Name:Khushbu Ahuja
Roll no:02
Sub:Security Lab
Assignment:07

AIM: To study packet sniffer tools Wireshark and TCPDUMP.

THEORY:

1. Introduction to Packet Sniffing

- **Define Packet Sniffing**: Explain what packet sniffing is and why it is used in network analysis and troubleshooting.
- **Purpose**: Describe the scenarios where packet sniffing tools like Wireshark and TCPDUMP are helpful (e.g., diagnosing network issues, security analysis, protocol debugging).

2. Overview of Wireshark

- **What is Wireshark?**: Provide a brief overview of Wireshark as a graphical network protocol analyzer.
- **Installation**: Explain how to install Wireshark on your system (Windows, Linux, or macOS).
- **Capturing Packets**: Describe how to start a capture session, select network interfaces, and begin capturing traffic.
- **Basic Features**:
    - **Filtering Packets**: How to apply display filters to narrow down captured packets.
    - **Packet Analysis**: How to inspect individual packets, view details about protocols, and follow TCP streams.
- **Exporting and Saving Captures**: Explain how to save captured data for later analysis and how to export it to different formats.

3. Overview of TCPDUMP

- **What is TCPDUMP?**: Introduce TCPDUMP as a command-line packet analyzer that provides similar functionality to Wireshark but in a terminal environment.
- **Installation**: Explain how to install TCPDUMP on your system (typically pre-installed on Unix-like systems).
- **Capturing Packets**: Describe how to use basic TCPDUMP commands to capture traffic.
    - Example: tcpdump -i eth0 (where eth0 is the network interface).
- **Filters in TCPDUMP**: Explain how to use filters to capture specific traffic types (e.g., tcpdump port 80 for HTTP traffic).
- **Output Options**: Describe how to save captured traffic to a file (-w option) and how to read from a file (-r option).

4. Comparison Between Wireshark and TCPDUMP

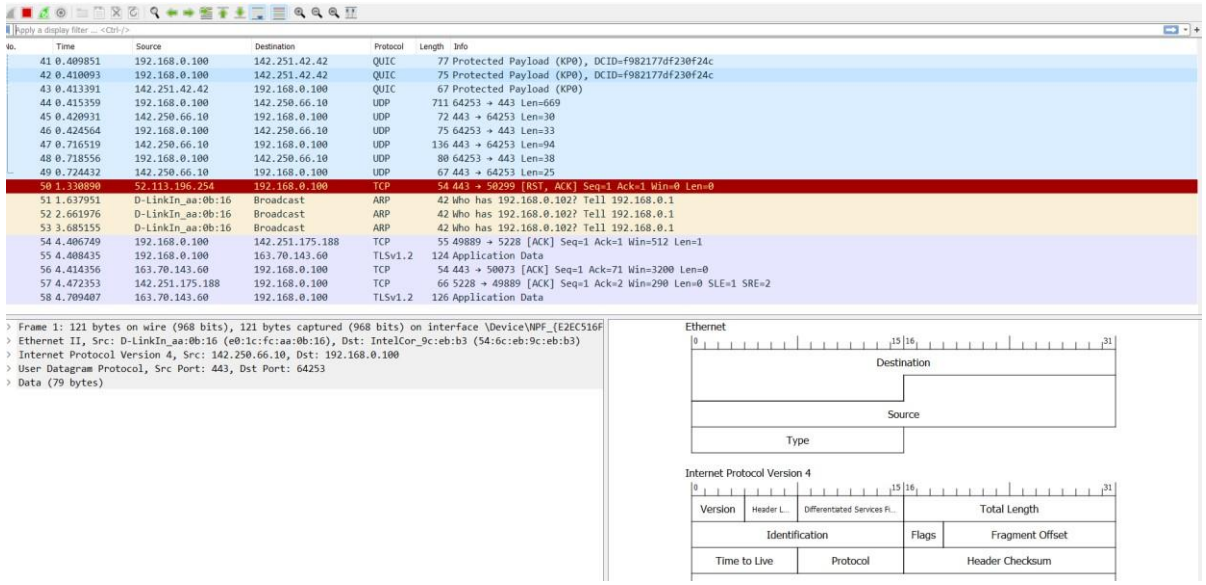
- **Interface**: Compare the graphical interface of Wireshark with the command-line interface of TCPDUMP.
- **Usability**: Discuss the ease of use for beginners versus experienced users.
- **Functionality**: Compare the advanced features available in Wireshark (e.g., protocol analysis, color coding) with the simpler, lightweight nature of TCPDUMP.
- **Performance**: Discuss situations where TCPDUMP might be preferred over Wireshark due to its lower resource usage.

