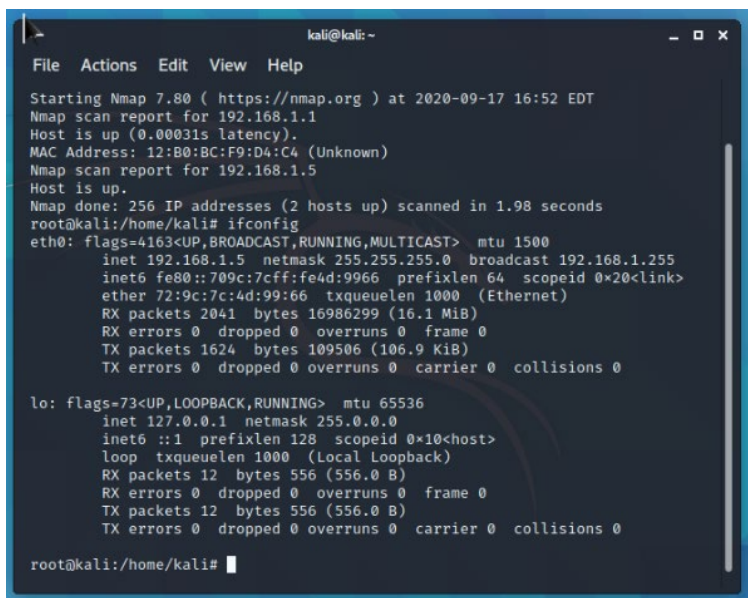


Lab 3: Packet Analysis (Part 2)

- This is an individual assignment, and worth 20 points.
- The due date is 2:30 (Sec 01) / 5:30 (Sec 76) on Friday, September 18.
- Follow the naming convention.
- **You should not scan any live servers using Nmap or send malicious packets using hping3. If caught, you may be expelled from school (not a joke!).**

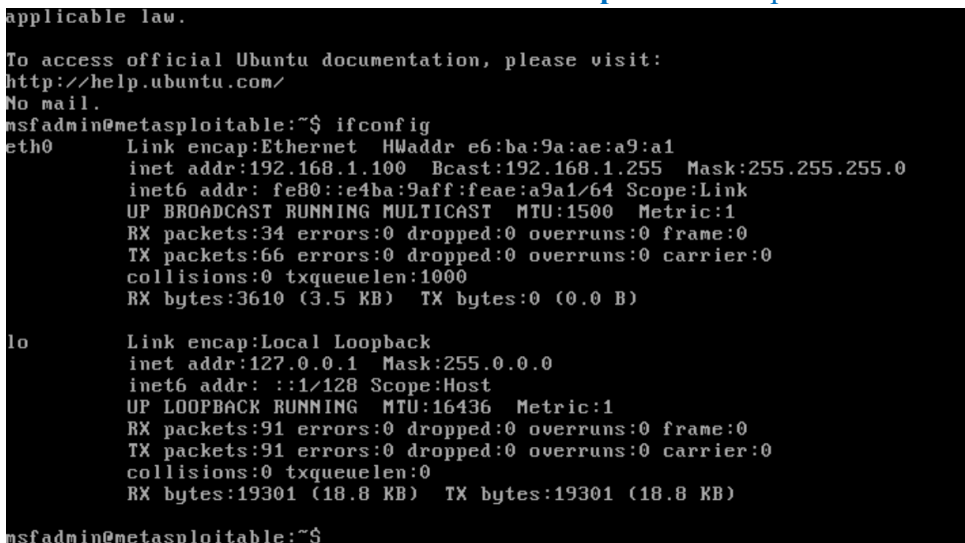
Task 1. Identifying the IP addresses

- Find the IP address and subnet mask of **Kali** (use ifconfig). Report the result with a screenshot.



```
kali@kali: ~  
File Actions Edit View Help  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-17 16:52 EDT  
Nmap scan report for 192.168.1.1  
Host is up (0.00031s latency).  
