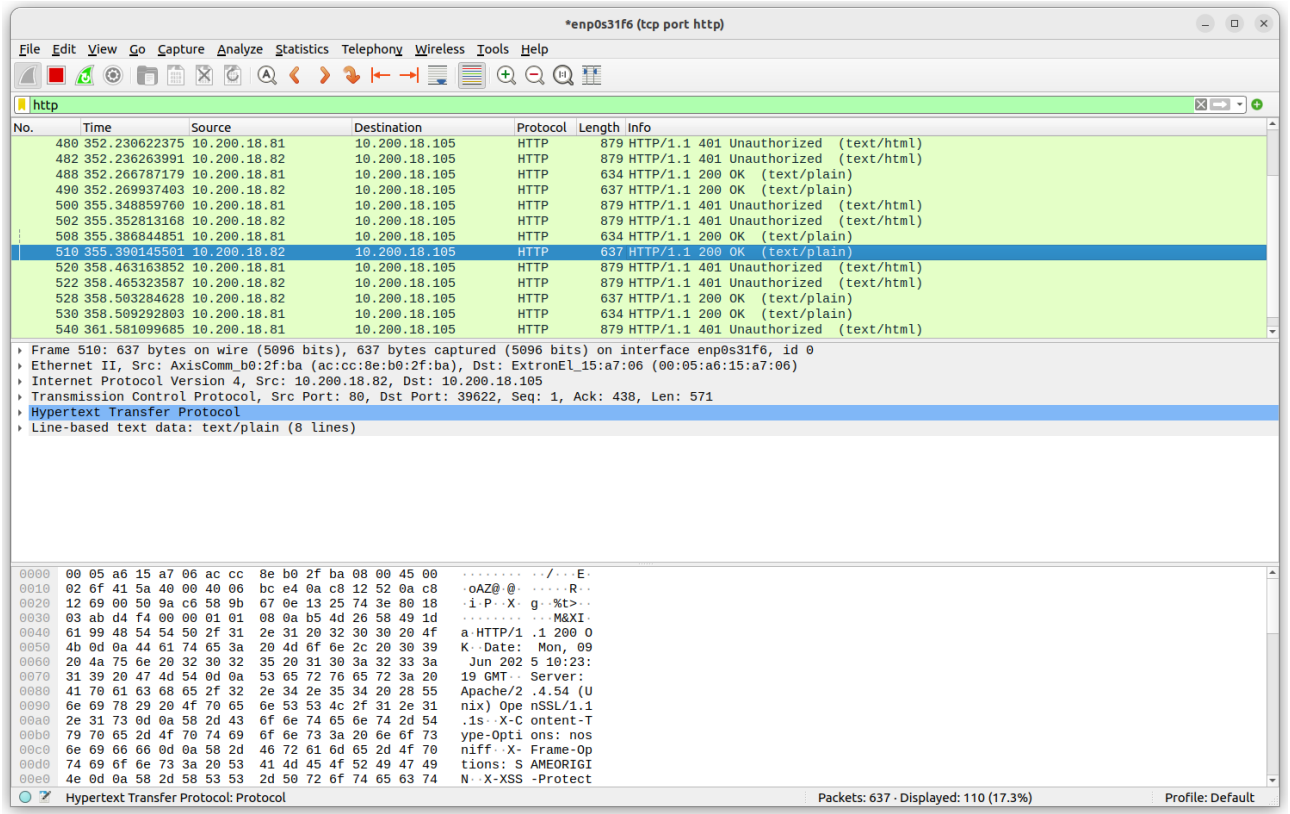


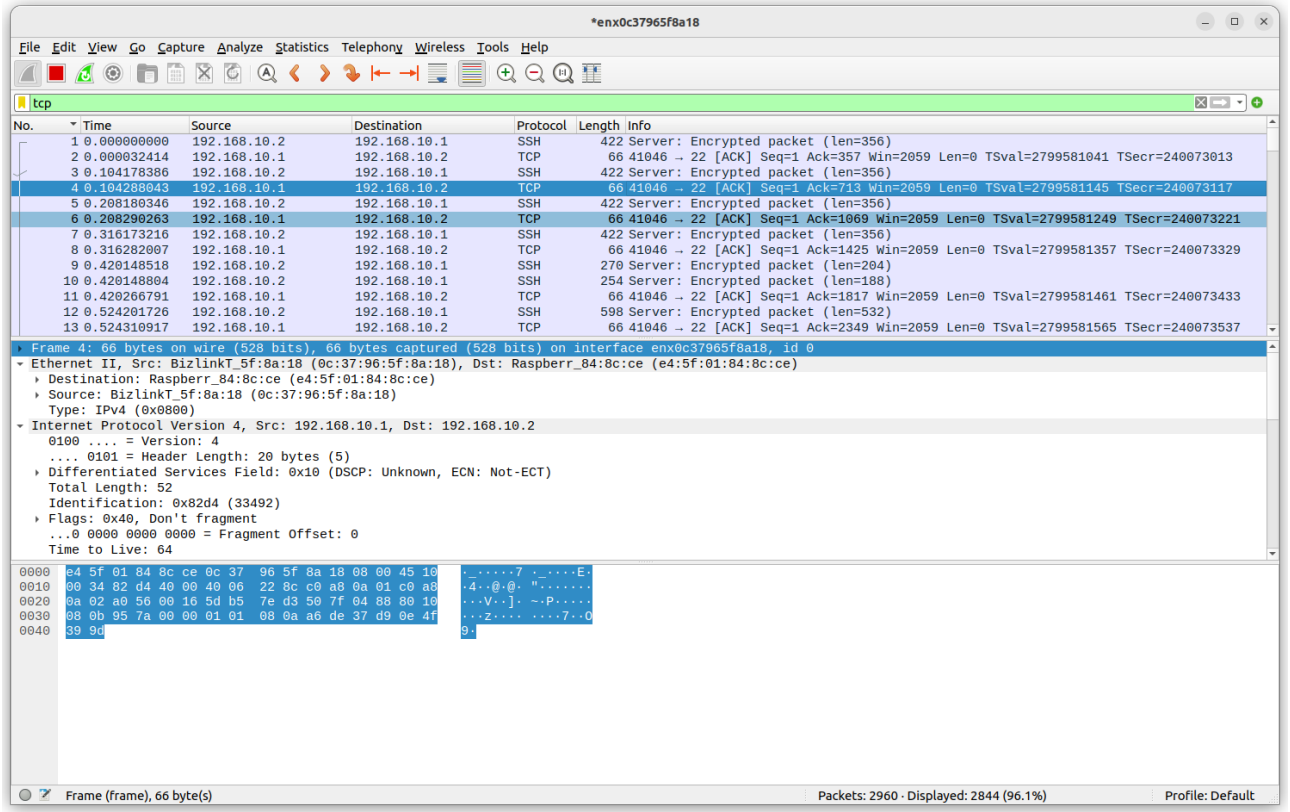

Traffic Capture

Ethernet

I see pachets captured, there