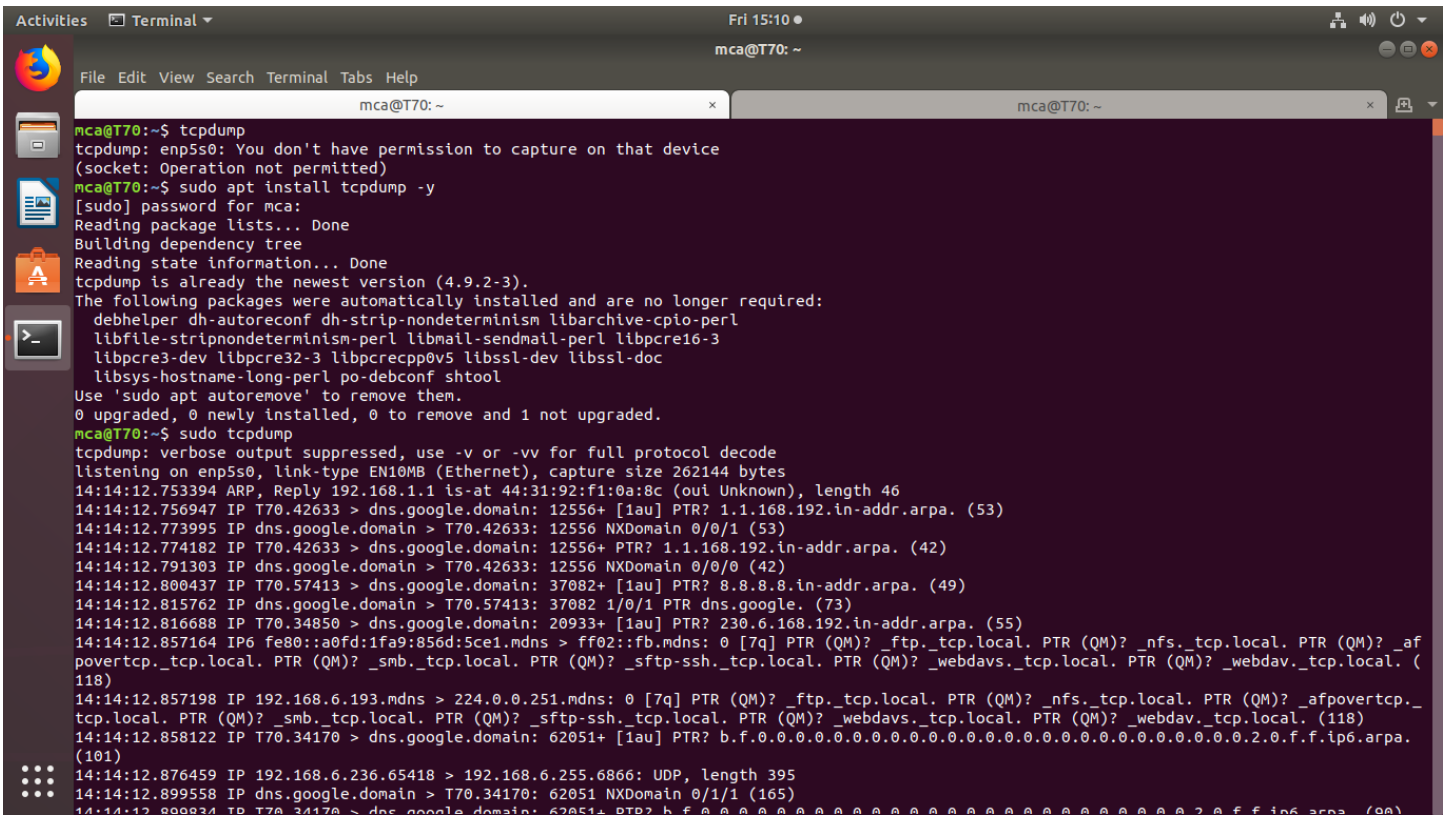
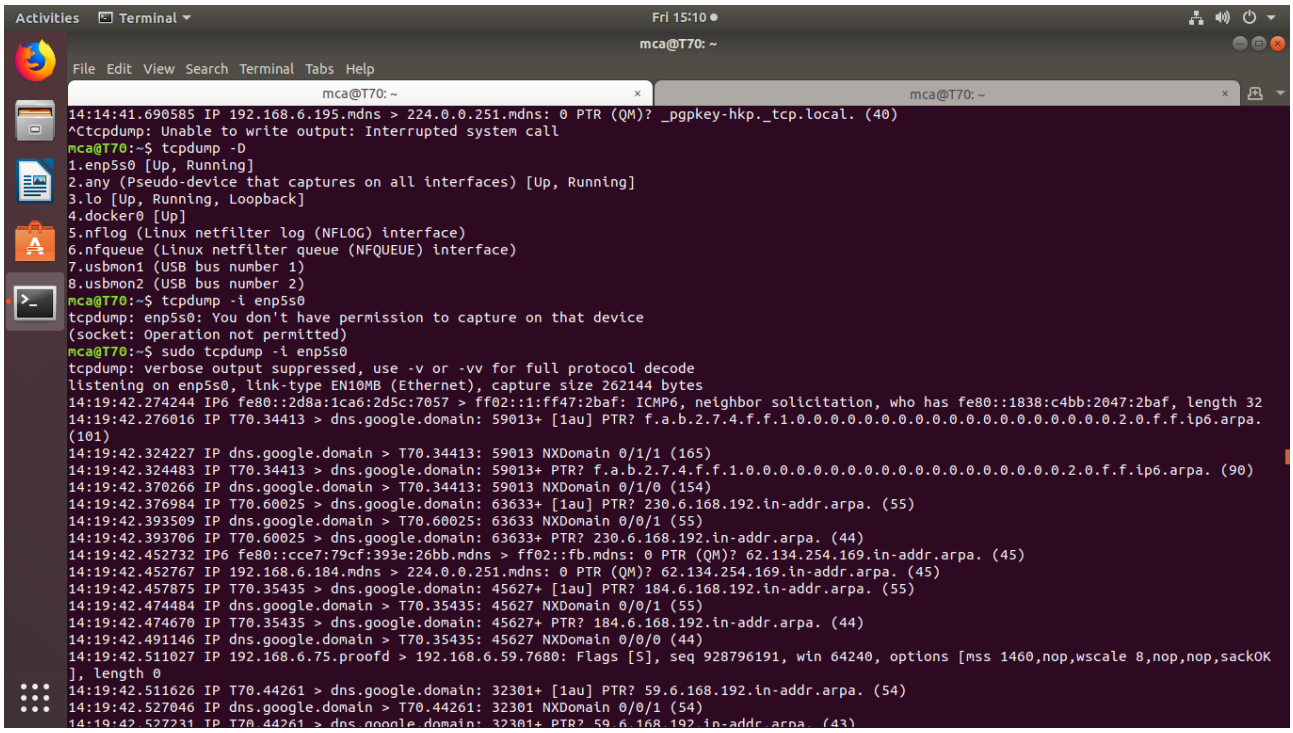
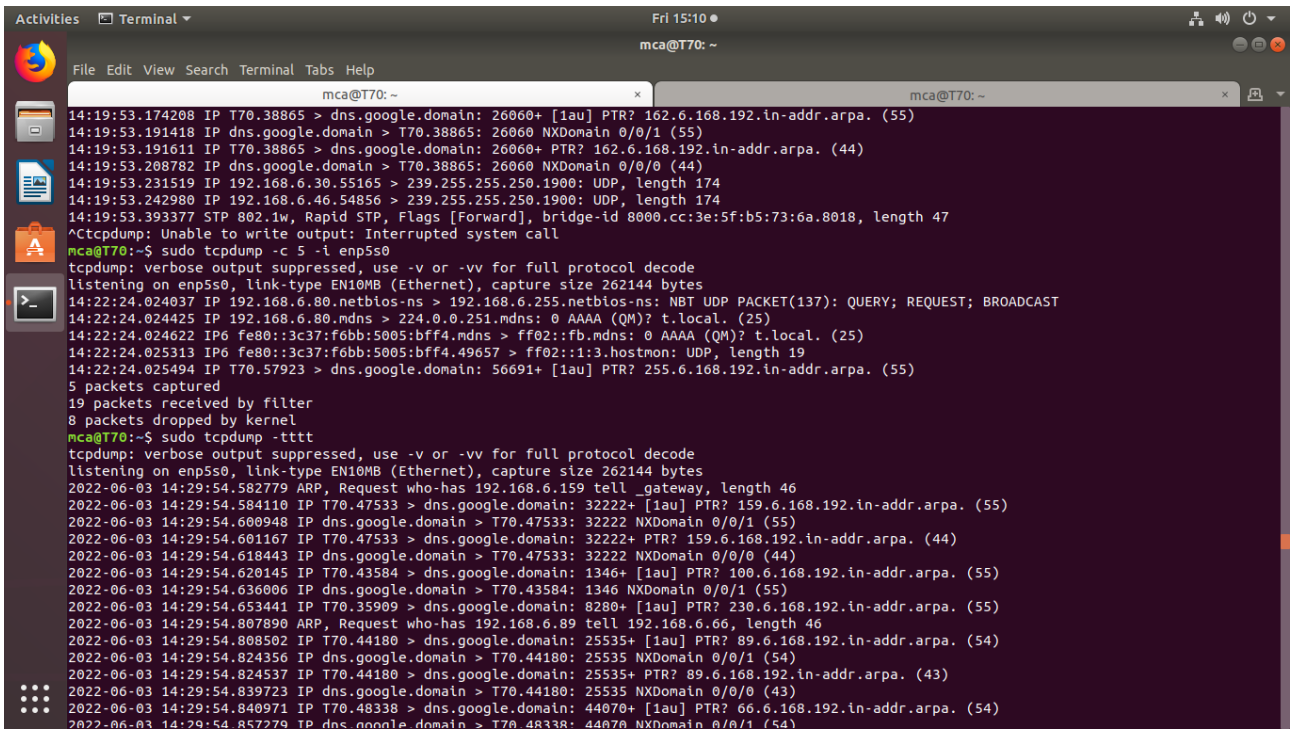
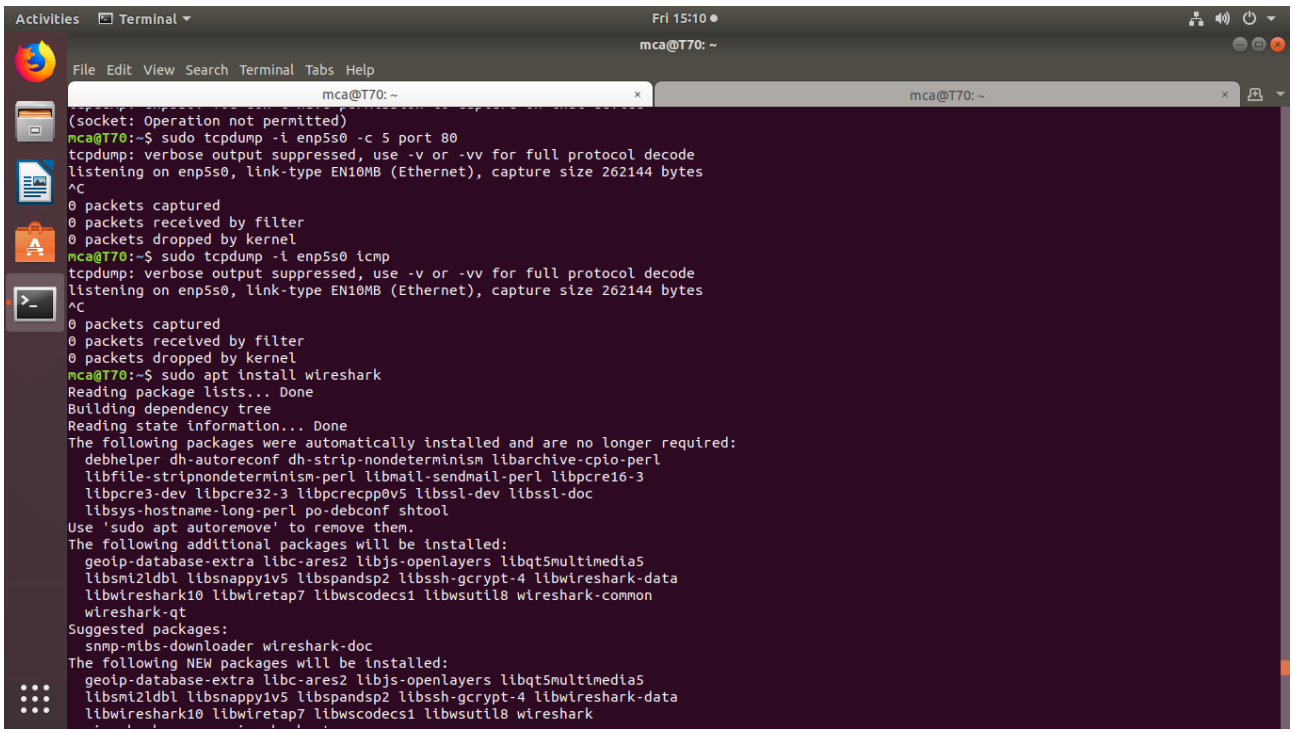
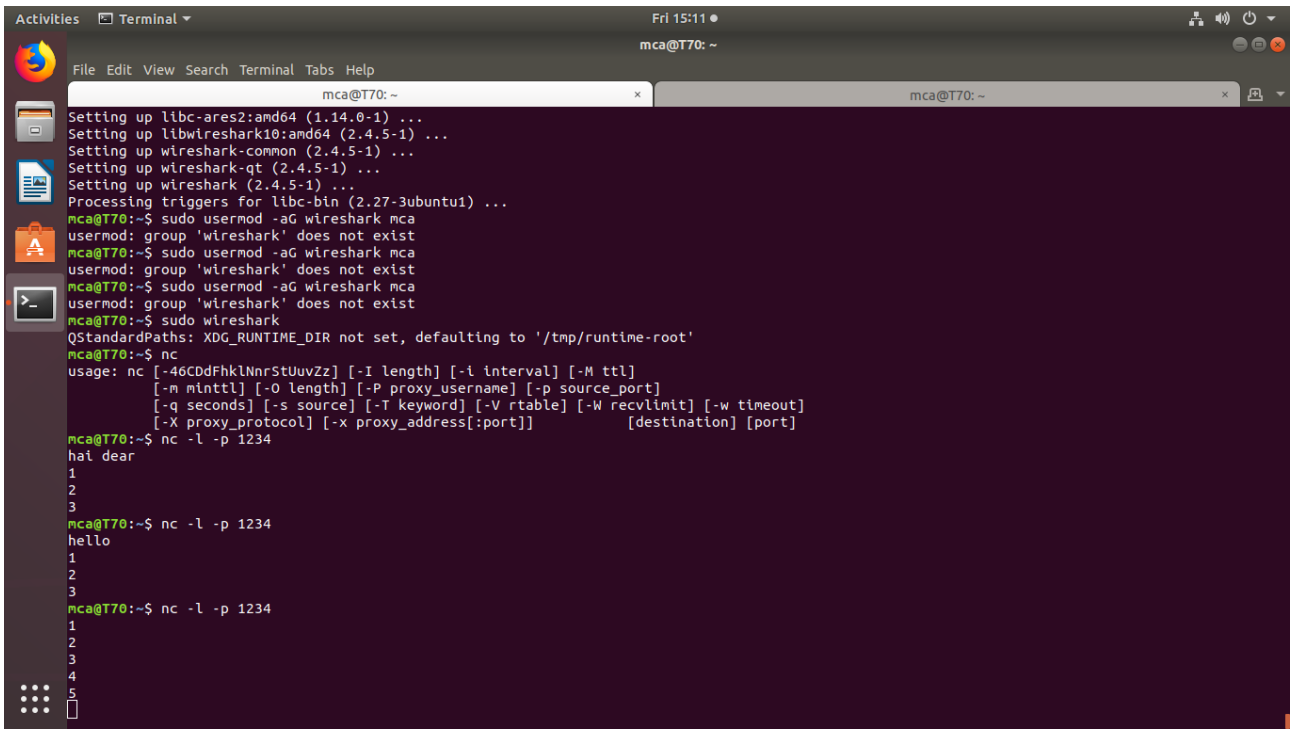
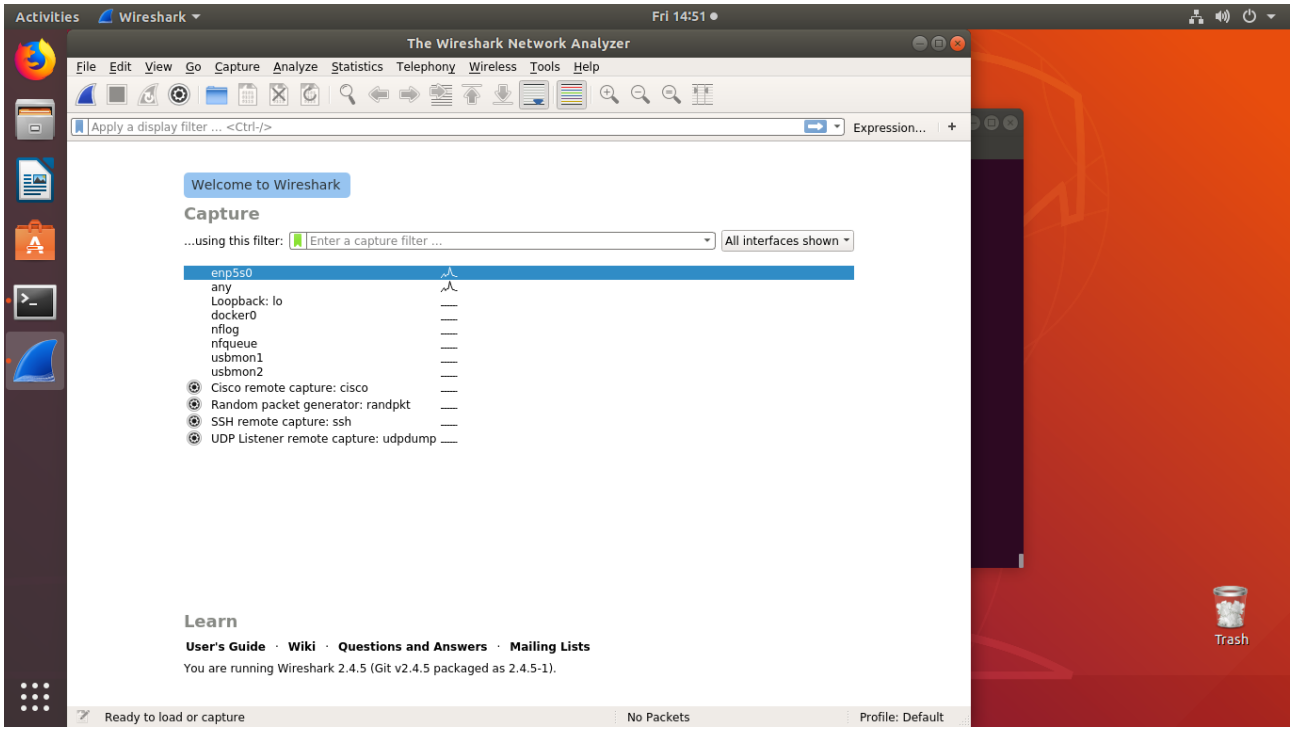

Activities
Terminal
Fri 15:10
mca@T70: ~
File Edit View Search Terminal Tabs Help
mca@T70: ~
mca@T70: ~
mca@T70:~$ tcpdump
tcpdump: enp5s0: You don't have permission to capture on that device
(socket: Operation not permitted)
mca@T70:~$ sudo apt install tcpdump -y
[sudo] password for mca:
Reading package lists... Done
Building dependency tree
Reading state information... Done
