

### **Aim: Examine the use of packet sniffer tool: Wireshark**

- a) Download and install wireshark and capture different packets like icmp, tcp and http packets**
- b) Explore how the packets can be traced based on different filters**
- c) Capture packets of FTP and retrieve login ID and Password**

### **Theory:-**

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.

Wireshark is used for:

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets.

Features of Wireshark :

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.

Create various statistics.

### **Steps:**

1. Open ubuntu terminal
2. Install wireshark  
# apt-get install wireshark
3. To know the name of your Ethernet interface: (Mostly it is "eth0")  
#ifconfig
4. Start wireshark  
#sudo wireshark
5. Once wireshark window opens, select the interface and click on start

### **a) 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 again reopened for analysis in offline mode.

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

### Commands:-

1. Capturing packets of a particular host

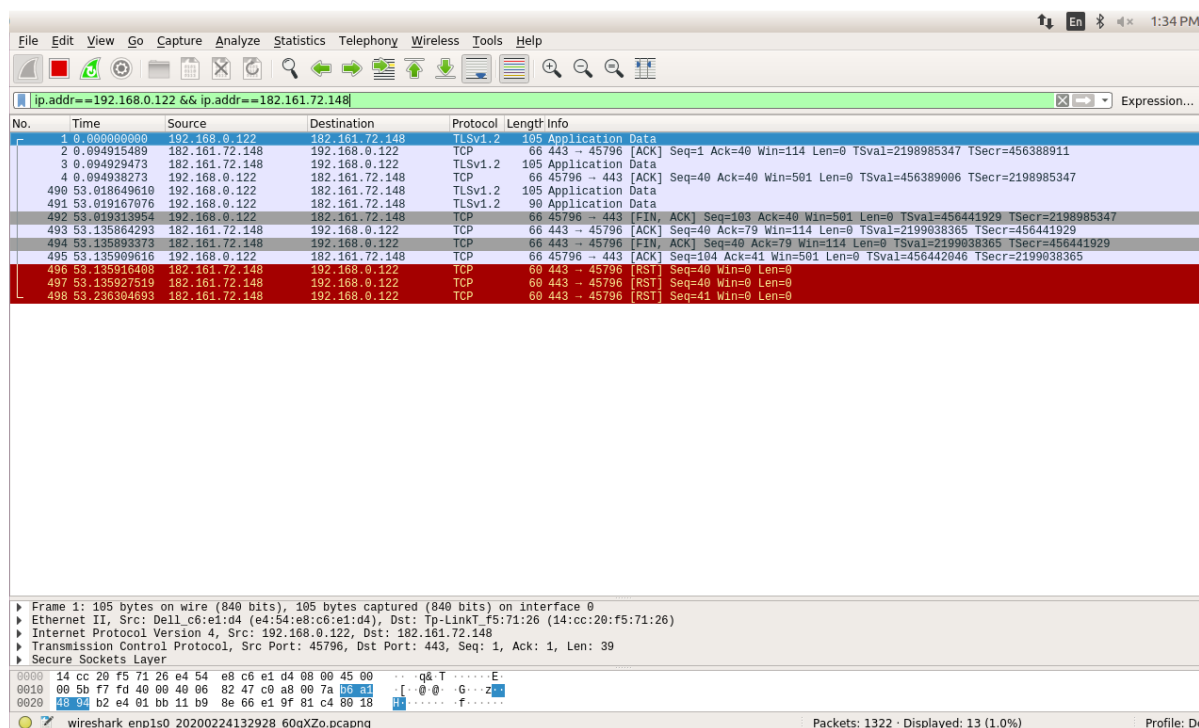
`ip.addr == 192.168.42.3`

Sets a filter for any packet with 192.168.42.3, as either the source or destination.

2. To capture a conversation between specified hosts

`ip.addr == 10.0.5.119 && ip.addr == 91.189.94.25`

Sets a conversation filter between the two defined IP addresses.



### b) Filtering Packets

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 or dns`

Sets a filter to display all http and dns requests.

