

## Modulo # 3 – Laboratorio # 5 : Captura de Conexiones IP

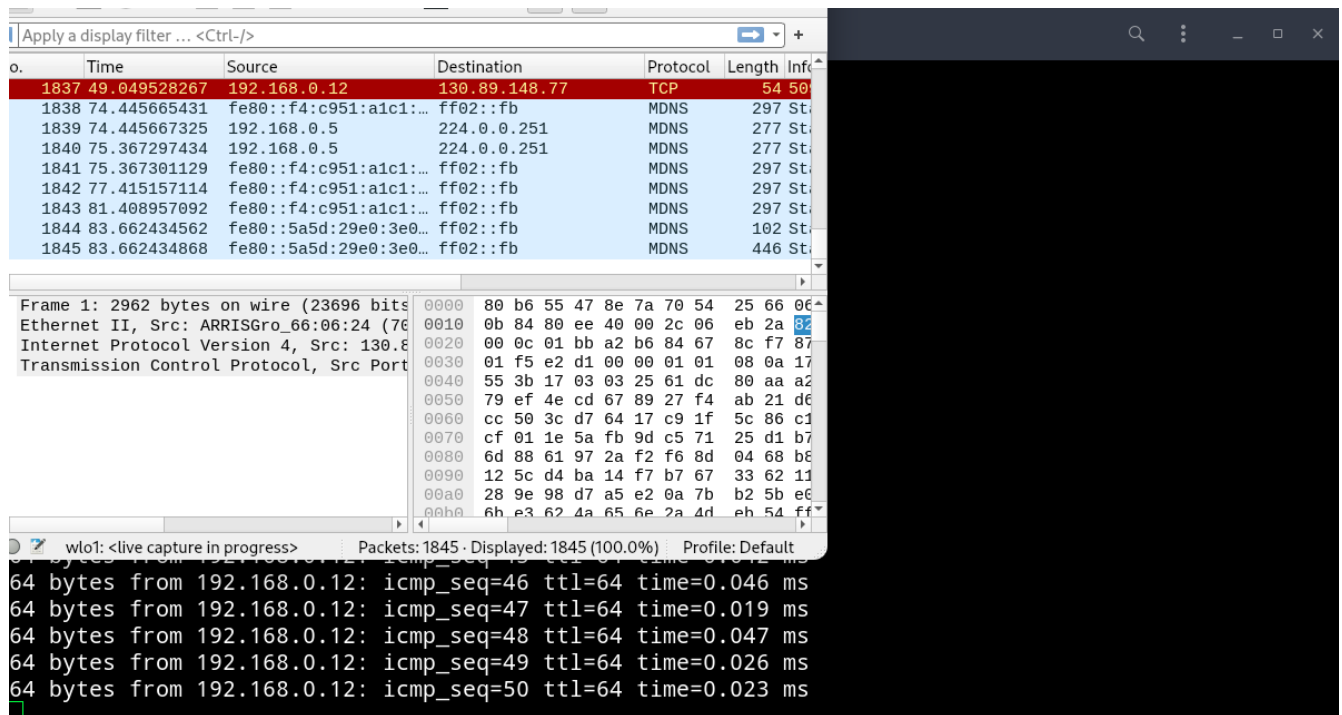
### 1. Ver la configuracion IP.

```
mikey@blooms:~  
~ ➤ ifconfig  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 244 bytes 18589 (18.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 244 bytes 18589 (18.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.0.12 netmask 255.255.255.0 broadcast 192.168.0.255  
    inet6 fe80::8d16:6a70:ce6b:4e50 prefixlen 64 scopeid 0x20<link>  
    ether 80:b6:55:47:8e:7a txqueuelen 1000 (Ethernet)  
    RX packets 264021 bytes 297148816 (283.3 MiB)  
    RX errors 0 dropped 41 overruns 0 frame 0  
    TX packets 88578 bytes 19965794 (19.0 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
~ ➤
```

### 2. Ahora haremos un ping.

```
ping 192.168.0.12  
ether 80:b6:55:47:8e:7a txqueuelen 1000 (Ethernet)  
RX packets 264021 bytes 297148816 (283.3 MiB)  
RX errors 0 dropped 41 overruns 0 frame 0  
TX packets 88578 bytes 19965794 (19.0 MiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
~ ➤ ping 192.168.0.20  
PING 192.168.0.20 (192.168.0.20) 56(84) bytes of data.  
From 192.168.0.12 icmp_seq=1 Destination Host Unreachable  
From 192.168.0.12 icmp_seq=2 Destination Host Unreachable  
From 192.168.0.12 icmp_seq=3 Destination Host Unreachable  
From 192.168.0.12 icmp_seq=4 Destination Host Unreachable  
From 192.168.0.12 icmp_seq=5 Destination Host Unreachable  
From 192.168.0.12 icmp_seq=6 Destination Host Unreachable  
^C  
--- 192.168.0.20 ping statistics ---  
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6131ms  
pipe 4  
~ ➤ ping 192.168.0.12  
PING 192.168.0.12 (192.168.0.12) 56(84) bytes of data.  
64 bytes from 192.168.0.12: icmp_seq=1 ttl=64 time=0.028 ms  
64 bytes from 192.168.0.12: icmp_seq=2 ttl=64 time=0.047 ms  
64 bytes from 192.168.0.12: icmp_seq=3 ttl=64 time=0.048 ms  
64 bytes from 192.168.0.12: icmp_seq=4 ttl=64 time=0.028 ms
```