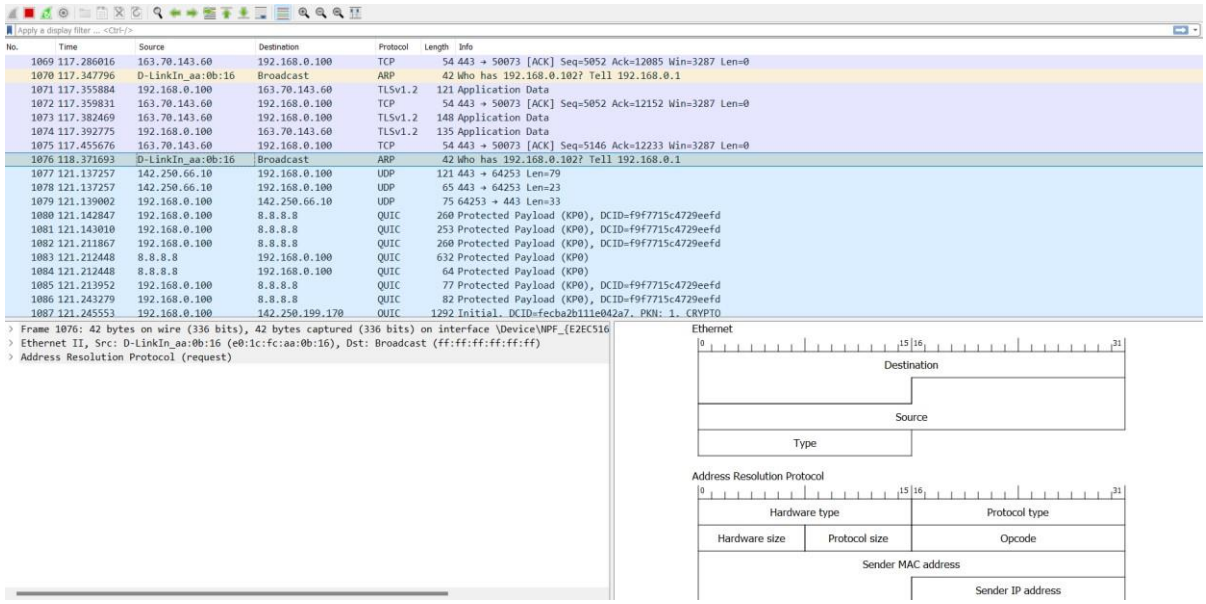
5. Practical Tasks

- **Capture Traffic**: Use both Wireshark and TCPDUMP to capture network traffic on your system. Try capturing traffic while browsing the web or using network services.
- **Analyze Traffic**: Identify specific protocols (e.g., HTTP, DNS) and analyze the captured packets. Compare the output and ease of analysis in both tools.
- **Save and Export**: Save captured packets in both tools and practice reading them in Wireshark or TCPDUMP.