tcpdump is already the newest version (4.9.2-3).
The following packages were automatically installed and are no longer required:
debhelper dh-autoreconf dh-strip-nondeterminism libarchive-cpio-perl
libfile-stripnondeterminism-perl libmail-sendmail-perl libpcre16-3
libpcre3-dev libpcre32-3 libpcrecpp0v5 libssl-dev libssl-doc
libsys-hostname-long-perl po-debconf shtool
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
mca@T70:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:14:12.753394 ARP, Reply 192.168.1.1 is-at 44:31:92:f1:0a:8c (oui Unknown), length 46
14:14:12.756947 IP T70.42633 > dns.google.domain: 12556+ [1au] PTR? 1.1.168.192.in-addr.arpa. (53)
14:14:12.773995 IP dns.google.domain > T70.42633: 12556 NXDomain 0/0/1 (53)
14:14:12.774182 IP T70.42633 > dns.google.domain: 12556+ PTR? 1.1.168.192.in-addr.arpa. (42)
14:14:12.791303 IP dns.google.domain > T70.42633: 12556 NXDomain 0/0/0 (42)
14:14:12.800437 IP T70.57413 > dns.google.domain: 37082+ [1au] PTR? 8.8.8.8.in-addr.arpa. (49)
14:14:12.815762 IP dns.google.domain > T70.57413: 37082 1/0/1 PTR dns.google. (73)
14:14:12.816688 IP T70.34850 > dns.google.domain: 20933+ [1au] PTR? 230.6.168.192.in-addr.arpa. (55)
14:14:12.857164 IP6 fe80::a0fd:1fa9:856d:5ce1.mdns > ff02::fb.mdns: 0 [7q] PTR (QM)? _ftp._tcp.local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _af
povertcp._tcp.local. PTR (QM)? _smb._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local. PTR (QM)? _webdav._tcp.local. (
118)
14:14:12.857198 IP 192.168.6.193.mdns > 224.0.0.251.mdns: 0 [7q] PTR (QM)? _ftp._tcp.local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _afpovertcp._
tcp.local. PTR (QM)? _smb._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _webdavs._tcp.local. PTR (QM)? _webdav._tcp.local. (118)
14:14:12.858122 IP T70.34170 > dns.google.domain: 62051+ [1au] PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa.