\*enp1s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
3676	71.293127199	203.212.24.46	192.168.0.122	DNS	254	Standard query response 0xd495 AAAA fls-eu.amazon.in CNAME fls-eu.amazon.com CNAME gateway.prod.e...
3701	71.455403868	203.212.24.46	192.168.0.122	DNS	127	Standard query response 0x0c95 AAAA unagi-eu.amazon.com SOA ns-921.amazon.com
3702	71.456777797	203.212.24.46	192.168.0.122	DNS	141	Standard query response 0x9730 AAAA completion.amazon.co.uk SOA ns-923.amazon.com
3706	71.490960909	203.212.24.46	192.168.0.122	DNS	95	Standard query response 0xe281 A unagi-eu.amazon.com A 54.239.36.249
3707	71.491626568	192.168.0.122	203.212.24.46	DNS	79	Standard query 0xb6ff A unagi-eu.amazon.com
3708	71.491695058	192.168.0.122	203.212.24.46	DNS	79	Standard query 0x388f AAAA unagi-eu.amazon.com
3709	71.492490139	203.212.24.46	192.168.0.122	DNS	99	Standard query response 0x3ee3 A completion.amazon.co.uk A 52.95.118.208
3710	71.492507951	203.212.24.46	192.168.0.122	DNS	95	Standard query response 0x6faf A unagi-eu.amazon.com A 54.239.36.249
3711	71.493065985	192.168.0.122	203.212.24.46	DNS	83	Standard query 0x6417 A completion.amazon.co.uk
3712	71.493106427	192.168.0.122	203.212.24.46	DNS	83	Standard query 0xb6f4 AAAA completion.amazon.co.uk
3713	71.493732843	203.212.24.46	192.168.0.122	DNS	127	Standard query response 0x300f AAAA unagi-eu.amazon.com SOA ns-921.amazon.com
3714	71.494100821	203.212.24.46	192.168.0.122	DNS	99	Standard query response 0x6417 A completion.amazon.co.uk A 52.95.118.208
3715	71.494135363	203.212.24.46	192.168.0.122	DNS	141	Standard query response 0xb6f4 AAAA completion.amazon.co.uk SOA ns-923.amazon.com
3809	74.862733234	192.168.0.122	203.212.24.18	DNS	91	Standard query 0x407f A images-na.ssl-images-amazon.com
3810	74.862750526	192.168.0.122	203.212.24.18	DNS	91	Standard query 0x407f A images-na.ssl-images-amazon.com
3811	74.862786458	192.168.0.122	203.212.24.18	DNS	91	Standard query 0xb118 AAAA images-na.ssl-images-amazon.com
3812	74.862793616	192.168.0.122	203.212.24.18	DNS	91	Standard query 0xb118 AAAA images-na.ssl-images-amazon.com
3813	74.864633635	203.212.24.18	192.168.0.122	DNS	217	Standard query response 0xb118 AAAA images-na.ssl-images-amazon.com CNAME m.media-amazon.com CNAM...
3814	74.864657580	203.212.24.18	192.168.0.122	DNS	289	Standard query response 0x407f A images-na.ssl-images-amazon.com CNAME m.media-amazon.com CNAME c...
3815	74.864698457	203.212.24.18	192.168.0.122	DNS	289	Standard query response 0x407f A images-na.ssl-images-amazon.com CNAME m.media-amazon.com CNAME c...
3816	74.864517941	203.212.24.46	192.168.0.122	DNS	217	Standard query response 0xb118 AAAA images-na.ssl-images-amazon.com CNAME m.media-amazon.com CNAM...
3817	74.865168115	192.168.0.122	203.212.24.18	DNS	91	Standard query 0x5584 A images-na.ssl-images-amazon.com
3818	74.865210805	192.168.0.122	203.212.24.18	DNS	91	Standard query 0x358e AAAA images-na.ssl-images-amazon.com
3819	74.866451557	203.212.24.18	192.168.0.122	DNS	289	Standard query response 0x5584 A images-na.ssl-images-amazon.com CNAME m.media-amazon.com CNAME c...
3820	74.866472910	203.212.24.18	192.168.0.122	DNS	217	Standard query response 0x358e AAAA images-na.ssl-images-amazon.com CNAME m.media-amazon.com CNAM...
3821	74.903107415	192.168.0.122	203.212.24.18	DNS	86	Standard query 0x674d A ocsf.scaib.amazonaws.com
3822	74.904373035	203.212.24.18	192.168.0.122	DNS	287	Standard query response 0x674d A ocsf.scaib.amazonaws.com A 13.227.178.113 A 13.227.178.148 A 1...
3823	74.904484100	192.168.0.122	203.212.24.18	DNS	86	Standard query 0x393c AAAA ocsf.scaib.amazonaws.com
3824	74.904486912	192.168.0.122	203.212.24.18	DNS	86	Standard query 0x393c AAAA ocsf.scaib.amazonaws.com
3825	74.905593761	203.212.24.18	192.168.0.122	DNS	167	Standard query response 0x939c AAAA ocsf.scaib.amazonaws.com SOA ns-612.awsdns-12.net
3826	74.905597550	203.212.24.18	192.168.0.122	DNS	167	Standard query response 0x939c AAAA ocsf.scaib.amazonaws.com SOA ns-612.awsdns-12.net
3827	74.905793291	192.168.0.122	203.212.24.18	DNS	86	Standard query 0x7a49 A ocsf.scaib.amazonaws.com
3828	74.907331758	203.212.24.18	192.168.0.122	DNS	287	Standard query response 0x7a49 A ocsf.scaib.amazonaws.com A 13.227.178.113 A 13.227.178.148 A 1...
3829	74.907474722	192.168.0.122	203.212.24.18	DNS	86	Standard query 0x73ab AAAA ocsf.scaib.amazonaws.com
3830	74.908567859	203.212.24.18	192.168.0.122	DNS	167	Standard query response 0x73ab AAAA ocsf.scaib.amazonaws.com SOA ns-612.awsdns-12.net