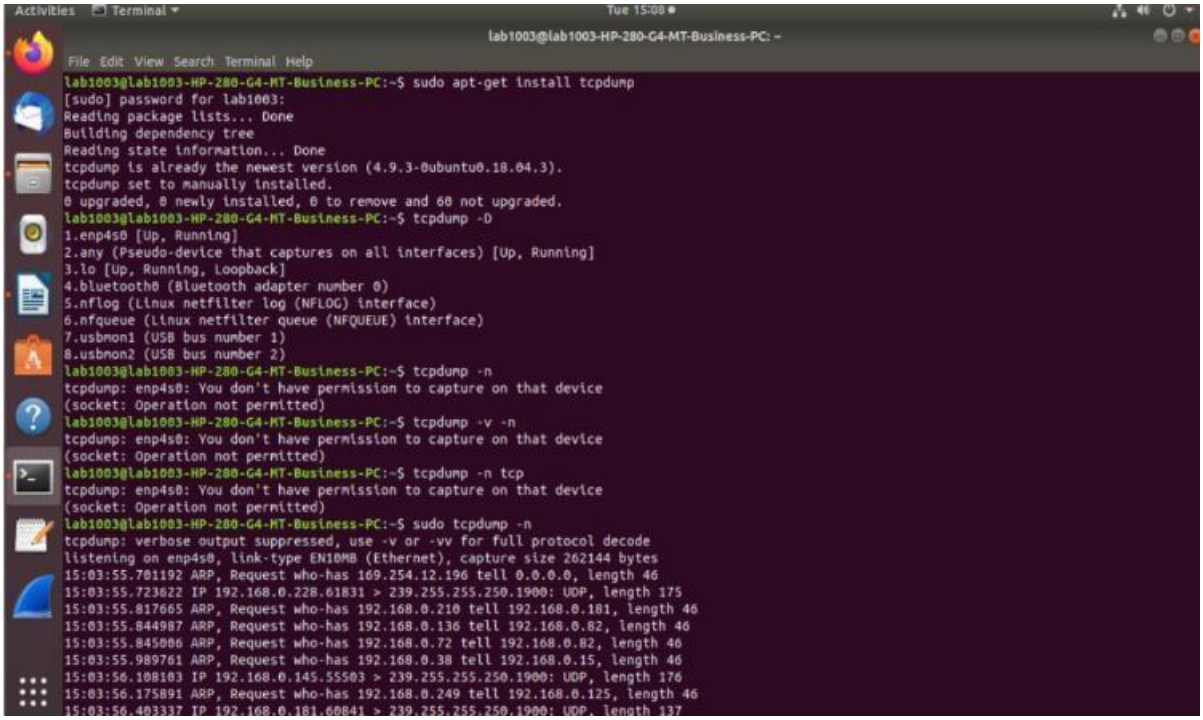
IMPLEMENTATION:

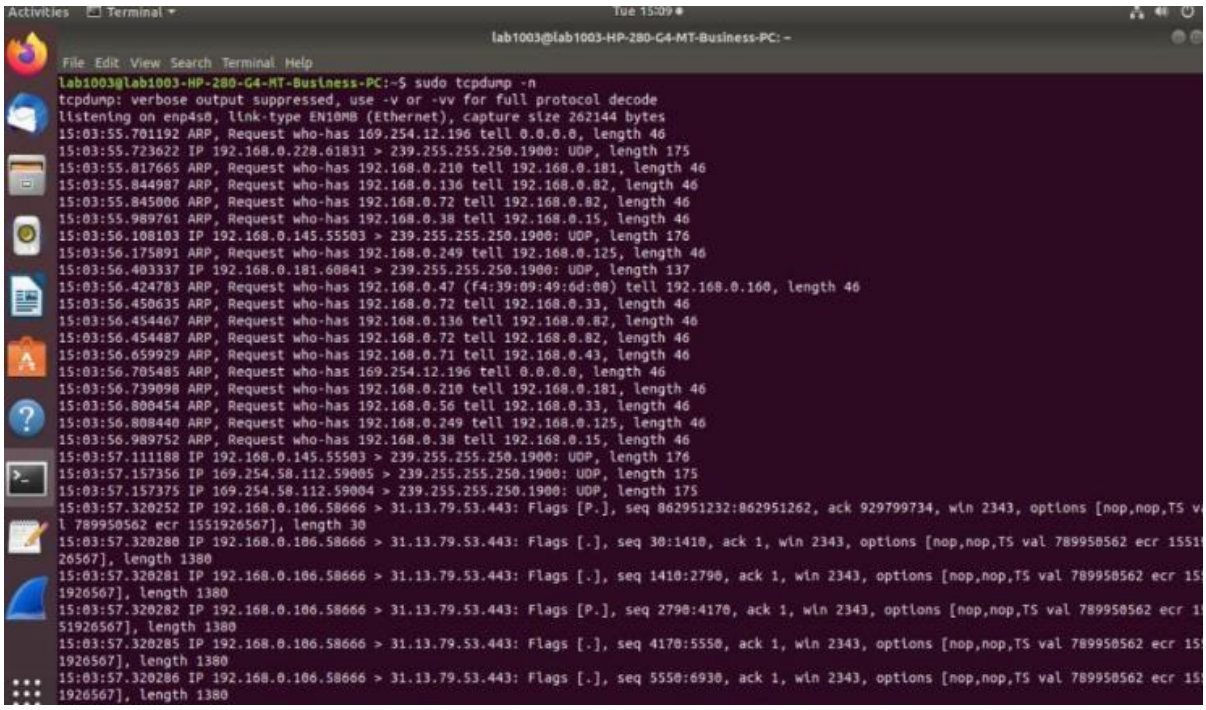
Wireshark:

