Ishita Hardasmalani

C14-2103058

EXPERIMENT NO.8

Aim: Study and implement of packet sniffer tool: Wireshark

Theory:

Wireshark is a widely-used network protocol analyzer that allows users to capture and inspect network traffic in real-time or from stored data. It offers a user-friendly interface with powerful features such as packet filtering, protocol analysis, and detailed packet inspection. Wireshark is invaluable for network troubleshooting, protocol development, and network security analysis, providing deep insights into network behavior and aiding in the detection of anomalies and security threats. With its extensive capabilities and cross-platform support, Wireshark is an essential tool for network administrators, security analysts, developers, and anyone involved in managing or securing network infrastructure.

Features of Wireshark:

1. Live Packet Capture: Wireshark can capture live network traffic from various interfaces, allowing real-time analysis of data packets as they flow through the network.

2. Deep Protocol Analysis: It provides detailed insights into network protocols by allowing users to inspect packet headers, payloads, and other data fields. This depth of analysis helps in understanding protocol behavior and identifying issues.

3. Flexible Filtering: Wireshark offers powerful filtering capabilities to focus on specific types of network traffic based on various criteria such as IP addresses, port numbers, protocols, and packet contents. This helps in isolating and analyzing relevant packets efficiently.

4. Customizable Display: Users can customize the display of captured packets to suit their preferences and requirements. This includes options to configure packet views, colorization, and protocol hierarchy, enhancing readability and analysis efficiency.

5. Comprehensive Statistics: Wireshark provides detailed statistics on captured network traffic, including traffic volume, protocol usage, packet timing, and error rates. These statistics offer valuable insights into network performance and behavior.

6. Cross-Platform Support: Wireshark is available for multiple operating systems, including Windows, macOS, and Linux, ensuring broad compatibility across different environments. This allows network administrators and analysts to use the tool across various platforms seamlessly.

Steps to download wireshark:

1. Open ubuntu terminal

2. Install wireshark

apt-get install wireshark

3. To know the name of your Ethernet interface: (Mostly it is “etht0”)

#ifconfig

4. Start wireshark

#sudo wireshark

5. Once wireshark window opens, select the interface and click on star

Capturing Packets:

After downloading and installing wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface.

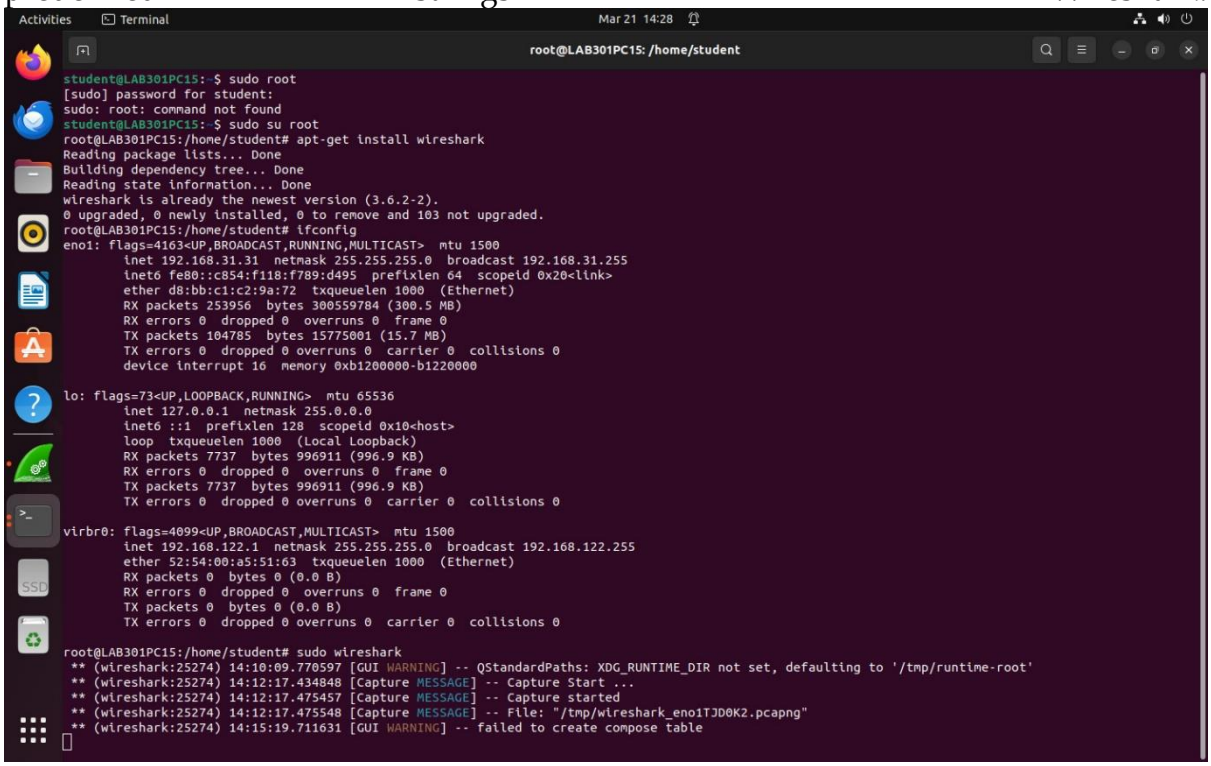
For example, if you want to capture traffic on the wireless network, click your wireless interface.You can configure advanced features by clicking Capture Options.