### 3. Ahora veremos que captura Wireshark.



The image shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets. The bottom pane shows the detailed view of the selected packet (Frame 1).

No.	Time	Source	Destination	Protocol	Length	Info
1837	49.049528267	192.168.0.12	130.89.148.77	TCP	54	5080 → 80 [RST] Seq=1921680122 Win=0 Len=0
1838	74.445665431	fe80::f4:c951:a1c1::...	ff02::fb	MDNS	297	Standard query response
1839	74.445667325	192.168.0.5	224.0.0.251	MDNS	277	Standard query response
1840	75.367297434	192.168.0.5	224.0.0.251	MDNS	277	Standard query response
1841	75.367301129	fe80::f4:c951:a1c1::...	ff02::fb	MDNS	297	Standard query response
1842	77.415157114	fe80::f4:c951:a1c1::...	ff02::fb	MDNS	297	Standard query response
1843	81.408957092	fe80::f4:c951:a1c1::...	ff02::fb	MDNS	297	Standard query response
1844	83.662434562	fe80::5a5d:29e0:3e0::...	ff02::fb	MDNS	102	Standard query response
1845	83.662434868	fe80::5a5d:29e0:3e0::...	ff02::fb	MDNS	446	Standard query response

Frame 1: 2962 bytes on wire (23696 bits) captured (eth0) on interface eth0  
Ethernet II, Src: ARRISGro\_66:06:24 (76:06:24:66:06:24), Dst: 01:00:0c:01:bb:a2 (08:00:0c:01:bb:a2)  
Internet Protocol Version 4, Src: 130.89.148.77, Destination: 192.168.0.5  
Transmission Control Protocol, Src Port: 5080, Dst Port: 80  
Sequence Number: 1921680122, Window: 0, Length: 0, Flags: RST, Seq=1921680122, Win=0, Len=0

64 bytes from 192.168.0.12: icmp\_seq=46 ttl=64 time=0.046 ms  
64 bytes from 192.168.0.12: icmp\_seq=47 ttl=64 time=0.019 ms  
64 bytes from 192.168.0.12: icmp\_seq=48 ttl=64 time=0.047 ms  
64 bytes from 192.168.0.12: icmp\_seq=49 ttl=64 time=0.026 ms  
64 bytes from 192.168.0.12: icmp\_seq=50 ttl=64 time=0.023 ms

```
ping www.cisco.com

^C
--- 192.168.0.12 ping statistics ---
101 packets transmitted, 101 received, 0% packet loss, time 102385ms
rtt min/avg/max/mdev = 0.018/0.037/0.081/0.013 ms
~ > ping www.google.com
PING www.google.com (172.217.3.68) 56(84) bytes of data.
64 bytes from mia07s54-in-f4.1e100.net (172.217.3.68): icmp_seq=1 ttl=115 time=69.7 ms
64 bytes from mia07s54-in-f4.1e100.net (172.217.3.68): icmp_seq=2 ttl=115 time=69.7 ms
64 bytes from mia07s54-in-f4.1e100.net (172.217.3.68): icmp_seq=3 ttl=115 time=68.2 ms
64 bytes from mia07s54-in-f4.1e100.net (172.217.3.68): icmp_seq=4 ttl=115 time=64.6 ms
64 bytes from mia07s54-in-f4.1e100.net (172.217.3.68): icmp_seq=5 ttl=115 time=66.1 ms
64 bytes from mia07s54-in-f4.1e100.net (172.217.3.68): icmp_seq=6 ttl=115 time=65.6 ms
^C
--- www.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 64.628/67.335/69.735/1.994 ms
~ > ping www.cisco.com
PING e2867.dsca.akamaiedge.net (184.26.52.119) 56(84) bytes of data.
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=1 ttl=52 time=76.7 ms
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=2 ttl=52 time=68.6 ms
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=3 ttl=52 time=64.9 ms
```