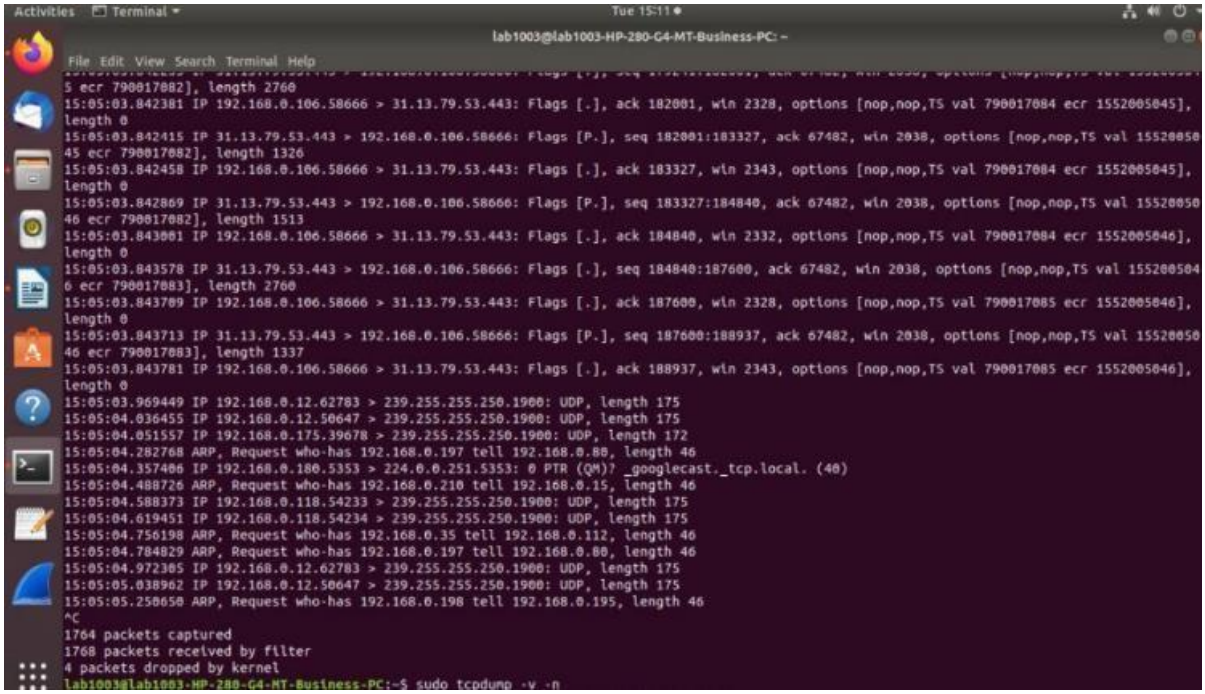


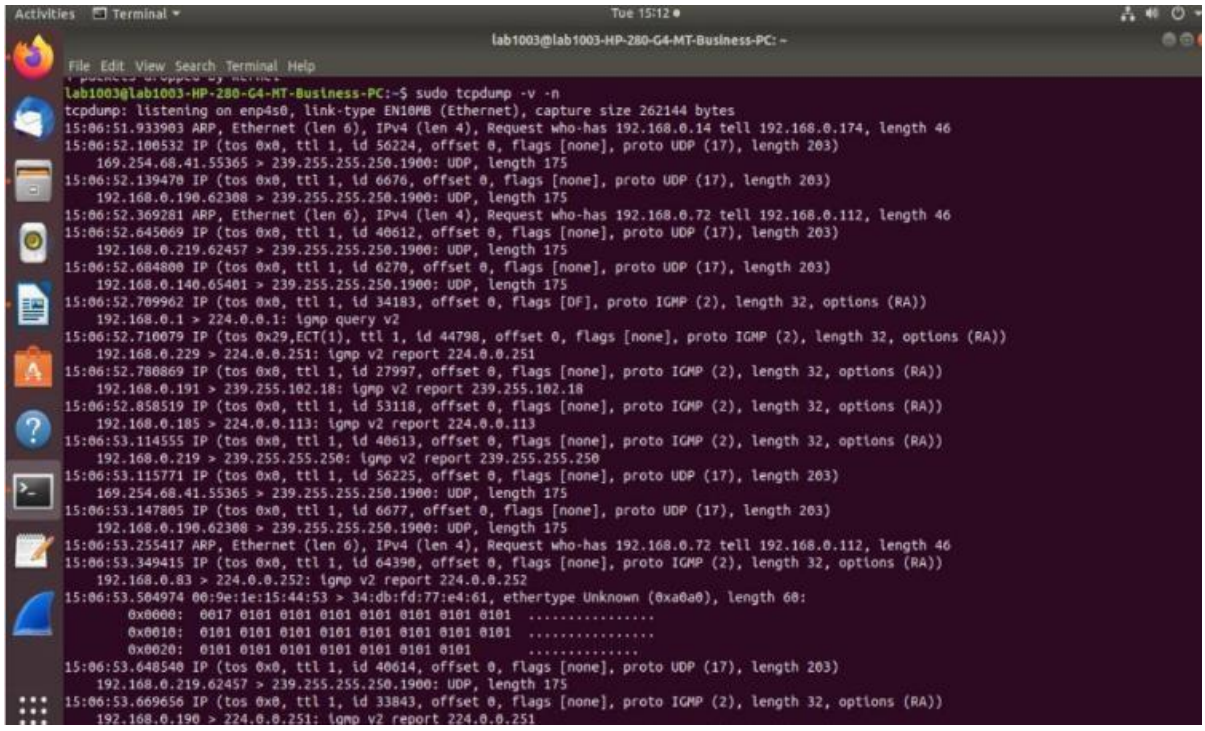


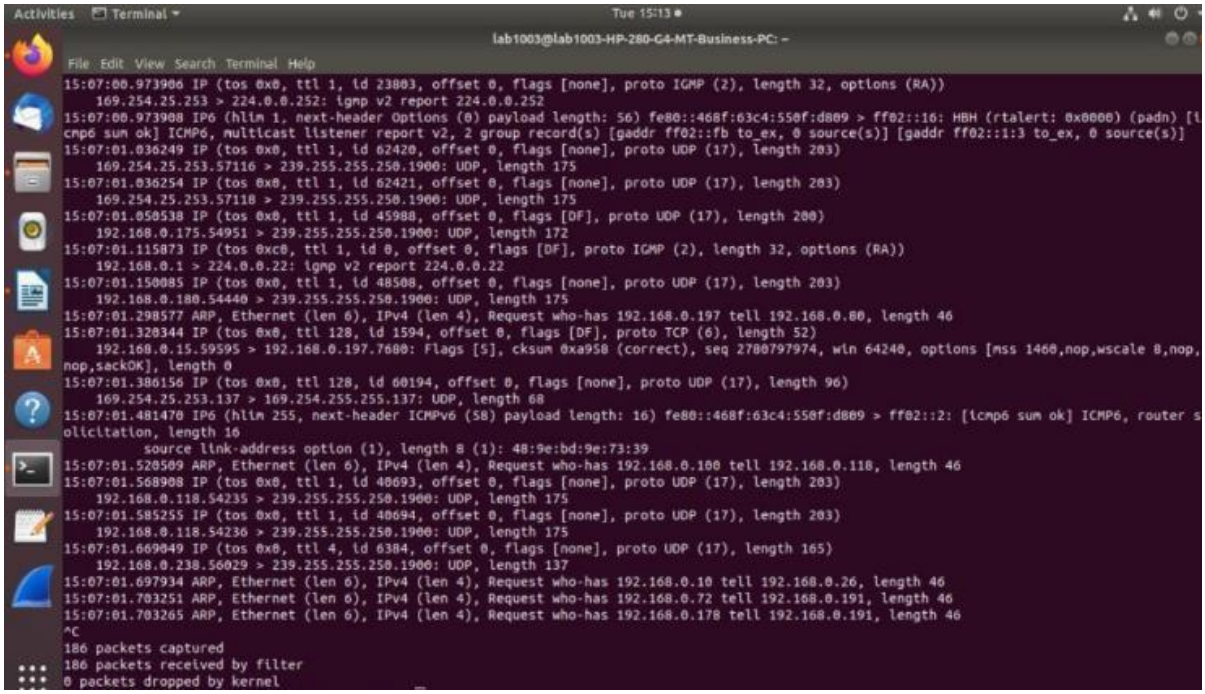
TCPDUMP


Activities
Terminal
Tue 15:08
lab1003@lab1003-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo apt-get install tcpdump
[sudo] password for lab1003:
Reading package lists... Done
Building dependency tree
Reading state information... Done
tcpdump is already the newest version (4.9.3-0ubuntu0.18.04.3).
tcpdump set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 60 not upgraded.
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tcpdump -D
1.enp4s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth0 (Bluetooth adapter number 0)
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)
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tcpdump -n
tcpdump: enp4s0: You don't have permission to capture on that device
(socket: Operation not permitted)
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tcpdump -v -n
tcpdump: enp4s0: You don't have permission to capture on that device
(socket: Operation not permitted)
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tcpdump -n tcp
tcpdump: enp4s0: You don't have permission to capture on that device
(socket: Operation not permitted)
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp4s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:03:55.701192 ARP, Request who-has 169.254.12.196 tell 0.0.0.0, length 46
15:03:55.723622 IP 192.168.0.228.61831 > 239.255.255.250.1900: UDP, length 175
15:03:55.817665 ARP, Request who-has 192.168.0.210 tell 192.168.0.181, length 46
15:03:55.844987 ARP, Request who-has 192.168.0.136 tell 192.168.0.82, length 46
