ASSIGNMENT

Submitted By,

Ashtami Prasad

S2 RMCA Batch A

Roll No:29

Wireshark

Wireshark allows you to filter the log either before the capture starts or during analysis, so you can narrow down and zero into what you are looking for in the network trace. For example, you can set a filter to see TCP traffic between two IP addresses. You can set it only to show you the packets sent from one computer. The filters in Wireshark are one of the primary reasons it became the standard tool for packet analysis.

WireShark installation:

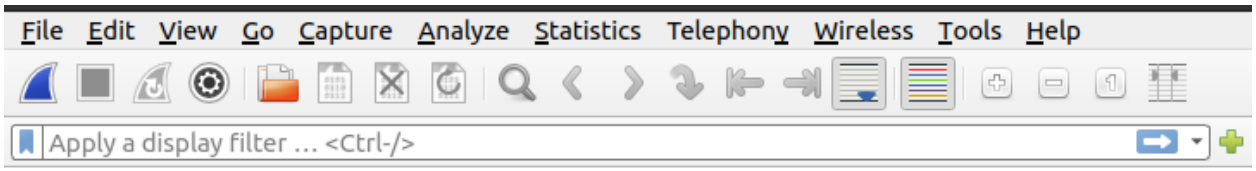
```
ashtami@ashtami-VirtualBox:~$ sudo apt-get install wireshark
[sudo] password for ashtami:
Reading package lists... Done
Building dependency tree
Reading state information... Done
wireshark is already the newest version (3.2.3-1).
0 upgraded, 0 newly installed, 0 to remove and 318 not upgraded.
```

WireShark Version:

```
ashtami@ashtami-VirtualBox:~$ wireshark --version
Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1)

Copyright 1998-2020 Gerald Combs <gerald@wireshark.org> and contributors.
License GPLv2+: GNU GPL version 2 or later <https://www.gnu.org/licenses/gpl-2.
0.html>
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) with Qt 5.12.8, with libpcap, with POSIX capabilities (Linux)
,
with libnl 3, with GLib 2.64.2, with zlib 1.2.11, with SMI 0.4.8, with c-ares
1.15.0, with Lua 5.2.4, with GnuTLS 3.6.13 and PKCS #11 support, with Gcrypt
1.8.5, with MIT Kerberos, with MaxMind DB resolver, with nghttp2 1.40.0, with
brotli, with LZ4, with Zstandard, with Snappy, with libxml2 2.9.10, with
QtMultimedia, without automatic updates, with SpeexDSP (using system library),
with SBC, with SpanDSP, without bcg729.

Running on Linux 5.8.0-43-generic, with Intel(R) Core(TM) i3-6006U CPU @ 2.00GH
z
(with SSE4.2), with 1064 MB of physical memory, with locale en_US.UTF-8, with
libpcap version 1.9.1 (with TPACKET_V3), with GnuTLS 3.6.13, with Gcrypt 1.8.5,
with brotli 1.0.7, with zlib 1.2.11, binary plugins supported (0 loaded).

Built using gcc 9.3.0.
```

```
ashtami@ashtami-VirtualBox:~$ sudo dpkg-reconfigure wireshark-common
ashtami@ashtami-VirtualBox:~$
```

```
ashtami@ashtami-VirtualBox:~$ sudo adduser $USER wireshark
Adding user `ashtami' to group `wireshark' ...
Adding user ashtami to group wireshark
Done.
ashtami@ashtami-VirtualBox:~$
```



