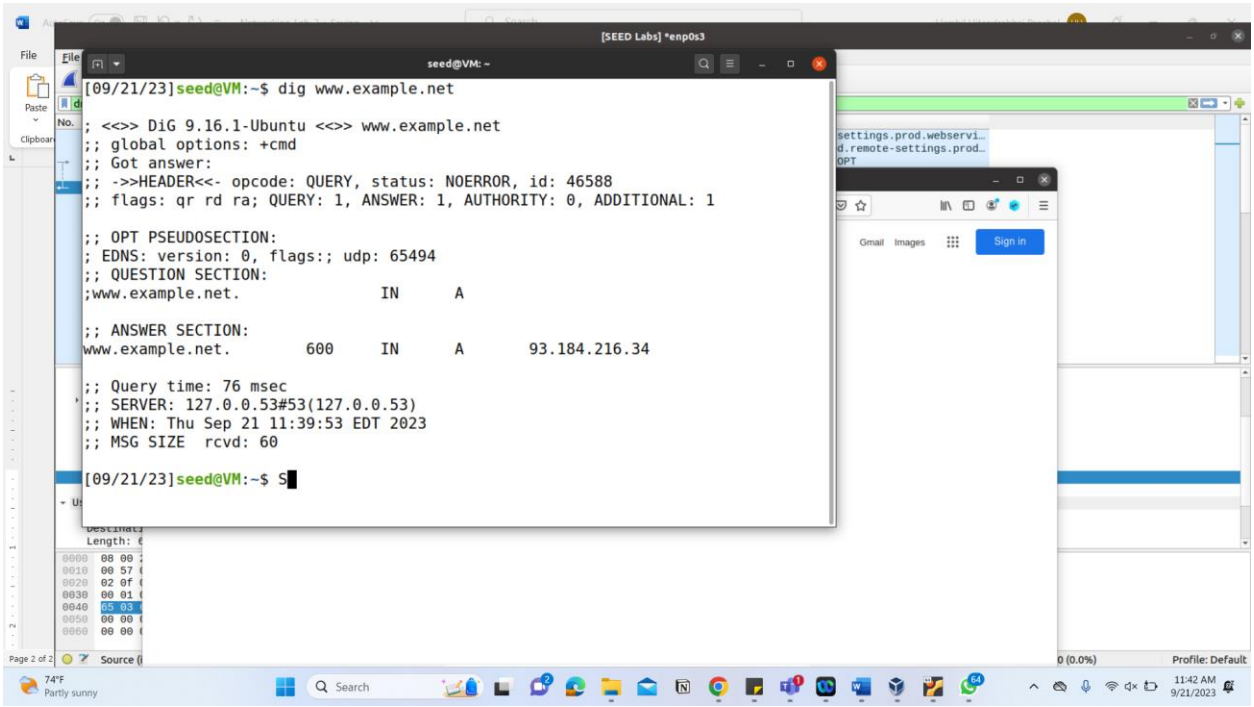
Course: Networking and Data Security COMP8677-1-R-2023F

Professor: Dr. Shaoquan Jiang

Prepared by

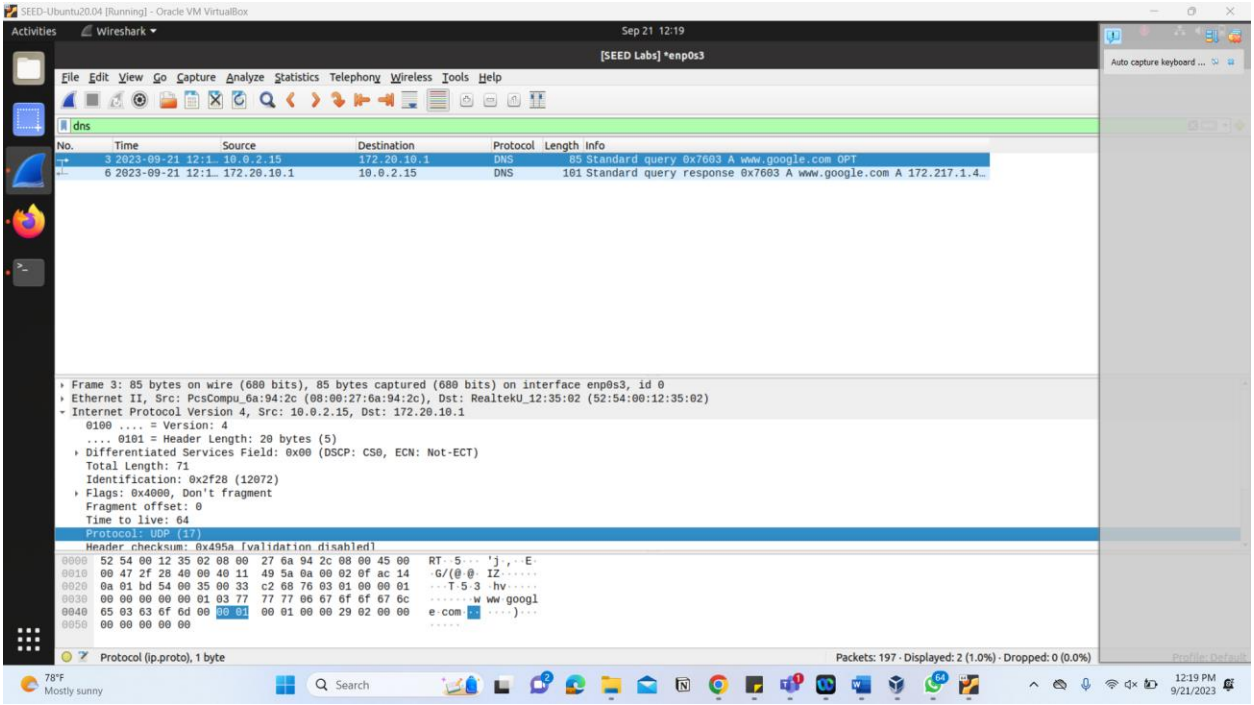
Harshil Hitendrabhai Panchal (110096129)

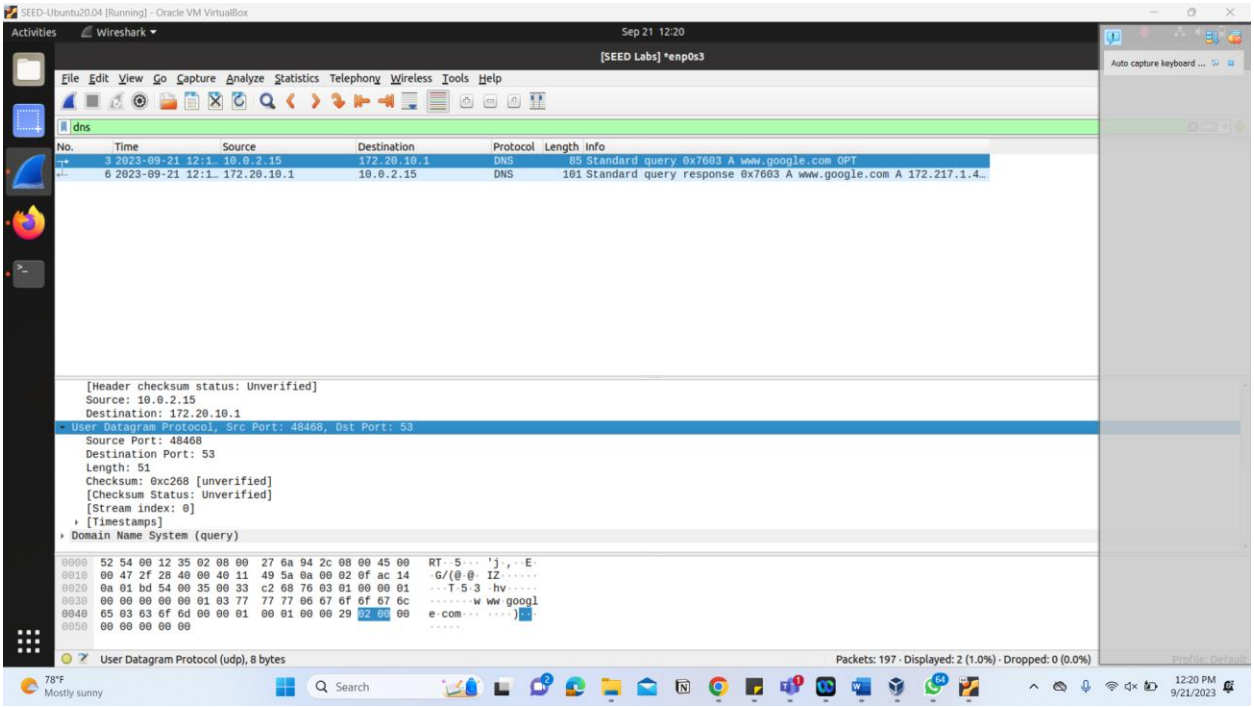
1.a. Try $ dig www.example.net to find out its ip address.