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
128	27.174869519	200.75.200.3	192.168.0.12	DNS	151	Standard query query
129	28.092246305	192.168.0.12	184.26.52.119	ICMP	98	Echo (ping) request
130	28.158325531	184.26.52.119	192.168.0.12	ICMP	98	Echo (ping) reply
131	28.158686680	192.168.0.12	200.75.200.3	DNS	86	Standard query response
132	28.176070030	200.75.200.3	192.168.0.12	DNS	151	Standard query query
133	29.094209565	192.168.0.12	184.26.52.119	ICMP	98	Echo (ping) request
134	29.160036727	184.26.52.119	192.168.0.12	ICMP	98	Echo (ping) reply
135	29.160366781	192.168.0.12	200.75.200.3	DNS	86	Standard query response
136	29.175057247	200.75.200.3	192.168.0.12	DNS	151	Standard query query

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 Ethernet II, Src: ARRISGro\_66:06:24 (78:06:24:66:06:24), Dst: 08:00:00:00:00:00  
 Address Resolution Protocol (request)

0000 80 b6 55 47 8e 7a 70 54 25 66 06 00  
 0010 08 00 06 04 00 01 70 54 25 66 06 00  
 0020 00 00 00 00 00 00 c0 a8 00 0c 00 00  
 0030 00 00 00 00 00 00 00 00 00 00 00 00

wlo1: <live capture in progress>    Packets: 140 · Displayed: 140 (100.0%)    Profile: Default

```

ping www.yahoo.com
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=13 ttl=52 time=69.7 ms
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=14 ttl=52 time=69.7 ms
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=15 ttl=52 time=68.2 ms
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=16 ttl=52 time=64.6 ms
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=17 ttl=52 time=66.1 ms
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=18 ttl=52 time=65.6 ms
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=19 ttl=52 time=69.7 ms
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=20 ttl=52 time=68.2 ms
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=21 ttl=52 time=64.6 ms
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=22 ttl=52 time=66.1 ms
64 bytes from a184-26-52-119.deploy.static.akamaitechnologies.com (184.26.52.119): icmp_seq=23 ttl=52 time=65.6 ms
^C
--- e2867.dsca.akamaiedge.net ping statistics ---
21 packets transmitted, 21 received, 0% packet loss, time 20025ms
rtt min/avg/max/mdev = 64.358/67.359/76.701/2.990 ms
> ping www.yahoo.com
PING me-ycpi-cf-www.g06.yahoodns.net (68.180.135.251) 56(84) bytes of data.

```

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
312	49.972862339	130.89.148.77	192.168.0.12	TCP	66	44:...
313	49.972862461	130.89.148.77	192.168.0.12	TLSv1.3	389	Ap...
314	49.973109878	192.168.0.12	130.89.148.77	TLSv1.3	101	Ap...
315	50.279221278	130.89.148.77	192.168.0.12	TCP	66	44:...
316	50.710302085	192.168.0.12	68.180.135.251	ICMP	98	Ec...
317	51.734378882	192.168.0.12	68.180.135.251	ICMP	98	Ec...
318	52.758422393	192.168.0.12	68.180.135.251	ICMP	98	Ec...
319	53.782311149	192.168.0.12	68.180.135.251	ICMP	98	Ec...
320	54.806404390	192.168.0.12	68.180.135.251	ICMP	98	Ec...

Frame 1: 60 bytes on wire (480 bits), Ethernet II, Src: ARRISGro\_66:06:24 (76:08:0a:00:06:24), Dst: 08:00:00:00:00:00, Protocol: ARP (request)

0000 80 b6 55 47 8e 7a 70 54 25 66 06  
0010 08 00 06 04 00 01 70 54 25 66 06  
0020 00 00 00 00 00 00 c0 a8 00 0c 00  
0030 00 00 00 00 00 00 00 00 00 00 00

wlo1: <live capture in progress>    Packets: 320 · Displayed: 320 (100.0%)    Profile: Default

```

.com (184.26.52.119): icmp_seq=13 ttl=5
.com (184.26.52.119): icmp_seq=14 ttl=5
.com (184.26.52.119): icmp_seq=15 ttl=5
.com (184.26.52.119): icmp_seq=16 ttl=5
.com (184.26.52.119): icmp_seq=17 ttl=5
.com (184.26.52.119): icmp_seq=18 ttl=5
.com (184.26.52.119): icmp_seq=19 ttl=5
.com (184.26.52.119): icmp_seq=20 ttl=5
.com (184.26.52.119): icmp_seq=21 ttl=5

--- e2867.dsca.akamaiedge.net ping statistics ---
21 packets transmitted, 21 received, 0% packet loss, time 20025ms
rtt min/avg/max/mdev = 64.358/67.359/76.701/2.990 ms
~> ping www.yahoo.com
PING me-ycpi-cf-www.g06.yahoodns.net (68.180.135.251) 56(84) bytes of data.

```