MAC Address: 12:B0:BC:F9:D4:C4 (Unknown)  
Nmap scan report for 192.168.1.5  
Host is up.  
Nmap done: 256 IP addresses (2 hosts up) scanned in 1.98 seconds  
root@kali:/home/kali# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.5 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::709c:7c:ff:fe4d:9966 prefixlen 64 scopeid 0x20<link>  
    ether 72:9c:7c:d9:99:66 txqueuelen 1000 (Ethernet)  
    RX packets 2041 bytes 16986299 (16.1 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1624 bytes 109506 (106.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
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 12 bytes 556 (556.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 12 bytes 556 (556.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@kali:/home/kali#
```

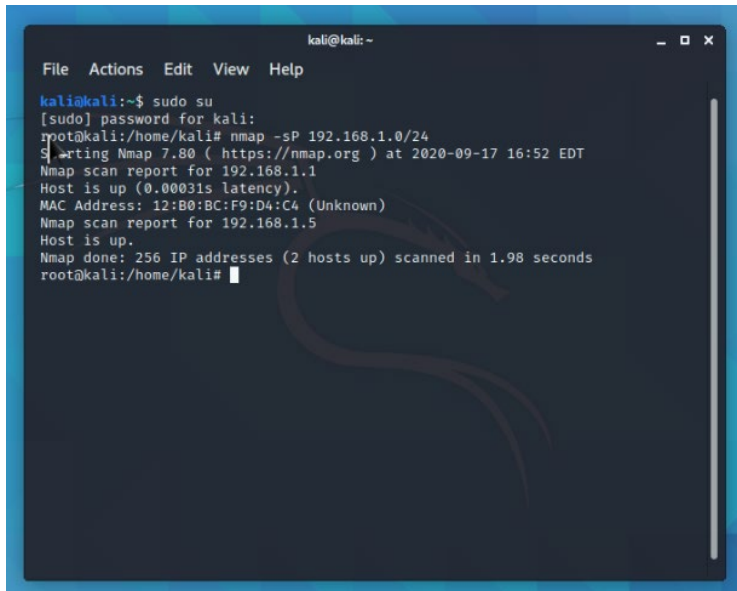
- Find the IP address and subnet mask of **Metasploitable**. Report the result with a screenshot.



```
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr e6:ba:9a:ae:a9:a1  
    inet addr:192.168.1.100 Bcast:192.168.1.255 Mask:255.255.255.0  
    inet6 addr: fe80::e4ba:9aff:feae:a9a1/64 Scope:Link  
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
    RX packets:34 errors:0 dropped:0 overruns:0 frame:0  
    TX packets:66 errors:0 dropped:0 overruns:0 carrier:0  
    collisions:0 txqueuelen:1000  
    RX bytes:3610 (3.5 KB) TX bytes:0 (0.0 B)  
  
lo        Link encap:Local Loopback  
    inet addr:127.0.0.1 Mask:255.0.0.0  
    inet6 addr: ::1/128 Scope:Host  
    UP LOOPBACK RUNNING MTU:16436 Metric:1  
    RX packets:91 errors:0 dropped:0 overruns:0 frame:0  
    TX packets:91 errors:0 dropped:0 overruns:0 carrier:0  
    collisions:0 txqueuelen:0  
    RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)  
  
msfadmin@metasploitable:~$
```

Task 2. Performing a Ping Sweeping

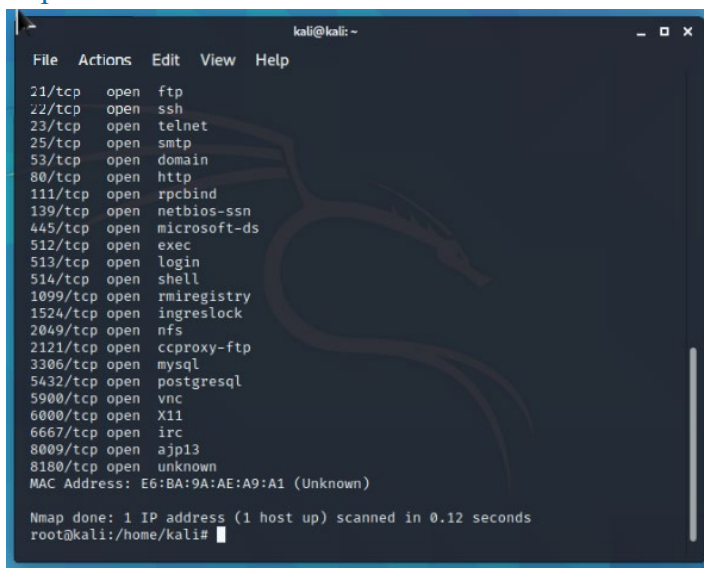
- Report the result with a screenshot.