(101)
14:14:12.876459 IP 192.168.6.236.65418 > 192.168.6.255.6866: UDP, length 395
14:14:12.899558 IP dns.google.domain > T70.34170: 62051 NXDomain 0/1/1 (165)

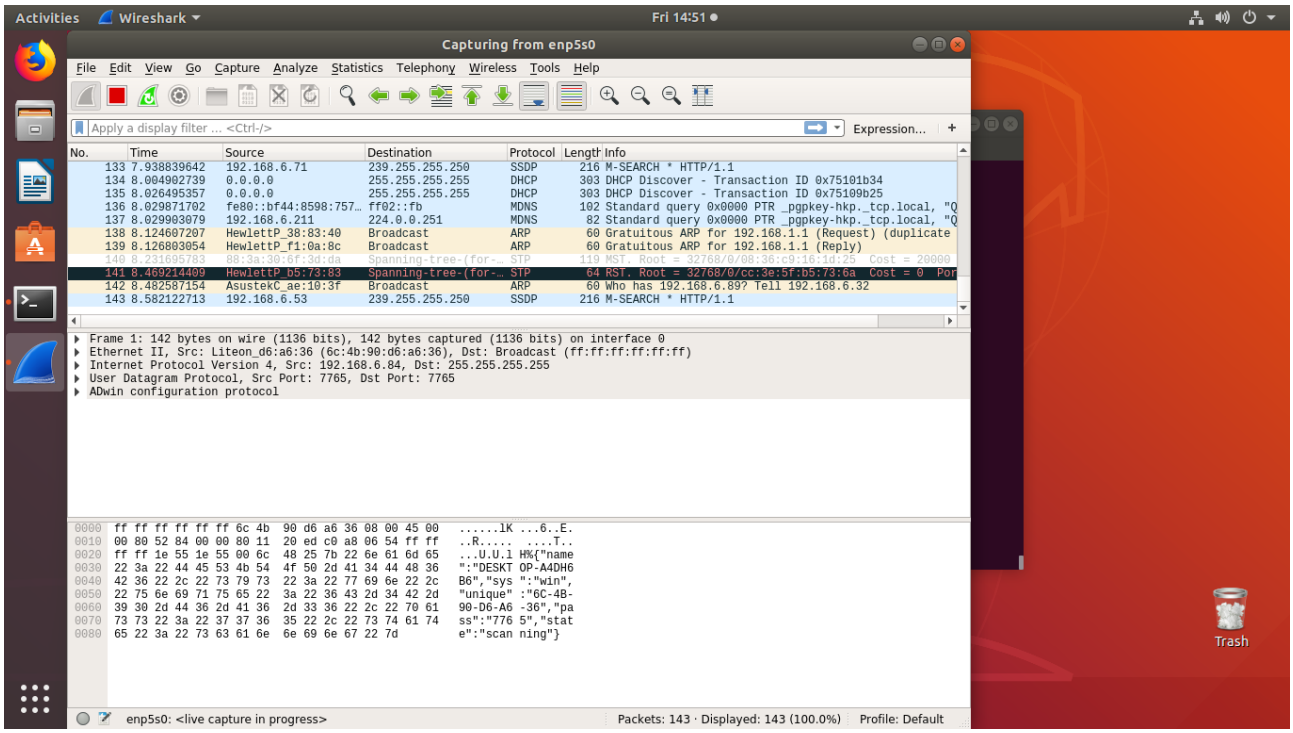

Activities
Terminal
Fri 15:10
mca@T70: ~
File Edit View Search Terminal Tabs Help
mca@T70: ~
mca@T70: ~
14:14:41.690585 IP 192.168.6.195.mdns > 224.0.0.251.mdns: 0 PTR (QM)? _pgpkey-hkp._tcp.local. (40)
^Ctcpdump: Unable to write output: Interrupted system call
mca@T70:~$ tcpdump -D
1.enp5s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.docker0 [Up]
5.nflog (Linux netfilter log (NFLOG) interface)
6.nfqueue (Linux netfilter queue (NFQUEUE) interface)
7.usbmon1 (USB bus number 1)
8.usbmon2 (USB bus number 2)
mca@T70:~$ tcpdump -i enp5s0
tcpdump: enp5s0: You don't have permission to capture on that device
(socket: Operation not permitted)
mca@T70:~$ sudo tcpdump -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:19:42.274244 IP6 fe80::2d8a:1ca6:2d5c:7057 > ff02::1:ff47:2baf: ICMP6, neighbor solicitation, who has fe80::1838:c4bb:2047:2baf, length 32
14:19:42.276016 IP T70.34413 > dns.google.domain: 59013+ [1au] PTR? f.a.b.2.7.4.f.f.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa.