15:03:55.845006 ARP, Request who-has 192.168.0.72 tell 192.168.0.82, length 46
15:03:55.989761 ARP, Request who-has 192.168.0.38 tell 192.168.0.15, length 46
15:03:56.108103 IP 192.168.0.145.55503 > 239.255.255.250.1900: UDP, length 176
15:03:56.175891 ARP, Request who-has 192.168.0.249 tell 192.168.0.125, length 46
15:03:56.403337 IP 192.168.0.181.60841 > 239.255.255.250.1900: UDP, length 137


Activities
Terminal
Tue 15:09
lab1003@lab1003-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp4s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:03:55.701192 ARP, Request who-has 169.254.12.196 tell 0.0.0.0, length 46
15:03:55.723622 IP 192.168.0.228.61831 > 239.255.255.250.1900: UDP, length 175
15:03:55.817665 ARP, Request who-has 192.168.0.210 tell 192.168.0.181, length 46
15:03:55.844987 ARP, Request who-has 192.168.0.136 tell 192.168.0.82, length 46
15:03:55.845006 ARP, Request who-has 192.168.0.72 tell 192.168.0.82, length 46
15:03:55.989761 ARP, Request who-has 192.168.0.38 tell 192.168.0.15, length 46
15:03:56.108103 IP 192.168.0.145.55503 > 239.255.255.250.1900: UDP, length 176
15:03:56.175891 ARP, Request who-has 192.168.0.249 tell 192.168.0.125, length 46
15:03:56.403337 IP 192.168.0.181.60841 > 239.255.255.250.1900: UDP, length 137
15:03:56.424783 ARP, Request who-has 192.168.0.47 (f4:39:09:49:6d:08) tell 192.168.0.160, length 46
15:03:56.450635 ARP, Request who-has 192.168.0.72 tell 192.168.0.33, length 46
15:03:56.454467 ARP, Request who-has 192.168.0.136 tell 192.168.0.82, length 46
15:03:56.454487 ARP, Request who-has 192.168.0.72 tell 192.168.0.82, length 46
15:03:56.659929 ARP, Request who-has 192.168.0.71 tell 192.168.0.43, length 46