As soon as you click the interface‘s name, you‘ll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

Click the stop capture button near the top left corner of the window when you want to stop capturing traffic Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order. Wireshark can record the capturing information in the file with extension .pcap (packet capture).

This file can be reopened for analysis in offline mode.

There is no need to remember filtering commands. Filters can be applied by putting predefined strings in Wireshark.



Activities Terminal Mar 21 14:27

Screenshot captured
You can paste the image from the clipboard.

```
After this operation, 310 kB of additional disk
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/
Fetched 108 kB in 1s (100 kB/s)
Selecting previously unselected package xinetd.
(Reading database ... 220509 files and directories currently installed.)
Preparing to unpack .../xinetd_1%3a2.3.15.3-1_amd64.deb ...
Unpacking xinetd (1:2.3.15.3-1) ...
Setting up xinetd (1:2.3.15.3-1) ...
Processing triggers for man-db (2.10.2-1) ...
root@LAB301PC15:/home/student# cd/etc
bash: cd/etc: No such file or directory
root@LAB301PC15:/home/student# cd /etc
root@LAB301PC15:/etc# ls
acpi                          mailcap
adduser.conf                  mailcap.order
alsa                          manpath.config
alternatives                  mdevctl.d
anacrontab                    mecabrc
apache2                       mime.types
apg.conf                      mke2fs.conf
apm                           ModemManager
apparmor                      modprobe.d
apparmor.d                    modules
apport                        modules-load.d
appstream.conf                mtab
apt                           mysql
avahi                         nanorc
bash.bashrc                   netconfig
bash_completion               netplan
bash_completion.d             network
bindresvport.blacklist        networkd-dispatcher
binfmt.d                      NetworkManager
bluetooth                     networks
brlapi.key                    newt
brltty                        nftables.conf
brltty.conf                   nsswitch.conf
ca-certificates               openal
ca-certificates.conf          openvpn
ca-certificates.conf.dpkg-old opt
chatscripts                   os-release
console-setup                 PackageKit
cracklib                      pam.conf
cron.d                        pam.d
cron.daily                    papersize
cron.hourly                   passwd
cron.monthly                  passwd-
```

Activities Terminal Mar 21 14:27

Screenshot captured
You can paste the image from the clipbord.

```
alsa                          manpath.config
alternatives                  mdevctl.d
anacrontab                    mecabrc
apache2                       mime.types
apg.conf                      mke2fs.conf
apm                           ModemManager
apparmor                      modprobe.d
apparmor.d                    modules
apport                        modules-load.d
appstream.conf                mtab
apt                           mysql
avahi                         nanorc
bash.bashrc                   netconfig
bash_completion               netplan
bash_completion.d             network
bindresvport.blacklist        networkd-dispatcher
binfmt.d                      NetworkManager
bluetooth                     networks
brlapi.key                    newt
brltty                        nftables.conf
brltty.conf                   nsswitch.conf
ca-certificates               openal
ca-certificates.conf          openvpn
ca-certificates.conf.dpkg-old opt
chatscripts                   os-release
console-setup                 PackageKit
cracklib                      pam.conf
cron.d                        pam.d
cron.daily                    papersize
cron.hourly                   passwd
cron.monthly                  passwd-
crontab                       pcmcia
cron.weekly                   perl
cups                          pki
cupshelpers                   pm
dbus-1                        pnm2ppa.conf
dconf                         polkit-1
debconf.conf                  ppp
debian_version                printcap
default                       profile
deluser.conf                  profile.d
depmod.d                      protocols
dhcp                          pulse
dictionaries-common           python3
dnsmasq.d                     python3.10
dnsmasq.d-available           qemu-ifdown
```