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo su  
[sudo] password for kali:  
root@kali:/home/kali# nmap -sP 192.168.1.0/24  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-17 16:52 EDT  
Nmap scan report for 192.168.1.1  
Host is up (0.00031s latency).  
MAC Address: 12:B0:BC:F9:D4:C4 (Unknown)  
Nmap scan report for 192.168.1.5  
Host is up.  
Nmap done: 256 IP addresses (2 hosts up) scanned in 1.98 seconds  
root@kali:/home/kali#
```

Task 3. Performing a Port Scanning

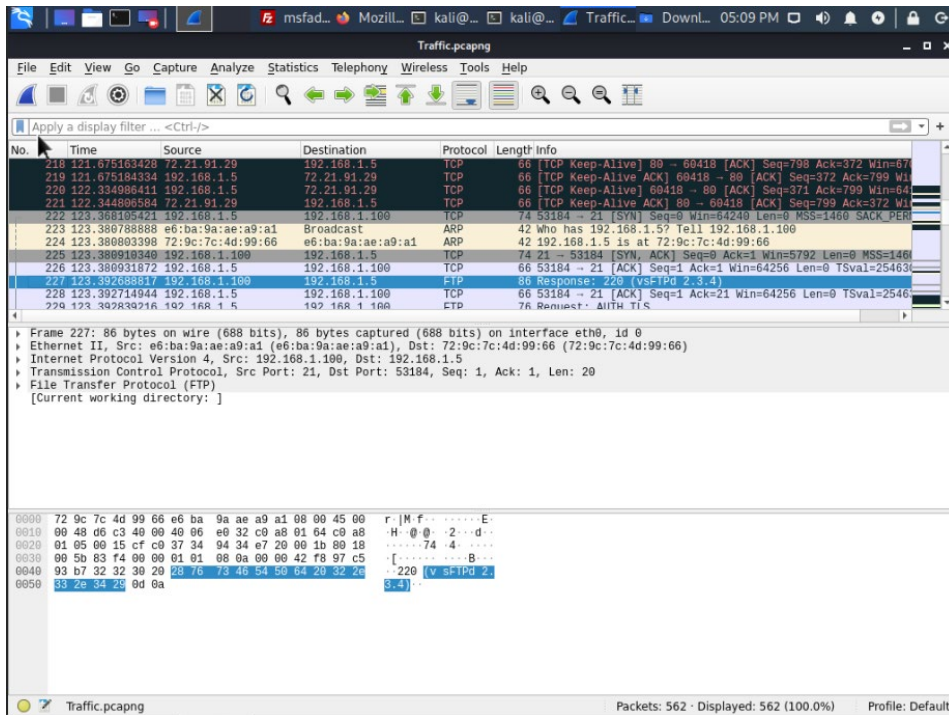
- Report the result with a screenshot.