15:03:56.705485 ARP, Request who-has 169.254.12.196 tell 0.0.0.0, length 46
15:03:56.739098 ARP, Request who-has 192.168.0.210 tell 192.168.0.181, length 46
15:03:56.800454 ARP, Request who-has 192.168.0.56 tell 192.168.0.33, length 46
15:03:56.808440 ARP, Request who-has 192.168.0.249 tell 192.168.0.125, length 46
15:03:56.989752 ARP, Request who-has 192.168.0.38 tell 192.168.0.15, length 46
15:03:57.111188 IP 192.168.0.145.55503 > 239.255.255.250.1900: UDP, length 176
15:03:57.157356 IP 169.254.58.112.59005 > 239.255.255.250.1900: UDP, length 175
15:03:57.157375 IP 169.254.58.112.59004 > 239.255.255.250.1900: UDP, length 175
15:03:57.320252 IP 192.168.0.106.58666 > 31.13.79.53.443: Flags [P.], seq 862951232:862951262, ack 929799734, win 2343, options [nop,nop,TS v
l 789950562 ecr 1551926567], length 30
15:03:57.320280 IP 192.168.0.106.58666 > 31.13.79.53.443: Flags [.], seq 30:1410, ack 1, win 2343, options [nop,nop,TS val 789950562 ecr 1551
26567], length 1380
15:03:57.320281 IP 192.168.0.106.58666 > 31.13.79.53.443: Flags [.], seq 1410:2790, ack 1, win 2343, options [nop,nop,TS val 789950562 ecr 15
1926567], length 1380
15:03:57.320282 IP 192.168.0.106.58666 > 31.13.79.53.443: Flags [P.], seq 2790:4170, ack 1, win 2343, options [nop,nop,TS val 789950562 ecr 1
51926567], length 1380
15:03:57.320285 IP 192.168.0.106.58666 > 31.13.79.53.443: Flags [.], seq 4170:5550, ack 1, win 2343, options [nop,nop,TS val 789950562 ecr 15
1926567], length 1380
15:03:57.320286 IP 192.168.0.106.58666 > 31.13.79.53.443: Flags [.], seq 5550:6930, ack 1, win 2343, options [nop,nop,TS val 789950562 ecr 15
1926567], length 1380