are some repeating packets of "standard query"

http traffic

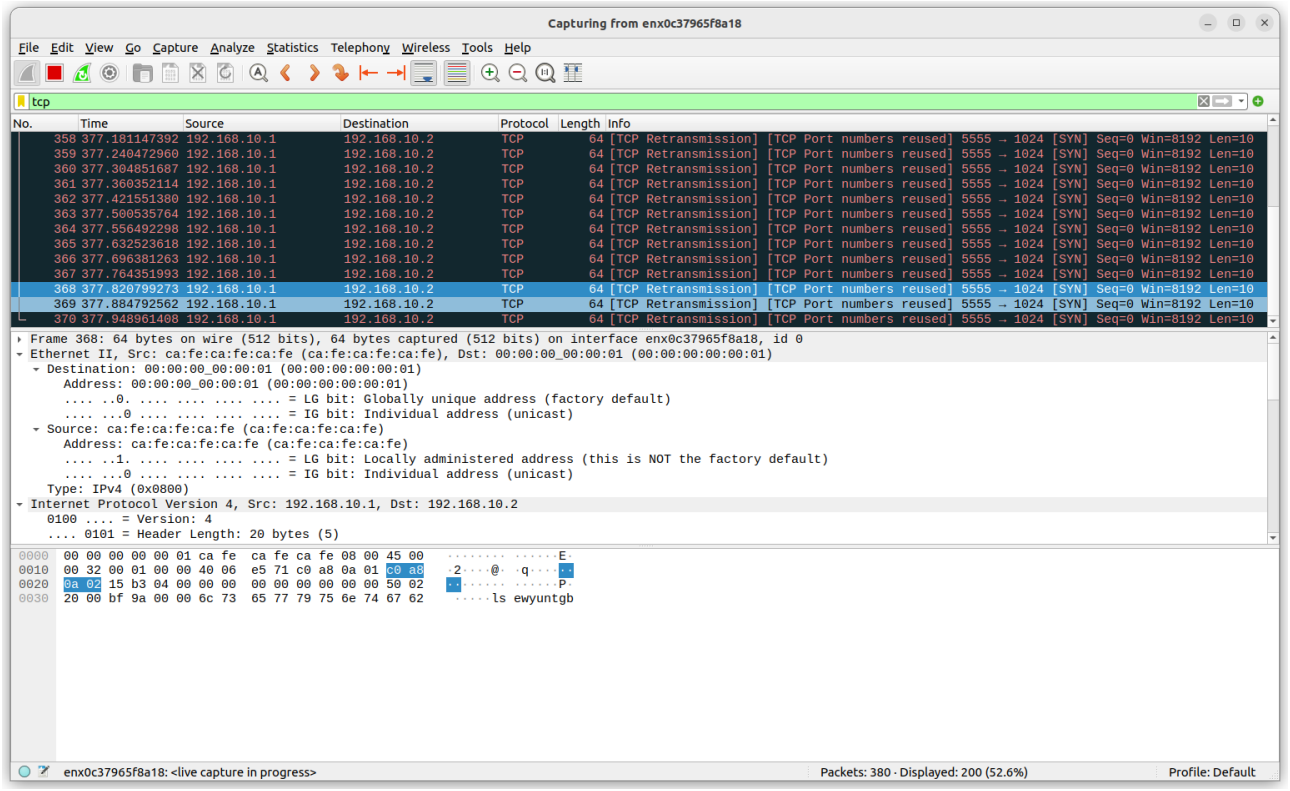
type http in the filter bracket and apply