Activities Terminal Mar 21 14:27

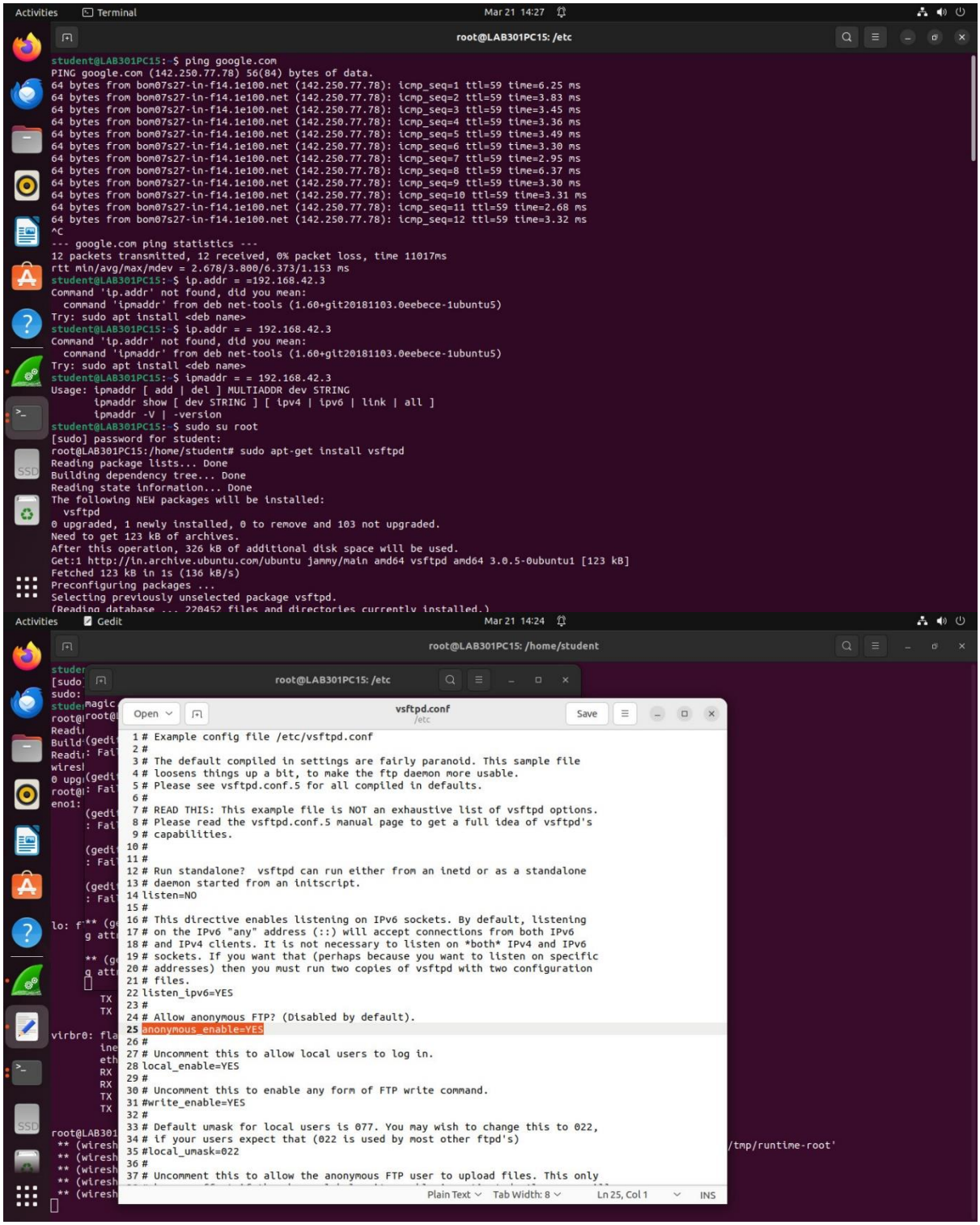
Screenshot captured
You can paste the image from the clipboard.

```
libblockdev                     UPower
libtbverbs.d                    usb_modeswitch.conf
libnl-3                         usb_modeswitch.d
libpaper.d                      vdpau_wrapper.cfg
libreoffice                     vim
libvirt                         vsftpd.conf
lighttpd                        vtrgb
locale.alias                    vulkan
locale.gen                      wgetrc
localtime                       wireshark
logcheck                        wpa_supplicant
login.defs                      X11
logrotate.conf                  xattr.conf
logrotate.d                     xdg
lsb-release                     xinetd.conf
lvm                             xinetd.d
machine-id                      xml
magic                           zsh_command_not_found
magic.mime
root@LAB301PC15:/etc# gedit vsftpd.conf

(gedit:26096): dconf-WARNING **: 14:23:37.015: failed to commit changes to dconf: Failed to execute child process “dbus-launch” (No such file or direc
tory)

(gedit:26096): dconf-WARNING **: 14:23:37.018: failed to commit changes to dconf: Failed to execute child process “dbus-launch” (No such file or direc
tory)

(gedit:26096): dconf-WARNING **: 14:23:37.127: failed to commit changes to dconf: Failed to execute child process “dbus-launch” (No such file or direc
tory)

(gedit:26096): dconf-WARNING **: 14:23:37.127: failed to commit changes to dconf: Failed to execute child process “dbus-launch” (No such file or direc
tory)

(gedit:26096): dconf-WARNING **: 14:23:37.127: failed to commit changes to dconf: Failed to execute child process “dbus-launch” (No such file or direc
tory)

** (gedit:26096): WARNING **: 14:23:57.084: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported

** (gedit:26096): WARNING **: 14:23:57.084: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

** (gedit:26096): WARNING **: 14:24:12.141: Set document metadata failed: Setting attribute metadata::gedit-position not supported

(gedit:26096): dconf-WARNING **: 14:24:12.169: failed to commit changes to dconf: Failed to execute child process “dbus-launch” (No such file or direc
tory)
root@LAB301PC15:/etc# service xinetd restart
root@LAB301PC15:/etc# service vsftpd restart
```

Activities Terminal Mar 21 14:27

Screenshot captured
You can paste the image from the clipboard.

```
student@LAB301PC15:~$ sudo su root
[sudo] password for student:
root@LAB301PC15:/home/student# sudo apt-get install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 103 not upgraded.
Need to get 123 kB of archives.
After this operation, 326 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 vsftpd amd64 3.0.5-0ubuntu1 [123 kB]
Fetched 123 kB in 1s (136 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 220452 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0ubuntu1_amd64.deb ...
Unpacking vsftpd (3.0.5-0ubuntu1) ...
Setting up vsftpd (3.0.5-0ubuntu1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.service.
Detected unsafe path transition / (owned by admini) → /run (owned by root) during canonicalization of /run/vsftpd.
Processing triggers for man-db (2.10.2-1) ...
root@LAB301PC15:/home/student# sudo apt-get install xinetd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  xinetd
0 upgraded, 1 newly installed, 0 to remove and 103 not upgraded.
Need to get 108 kB of archives.
After this operation, 310 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 xinetd amd64 1:2.3.15.3-1 [108 kB]
Fetched 108 kB in 1s (100 kB/s)
Selecting previously unselected package xinetd.
(Reading database ... 220509 files and directories currently installed.)
Preparing to unpack .../xinetd_1%3a2.3.15.3-1_amd64.deb ...
Unpacking xinetd (1:2.3.15.3-1) ...
Setting up xinetd (1:2.3.15.3-1) ...
Processing triggers for man-db (2.10.2-1) ...
root@LAB301PC15:/home/student# cd/etc
bash: cd/etc: No such file or directory
root@LAB301PC15:/home/student# cd /etc
root@LAB301PC15:/etc# ls
acpi                            mailcap
adduser.conf                    mailcap.order
alias                           manpath.config
```