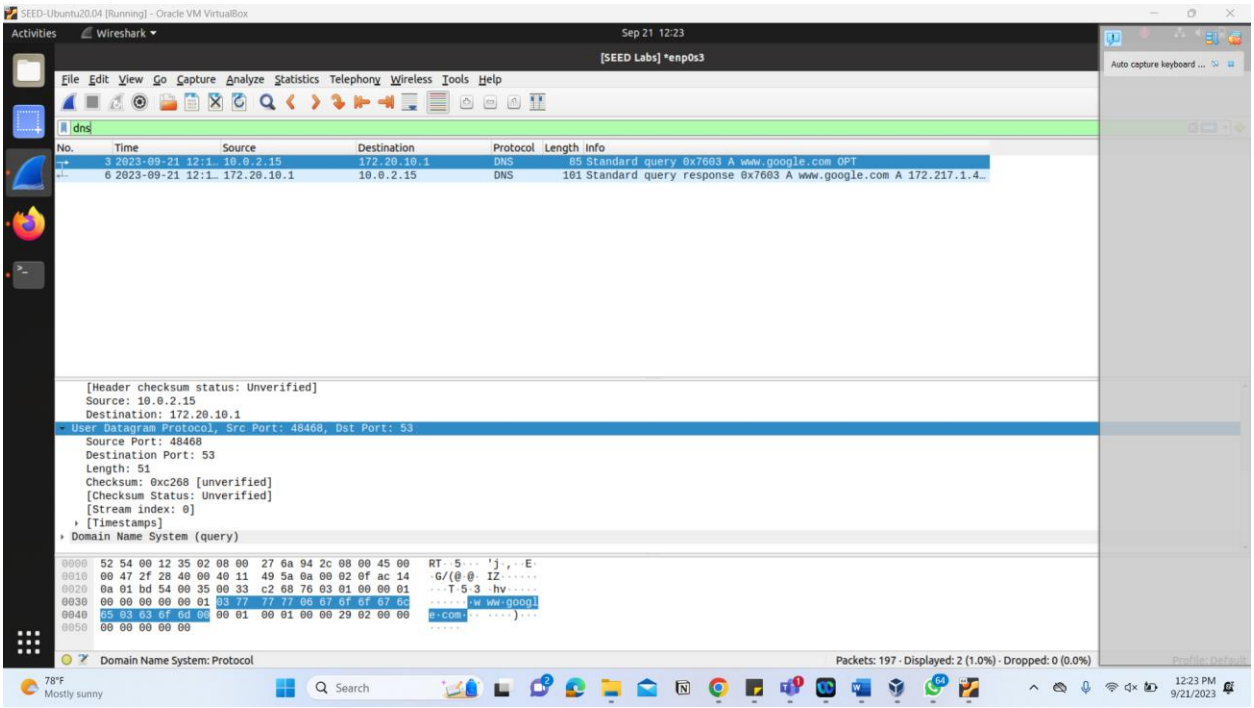
1.b. run Wireshark on your VM, then $ dig www.example.net and stop wireshark. Look at the DNS request packet (using filter DNS to find it easily), confirm that the transport layer protocol is UDP. What are the values of this UDP header (you need to first check the header fields learned in class)?

- **Used www.google.com instead of www.example.net**


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 12:19
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
3 2023-09-21 12:1… 10.0.2.15 172.20.10.1 DNS 85 Standard query 0x7603 A www.google.com OPT
6 2023-09-21 12:1… 172.20.10.1 10.0.2.15 DNS 101 Standard query response 0x7603 A www.google.com A 172.217.1.4…
Frame 3: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_6a:94:2c (08:00:27:6a:94:2c), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.20.10.1
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 71
Identification: 0x2f28 (12072)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0x495a [validation disabled]
0000 52 54 00 12 35 02 08 00 27 6a 94 2c 08 00 45 00
0010 00 47 2f 28 40 00 40 11 49 5a 0a 00 02 0f ac 14
0020 0a 01 bd 54 00 35 00 33 c2 68 76 03 01 00 00 01
0030 00 00 00 00 00 01 03 77 77 77 06 67 6f 6f 67 6c
0040 65 03 63 6f 6d 00 00 01 00 01 00 00 29 02 00 00
0050 00 00 00 00 00
Protocol (ip.proto), 1 byte
Packets: 197 · Displayed: 2 (1.0%) · Dropped: 0 (0.0%)
78°F
Mostly sunny
Search
12:19 PM
9/21/2023

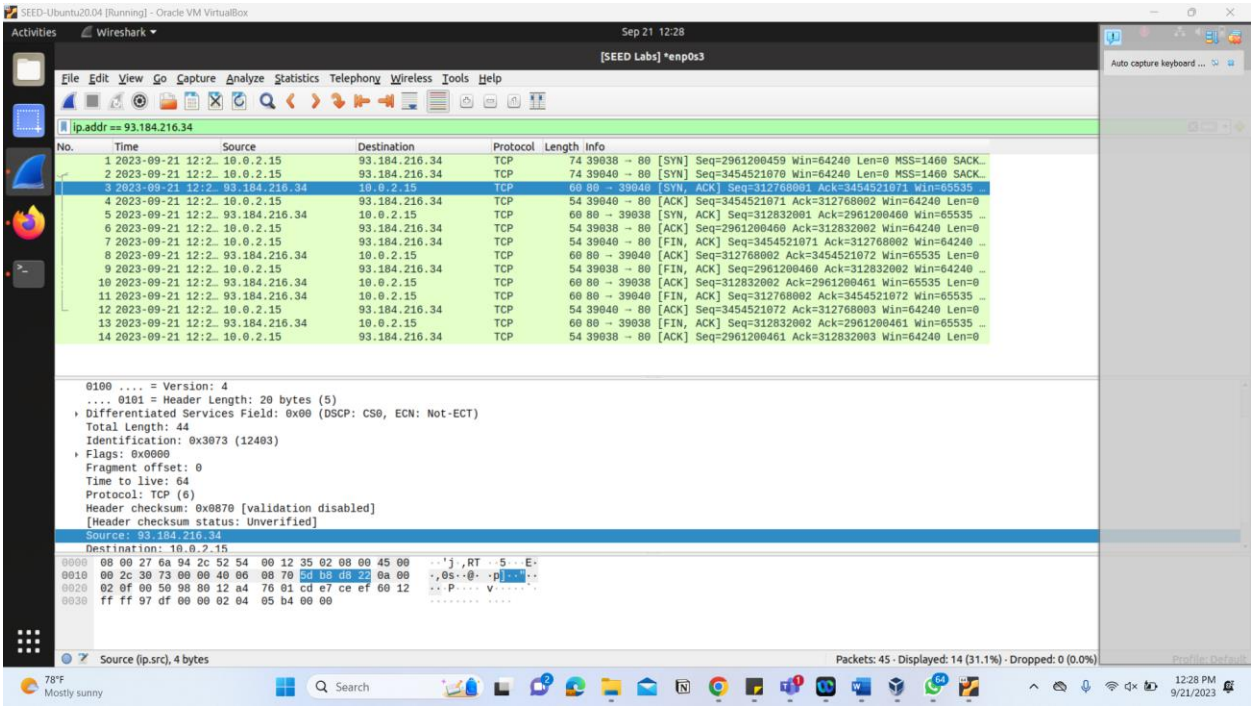

SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 12:20
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
3 2023-09-21 12:1… 10.0.2.15 172.20.10.1 DNS 85 Standard query 0x7603 A www.google.com OPT
6 2023-09-21 12:1… 172.20.10.1 10.0.2.15 DNS 101 Standard query response 0x7603 A www.google.com A 172.217.1.4…
[Header checksum status: Unverified]
Source: 10.0.2.15
Destination: 172.20.10.1
User Datagram Protocol, Src Port: 48468, Dst Port: 53
Source Port: 48468
Destination Port: 53
Length: 51
Checksum: 0xc268 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
Domain Name System (query)
0000 52 54 00 12 35 02 08 00 27 6a 94 2c 08 00 45 00
0010 00 47 2f 28 40 00 40 11 49 5a 0a 00 02 0f ac 14
0020 0a 01 bd 54 00 35 00 33 c2 68 76 03 01 00 00 01
0030 00 00 00 00 00 01 03 77 77 77 06 67 6f 6f 67 6c
0040 65 03 63 6f 6d 00 00 01 00 01 00 00 29 02 06 00
0050 00 00 00 00 00
User Datagram Protocol (udp), 8 bytes
Packets: 197 · Displayed: 2 (1.0%) · Dropped: 0 (0.0%)
78°F
Mostly sunny
Search
12:20 PM
9/21/2023