Frame 3830: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface 0  
 Ethernet II, Src: Tp-LinkTf5:71:26 (14:cc:20:f5:71:26), Dst: Dell\_c6:e1:d4 (e4:54:e8:c6:e1:d4)  
 Internet Protocol Version 4, Src: 203.212.24.18, Dst: 192.168.0.122  
 User Datagram Protocol, Src Port: 53, Dst Port: 52524  
 Domain Name System (response)

0000 e4 54 e8 c6 e1 d4 14 cc 20 f5 71 26 08 00 45 00 -T----- q&-E-  
 0010 00 99 cc 9b 00 00 3d 11 0b b9 cb d4 18 12 c0 a8 -.....-z-.....  
 0020 00 7a 00 35 cc 1e 00 8d c3 88 73 ab 81 00 00 01 -z-.....-s-.....

Domain Name System: Protocol

Packets: 3923 · Displayed: 151 (3.8%) Profile: Default

## 2. To filter packets for specific port

tcp.port==4000

Sets a filter for any TCP packet with 4000 as a source or destination port.

\*enp1s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
3831	74.908778533	192.168.0.122	13.227.178.113	TCP	74	46120 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=343982786 TSecr=0 WS=128
3832	74.908779845	192.168.0.122	13.227.178.113	TCP	74	46122 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=343982786 TSecr=0 WS=128
3833	74.912228569	13.227.178.113	192.168.0.122	TCP	74	80 → 46122 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1440 SACK_PERM=1 TSval=290952749 TSecr=3439...
3834	74.912245864	192.168.0.122	13.227.178.113	TCP	66	46122 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=343982790 TSecr=290952749
3835	74.912272587	13.227.178.113	192.168.0.122	TCP	74	80 → 46120 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1440 SACK_PERM=1 TSval=295444451 TSecr=3439...
3836	74.912275523	192.168.0.122	13.227.178.113	TCP	66	46120 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=343982790 TSecr=295444451
3837	74.912417984	192.168.0.122	13.227.178.113	OCSP	454	Request
3838	74.912650496	192.168.0.122	13.227.178.113	OCSP	454	Request
3839	74.914689826	13.227.178.113	192.168.0.122	TCP	66	80 → 46122 [ACK] Seq=1 Ack=389 Win=30208 Len=0 TSval=290952750 TSecr=343982790
3840	74.915727982	13.227.178.113	192.168.0.122	TCP	66	80 → 46120 [ACK] Seq=1 Ack=389 Win=30208 Len=0 TSval=295444451 TSecr=343982790
3841	75.152448731	13.227.178.113	192.168.0.122	OCSP	1072	Response
3842	75.152491558	192.168.0.122	13.227.178.113	TCP	66	46122 → 80 [ACK] Seq=389 Ack=1007 Win=64128 Len=0 TSval=343983030 TSecr=290952773
3843	75.153361055	13.227.178.113	192.168.0.122	OCSP	1072	Response
3844	75.153394305	192.168.0.122	13.227.178.113	TCP	66	46120 → 80 [ACK] Seq=389 Ack=1007 Win=64128 Len=0 TSval=343983031 TSecr=295444475
3873	85.164758584	192.168.0.122	13.227.178.113	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=388 Ack=1007 Win=64128 Len=0 TSval=343993042 TSecr=295444475
3874	85.164774329	192.168.0.122	13.227.178.113	TCP	66	[TCP Keep-Alive] 46122 → 80 [ACK] Seq=388 Ack=1007 Win=64128 Len=0 TSval=343993042 TSecr=290952773
3875	85.167648928	13.227.178.113	192.168.0.122	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=1007 Ack=389 Win=30208 Len=0 TSval=295445476 TSecr=2489
3876	85.168321389	13.227.178.113	192.168.0.122	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=1007 Ack=389 Win=30208 Len=0 TSval=290953775 TSecr=3439...
3918	95.404661733	192.168.0.122	13.227.178.113	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=388 Ack=1007 Win=64128 Len=0 TSval=344003282 TSecr=295445476
3919	95.404678126	192.168.0.122	13.227.178.113	TCP	66	[TCP Keep-Alive] 46122 → 80 [ACK] Seq=388 Ack=1007 Win=64128 Len=0 TSval=344003282 TSecr=290953775
3920	95.406824648	13.227.178.113	192.168.0.122	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=1007 Ack=389 Win=30208 Len=0 TSval=295446500 TSecr=3439...
3921	95.407855302	13.227.178.113	192.168.0.122	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=1007 Ack=389 Win=30208 Len=0 TSval=290954799 TSecr=3439...
3937	105.644522603	192.168.0.122	13.227.178.113	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=388 Ack=1007 Win=64128 Len=0 TSval=344013521 TSecr=295446500
3938	105.644530819	192.168.0.122	13.227.178.113	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=388 Ack=1007 Win=64128 Len=0 TSval=344013521 TSecr=290954799
3939	105.648072040	13.227.178.113	192.168.0.122	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=1007 Ack=389 Win=30208 Len=0 TSval=295447524 TSecr=3439...
3940	105.648258558	13.227.178.113	192.168.0.122	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=1007 Ack=389 Win=30208 Len=0 TSval=290955823 TSecr=3439...
3978	115.884526742	192.168.0.122	13.227.178.113	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=388 Ack=1007 Win=64128 Len=0 TSval=344023761 TSecr=295447524
3979	115.884540132	192.168.0.122	13.227.178.113	TCP	66	[TCP Keep-Alive] 46122 → 80 [ACK] Seq=388 Ack=1007 Win=64128 Len=0 TSval=344023761 TSecr=290955823
3980	115.887497930	13.227.178.113	192.168.0.122	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=1007 Ack=389 Win=30208 Len=0 TSval=290956847 TSecr=3439...
3981	115.887891870	13.227.178.113	192.168.0.122	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=1007 Ack=389 Win=30208 Len=0 TSval=295448548 TSecr=3439...
4016	126.124593603	192.168.0.122	13.227.178.113	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=388 Ack=1007 Win=64128 Len=0 TSval=344034001 TSecr=295448548
4017	126.124609072	192.168.0.122	13.227.178.113	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=388 Ack=1007 Win=64128 Len=0 TSval=344034001 TSecr=290956847
4018	126.129933747	13.227.178.113	192.168.0.122	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=1007 Ack=389 Win=30208 Len=0 TSval=290957871 TSecr=3439...
4019	126.131740977	13.227.178.113	192.168.0.122	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=1007 Ack=389 Win=30208 Len=0 TSval=295449572 TSecr=2489
4051	136.368486444	192.168.0.122	13.227.178.113	TCP	66	[TCP Keep-Alive] 46120 → 80 [ACK] Seq=388 Ack=1007 Win=64128 Len=0 TSval=344044245 TSecr=295449572