Commands:-

1. Capturing packets of a particular host

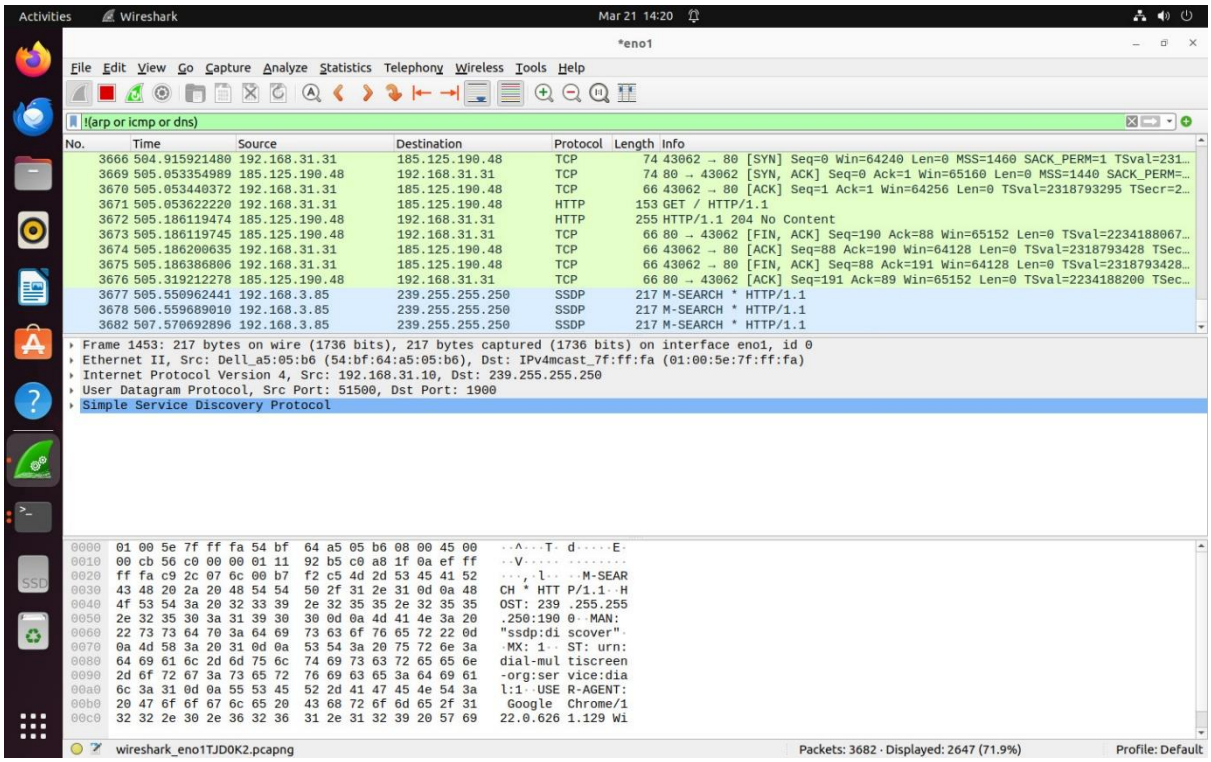
ip.addr = = 192.163.31.45

Sets a filter for any packet with 192.163.31.45, as either the source or destination.

2. To capture a conversation between specified hosts

ip.addr == 192.163.31.45 && ip.addr == 104.26.2.23

Sets a conversation filter between the two defined IP addresses



The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type —dns and you'll see only DNS packets. When you start typing, Wireshark will help you auto complete your filter.

Commands:-

1. To filter packets for a specific protocol : http

Activities Wireshark Mar 21 14:20

*eno1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

No.	Time	Source	Destination	Protocol	Length	Info
3324	468.026479191	192.168.3.85	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3329	468.925605676	192.44.44.202	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3330	468.925606036	192.44.44.202	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3336	469.033273370	192.168.3.85	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3339	469.941369469	192.44.44.202	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3340	469.941369865	192.44.44.202	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3342	470.035293232	192.168.3.85	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3359	470.956869286	192.44.44.202	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3360	470.956869631	192.44.44.202	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
3384	471.627602550	192.168.31.17	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3466	474.627255088	192.168.31.17	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3499	477.641736101	192.168.31.17	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1

```
Frame 1453: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface eno1, id 0
Ethernet II, Src: Dell_a5:05:b6 (54:bf:64:a5:05:b6), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.31.10, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 51500, Dst Port: 1900
Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 54 bf  64 a5 05 b6 08 00 45 00   ··^···T· d·····E·
0010  00 cb 56 c0 00 00 01 11  92 b5 c0 a8 1f 0a ef ff   ··V····· ........
0020  ff fa c9 2c 07 6c 00 b7  f2 c5 4d 2d 53 45 41 52   ···,·l·· ··M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN:
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST: urn:
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e   dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61   -org:ser vice:dia
00a0  6c 3a 31 0d 0a 55 53 45  52 2d 41 47 45 4e 54 3a   l:1··USE R-AGENT:
00b0  20 47 6f 6f 67 6c 65 20  43 68 72 6f 6d 65 2f 31    Google  Chrome/1
00c0  32 32 2e 30 2e 36 32 36  31 2e 31 32 39 20 57 69   22.0.626 1.129 Wi
```