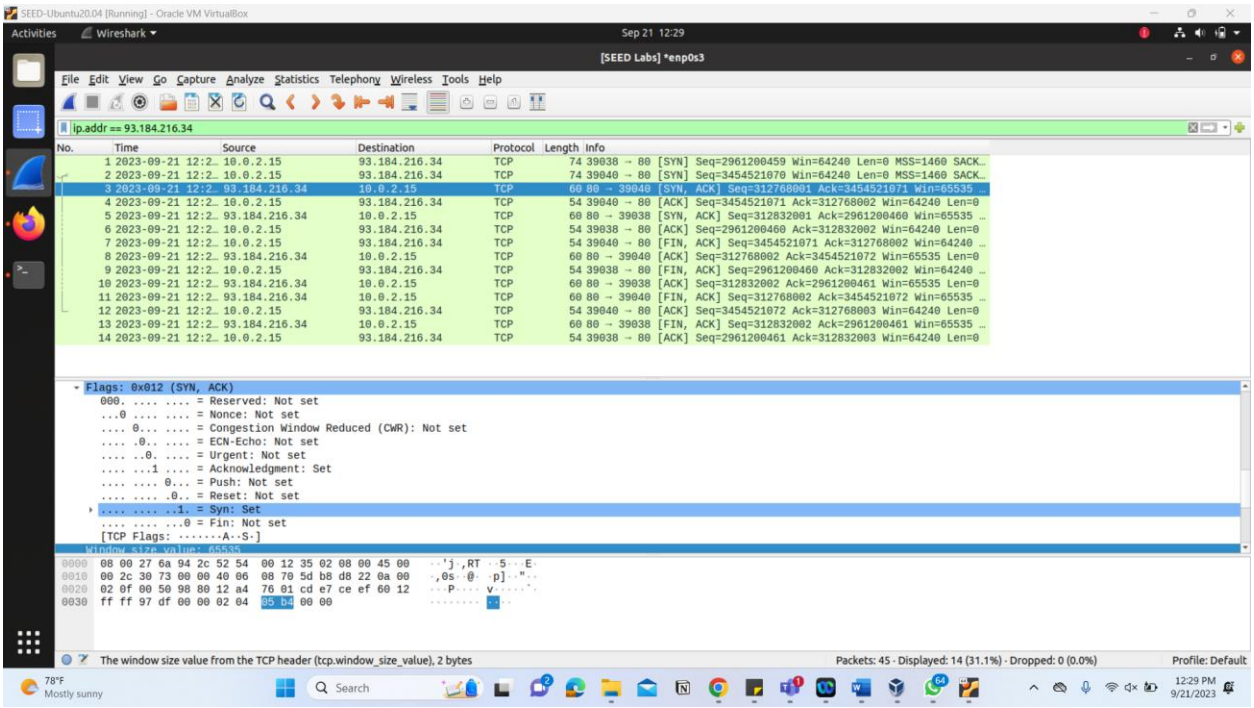
1.c. In the DNS request packet in step b, the destination IP is your local DNS server's IP. What is this value? As said, DNS is serviced by UDP and has no connection setup before sending DNS request. You can confirm this by checking that there is no any packet in Wireshark exchanged between your VM and local DNS server, prior to the DNS request packet (show the screen shot of the window of Wireshark for the list of packets).



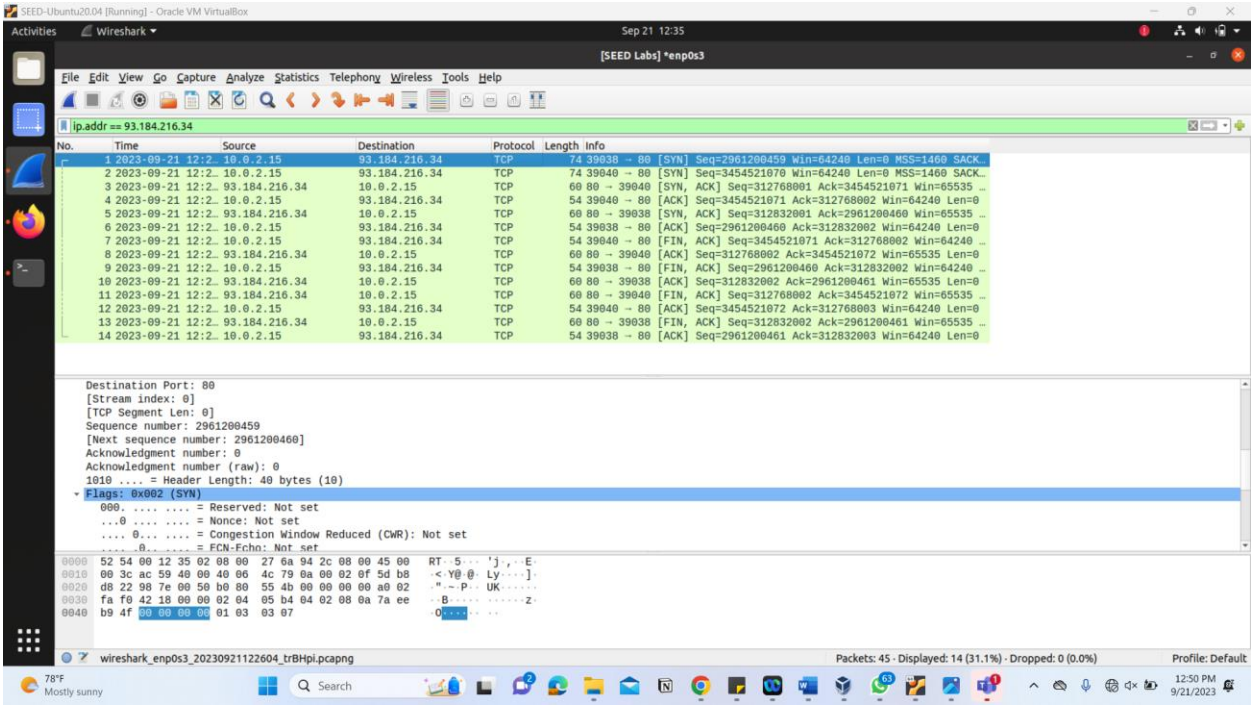
In the above Screenshot, you can see that there are only 2 DNS packet exchanged.

2.