(101)
14:19:42.324227 IP dns.google.domain > T70.34413: 59013 NXDomain 0/1/1 (165)
14:19:42.324483 IP T70.34413 > dns.google.domain: 59013+ PTR? f.a.b.2.7.4.f.f.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
14:19:42.370266 IP dns.google.domain > T70.34413: 59013 NXDomain 0/1/0 (154)
14:19:42.376984 IP T70.60025 > dns.google.domain: 63633+ [1au] PTR? 230.6.168.192.in-addr.arpa. (55)
14:19:42.393509 IP dns.google.domain > T70.60025: 63633 NXDomain 0/0/1 (55)
14:19:42.393706 IP T70.60025 > dns.google.domain: 63633+ PTR? 230.6.168.192.in-addr.arpa. (44)
14:19:42.452732 IP6 fe80::cce7:79cf:393e:26bb.mdns > ff02::fb.mdns: 0 PTR (QM)? 62.134.254.169.in-addr.arpa. (45)
14:19:42.452767 IP 192.168.6.184.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 62.134.254.169.in-addr.arpa. (45)
14:19:42.457875 IP T70.35435 > dns.google.domain: 45627+ [1au] PTR? 184.6.168.192.in-addr.arpa. (55)
14:19:42.474484 IP dns.google.domain > T70.35435: 45627 NXDomain 0/0/1 (55)
14:19:42.474670 IP T70.35435 > dns.google.domain: 45627+ PTR? 184.6.168.192.in-addr.arpa. (44)
14:19:42.491146 IP dns.google.domain > T70.35435: 45627 NXDomain 0/0/0 (44)
14:19:42.511027 IP 192.168.6.75.proofd > 192.168.6.59.7680: Flags [S], seq 928796191, win 64240, options [mss 1460,nop,wscale 8,nop,nop,sackOK
], length 0
14:19:42.511626 IP T70.44261 > dns.google.domain: 32301+ [1au] PTR? 59.6.168.192.in-addr.arpa. (54)
14:19:42.527046 IP dns.google.domain > T70.44261: 32301 NXDomain 0/0/1 (54)

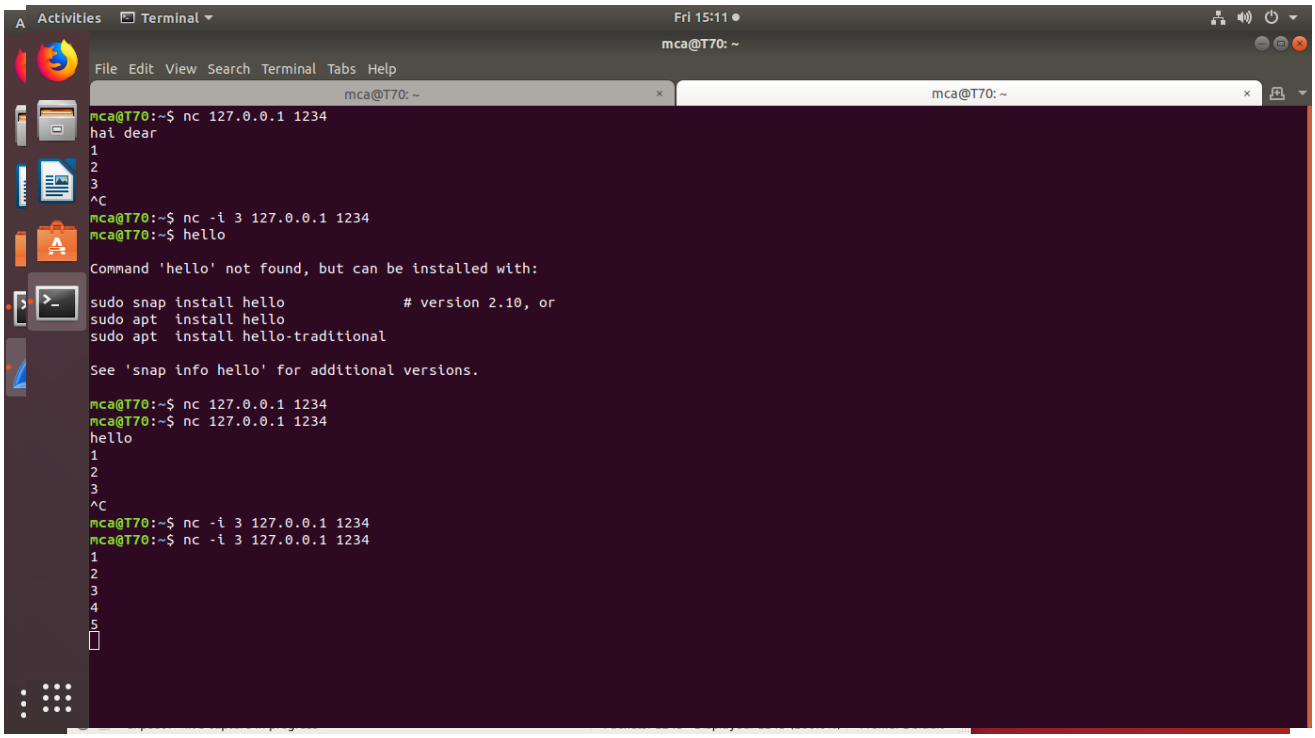

Activities
Terminal
Fri 15:10
mca@T70: ~
File Edit View Search Terminal Tabs Help
mca@T70: ~
mca@T70: ~
14:19:53.174208 IP T70.38865 > dns.google.domain: 26060+ [1au] PTR? 162.6.168.192.in-addr.arpa. (55)
14:19:53.191418 IP dns.google.domain > T70.38865: 26060 NXDomain 0/0/1 (55)
14:19:53.191611 IP T70.38865 > dns.google.domain: 26060+ PTR? 162.6.168.192.in-addr.arpa. (44)
14:19:53.208782 IP dns.google.domain > T70.38865: 26060 NXDomain 0/0/0 (44)
14:19:53.231519 IP 192.168.6.30.55165 > 239.255.255.250.1900: UDP, length 174
14:19:53.242980 IP 192.168.6.46.54856 > 239.255.255.250.1900: UDP, length 174
14:19:53.393377 STP 802.1w, Rapid STP, Flags [Forward], bridge-id 8000.cc:3e:5f:b5:73:6a.8018, length 47
^Ctcpdump: Unable to write output: Interrupted system call
mca@T70:~$ sudo tcpdump -c 5 -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:22:24.024037 IP 192.168.6.80.netbios-ns > 192.168.6.255.netbios-ns: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
14:22:24.024425 IP 192.168.6.80.mdns > 224.0.0.251.mdns: 0 AAAA (QM)? t.local. (25)
14:22:24.024622 IP6 fe80::3c37:f6bb:5005:bff4.mdns > ff02::fb.mdns: 0 AAAA (QM)? t.local. (25)
14:22:24.025313 IP6 fe80::3c37:f6bb:5005:bff4.49657 > ff02::1:3.hostmon: UDP, length 19
14:22:24.025494 IP T70.57923 > dns.google.domain: 56691+ [1au] PTR? 255.6.168.192.in-addr.arpa. (55)