Request: Boolean Packets: 3500 · Displayed: 668 (19.1%) Profile: Default

Activities Wireshark Mar 21 14:18

*eno1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Go to the next packet

tcp.flags.reset==0

No.	Time	Source	Destination	Protocol	Length	Info
1040	106.851198981	192.168.31.31	162.213.33.48	TCP	74	39088 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=86…
1051	107.855891618	192.168.31.31	162.213.33.48	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39088 → 443 [SYN] Seq=…
1061	108.879792734	192.168.31.31	162.213.33.48	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39088 → 443 [SYN] Seq=…
1070	109.903778441	192.168.31.31	162.213.33.48	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39088 → 443 [SYN] Seq=…
1077	110.927889319	192.168.31.31	162.213.33.48	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39088 → 443 [SYN] Seq=…
1081	111.951781236	192.168.31.31	162.213.33.48	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39088 → 443 [SYN] Seq=…
1086	113.967792344	192.168.31.31	162.213.33.48	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39088 → 443 [SYN] Seq=…
1456	204.910478506	192.168.31.31	91.189.91.98	TCP	74	40162 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=139…
1458	205.118600276	91.189.91.98	192.168.31.31	TCP	74	80 → 40162 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1440 SACK_PERM=…
1459	205.118681087	192.168.31.31	91.189.91.98	TCP	66	40162 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1394942343 TSecr=1…
1460	205.118854833	192.168.31.31	91.189.91.98	HTTP	153	GET / HTTP/1.1
1461	205.327323103	91.189.91.98	192.168.31.31	HTTP	251	HTTP/1.1 204 No Content

```
Frame 1456: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eno1, id 0
Ethernet II, Src: Micro-St_c2:9a:72 (d8:bb:c1:c2:9a:72), Dst: 9c:53:22:05:6a:19 (9c:53:22:05:6a:19)
Internet Protocol Version 4, Src: 192.168.31.31, Dst: 91.189.91.98
Transmission Control Protocol, Src Port: 40162, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  9c 53 22 05 6a 19 d8 bb  c1 c2 9a 72 08 00 45 00   ·S"·j··· ···r··E·
0010  00 3c 4d 71 40 00 40 06  56 64 c0 a8 1f 1f 5b bd   ·<Mq@·@· Vd····[·
0020  5b 62 9c e2 00 50 44 12  0a 8f 00 00 00 00 a0 02   [b···PD· ........
0030  fa f0 97 15 00 00 02 04  05 b4 04 02 08 0a 53 25   ........ ......S%
0040  20 b7 00 00 00 00 01 03  03 07                      ........ ··
```

wireshark_eno1TJD0K2.pcapng Packets: 2646 · Displayed: 20 (0.8%) Profile: Default

Activities Wireshark Mar 21 14:17

*eno1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
1456	204.910478506	192.168.31.31	91.189.91.98	TCP	74	40162 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1394…
1458	205.118600276	91.189.91.98	192.168.31.31	TCP	74	80 → 40162 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1440 SACK_PERM=1…
1459	205.118681087	192.168.31.31	91.189.91.98	TCP	66	40162 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1394942343 TSecr=18…
1460	205.118854833	192.168.31.31	91.189.91.98	HTTP	153	GET / HTTP/1.1
1461	205.327323103	91.189.91.98	192.168.31.31	HTTP	251	HTTP/1.1 204 No Content
1462	205.327323362	91.189.91.98	192.168.31.31	TCP	66	80 → 40162 [FIN, ACK] Seq=186 Ack=88 Win=65152 Len=0 TSval=1801378536 …
1463	205.327398933	192.168.31.31	91.189.91.98	TCP	66	40162 → 80 [ACK] Seq=88 Ack=186 Win=64128 Len=0 TSval=1394942552 TSecr…
1464	205.327579338	192.168.31.31	91.189.91.98	TCP	66	40162 → 80 [FIN, ACK] Seq=88 Ack=187 Win=64128 Len=0 TSval=1394942552 …
1465	205.536095508	91.189.91.98	192.168.31.31	TCP	66	80 → 40162 [ACK] Seq=187 Ack=89 Win=65152 Len=0 TSval=1801378744 TSecr…

```
▸ Frame 1456: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eno1, id 0
▸ Ethernet II, Src: Micro-St_c2:9a:72 (d8:bb:c1:c2:9a:72), Dst: 9c:53:22:05:6a:19 (9c:53:22:05:6a:19)
▸ Internet Protocol Version 4, Src: 192.168.31.31, Dst: 91.189.91.98
▸ Transmission Control Protocol, Src Port: 40162, Dst Port: 80, Seq: 0, Len: 0

0000  9c 53 22 05 6a 19 d8 bb  c1 c2 9a 72 08 00 45 00   ·S"·j··· ···r··E·
0010  00 3c 4d 71 40 00 40 06  56 64 c0 a8 1f 1f 5b bd   ·<Mq@·@· Vd····[·
0020  5b 62 9c e2 00 50 44 12  0a 8f 00 00 00 00 a0 02   [b···PD· ********
0030  fa f0 97 15 00 00 02 04  05 b4 04 02 08 0a 53 25   ******** ******S%
0040  20 b7 00 00 00 00 01 03  03 07                      ******** **
```