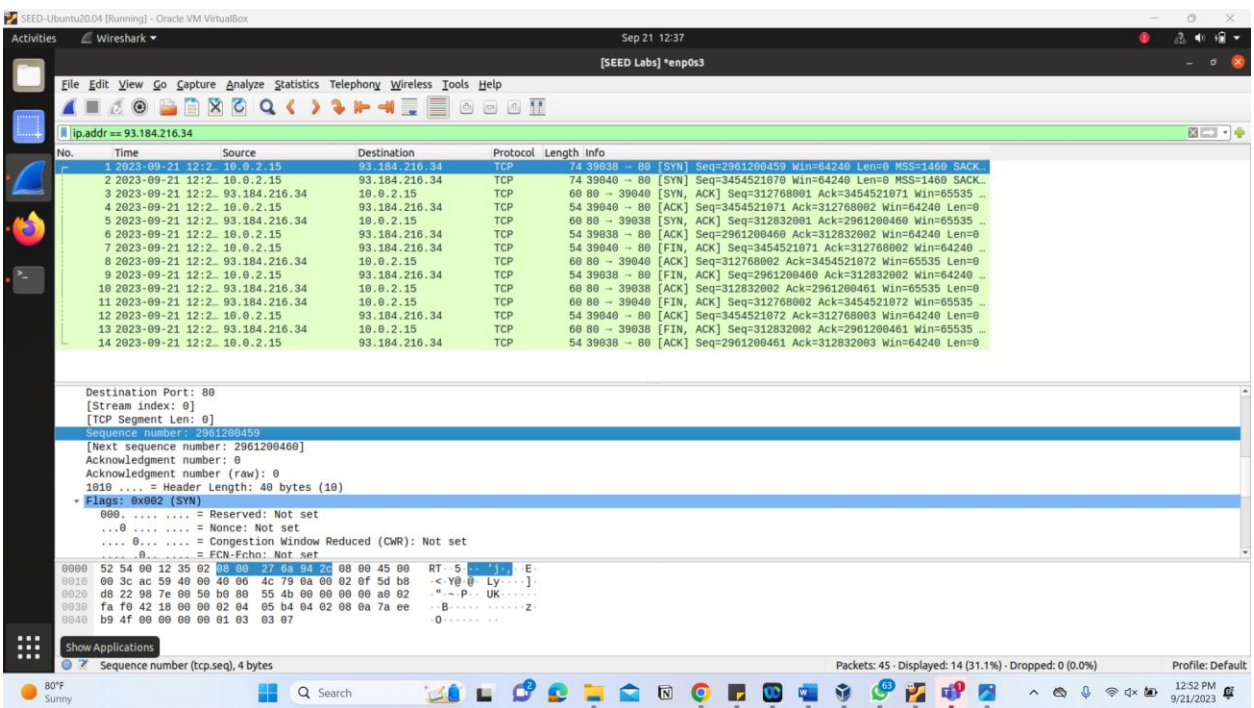

SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 12:28
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 93.184.216.34
No. Time Source Destination Protocol Length Info
1 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 74 39038 → 80 [SYN] Seq=2961200459 Win=64240 Len=0 MSS=1460 SACK…
2 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 74 39040 → 80 [SYN] Seq=3454521070 Win=64240 Len=0 MSS=1460 SACK…
3 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [SYN, ACK] Seq=312768001 Ack=3454521071 Win=65535 …
4 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [ACK] Seq=3454521071 Ack=312768002 Win=64240 Len=0
5 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [SYN, ACK] Seq=312832001 Ack=2961200460 Win=65535 …
6 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [ACK] Seq=2961200460 Ack=312832002 Win=64240 Len=0
7 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [FIN, ACK] Seq=3454521071 Ack=312768002 Win=64240 …
8 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [ACK] Seq=312768002 Ack=3454521072 Win=65535 Len=0
9 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [FIN, ACK] Seq=2961200460 Ack=312832002 Win=64240 …
10 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [ACK] Seq=312832002 Ack=2961200461 Win=65535 Len=0
11 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [FIN, ACK] Seq=312768002 Ack=3454521072 Win=65535 …
12 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [ACK] Seq=3454521072 Ack=312768003 Win=64240 Len=0
13 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [FIN, ACK] Seq=312832002 Ack=2961200461 Win=65535 …
14 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [ACK] Seq=2961200461 Ack=312832003 Win=64240 Len=0
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 44
Identification: 0x3073 (12403)
Flags: 0x0000
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x0870 [validation disabled]
[Header checksum status: Unverified]
Source: 93.184.216.34
Destination: 10.0.2.15
0000 08 00 27 6a 94 2c 52 54 00 12 35 02 08 00 45 00
0010 00 2c 30 73 00 00 40 06 08 70 5d b8 d8 22 0a 00
0020 02 0f 00 50 98 80 12 a4 76 01 cd e7 ce ef 60 12
0030 ff ff 97 df 00 00 02 04 05 b4 00 00
Source (ip.src), 4 bytes
Packets: 45 · Displayed: 14 (31.1%) · Dropped: 0 (0.0%)
Profile: Default
78°F
Mostly sunny
Search
12:28 PM
9/21/2023


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 12:29
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 93.184.216.34
No. Time Source Destination Protocol Length Info
1 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 74 39038 → 80 [SYN] Seq=2961200459 Win=64240 Len=0 MSS=1460 SACK…
2 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 74 39040 → 80 [SYN] Seq=3454521070 Win=64240 Len=0 MSS=1460 SACK…
3 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [SYN, ACK] Seq=312768001 Ack=3454521071 Win=65535 …
4 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [ACK] Seq=3454521071 Ack=312768002 Win=64240 Len=0
5 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [SYN, ACK] Seq=312832001 Ack=2961200460 Win=65535 …
6 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [ACK] Seq=2961200460 Ack=312832002 Win=64240 Len=0
7 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [FIN, ACK] Seq=3454521071 Ack=312768002 Win=64240 …
8 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [ACK] Seq=312768002 Ack=3454521072 Win=65535 Len=0
9 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [FIN, ACK] Seq=2961200460 Ack=312832002 Win=64240 …
10 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [ACK] Seq=312832002 Ack=2961200461 Win=65535 Len=0
11 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [FIN, ACK] Seq=312768002 Ack=3454521072 Win=65535 …
12 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [ACK] Seq=3454521072 Ack=312768003 Win=64240 Len=0
13 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [FIN, ACK] Seq=312832002 Ack=2961200461 Win=65535 …
14 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [ACK] Seq=2961200461 Ack=312832003 Win=64240 Len=0
Flags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....1. = Syn: Set
....0 = Fin: Not set
[TCP Flags: ·····A··S·]
Window size value: 65535
0000 08 00 27 6a 94 2c 52 54 00 12 35 02 08 00 45 00
0010 00 2c 30 73 00 00 40 06 08 70 5d b8 d8 22 0a 00
0020 02 0f 00 50 98 80 12 a4 76 01 cd e7 ce ef 60 12
0030 ff ff 97 df 00 00 02 04 05 b4 00 00
The window size value from the TCP header (tcp.window_size_value), 2 bytes
Packets: 45 · Displayed: 14 (31.1%) · Dropped: 0 (0.0%)
Profile: Default
78°F
Mostly sunny
Search
12:29 PM
9/21/2023

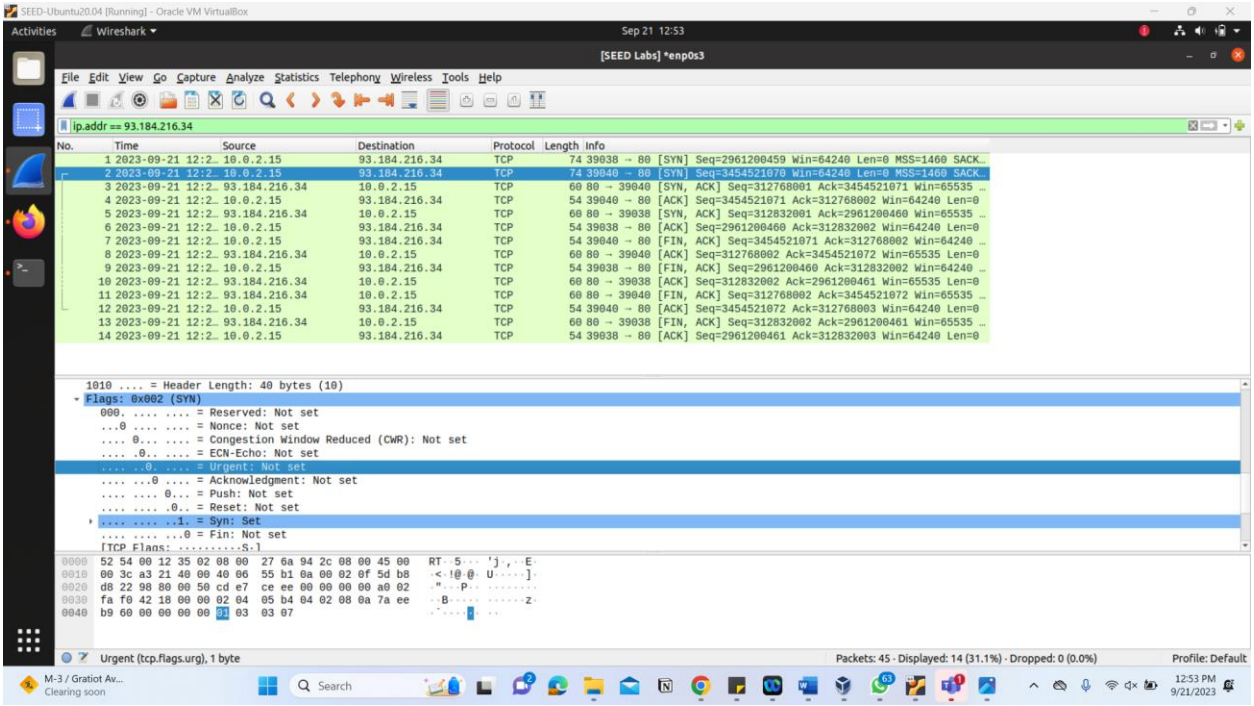
3.a.