5 packets captured
19 packets received by filter
8 packets dropped by kernel
mca@T70:~$ sudo tcpdump -tttt
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
2022-06-03 14:29:54.582779 ARP, Request who-has 192.168.6.159 tell _gateway, length 46
2022-06-03 14:29:54.584110 IP T70.47533 > dns.google.domain: 32222+ [1au] PTR? 159.6.168.192.in-addr.arpa. (55)
2022-06-03 14:29:54.600948 IP dns.google.domain > T70.47533: 32222 NXDomain 0/0/1 (55)
2022-06-03 14:29:54.601167 IP T70.47533 > dns.google.domain: 32222+ PTR? 159.6.168.192.in-addr.arpa. (44)
2022-06-03 14:29:54.618443 IP dns.google.domain > T70.47533: 32222 NXDomain 0/0/0 (44)
2022-06-03 14:29:54.620145 IP T70.43584 > dns.google.domain: 1346+ [1au] PTR? 100.6.168.192.in-addr.arpa. (55)
2022-06-03 14:29:54.636006 IP dns.google.domain > T70.43584: 1346 NXDomain 0/0/1 (55)
2022-06-03 14:29:54.653441 IP T70.35909 > dns.google.domain: 8280+ [1au] PTR? 230.6.168.192.in-addr.arpa. (55)
2022-06-03 14:29:54.807890 ARP, Request who-has 192.168.6.89 tell 192.168.6.66, length 46
2022-06-03 14:29:54.808502 IP T70.44180 > dns.google.domain: 25535+ [1au] PTR? 89.6.168.192.in-addr.arpa. (54)
2022-06-03 14:29:54.824356 IP dns.google.domain > T70.44180: 25535 NXDomain 0/0/1 (54)
2022-06-03 14:29:54.824537 IP T70.44180 > dns.google.domain: 25535+ PTR? 89.6.168.192.in-addr.arpa. (43)
2022-06-03 14:29:54.839723 IP dns.google.domain > T70.44180: 25535 NXDomain 0/0/0 (43)
2022-06-03 14:29:54.840971 IP T70.48338 > dns.google.domain: 44070+ [1au] PTR? 66.6.168.192.in-addr.arpa. (54)


Activities
Terminal
Fri 15:10
mca@T70: ~
File Edit View Search Terminal Tabs Help
mca@T70: ~
mca@T70: ~
(socket: Operation not permitted)
mca@T70:~$ sudo tcpdump -i enp5s0 -c 5 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
mca@T70:~$ sudo tcpdump -i enp5s0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
mca@T70:~$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
debhelper dh-autoreconf dh-strip-nondeterminism libarchive-cpio-perl
libfile-stripnondeterminism-perl libmail-sendmail-perl libpcre16-3
libpcre3-dev libpcre32-3 libpcrecpp0v5 libssl-dev libssl-doc
libsys-hostname-long-perl po-debconf shtool
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
geoip-database-extra libc-ares2 libjs-openlayers libqt5multimedia5
libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data
libwireshark10 libwiretap7 libwscodecs1 libwsutil8 wireshark-common
wireshark-qt
Suggested packages:
snmp-mibs-downloader wireshark-doc
The following NEW packages will be installed:
geoip-database-extra libc-ares2 libjs-openlayers libqt5multimedia5
libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data
libwireshark10 libwiretap7 libwscodecs1 libwsutil8 wireshark


Activities
Terminal
Fri 15:11
mca@T70: ~
File Edit View Search Terminal Tabs Help
mca@T70: ~
mca@T70: ~
Setting up libc-ares2:amd64 (1.14.0-1) ...