wireshark_eno1TJD0K2.pcapng Packets: 2308 · Displayed: 9 (0.4%) Profile: Default

Activities Wireshark Mar 21 14:17

*eno1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

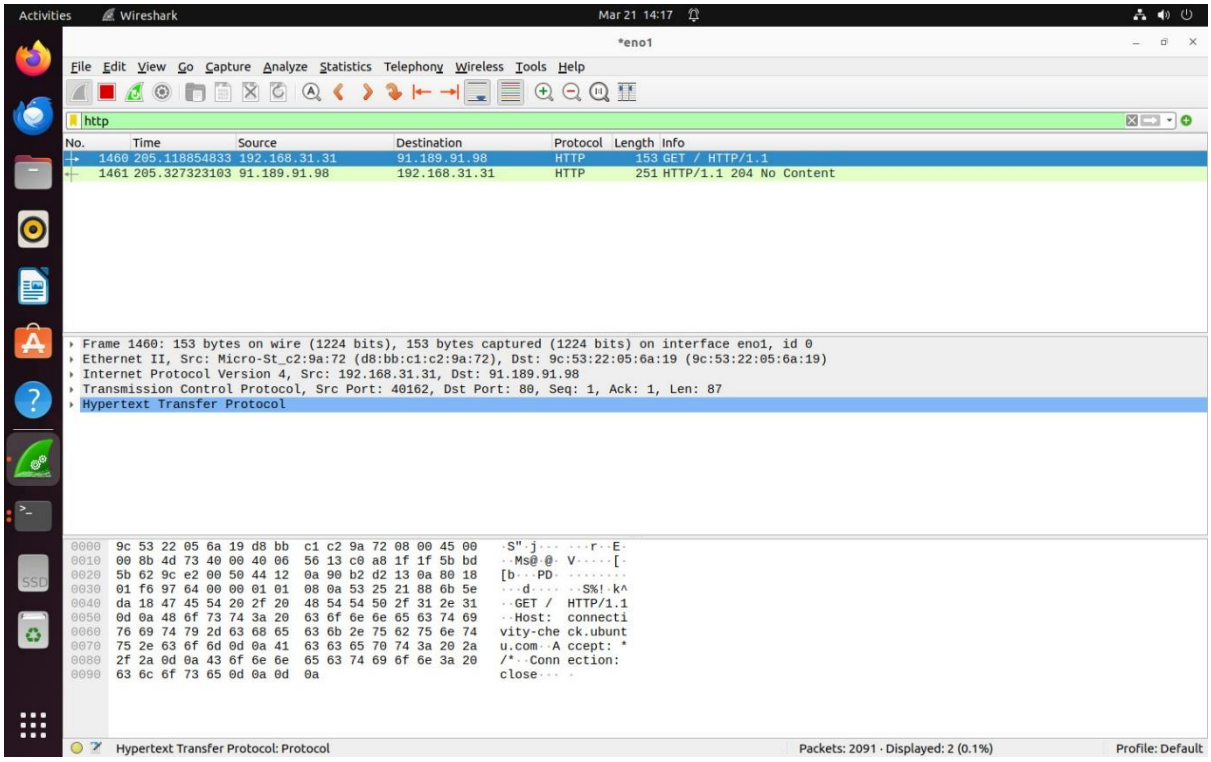
Draw packets using your coloring rules

dns

No.	Time	Source	Destination	Protocol	Length	Info
947	98.171550826	203.212.24.46	192.168.31.31	DNS	97	Standard query response 0xa97b A google.com A 142.250.77.78 OPT
948	98.171551078	203.212.24.46	192.168.31.31	DNS	109	Standard query response 0xfba3 AAAA google.com AAAA 2404:6800:4009:81…
951	98.179630217	192.168.31.31	203.212.24.46	DNS	97	Standard query 0x22f5 PTR 78.77.250.142.in-addr.arpa OPT
952	98.183509869	203.212.24.46	192.168.31.31	DNS	136	Standard query response 0x22f5 PTR 78.77.250.142.in-addr.arpa PTR bom…
1036	106.848316305	192.168.31.31	203.212.24.46	DNS	89	Standard query 0xed8c A metrics.ubuntu.com OPT
1037	106.848523037	192.168.31.31	203.212.24.46	DNS	89	Standard query 0x7aac AAAA metrics.ubuntu.com OPT
1038	106.850065696	203.212.24.46	192.168.31.31	DNS	169	Standard query response 0xed8c A metrics.ubuntu.com A 162.213.33.48 N…
1039	106.850744275	203.212.24.46	192.168.31.31	DNS	150	Standard query response 0x7aac AAAA metrics.ubuntu.com SOA ns1.canoni…
1088	114.906532016	192.168.31.31	203.212.24.46	DNS	100	Standard query 0x3ccd AAAA connectivity-check.ubuntu.com OPT
1089	114.909093196	203.212.24.46	192.168.31.31	DNS	500	Standard query response 0x3ccd AAAA connectivity-check.ubuntu.com AAA…
1454	204.906051754	192.168.31.31	203.212.24.46	DNS	100	Standard query 0x6720 A connectivity-check.ubuntu.com OPT
1455	204.908835347	203.212.24.46	192.168.31.31	DNS	356	Standard query response 0x6720 A connectivity-check.ubuntu.com A 91.1…

```
▸ Frame 1455: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits) on interface eno1, id 0
▸ Ethernet II, Src: 9c:53:22:05:6a:19 (9c:53:22:05:6a:19), Dst: Micro-St_c2:9a:72 (d8:bb:c1:c2:9a:72)
▸ Internet Protocol Version 4, Src: 203.212.24.46, Dst: 192.168.31.31
▸ User Datagram Protocol, Src Port: 53, Dst Port: 57962
▸ Domain Name System (response)

0000  d8 bb c1 c2 9a 72 9c 53  22 05 6a 19 08 00 45 00   ******r· S"·j···E·
0010  01 56 5f cd 00 00 3d 11  59 00 cb d4 18 2e c0 a8   ·V_···=· Y·····,··
0020  1f 1f 00 35 e2 6a 01 42  d4 bf 67 20 81 80 00 01   ···5·j·B ··g ····