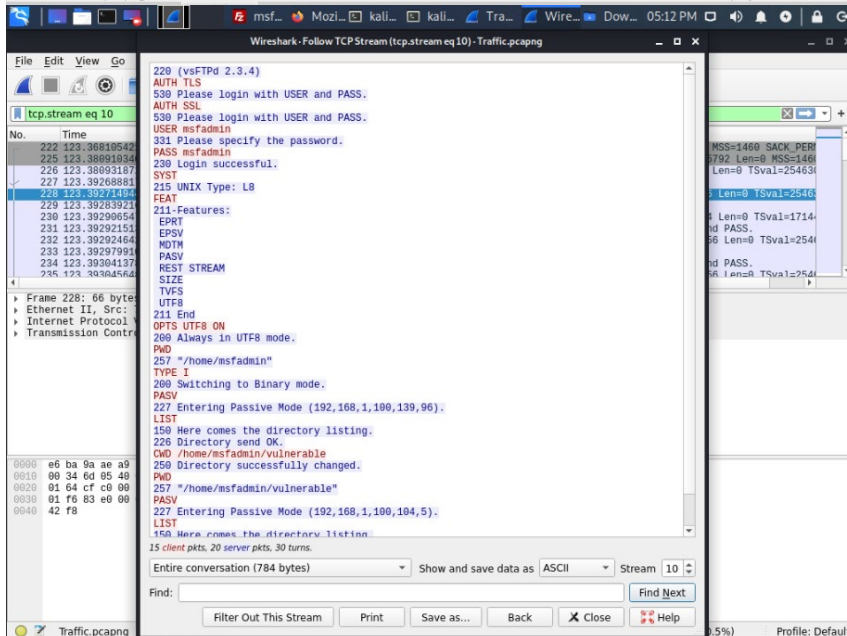
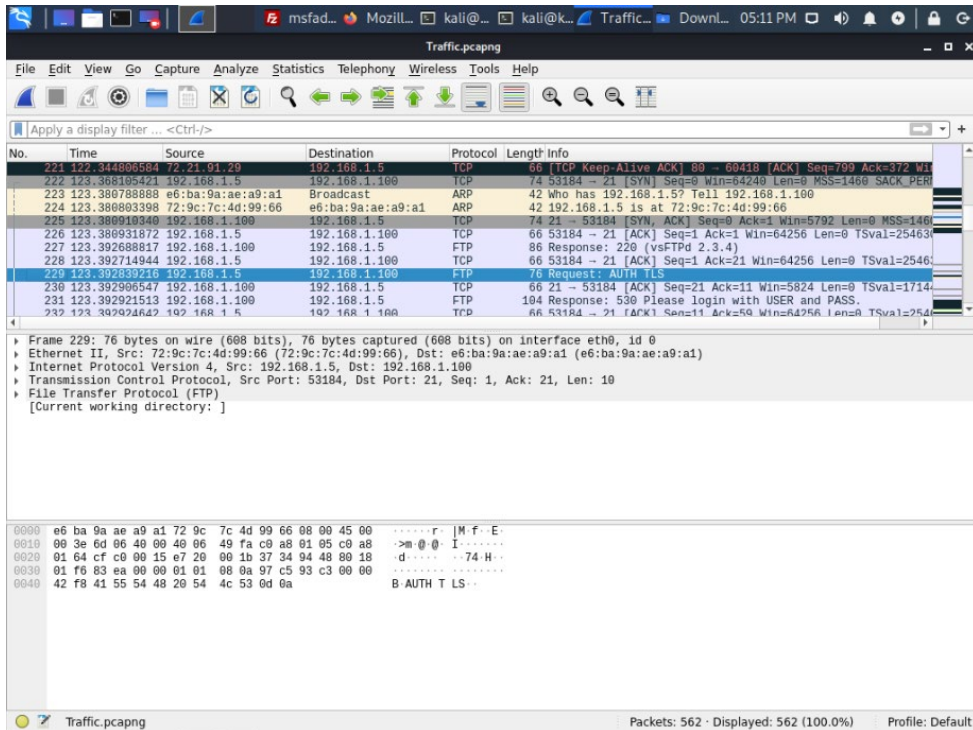
```
kali@kali: ~  
File Actions Edit View Help  
21/tcp open ftp  
22/tcp open ssh  
23/tcp open telnet  
25/tcp open smtp  
53/tcp open domain  
80/tcp open http  
111/tcp open rpcbind  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
512/tcp open exec  
513/tcp open login  
514/tcp open shell  
1099/tcp open rmiregistry  
1524/tcp open ingreslock  
2049/tcp open nfs  
2121/tcp open ccproxy-ftp  
3306/tcp open mysql  
5432/tcp open postgresql  
5900/tcp open vnc  
6000/tcp open X11  
6667/tcp open irc  
8009/tcp open ajp13  
8180/tcp open unknown  
MAC Address: E6:BA:9A:AE:A9:A1 (Unknown)  
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds  
root@kali:/home/kali#
```

Task 4. Analyzing FTP Signatures

- 1) Identify the TCP packets used for the initial three-way handshake for the connection to the ftp server. Take a screenshot of those TCP packets. Those packets are placed right before the first ftp packet.