Frame 3831: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
 Ethernet II, Src: Dell\_c6:e1:d4 (e4:54:e8:c6:e1:d4), Dst: Tp-LinkTf5:71:26 (14:cc:20:f5:71:26)  
 Internet Protocol Version 4, Src: 192.168.0.122, Dst: 13.227.178.113  
 Transmission Control Protocol, Src Port: 46120, Dst Port: 80, Seq: 0, Len: 0

0000 14 cc 20 f5 71 26 e4 54 e8 c6 e1 d4 08 00 45 00 -...q&-T-----E-  
 0010 00 3c 9f 98 40 00 06 19 ad c0 a8 0a 0d e3 -<-...@-.....z-  
 0020 b2 71 b4 28 0e 50 e9 95 19 5a 00 00 00 a0 02 -(-P-.....Z-.....

wireshark\_enp1s0\_20200224133449\_stoVPO.pcapng

Packets: 4078 · Displayed: 42 (1.0%) Profile: Default

### 3. Filter specific packets tcp.flags.reset==0 Displays all TCP resets.

The screenshot shows the Wireshark interface with the filter `tcp.flags.reset==0` applied. The packet list displays various TCP segments, including those with the `RESET` flag set. The packet details pane shows the structure of a TCP segment, including the header and application data. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
3757	71.787687823	192.168.0.122	54.239.36.249	TCP	54	33260 → 443 [ACK] Seq=518 Ack=5761 Win=61568 Len=0
3758	71.787699961	54.239.36.249	192.168.0.122	TLSv1.2	203	Server Key Exchange, Server Hello Done
3759	71.787784177	192.168.0.122	54.239.36.249	TCP	54	33260 → 443 [ACK] Seq=518 Ack=5910 Win=61440 Len=0
3760	71.790790332	192.168.0.122	54.239.36.249	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
3761	71.790953402	192.168.0.122	54.239.36.249	TLSv1.2	1291	Application Data
3762	71.797505360	192.168.0.122	54.239.36.249	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
3763	71.797669181	192.168.0.122	54.239.36.249	TCP	1494	33260 → 443 [ACK] Seq=644 Ack=5910 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
3764	71.797678274	192.168.0.122	54.239.36.249	TCP	1494	33260 → 443 [ACK] Seq=2084 Ack=5910 Win=64128 Len=1440 [TCP segment of a reassembled PDU]
3765	71.797845738	192.168.0.122	54.239.36.249	TLSv1.2	496	Application Data
3766	71.801600009	54.239.36.249	192.168.0.122	TLSv1.2	203	[TCP Spurious Retransmission], Ignored Unknown Record
3767	71.801636380	192.168.0.122	54.239.36.249	TCP	66	[TCP Dup ACK 3748#1] 33262 → 443 [ACK] Seq=1881 Ack=5910 Win=64128 Len=0 SLE=5761 SRE=5910
3768	71.810182077	54.239.36.249	192.168.0.122	TCP	203	[TCP Spurious Retransmission] 443 → 33260 [PSH, ACK] Seq=5761 Ack=518 Win=28160 Len=149[Reassembl...
3769	71.810212880	192.168.0.122	54.239.36.249	TCP	66	[TCP Dup ACK 3748#1] 33262 → 443 [ACK] Seq=1881 Ack=5910 Win=64128 Len=0 SLE=5761 SRE=5910
3770	71.831722072	54.239.36.249	192.168.0.122	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
3771	71.931752697	192.168.0.122	54.239.36.249	TCP	54	33262 → 443 [ACK] Seq=1881 Ack=5961 Win=64128 Len=0