0030  00 0c 00 03 00 01 12 63  6f 6e 6e 65 63 74 69 76   *******c onnectiv
0040  69 74 79 2d 63 68 65 63  6b 06 75 62 75 6e 74 75   ity-chec k·ubuntu
0050  03 63 6f 6d 00 00 01 00  01 c0 0c 00 01 00 01 00   ·com···· ********
0060  00 00 1b 00 04 5b bd 5b  62 c0 0c 00 01 00 01 00   *****[·[ b*******
0070  00 00 1b 00 04 b9 7d be  30 c0 0c 00 01 00 01 00   ******}· 0*******
0080  00 00 1b 00 04 b9 7d be  62 c0 0c 00 01 00 01 00   ******}· b*******
0090  00 00 1b 00 04 b9 7d be  31 c0 0c 00 01 00 01 00   ******}· 1*******
00a0  00 00 1b 00 04 b9 7d be  61 c0 0c 00 01 00 01 00   ******}· a*******
00b0  00 00 1b 00 04 5b bd 5b  31 c0 0c 00 01 00 01 00   *****[·[ 1*******
00c0  00 00 1b 00 04 b9 7d be  12 c0 0c 00 01 00 01 00   ******}· ********
```

Domain Name System: Protocol Packets: 2116 · Displayed: 14 (0.7%) Profile: Default



<u>To capture packets from the FTP server. (Login ID and Password)</u>

What is FTP?

FTP stands for File Transfer Protocol. As the name suggest this network protocol allows you to transfer files or directories from one host to another over the network whether it is your LAN or Internet.The package required to install FTP is known as VSFTPD (Very Secure File Transfer ProtocolDaemon)/

Steps:-

1. Get root access: $ sudo su root

2. Find your ip address: # ifconfig

<u>Installation of FTP server in Ubuntu</u>

Name of Packages required: VSFTPD, XINETD

1. # sudo apt-get install vsftpd

2. # sudo apt-get install xinetd

The above command will install and start the xinetd superserver on your system. The chances are that you already have xinetd installed on your system. In that case you can omit the above installation command. In the next step we need to edit the FTP server's configuration file which is present in /etc/vsftpd.conf.

3. # cd /etc

4. # ls

5. # gedit vsftpd.conf

Change the following line:

Anonymous_enable=NO To Anonymous_enable=YES

This will instruct the FTP server to allow connecting with an anonymous client.

6. Save and close the gedit file

Now, that we are ready we can start the FTP server in the normal mode with:

7. # service xinetd restart

8. # service vsftpd restart OR # init.d/vsftpd restart

Connecting to a client present in other machine

$ ftp ip address of the FTP server

Name: anonymous

Please specify the password.