Welcome to Wireshark

Capture

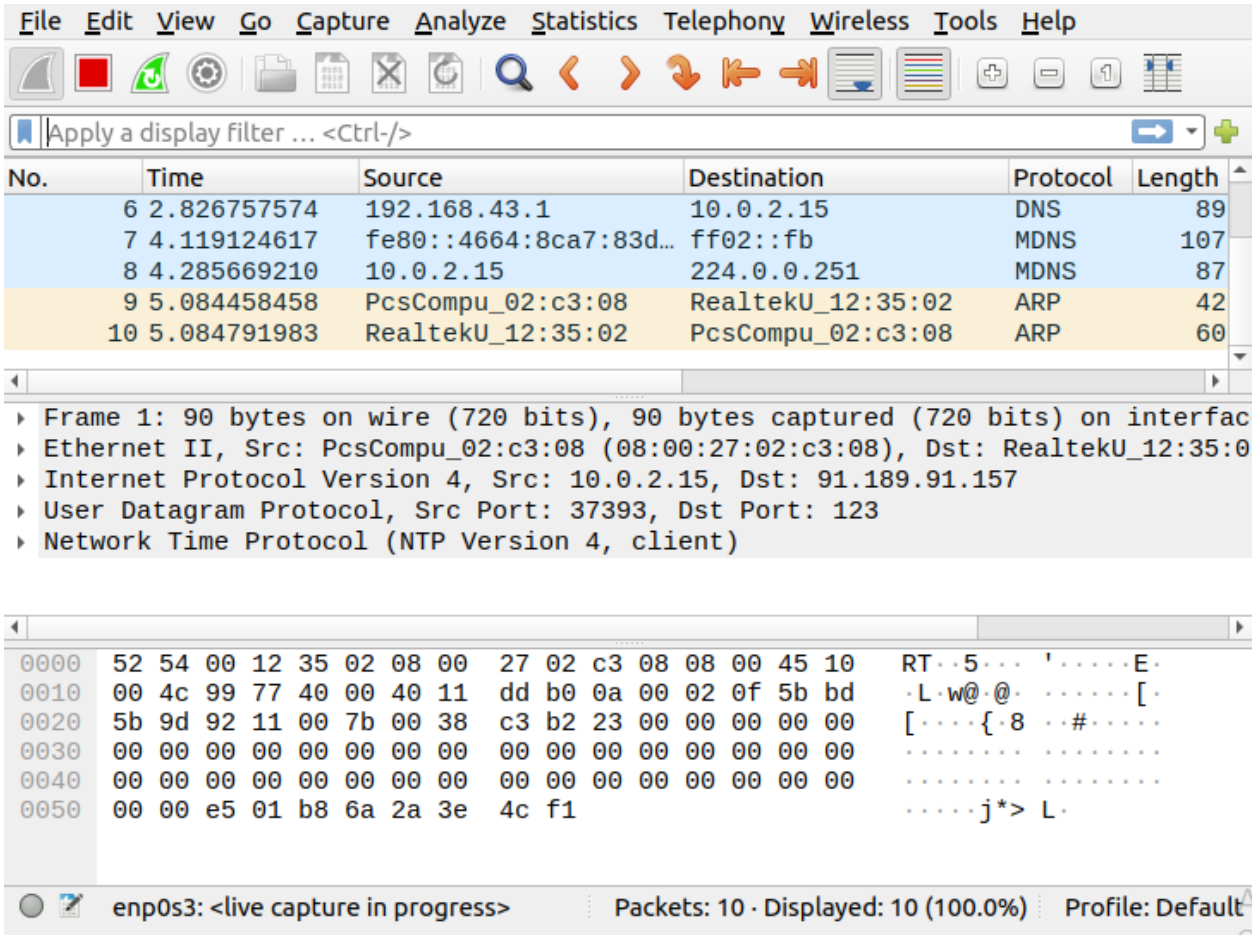
…using this filter: Enter a capture filter … All interfaces shown

Cisco remote capture: ciscodump	
DisplayPort AUX channel monitor capture: dpauxmon	
Random packet generator: randpkt	
systemd Journal Export: sdjournal	
SSH remote capture: sshdump	
UDP Listener remote capture: udpdump	

Learn

User's Guide · **Wiki** · **Questions and Answers** · **Mailing Lists**

You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).



Netcat

```
ashtami@ashtami-VirtualBox:~$ sudo apt-get install netcat
[sudo] password for ashtami:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  netcat
0 upgraded, 1 newly installed, 0 to remove and 318 not upgraded.
Need to get 2,172 B of archives.
After this operation, 15.4 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 netcat all 1.206
-1ubuntu1 [2,172 B]
Fetched 2,172 B in 2s (1,113 B/s)
Selecting previously unselected package netcat.
(Reading database ... 160612 files and directories currently installed.)
Preparing to unpack .../netcat_1.206-1ubuntu1_all.deb ...
Unpacking netcat (1.206-1ubuntu1) ...
Setting up netcat (1.206-1ubuntu1) ...
```

Nc

```
ashtami@ashtami-VirtualBox:~$ nc -h
OpenBSD netcat (Debian patchlevel 1.206-1ubuntu1)
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]
        Command Summary:
                -4              Use IPv4
                -6              Use IPv6
                -b              Allow broadcast
                -C              Send CRLF as line-ending
                -D              Enable the debug socket option
                -d              Detach from stdin
                -F              Pass socket fd
                -h              This help text
                -I length       TCP receive buffer length
                -i interval     Delay interval for lines sent, ports scanned
                -k              Keep inbound sockets open for multiple connects
                -l              Listen mode, for inbound connects
                -M ttl          Outgoing TTL / Hop Limit
                -m minttl       Minimum incoming TTL / Hop Limit
                -N              Shutdown the network socket after EOF on stdin
                -n              Suppress name/port resolutions
                -O length       TCP send buffer length
                -P proxyuser    Username for proxy authentication
                -p port         Specify local port for remote connects
                -q secs         quit after EOF on stdin and delay of secs
```