3773	71.940580009	54.239.36.249	192.168.0.122	TLSv1.2	587	Application Data
3774	71.940604346	192.168.0.122	54.239.36.249	TCP	54	33262 → 443 [ACK] Seq=1881 Ack=6494 Win=64128 Len=0
3775	71.940788286	54.239.36.249	192.168.0.122	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
3776	71.940797343	192.168.0.122	54.239.36.249	TCP	54	33260 → 443 [ACK] Seq=3966 Ack=5961 Win=64128 Len=0
3777	71.942013745	54.239.36.249	192.168.0.122	TCP	60	443 → 33260 [ACK] Seq=5961 Ack=3524 Win=33792 Len=0
3778	71.949375063	54.239.36.249	192.168.0.122	TLSv1.2	565	Application Data
3779	71.949405823	192.168.0.122	54.239.36.249	TCP	54	33260 → 443 [ACK] Seq=3966 Ack=6472 Win=64128 Len=0
3780	71.949411742	54.239.36.249	192.168.0.122	TLSv1.2	105	Application Data
3781	71.949417102	192.168.0.122	54.239.36.249	TCP	54	33260 → 443 [ACK] Seq=3966 Ack=6523 Win=64128 Len=0
3782	71.949417102	54.239.36.249	192.168.0.122	TLSv1.2	504	[TCP Spurious Retransmission], Application Data
3783	72.051974998	192.168.0.122	54.239.36.249	TCP	66	[TCP Dup ACK 3774#1] 33262 → 443 [ACK] Seq=1881 Ack=6494 Win=64128 Len=0 SLE=5961 SRE=6494
3798	73.569050873	192.168.0.122	52.19.12.128	TLSv1.2	243	Application Data
3799	73.569197165	192.168.0.122	52.19.12.128	TLSv1.2	782	Application Data, Application Data
3800	73.569678743	192.168.0.122	52.19.12.128	TLSv1.2	104	Application Data
3801	73.703876319	52.19.12.128	192.168.0.122	TLSv1.2	104	Application Data
3802	73.703919809	192.168.0.122	52.19.12.128	TCP	66	35626 → 443 [ACK] Seq=1575 Ack=5652 Win=64128 Len=0 TSval=4061645474 TSecr=1191236444
3803	73.705163836	52.19.12.128	192.168.0.122	TCP	66	443 → 35626 [ACK] Seq=5652 Ack=1575 Win=30464 Len=0 TSval=1191236444 TSecr=4061645340
3804	73.706727105	52.19.12.128	192.168.0.122	TLSv1.2	260	Application Data
3805	73.706745684	192.168.0.122	52.19.12.128	TCP	66	35626 → 443 [ACK] Seq=1575 Ack=5846 Win=64128 Len=0 TSval=4061645477 TSecr=1191236445
3831	74.908763533	192.168.0.122	13.227.178.113	TCP	74	46120 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=343982786 TSecr=0 WS=128

Frame 3831: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
Ethernet II, Src: Dell\_c6:e1:d4 (e4:54:e8:c6:e1:d4), Dst: Tp-LinkT\_f5:71:26 (14:cc:20:f5:71:26)  
Internet Protocol Version 4, Src: 192.168.0.122, Dst: 13.227.178.113  
Transmission Control Protocol, Src Port: 46120, Dst Port: 80, Seq: 0, Len: 0

0000 14 cc 20 f5 71 26 e4 54 e8 c6 e1 d4 00 00 45 00 -- q6 T .....E-  
0010 00 3c 9f 98 40 00 00 06 19 ad c0 a8 00 7a 0d e3 -- <...@...Z...  
0020 b2 71 b4 28 00 50 e0 95 19 5a 00 00 00 a0 02 -- q(.P...Z.....

Wireshark\_enp1s0\_20200224133449\_stoVPO.pcapng Packets: 4241 · Displayed: 3568 (84.1%) Profile: Default