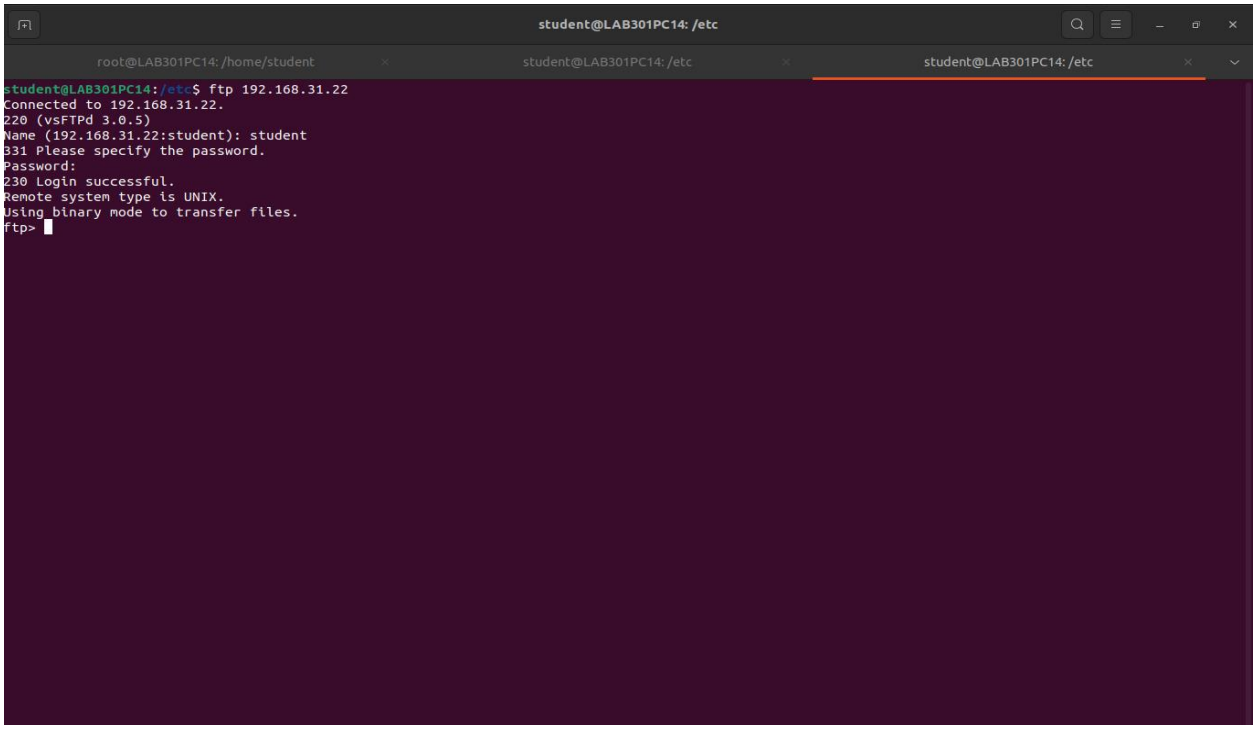
Password:

Login successful. (even if the login is not successful then also wireshark will capture the id and password)

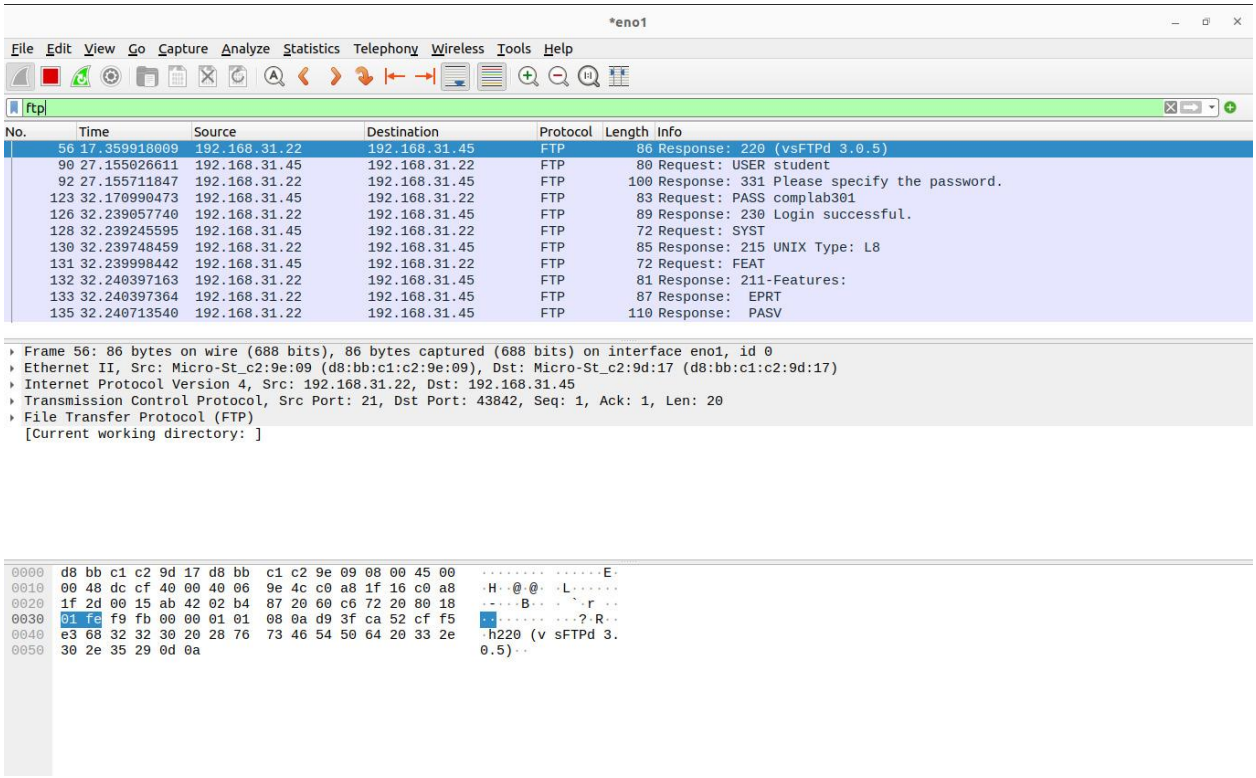
ftp>

ftp> quit

Goodbye.



Start WIRESHARK. In the FILTER field put FTP. This will filter all FTP packets



While the client is establishing a connection with the FTP server, the wireshark running in the background of the FTP server is able to capture all FTP packets. So, the Name and Password entered by the client is visible in plain text in Wireshark. Apart from that the source and the destination address is also visible. If many clients are trying to connect with the server then source address, name and password are visible for all of them.