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 12:35
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 93.184.216.34
No. Time Source Destination Protocol Length Info
1 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 74 39038 → 80 [SYN] Seq=2961200459 Win=64240 Len=0 MSS=1460 SACK…
2 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 74 39040 → 80 [SYN] Seq=3454521070 Win=64240 Len=0 MSS=1460 SACK…
3 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [SYN, ACK] Seq=312768001 Ack=3454521071 Win=65535 …
4 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [ACK] Seq=3454521071 Ack=312768002 Win=64240 Len=0
5 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [SYN, ACK] Seq=312832001 Ack=2961200460 Win=65535 …
6 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [ACK] Seq=2961200460 Ack=312832002 Win=64240 Len=0
7 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [FIN, ACK] Seq=3454521071 Ack=312768002 Win=64240 …
8 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [ACK] Seq=312768002 Ack=3454521072 Win=65535 Len=0
9 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [FIN, ACK] Seq=2961200460 Ack=312832002 Win=64240 …
10 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [ACK] Seq=312832002 Ack=2961200461 Win=65535 Len=0
11 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [FIN, ACK] Seq=312768002 Ack=3454521072 Win=65535 …
12 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [ACK] Seq=3454521072 Ack=312768003 Win=64240 Len=0
13 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [FIN, ACK] Seq=312832002 Ack=2961200461 Win=65535 …
14 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [ACK] Seq=2961200461 Ack=312832003 Win=64240 Len=0
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 2961200459
[Next sequence number: 2961200460]
Acknowledgment number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... ..0. .... = ECN-Echo: Not set
0000 52 54 00 12 35 02 08 00 27 6a 94 2c 08 00 45 00
0010 00 3c ac 59 40 00 40 06 4c 79 0a 00 02 0f 5d b8
0020 d8 22 98 7e 00 50 b0 80 55 4b 00 00 00 00 a0 02
0030 fa f0 42 18 00 00 02 04 05 b4 04 02 08 0a 7a ee
0040 b9 4f 00 00 00 00 01 03 03 07
wireshark_enp0s3_20230921122604_trBHpi.pcapng
Packets: 45 · Displayed: 14 (31.1%) · Dropped: 0 (0.0%)
Profile: Default
78°F
Mostly sunny
Search
12:50 PM
9/21/2023

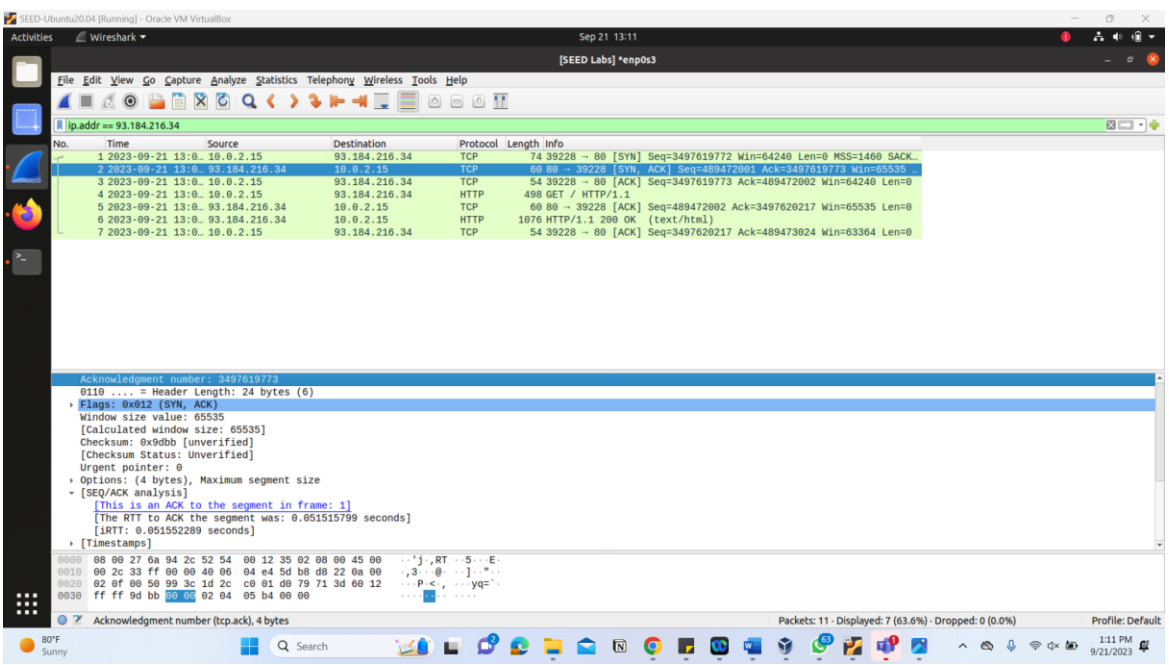
3.b.

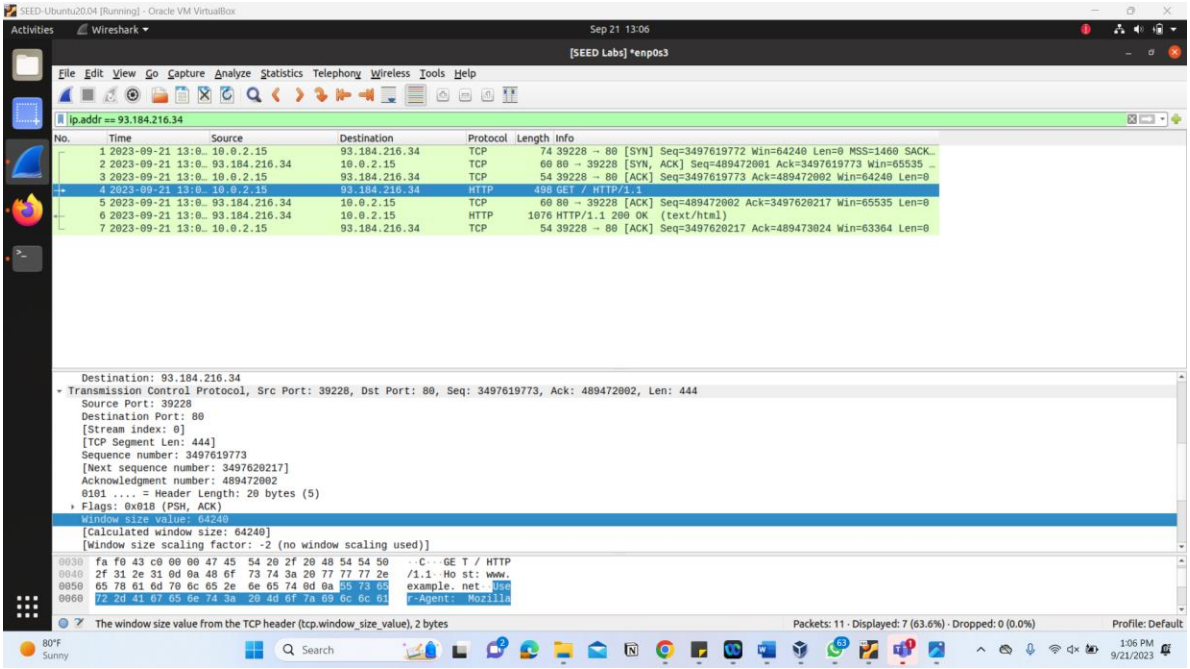

SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 12:37
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 93.184.216.34
No. Time Source Destination Protocol Length Info
1 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 74 39038 → 80 [SYN] Seq=2961200459 Win=64240 Len=0 MSS=1460 SACK…
2 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 74 39040 → 80 [SYN] Seq=3454521070 Win=64240 Len=0 MSS=1460 SACK…
3 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [SYN, ACK] Seq=312768001 Ack=3454521071 Win=65535 …
4 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [ACK] Seq=3454521071 Ack=312768002 Win=64240 Len=0
5 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [SYN, ACK] Seq=312832001 Ack=2961200460 Win=65535 …
6 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [ACK] Seq=2961200460 Ack=312832002 Win=64240 Len=0
7 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [FIN, ACK] Seq=3454521071 Ack=312768002 Win=64240 …
8 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [ACK] Seq=312768002 Ack=3454521072 Win=65535 Len=0
9 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [FIN, ACK] Seq=2961200460 Ack=312832002 Win=64240 …
10 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [ACK] Seq=312832002 Ack=2961200461 Win=65535 Len=0
11 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [FIN, ACK] Seq=312768002 Ack=3454521072 Win=65535 …
12 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [ACK] Seq=3454521072 Ack=312768003 Win=64240 Len=0
13 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [FIN, ACK] Seq=312832002 Ack=2961200461 Win=65535 …
14 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [ACK] Seq=2961200461 Ack=312832003 Win=64240 Len=0
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 2961200459
[Next sequence number: 2961200460]
Acknowledgment number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... ..0. .... = ECN-Echo: Not set
0000 52 54 00 12 35 02 08 00 27 6a 94 2c 08 00 45 00
0010 00 3c ac 59 40 00 40 06 4c 79 0a 00 02 0f 5d b8
0020 d8 22 98 7e 00 50 b0 80 55 4b 00 00 00 00 a0 02
0030 fa f0 42 18 00 00 02 04 05 b4 04 02 08 0a 7a ee
0040 b9 4f 00 00 00 00 01 03 03 07
Show Applications
Sequence number (tcp.seq), 4 bytes
Packets: 45 · Displayed: 14 (31.1%) · Dropped: 0 (0.0%)
Profile: Default
80°F
Sunny
Search
12:52 PM
9/21/2023

3.c.