### 4. Filter for http request packets http.request Displays all HTTP GET requests.

The screenshot shows the Wireshark interface with the filter `http.request` applied. The packet list displays various HTTP GET requests. The packet details pane shows the structure of an HTTP GET request, including the header and body. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.140	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
2	1.001158301	192.168.0.140	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
3	3.794593103	192.168.0.117	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
4	3.884649025	192.168.0.116	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
7	4.794849759	192.168.0.117	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
8	4.880601617	192.168.0.116	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
11	7.785493223	192.168.0.117	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
12	5.886834470	192.168.0.116	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
14	6.796168457	192.168.0.117	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
15	6.887994011	192.168.0.116	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
49	21.079418813	192.168.0.102	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
50	22.080558581	192.168.0.102	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
52	23.081578118	192.168.0.102	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
53	24.081861674	192.168.0.102	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
116	45.003433026	192.168.0.114	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
127	46.003150298	192.168.0.114	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
213	47.003545213	192.168.0.114	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1081	48.003007411	192.168.0.114	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
1294	51.639631957	192.168.0.103	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
1664	52.640587191	192.168.0.103	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
1721	53.641487993	192.168.0.103	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
1728	54.642236697	192.168.0.103	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
1769	65.168179855	192.168.0.144	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
1774	66.168030904	192.168.0.144	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
1777	67.169224018	192.168.0.144	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
1780	68.170131327	192.168.0.144	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
2406	69.938426441	192.168.0.101	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
3426	70.939064737	192.168.0.101	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
3772	71.939003990	192.168.0.101	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
3832	74.912412936	192.168.0.101	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
3837	74.912417984	192.168.0.122	13.227.178.113	OCSP	454	Request
3838	74.912650496	192.168.0.122	13.227.178.113	OCSP	454	Request
3849	77.563629426	192.168.0.139	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
3850	77.669270671	192.168.0.141	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
3851	78.243576344	192.168.0.137	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1

Frame 3792: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on interface 0  
Ethernet II, Src: Dell\_c6:38:a1 (e4:54:e8:c6:38:a1), Dst: IPv4mcast\_7f:ff:fa (01:00:5e:7f:ff:fa)  
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 239.255.255.250  
User Datagram Protocol, Src Port: 56934, Dst Port: 1900  
Simple Service Discovery Protocol

0000 01 00 5e 7f ff fa e4 54 e8 c6 38 a1 00 00 45 00 -- A...T...8...E-  
0010 00 c7 93 92 40 00 01 11 34 8c c0 a8 00 65 ef ff -- ...@...4...e...  
0020 ff fa de 66 07 6c 00 b3 9e c5 4d 2d 53 45 41 52 -- f.1...M-SEAR

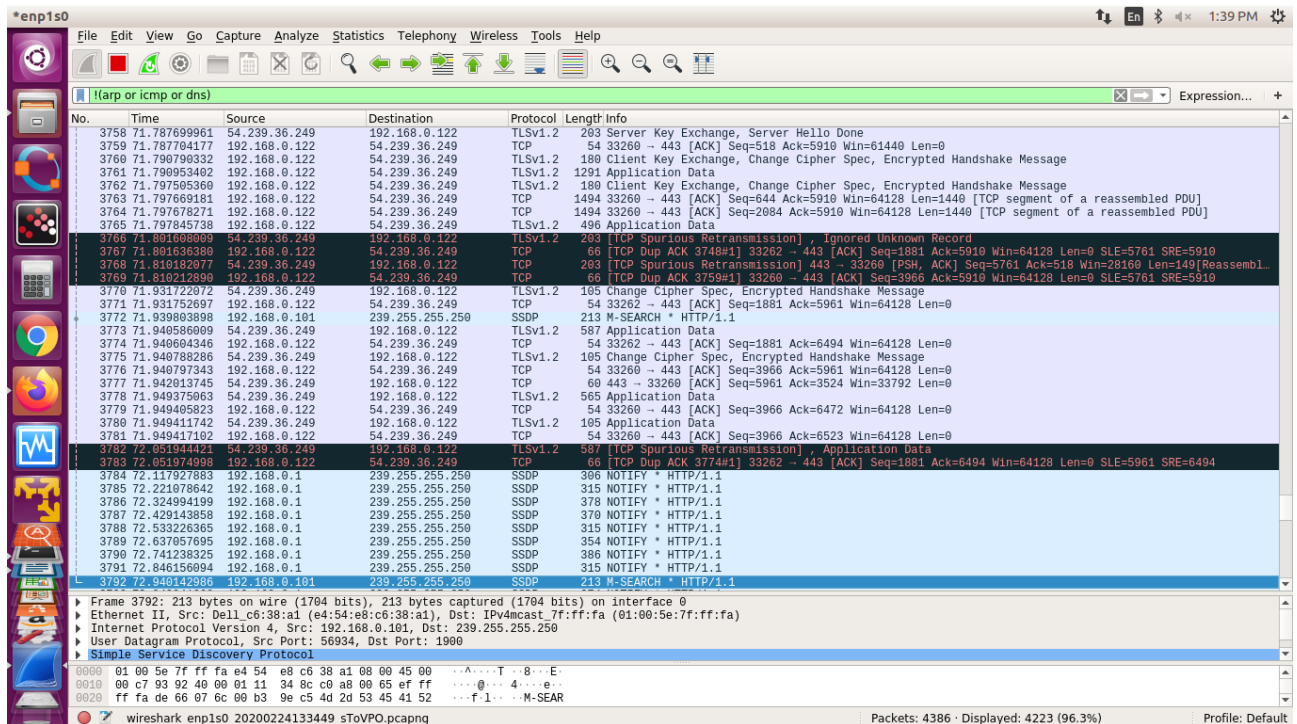
Wireshark\_enp1s0\_20200224133449\_stoVPO.pcapng Packets: 4364 · Displayed: 134 (3.1%) Profile: Default