- 2) Identify the TCP stream used for the authentication of the client to the FTP server. [Take a screenshot of the TCP stream.](#)



3) Identify the first and last FTP-DATA packets used for the uploading of the text file. Take a screenshot for each (two required).

The top screenshot shows a Wireshark capture of an FTP session. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
285	14.789558282	192.168.1.100	192.168.1.5	FTP-DA	134	FTP Data: 68 bytes (PASV) (LIST)
311	151.433222247	192.168.1.100	192.168.1.5	FTP-DA	333	FTP Data: 207 bytes (PASV) (LIST)
373	190.344395360	192.168.1.5	192.168.1.100	FTP-DA	2962	FTP Data: 2896 bytes (PASV) (STOR RomeoJuliet.txt)
374	190.344496860	192.168.1.5	192.168.1.100	FTP-DA	2962	FTP Data: 2896 bytes (PASV) (STOR RomeoJuliet.txt)
379	190.344505307	192.168.1.5	192.168.1.100	FTP-DA	2962	FTP Data: 2896 bytes (PASV) (STOR RomeoJuliet.txt)
380	190.344512394	192.168.1.5	192.168.1.100	FTP-DA	2962	FTP Data: 2896 bytes (PASV) (STOR RomeoJuliet.txt)
381	190.344514012	192.168.1.5	192.168.1.100	FTP-DA	2962	FTP Data: 2896 bytes (PASV) (STOR RomeoJuliet.txt)
382	190.344516748	192.168.1.5	192.168.1.100	FTP-DA	2962	FTP Data: 2896 bytes (PASV) (STOR RomeoJuliet.txt)
383	190.344519939	192.168.1.5	192.168.1.100	FTP-DA	2962	FTP Data: 2896 bytes (PASV) (STOR RomeoJuliet.txt)
384	190.344523661	192.168.1.5	192.168.1.100	FTP-DA	2962	FTP Data: 2896 bytes (PASV) (STOR RomeoJuliet.txt)
386	190.344671179	192.168.1.5	192.168.1.100	FTP-DA	2962	FTP Data: 2896 bytes (PASV) (STOR RomeoJuliet.txt)
388	190.344678198	192.168.1.5	192.168.1.100	FTP-DA	2962	FTP Data: 2896 bytes (PASV) (STOR RomeoJuliet.txt)

The packet details pane for frame 285 shows:

- Frame 285: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface eth0, id 0
- Ethernet II, Src: e6:ba:9a:ae:a9:a1 (e6:ba:9a:ae:a9:a1), Dst: 72:9c:7c:4d:99:66 (72:9c:7c:4d:99:66)
- Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.5
- Transmission Control Protocol, Src Port: 35680, Dst Port: 54269, Seq: 1, Ack: 1, Len: 68
- FTP Data (68 bytes data)
- Setup frame: 277
- Setup method: PASV
- Command: LIST
- Command frame: 279
- [Current working directory: /home/msfadmin]
- Line-based text data (1 lines)

The bottom screenshot shows a similar capture. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
432	190.345935319	192.168.1.5	192.168.1.100	FTP-DA	8754	FTP Data: 8688 bytes (PASV) (STOR RomeoJuliet.txt)
433	190.345942424	192.168.1.5	192.168.1.100	FTP-DA	23234	FTP Data: 23168 bytes (PASV) (STOR RomeoJuliet.txt)
434	190.345947886	192.168.1.5	192.168.1.100	FTP-DA	23234	FTP Data: 23168 bytes (PASV) (STOR RomeoJuliet.txt)
437	190.346052461	192.168.1.5	192.168.1.100	FTP-DA	2962	FTP Data: 2896 bytes (PASV) (STOR RomeoJuliet.txt)