Activities
Terminal
Tue 15:11
lab1003@lab1003-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
5 ecr 790017082], length 2760
15:05:03.842381 IP 192.168.0.106.58666 > 31.13.79.53.443: Flags [.], ack 182001, win 2328, options [nop,nop,TS val 790017084 ecr 1552005045], length 0
15:05:03.842415 IP 31.13.79.53.443 > 192.168.0.106.58666: Flags [P.], seq 182001:183327, ack 67482, win 2038, options [nop,nop,TS val 1552005045 ecr 790017082], length 1326
15:05:03.842458 IP 192.168.0.106.58666 > 31.13.79.53.443: Flags [.], ack 183327, win 2343, options [nop,nop,TS val 790017084 ecr 1552005045], length 0
15:05:03.842869 IP 31.13.79.53.443 > 192.168.0.106.58666: Flags [P.], seq 183327:184840, ack 67482, win 2038, options [nop,nop,TS val 1552005046 ecr 790017082], length 1513
15:05:03.843001 IP 192.168.0.106.58666 > 31.13.79.53.443: Flags [.], ack 184840, win 2332, options [nop,nop,TS val 790017084 ecr 1552005046], length 0
15:05:03.843578 IP 31.13.79.53.443 > 192.168.0.106.58666: Flags [.], seq 184840:187600, ack 67482, win 2038, options [nop,nop,TS val 1552005046 ecr 790017083], length 2760
15:05:03.843789 IP 192.168.0.106.58666 > 31.13.79.53.443: Flags [.], ack 187600, win 2328, options [nop,nop,TS val 790017085 ecr 1552005046], length 0
15:05:03.843713 IP 31.13.79.53.443 > 192.168.0.106.58666: Flags [P.], seq 187600:188937, ack 67482, win 2038, options [nop,nop,TS val 1552005046 ecr 790017083], length 1337
15:05:03.843781 IP 192.168.0.106.58666 > 31.13.79.53.443: Flags [.], ack 188937, win 2343, options [nop,nop,TS val 790017085 ecr 1552005046], length 0
15:05:03.969449 IP 192.168.0.12.62783 > 239.255.255.250.1900: UDP, length 175
15:05:04.036455 IP 192.168.0.12.50647 > 239.255.255.250.1900: UDP, length 175
15:05:04.051557 IP 192.168.0.175.39678 > 239.255.255.250.1900: UDP, length 172
15:05:04.282768 ARP, Request who-has 192.168.0.197 tell 192.168.0.88, length 46
15:05:04.357486 IP 192.168.0.180.5353 > 224.0.0.251.5353: 0 PTR (QM)? _googlecast._tcp.local. (40)
15:05:04.488726 ARP, Request who-has 192.168.0.210 tell 192.168.0.15, length 46
15:05:04.588373 IP 192.168.0.118.54233 > 239.255.255.250.1900: UDP, length 175
15:05:04.619451 IP 192.168.0.118.54234 > 239.255.255.250.1900: UDP, length 175
15:05:04.756198 ARP, Request who-has 192.168.0.35 tell 192.168.0.112, length 46
15:05:04.784829 ARP, Request who-has 192.168.0.197 tell 192.168.0.88, length 46
15:05:04.972385 IP 192.168.0.12.62783 > 239.255.255.250.1900: UDP, length 175
15:05:05.038962 IP 192.168.0.12.50647 > 239.255.255.250.1900: UDP, length 175
15:05:05.250658 ARP, Request who-has 192.168.0.198 tell 192.168.0.195, length 46
^C
1764 packets captured
1768 packets received by filter
4 packets dropped by kernel
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -v -n