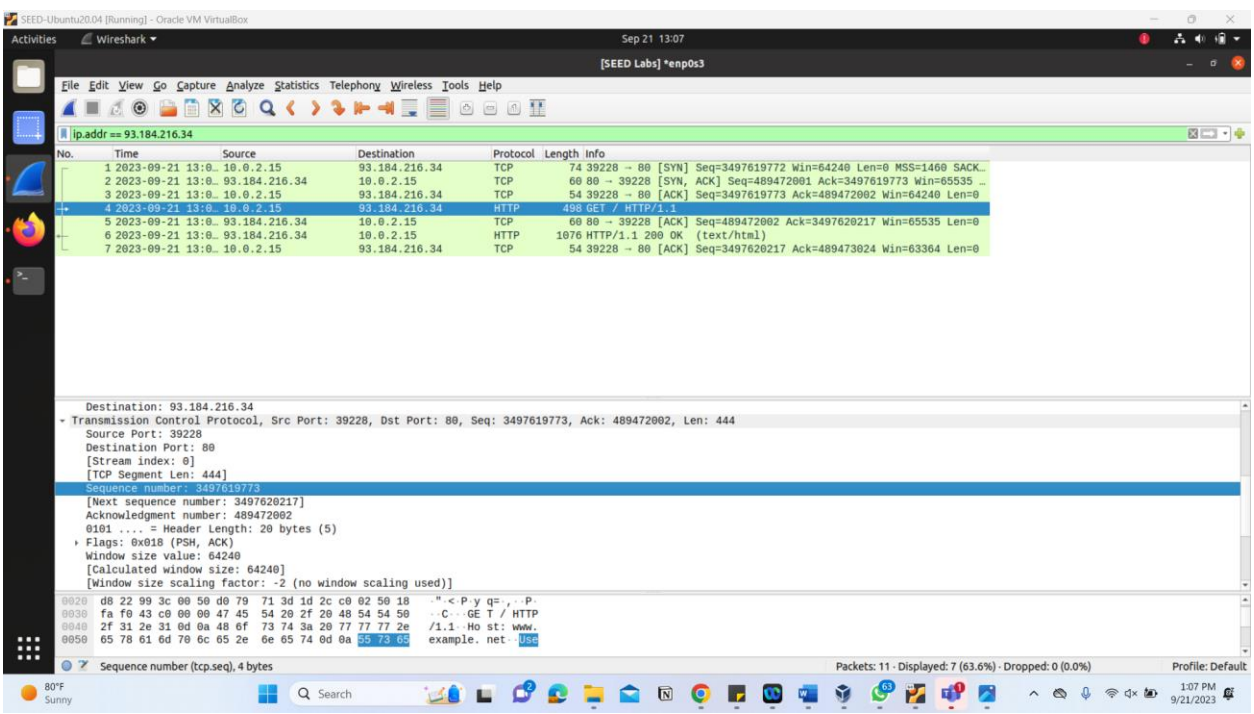

SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 12:53
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 93.184.216.34
No. Time Source Destination Protocol Length Info
1 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 74 39038 → 80 [SYN] Seq=2961200459 Win=64240 Len=0 MSS=1460 SACK…
2 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 74 39040 → 80 [SYN] Seq=3454521070 Win=64240 Len=0 MSS=1460 SACK…
3 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [SYN, ACK] Seq=312768001 Ack=3454521071 Win=65535 …
4 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [ACK] Seq=3454521071 Ack=312768002 Win=64240 Len=0
5 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [SYN, ACK] Seq=312832001 Ack=2961200460 Win=65535 …
6 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [ACK] Seq=2961200460 Ack=312832002 Win=64240 Len=0
7 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [FIN, ACK] Seq=3454521071 Ack=312768002 Win=64240 …
8 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [ACK] Seq=312768002 Ack=3454521072 Win=65535 Len=0
9 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [FIN, ACK] Seq=2961200460 Ack=312832002 Win=64240 …
10 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [ACK] Seq=312832002 Ack=2961200461 Win=65535 Len=0
11 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39040 [FIN, ACK] Seq=312768002 Ack=3454521072 Win=65535 …
12 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39040 → 80 [ACK] Seq=3454521072 Ack=312768003 Win=64240 Len=0
13 2023-09-21 12:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39038 [FIN, ACK] Seq=312832002 Ack=2961200461 Win=65535 …
14 2023-09-21 12:2… 10.0.2.15 93.184.216.34 TCP 54 39038 → 80 [ACK] Seq=2961200461 Ack=312832003 Win=64240 Len=0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....1. = Syn: Set
....0 = Fin: Not set
[TCP Flags: ·····S·]
Urgent (tcp.flags.urg), 1 byte
Packets: 45 · Displayed: 14 (31.1%) · Dropped: 0 (0.0%)
Profile: Default
M-3 / Gratiot Av…
Clearing soon
Search
12:53 PM
9/21/2023

3.d.

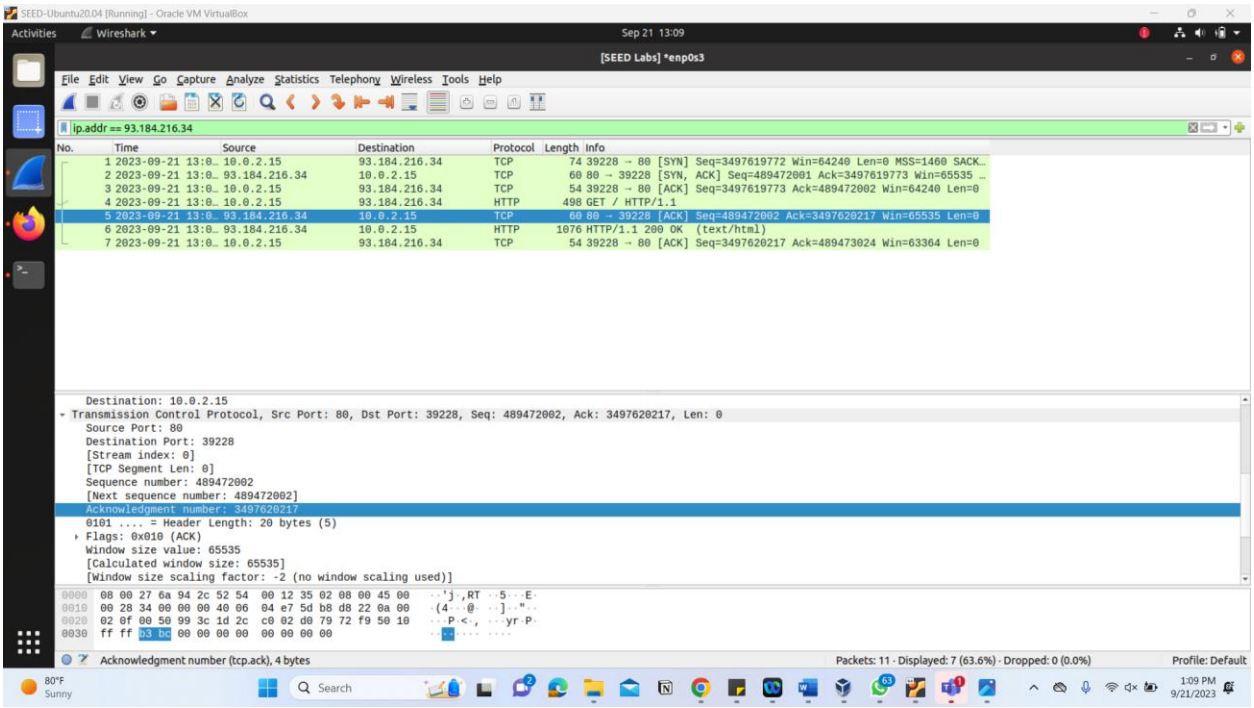

SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 13:11
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 93.184.216.34
No. Time Source Destination Protocol Length Info
1 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 74 39228 → 80 [SYN] Seq=3497619772 Win=64240 Len=0 MSS=1460 SACK…
2 2023-09-21 13:0… 93.184.216.34 10.0.2.15 TCP 60 80 → 39228 [SYN, ACK] Seq=489472001 Ack=3497619773 Win=65535 …
3 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 54 39228 → 80 [ACK] Seq=3497619773 Ack=489472002 Win=64240 Len=0
4 2023-09-21 13:0… 10.0.2.15 93.184.216.34 HTTP 498 GET / HTTP/1.1
5 2023-09-21 13:0… 93.184.216.34 10.0.2.15 TCP 60 80 → 39228 [ACK] Seq=489472002 Ack=3497620217 Win=65535 Len=0
6 2023-09-21 13:0… 93.184.216.34 10.0.2.15 HTTP 1076 HTTP/1.1 200 OK (text/html)
7 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 54 39228 → 80 [ACK] Seq=3497620217 Ack=489473024 Win=63364 Len=0
Acknowledgment number: 3497619773
0110 .... = Header Length: 24 bytes (6)
Flags: 0x012 (SYN, ACK)
Window size value: 65535
[Calculated window size: 65535]
Checksum: 0x9dbb [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (4 bytes), Maximum segment size
[SEQ/ACK analysis]
[This is an ACK to the segment in frame: 1]
[The RTT to ACK the segment was: 0.051515799 seconds]
[iRTT: 0.051552289 seconds]
[Timestamps]
Acknowledgment number (tcp.ack), 4 bytes
Packets: 11 · Displayed: 7 (63.6%) · Dropped: 0 (0.0%)
Profile: Default
80°F
Sunny
Search
1:11 PM
9/21/2023