## 5. To filter traffic except given protocol packets

!(arp or icmp or dns)

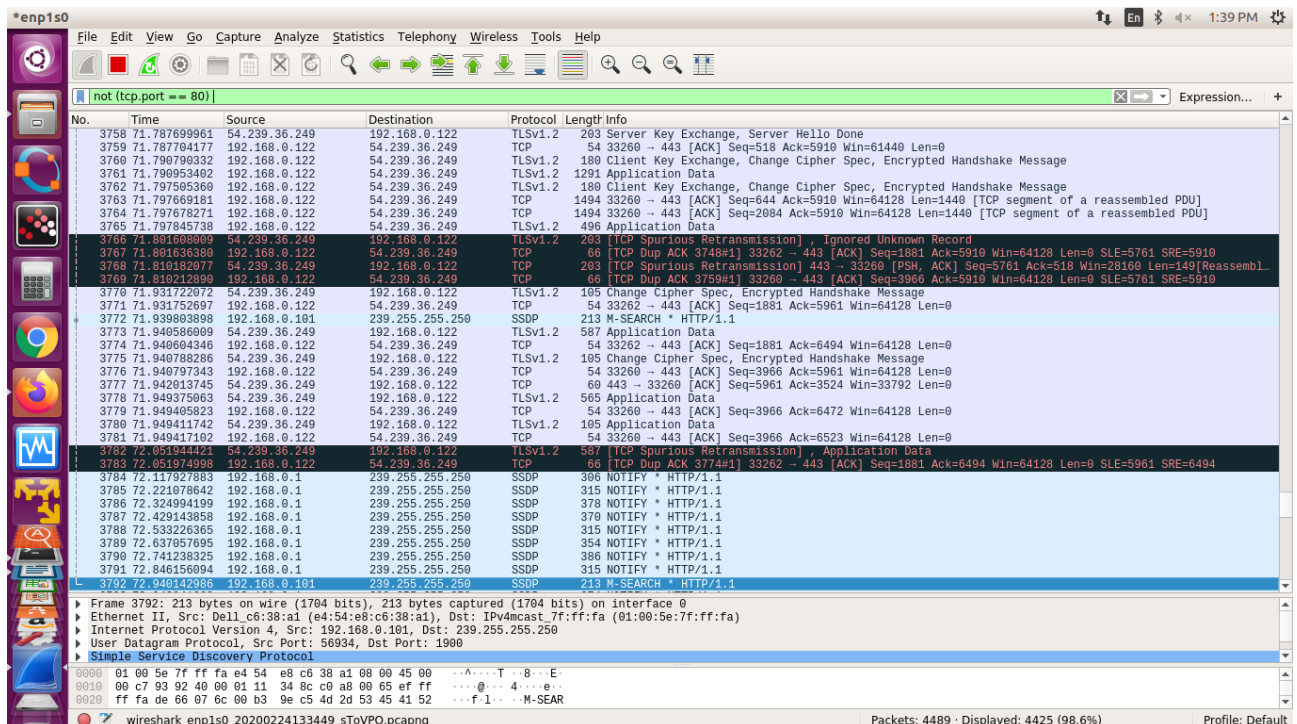
Masks out arp, icmp, dns, or whatever other protocols may be background noise, allowing you to focus on the traffic of interest.



## 6. Capturing packets after applying multiple filters

not (tcp.port == 80) and not (tcp.port == 25)

Get all packets which are not HTTP or UDP.



To stop capturing click on the “red square”

### c) To capture packets of FTP server. (Login ID and Password)

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 Protocol Daemon)