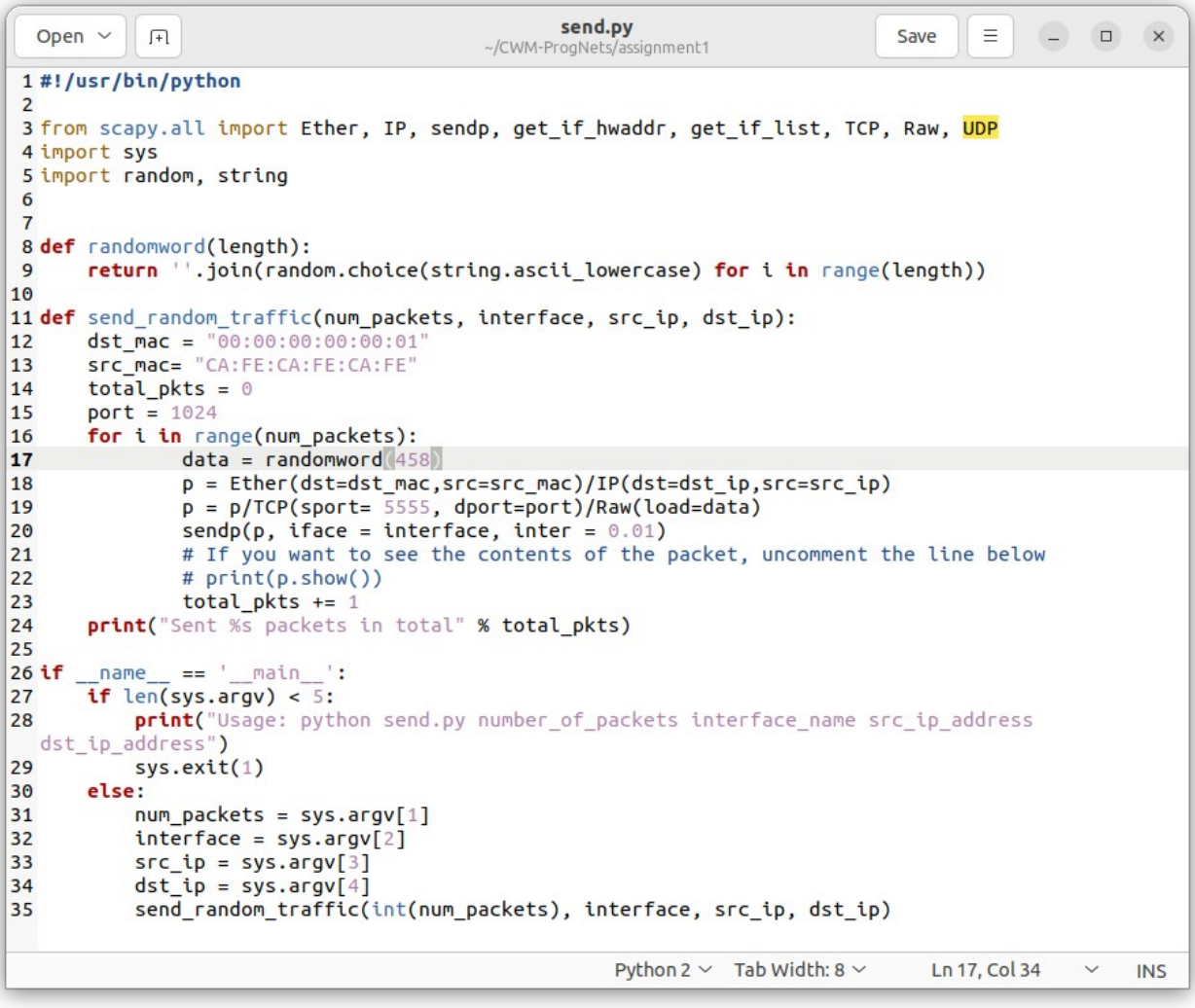



Filter: !(udp.port == 53) && udp filter out DNS message and show only udp packets

Packet size is 64 bytes

Protocol used is UDP


Capturing from enx0c37965f8a18
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
358 377.181147392 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
359 377.240472960 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
360 377.304851687 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
361 377.360352114 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
362 377.421551380 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
363 377.500535764 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
364 377.556492298 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
365 377.632523618 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
366 377.696381263 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
367 377.764351993 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
368 377.820799273 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
369 377.884792562 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
370 377.948961408 192.168.10.1 192.168.10.2 TCP 64 [TCP Retransmission] [TCP Port numbers reused] 5555 → 1024 [SYN] Seq=0 Win=8192 Len=10
Frame 368: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface enx0c37965f8a18, id 0
Ethernet II, Src: ca:fe:ca:fe:ca:fe (ca:fe:ca:fe:ca:fe), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
Destination: 00:00:00_00:00:01 (00:00:00:00:00:01)
Address: 00:00:00_00:00:01 (00:00:00:00:00:01)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: ca:fe:ca:fe:ca:fe (ca:fe:ca:fe:ca:fe)