Activities
Terminal
Tue 15:12
lab1003@lab1003-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -v -n
tcpdump: listening on enp4s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:06:51.933903 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.14 tell 192.168.0.174, length 46
15:06:52.100532 IP (tos 0x0, ttl 1, id 56224, offset 0, flags [none], proto UDP (17), length 203)
169.254.68.41.55365 > 239.255.255.250.1900: UDP, length 175
15:06:52.139470 IP (tos 0x0, ttl 1, id 6676, offset 0, flags [none], proto UDP (17), length 203)
192.168.0.190.62308 > 239.255.255.250.1900: UDP, length 175
15:06:52.369281 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.72 tell 192.168.0.112, length 46
15:06:52.645069 IP (tos 0x0, ttl 1, id 40612, offset 0, flags [none], proto UDP (17), length 203)
192.168.0.219.62457 > 239.255.255.250.1900: UDP, length 175
15:06:52.684800 IP (tos 0x0, ttl 1, id 6270, offset 0, flags [none], proto UDP (17), length 203)
192.168.0.140.65401 > 239.255.255.250.1900: UDP, length 175
15:06:52.709962 IP (tos 0x0, ttl 1, id 34183, offset 0, flags [DF], proto IGMP (2), length 32, options (RA))
192.168.0.1 > 224.0.0.1: igmp query v2
15:06:52.710079 IP (tos 0x29,ECT(1), ttl 1, id 44798, offset 0, flags [none], proto IGMP (2), length 32, options (RA))
192.168.0.229 > 224.0.0.251: igmp v2 report 224.0.0.251
15:06:52.780869 IP (tos 0x0, ttl 1, id 27997, offset 0, flags [none], proto IGMP (2), length 32, options (RA))
192.168.0.191 > 239.255.102.18: igmp v2 report 239.255.102.18
15:06:52.858519 IP (tos 0x0, ttl 1, id 53118, offset 0, flags [none], proto IGMP (2), length 32, options (RA))
192.168.0.185 > 224.0.0.113: igmp v2 report 224.0.0.113
15:06:53.114555 IP (tos 0x0, ttl 1, id 40613, offset 0, flags [none], proto IGMP (2), length 32, options (RA))
192.168.0.219 > 239.255.255.250: igmp v2 report 239.255.255.250
15:06:53.115771 IP (tos 0x0, ttl 1, id 56225, offset 0, flags [none], proto UDP (17), length 203)
169.254.68.41.55365 > 239.255.255.250.1900: UDP, length 175
15:06:53.147805 IP (tos 0x0, ttl 1, id 6677, offset 0, flags [none], proto UDP (17), length 203)
192.168.0.190.62308 > 239.255.255.250.1900: UDP, length 175
15:06:53.255417 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.72 tell 192.168.0.112, length 46
15:06:53.349415 IP (tos 0x0, ttl 1, id 64390, offset 0, flags [none], proto IGMP (2), length 32, options (RA))
192.168.0.83 > 224.0.0.252: igmp v2 report 224.0.0.252
15:06:53.504974 00:9e:1e:15:44:53 > 34:db:fd:77:e4:61, ethertype Unknown (0xa0a0), length 60:
0x0000: 0017 0101 0101 0101 0101 0101 0101 0101 ....
0x0010: 0101 0101 0101 0101 0101 0101 0101 0101 ....
0x0020: 0101 0101 0101 0101 0101 0101 0101 0101 ....
15:06:53.648540 IP (tos 0x0, ttl 1, id 40614, offset 0, flags [none], proto UDP (17), length 203)
192.168.0.219.62457 > 239.255.255.250.1900: UDP, length 175
15:06:53.669656 IP (tos 0x0, ttl 1, id 33843, offset 0, flags [none], proto IGMP (2), length 32, options (RA))
192.168.0.190 > 224.0.0.251: igmp v2 report 224.0.0.251



CONCLUSION:

- **Summary**: Recap the key differences between Wireshark and TCPDUMP and their respective strengths.
- **Use Cases**: Suggest scenarios where one tool might be more appropriate than the other.
- **Reflection**: Share any insights or challenges you encountered during your study of these tool.