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 13:06
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 93.184.216.34
No. Time Source Destination Protocol Length Info
1 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 74 39228 → 80 [SYN] Seq=3497619772 Win=64240 Len=0 MSS=1460 SACK…
2 2023-09-21 13:0… 93.184.216.34 10.0.2.15 TCP 60 80 → 39228 [SYN, ACK] Seq=489472001 Ack=3497619773 Win=65535 …
3 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 54 39228 → 80 [ACK] Seq=3497619773 Ack=489472002 Win=64240 Len=0
4 2023-09-21 13:0… 10.0.2.15 93.184.216.34 HTTP 498 GET / HTTP/1.1
5 2023-09-21 13:0… 93.184.216.34 10.0.2.15 TCP 60 80 → 39228 [ACK] Seq=489472002 Ack=3497620217 Win=65535 Len=0
6 2023-09-21 13:0… 93.184.216.34 10.0.2.15 HTTP 1076 HTTP/1.1 200 OK (text/html)
7 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 54 39228 → 80 [ACK] Seq=3497620217 Ack=489473024 Win=63364 Len=0
Destination: 93.184.216.34
Transmission Control Protocol, Src Port: 39228, Dst Port: 80, Seq: 3497619773, Ack: 489472002, Len: 444
Source Port: 39228
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 444]
Sequence number: 3497619773
[Next sequence number: 3497620217]
Acknowledgment number: 489472002
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
0030 fa f0 43 c0 00 00 47 45 54 20 2f 20 48 54 54 50 ··C···GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1··Ho st: www.
0050 65 78 61 6d 70 6c 65 2e 6e 65 74 0d 0a 55 73 65 example. net··Use
0060 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
The window size value from the TCP header (tcp.window_size_value), 2 bytes
Packets: 11 · Displayed: 7 (63.6%) · Dropped: 0 (0.0%)
Profile: Default
80°F Sunny
Search
1:06 PM 9/21/2023

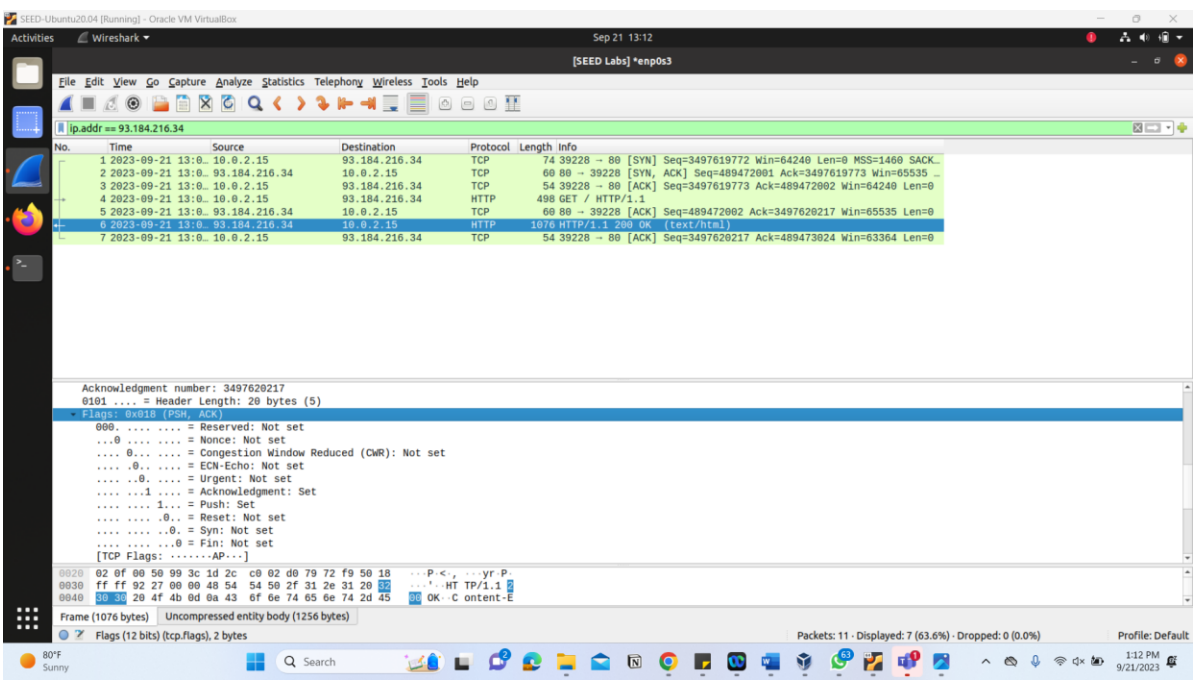
3.e.


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 13:07
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 93.184.216.34
No. Time Source Destination Protocol Length Info
1 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 74 39228 → 80 [SYN] Seq=3497619772 Win=64240 Len=0 MSS=1460 SACK…
2 2023-09-21 13:0… 93.184.216.34 10.0.2.15 TCP 60 80 → 39228 [SYN, ACK] Seq=489472001 Ack=3497619773 Win=65535 …
3 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 54 39228 → 80 [ACK] Seq=3497619773 Ack=489472002 Win=64240 Len=0
4 2023-09-21 13:0… 10.0.2.15 93.184.216.34 HTTP 498 GET / HTTP/1.1
5 2023-09-21 13:0… 93.184.216.34 10.0.2.15 TCP 60 80 → 39228 [ACK] Seq=489472002 Ack=3497620217 Win=65535 Len=0
6 2023-09-21 13:0… 93.184.216.34 10.0.2.15 HTTP 1076 HTTP/1.1 200 OK (text/html)
7 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 54 39228 → 80 [ACK] Seq=3497620217 Ack=489473024 Win=63364 Len=0
Destination: 93.184.216.34
Transmission Control Protocol, Src Port: 39228, Dst Port: 80, Seq: 3497619773, Ack: 489472002, Len: 444
Source Port: 39228
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 444]
Sequence number: 3497619773
[Next sequence number: 3497620217]
Acknowledgment number: 489472002
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 64240
[Calculated window size: 64240]
[Window size scaling factor: -2 (no window scaling used)]
0020 d8 22 99 3c 00 50 d0 79 71 3d 1d 2c c0 02 50 18 ·"·<·P·y q=·,··P·
0030 fa f0 43 c0 00 00 47 45 54 20 2f 20 48 54 54 50 ··C···GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1··Ho st: www.
0050 65 78 61 6d 70 6c 65 2e 6e 65 74 0d 0a 55 73 65 example. net··Use
Sequence number (tcp.seq), 4 bytes
Packets: 11 · Displayed: 7 (63.6%) · Dropped: 0 (0.0%)
Profile: Default
80°F Sunny
Search
1:07 PM 9/21/2023