Address: ca:fe:ca:fe:ca:fe (ca:fe:ca:fe:ca:fe)
.... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.2
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
0000 00 00 00 00 00 01 ca fe ca fe ca fe 08 00 45 00
0010 00 32 00 01 00 00 40 06 e5 71 c0 a8 0a 01 c0 a8
0020 0a 02 15 b3 04 00 00 00 00 00 00 00 50 02
0030 20 00 bf 9a 00 00 6c 73 65 77 79 75 6e 74 67 62 ls ewyuntgb
enx0c37965f8a18: <live capture in progress>
Packets: 380 · Displayed: 200 (52.6%)
Profile: Default


Open
send.py
~/CWM-ProgNets/assignment1
Save
#!/usr/bin/python
from scapy.all import Ether, IP, sendp, get_if_hwaddr, get_if_list, TCP, Raw, UDP
import sys
import random, string
def randomword(length):
return ''.join(random.choice(string.ascii_lowercase) for i in range(length))
def send_random_traffic(num_packets, interface, src_ip, dst_ip):
dst_mac = "00:00:00:00:00:01"
src_mac= "CA:FE:CA:FE:CA:FE"
total_pkts = 0
port = 1024
for i in range(num_packets):
data = randomword(458)
p = Ether(dst=dst_mac,src=src_mac)/IP(dst=dst_ip,src=src_ip)
p = p/TCP(sport= 5555, dport=port)/Raw(load=data)
sendp(p, iface = interface, inter = 0.01)
# If you want to see the contents of the packet, uncomment the line below
# print(p.show())
total_pkts += 1
print("Sent %s packets in total" % total_pkts)
if __name__ == '__main__':
if len(sys.argv) < 5:
print("Usage: python send.py number_of_packets interface_name src_ip_address dst_ip_address")
sys.exit(1)
else:
num_packets = sys.argv[1]
interface = sys.argv[2]
src_ip = sys.argv[3]
dst_ip = sys.argv[4]
send_random_traffic(int(num_packets), interface, src_ip, dst_ip)
Python 2
Tab Width: 8
Ln 17, Col 34
INS