#### Steps:-

1. Get root access: `$ sudo su root`
2. Find your ip address: `# ifconfig`

#### Installation of FTP server in Ubuntu

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`

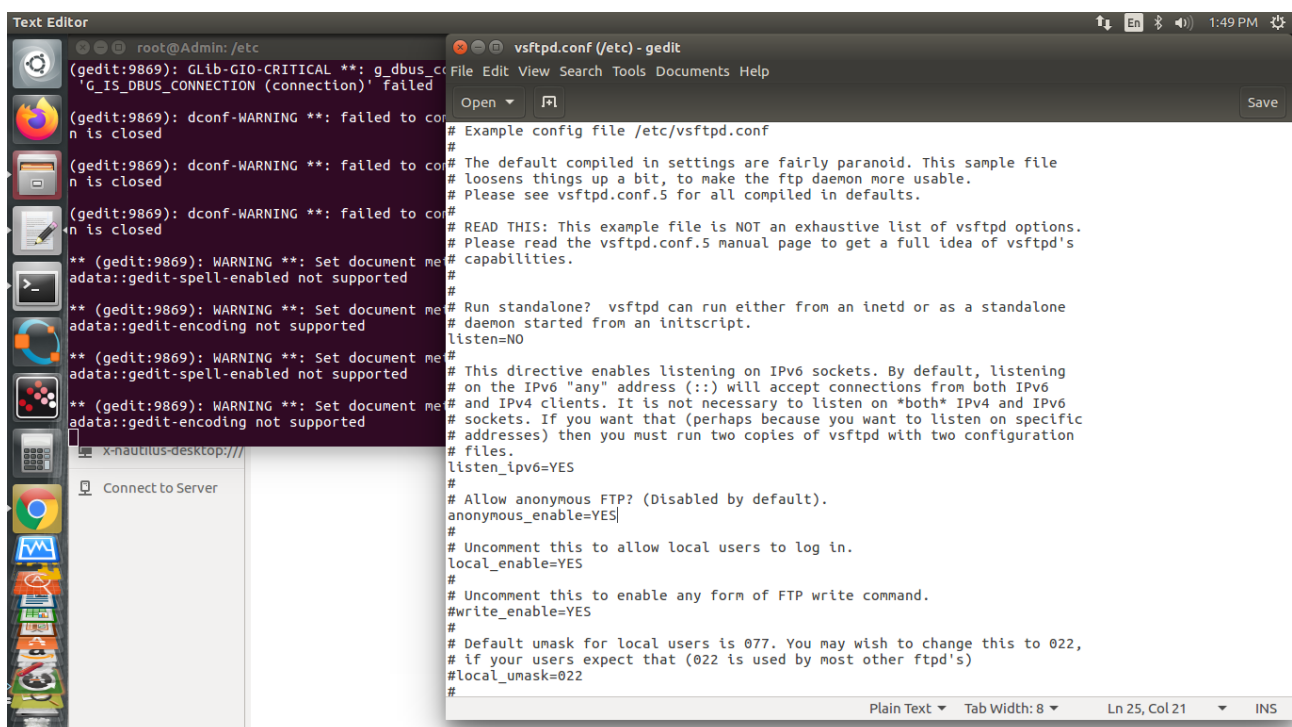
3. `# cd /etc`
4. `# ls`
5. `# gedit vsftpd.conf`

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



The screenshot shows a Linux desktop environment. On the left, a terminal window displays the command prompt `root@Admin: /etc` and several warning messages from `gedit` and `dconf`. On the right, a text editor window titled `vsftpd.conf (/etc) - gedit` shows the configuration file `/etc/vsftpd.conf`. The file content includes comments and directives for the vsftpd daemon. The line `anonymous_enable=YES` is highlighted, indicating the change from `NO` to `YES`. Other visible lines include `listen=NO`, `listen_ipv6=YES`, `local_enable=YES`, `write_enable=YES`, and `local_umask=022`. The status bar at the bottom of the text editor shows `Plain Text`, `Tab Width: 8`, `Ln 25, Col 21`, and `INS`.

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

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

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.

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 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.

The screenshot displays a Linux desktop environment. In the foreground, the Wireshark network protocol analyzer is open, capturing traffic on the 'enp1s0' interface. The filter is set to 'ftp'. The packet list shows several FTP packets, including login requests and responses. The packet details pane for packet 160 shows the FTP protocol structure, including the 'USER' and 'PASS' fields. The packet bytes pane shows the raw data. In the background, a terminal window is open, showing the output of the 'ftp' command. The terminal shows the user 'admini' connecting to the FTP server at 192.168.0.102. The user enters 'anonymous' as the name and a password (which is visible in the terminal output). The terminal shows the login is successful and the user is prompted to enter a password. The terminal also shows the user entering 'quit' and the server responding with 'Goodbye'.

No.	Time	Source	Destination	Protocol	Length	Info
160	31.707656272	192.168.0.105	192.168.0.102	FTP	86	Response: 220 (vsFTPD 3.0.3)
187	36.938807301	192.168.0.102	192.168.0.105	FTP	82	Request: USER anonymous
189	36.939409076	192.168.0.105	192.168.0.102	FTP	100	Response: 331 Please spec...
191	37.946797877	192.168.0.102	192.168.0.105	FTP	76	Request: PASS lol
193	38.009423026	192.168.0.105	192.168.0.102	FTP	89	Response: 230 Login succe...
195	38.009549770	192.168.0.102	192.168.0.105	FTP	72	Request: SYST
197	38.010043562	192.168.0.105	192.168.0.102	FTP	85	Response: 215 UNIX Type: L8
236	47.082944072	192.168.0.102	192.168.0.105	FTP	70	Request: QUIT
237	47.083419784	192.168.0.105	192.168.0.102	FTP	70	Response: 221

```
admini@Admin:~$ ftp 192.168.0.102
Connected to 192.168.0.102.
220 (vsFTPD 3.0.3)
Name (192.168.0.102:admini): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ^C
ftp> exit
221 Goodbye.
admini@Admin:~$ ftp 192.168.0.105
Connected to 192.168.0.105.
220 (vsFTPD 3.0.3)
Name (192.168.0.105:admini): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quit
221 Goodbye.
admini@Admin:~$
```