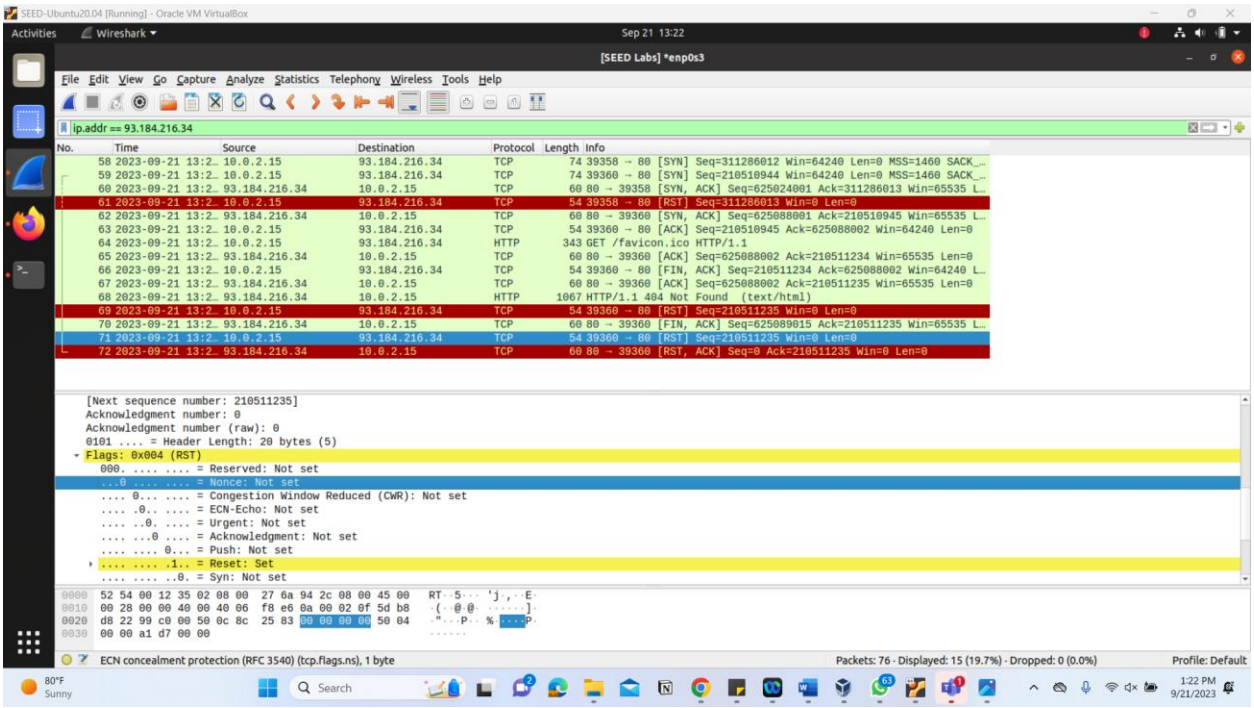
3.f.


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 13:09
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 93.184.216.34
No. Time Source Destination Protocol Length Info
1 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 74 39228 → 80 [SYN] Seq=3497619772 Win=64240 Len=0 MSS=1460 SACK…
2 2023-09-21 13:0… 93.184.216.34 10.0.2.15 TCP 60 80 → 39228 [SYN, ACK] Seq=489472001 Ack=3497619773 Win=65535 …
3 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 54 39228 → 80 [ACK] Seq=3497619773 Ack=489472002 Win=64240 Len=0
4 2023-09-21 13:0… 10.0.2.15 93.184.216.34 HTTP 498 GET / HTTP/1.1
5 2023-09-21 13:0… 93.184.216.34 10.0.2.15 TCP 60 80 → 39228 [ACK] Seq=489472002 Ack=3497620217 Win=65535 Len=0
6 2023-09-21 13:0… 93.184.216.34 10.0.2.15 HTTP 1076 HTTP/1.1 200 OK (text/html)
7 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 54 39228 → 80 [ACK] Seq=3497620217 Ack=489473024 Win=63364 Len=0
Destination: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 39228, Seq: 489472002, Ack: 3497620217, Len: 0
Source Port: 80
Destination Port: 39228
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 489472002
[Next sequence number: 489472002]
Acknowledgment number: 3497620217
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window size value: 65535
[Calculated window size: 65535]
[Window size scaling factor: -2 (no window scaling used)]
Acknowledgment number (tcp.ack), 4 bytes
Packets: 11 · Displayed: 7 (63.6%) · Dropped: 0 (0.0%)
Profile: Default
80°F Sunny
Search
1:09 PM 9/21/2023

3.g.


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 13:12
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 93.184.216.34
No. Time Source Destination Protocol Length Info
1 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 74 39228 → 80 [SYN] Seq=3497619772 Win=64240 Len=0 MSS=1460 SACK…
2 2023-09-21 13:0… 93.184.216.34 10.0.2.15 TCP 60 80 → 39228 [SYN, ACK] Seq=489472001 Ack=3497619773 Win=65535 …
3 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 54 39228 → 80 [ACK] Seq=3497619773 Ack=489472002 Win=64240 Len=0
4 2023-09-21 13:0… 10.0.2.15 93.184.216.34 HTTP 498 GET / HTTP/1.1
5 2023-09-21 13:0… 93.184.216.34 10.0.2.15 TCP 60 80 → 39228 [ACK] Seq=489472002 Ack=3497620217 Win=65535 Len=0
6 2023-09-21 13:0… 93.184.216.34 10.0.2.15 HTTP 1076 HTTP/1.1 200 OK (text/html)
7 2023-09-21 13:0… 10.0.2.15 93.184.216.34 TCP 54 39228 → 80 [ACK] Seq=3497620217 Ack=489473024 Win=63364 Len=0
Acknowledgment number: 3497620217
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····AP···]
Frame (1076 bytes)
Uncompressed entity body (1256 bytes)
Flags (12 bits) (tcp.flags), 2 bytes
Packets: 11 · Displayed: 7 (63.6%) · Dropped: 0 (0.0%)
Profile: Default
80°F Sunny
Search
1:12 PM 9/21/2023

3.h.


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities
Wireshark
Sep 21 13:22
[SEED Labs] *enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 93.184.216.34
No. Time Source Destination Protocol Length Info
58 2023-09-21 13:2… 10.0.2.15 93.184.216.34 TCP 74 39358 → 80 [SYN] Seq=311286012 Win=64240 Len=0 MSS=1460 SACK_…
59 2023-09-21 13:2… 10.0.2.15 93.184.216.34 TCP 74 39360 → 80 [SYN] Seq=210510944 Win=64240 Len=0 MSS=1460 SACK_…
60 2023-09-21 13:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39358 [SYN, ACK] Seq=625024001 Ack=311286013 Win=65535 L…
61 2023-09-21 13:2… 10.0.2.15 93.184.216.34 TCP 54 39358 → 80 [RST] Seq=311286013 Win=0 Len=0
62 2023-09-21 13:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39360 [SYN, ACK] Seq=625088001 Ack=210510945 Win=65535 L…
63 2023-09-21 13:2… 10.0.2.15 93.184.216.34 TCP 54 39360 → 80 [ACK] Seq=210510945 Ack=625088002 Win=64240 Len=0
64 2023-09-21 13:2… 10.0.2.15 93.184.216.34 HTTP 343 GET /favicon.ico HTTP/1.1
65 2023-09-21 13:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39360 [ACK] Seq=625088002 Ack=210511234 Win=65535 Len=0
66 2023-09-21 13:2… 10.0.2.15 93.184.216.34 TCP 54 39360 → 80 [FIN, ACK] Seq=210511234 Ack=625088002 Win=64240 L…
67 2023-09-21 13:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39360 [ACK] Seq=625088002 Ack=210511235 Win=65535 Len=0
68 2023-09-21 13:2… 93.184.216.34 10.0.2.15 HTTP 1067 HTTP/1.1 404 Not Found (text/html)
69 2023-09-21 13:2… 10.0.2.15 93.184.216.34 TCP 54 39360 → 80 [RST] Seq=210511235 Win=0 Len=0
70 2023-09-21 13:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39360 [FIN, ACK] Seq=625089015 Ack=210511235 Win=65535 L…
71 2023-09-21 13:2… 10.0.2.15 93.184.216.34 TCP 54 39360 → 80 [RST] Seq=210511235 Win=0 Len=0
72 2023-09-21 13:2… 93.184.216.34 10.0.2.15 TCP 60 80 → 39360 [RST, ACK] Seq=0 Ack=210511235 Win=0 Len=0
[Next sequence number: 210511235]
Acknowledgment number: 0
Acknowledgment number (raw): 0
0101 .... = Header Length: 20 bytes (5)
Flags: 0x004 (RST)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .1.. = Reset: Set
....0. = Syn: Not set
0000 52 54 00 12 35 02 08 00 27 6a 94 2c 08 00 45 00
0010 00 28 00 00 40 00 40 06 f8 e6 0a 00 02 0f 5d b8
0020 d8 22 99 c0 00 50 0c 8c 25 83 00 00 00 00 50 04
0030 00 00 a1 d7 00 00
ECN concealment protection (RFC 3540) (tcp.flags.ns), 1 byte
Packets: 76 · Displayed: 15 (19.7%) · Dropped: 0 (0.0%)
Profile: Default
80°F
Sunny
Search
1:22 PM
9/21/2023