Setting up libwireshark10:amd64 (2.4.5-1) ...
Setting up wireshark-common (2.4.5-1) ...
Setting up wireshark-qt (2.4.5-1) ...
Setting up wireshark (2.4.5-1) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
mca@T70:~$ sudo usermod -aG wireshark mca
usermod: group 'wireshark' does not exist
mca@T70:~$ sudo usermod -aG wireshark mca
usermod: group 'wireshark' does not exist
mca@T70:~$ sudo usermod -aG wireshark mca
usermod: group 'wireshark' does not exist
mca@T70:~$ sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
mca@T70:~$ nc
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
[-m minttl] [-O length] [-P proxy_username] [-p source_port]
[-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
[-X proxy_protocol] [-x proxy_address[:port]] [destination] [port]
mca@T70:~$ nc -l -p 1234
hai dear
1
2
3
mca@T70:~$ nc -l -p 1234
hello
1
2
3
mca@T70:~$ nc -l -p 1234
1
2
3
4
5


Activities
Wireshark
Fri 14:51
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
enp5s0
any
Loopback: lo
docker0
nflog
nfqueue
usbmon1
usbmon2
Cisco remote capture: cisco
Random packet generator: randpkt
SSH remote capture: ssh
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.4.5 (Git v2.4.5 packaged as 2.4.5-1).
Ready to load or capture
No Packets
Profile: Default
Trash


Activities
Wireshark
Fri 14:51
Capturing from enp5s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
133 7.938839642 192.168.6.71 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
134 8.004902739 0.0.0.0 255.255.255.255 DHCP 303 DHCP Discover - Transaction ID 0x75101b34
135 8.026495357 0.0.0.0 255.255.255.255 DHCP 303 DHCP Discover - Transaction ID 0x75109b25
136 8.029871702 fe80::bf44:8598:757… ff02::fb MDNS 102 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "Q
137 8.029903079 192.168.6.211 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _pgpkey-hkp._tcp.local, "Q
138 8.124607207 HewlettP_38:83:40 Broadcast ARP 60 Gratuitous ARP for 192.168.1.1 (Request) (duplicate
139 8.126803054 HewlettP_f1:0a:8c Broadcast ARP 60 Gratuitous ARP for 192.168.1.1 (Reply)
140 8.231695783 88:3a:30:6f:3d:da Spanning-tree-(for-… STP 119 MST. Root = 32768/0/08:36:c9:16:1d:25 Cost = 20000
141 8.469214409 HewlettP_b5:73:83 Spanning-tree-(for-… STP 64 RST. Root = 32768/0/cc:3e:5f:b5:73:6a Cost = 0 Por
142 8.482587154 AsustekC_ae:10:3f Broadcast ARP 60 Who has 192.168.6.89? Tell 192.168.6.32
143 8.582122713 192.168.6.53 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
Frame 1: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
Ethernet II, Src: Liteon_d6:a6:36 (6c:4b:90:d6:a6:36), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.6.84, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 7765, Dst Port: 7765
ADwin configuration protocol
0000 ff ff ff ff ff ff 6c 4b 90 d6 a6 36 08 00 45 00 ......lK ...6..E.
0010 00 80 52 84 00 00 80 11 20 ed c0 a8 06 54 ff ff ..R..... ....T..
0020 ff ff 1e 55 1e 55 00 6c 48 25 7b 22 6e 61 6d 65 ...U.U.l H%{"name
0030 22 3a 22 44 45 53 4b 54 4f 50 2d 41 34 44 48 36 ":"DESKT OP-A4DH6
0040 42 36 22 2c 22 73 79 73 22 3a 22 77 69 6e 22 2c B6","sys ":"win",
0050 22 75 6e 69 71 75 65 22 3a 22 36 43 2d 34 42 2d "unique" :"6C-4B-
0060 39 30 2d 44 36 2d 41 36 2d 33 36 22 2c 22 70 61 90-D6-A6 -36","pa
0070 73 73 22 3a 22 37 37 36 35 22 2c 22 73 74 61 74 ss":"776 5","stat
0080 65 22 3a 22 73 63 61 6e 6e 69 6e 67 22 7d e":"scan ning"}
enp5s0: <live capture in progress>
Packets: 143 · Displayed: 143 (100.0%)
Profile: Default
Trash


Activities
Terminal
Fri 15:11
mca@T70: ~
File Edit View Search Terminal Tabs Help
mca@T70: ~
mca@T70: ~
mca@T70:~$ nc 127.0.0.1 1234
hai dear
1
2
3
^C
mca@T70:~$ nc -i 3 127.0.0.1 1234
mca@T70:~$ hello
Command 'hello' not found, but can be installed with:
sudo snap install hello # version 2.10, or
sudo apt install hello
sudo apt install hello-traditional
See 'snap info hello' for additional versions.
mca@T70:~$ nc 127.0.0.1 1234
mca@T70:~$ nc 127.0.0.1 1234
hello
1
2
3
^C
mca@T70:~$ nc -i 3 127.0.0.1 1234
mca@T70:~$ nc -i 3 127.0.0.1 1234
1
2
3
4
5