439	190.346058645	192.168.1.5	192.168.1.100	FTP-DA	2962	FTP Data: 2896 bytes (PASV) (STOR RomeoJuliet.txt)
444	190.346097056	192.168.1.5	192.168.1.100	FTP-DA	10202	FTP Data: 10136 bytes (PASV) (STOR RomeoJuliet.txt)
445	190.346102100	192.168.1.5	192.168.1.100	FTP-DA	1466	FTP Data: 1400 bytes (PASV) (STOR RomeoJuliet.txt)
447	190.346106710	192.168.1.5	192.168.1.100	FTP-DA	1514	FTP Data: 1448 bytes (PASV) (STOR RomeoJuliet.txt)
448	190.346108123	192.168.1.5	192.168.1.100	FTP-DA	152	FTP Data: 86 bytes (PASV) (STOR RomeoJuliet.txt)
484	190.359173075	192.168.1.100	192.168.1.5	FTP-DA	486	FTP Data: 340 bytes (PASV) (LIST)

The packet details pane for frame 484 shows:

- Frame 484: 486 bytes on wire (3248 bits), 486 bytes captured (3248 bits) on interface eth0, id 0
- Ethernet II, Src: e6:ba:9a:ae:a9:a1 (e6:ba:9a:ae:a9:a1), Dst: 72:9c:7c:4d:99:66 (72:9c:7c:4d:99:66)
- Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.5
- Transmission Control Protocol, Src Port: 43711, Dst Port: 42241, Seq: 1, Ack: 1, Len: 340
- FTP Data (340 bytes data)
- Setup frame: 478
- Setup method: PASV
- Command: LIST
- Command frame: 479
- [Current working directory: /home/msfadmin/vulnerable]
- Line-based text data (5 lines)

4) Discuss security implications of this transfer.

It's unsecure, we were able to connect to the Metaspolitable desktop with their credentials and IP address. As such we had read/write privileges which is extremely dangerous.

Task 5. SYN Flooding Attack

1) Report your Wireshark capture in a screenshot. Show only SYN packets.

The screenshot displays a Kali Linux desktop environment. In the foreground, a terminal window shows the execution of a SYN flood attack using the `hping3` tool. The command `hping3 192.168.1.100 -i 10000 -S -C` is run, which floods the target IP with SYN packets. The terminal output shows the hping process running in flood mode and a statistics summary indicating 224,283 packets transmitted with 100% packet loss.

In the background, the Wireshark network capture tool is open, showing a list of captured packets. The filter `tcp` is applied, and the packet list shows several SYN packets from the source IP `192.168.1.100` to the destination IP `192.168.1.100`. The packet details pane shows the first packet's structure, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) fields.

Wireshark Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.100	192.168.1.100	TCP	54	35347 → 0 [SYN] Seq=0 Win=512
2	0.000015741	192.168.1.100	192.168.1.100	TCP	54	35348 → 0 [SYN] Seq=0 Win=512
3	0.000028021	192.168.1.100	192.168.1.100	TCP	54	35349 → 0 [SYN] Seq=0 Win=512
4	0.000042254	192.168.1.100	192.168.1.100	TCP	54	35350 → 0 [SYN] Seq=0 Win=512
5	0.000053108	192.168.1.100	192.168.1.100	TCP	54	35351 → 0 [SYN] Seq=0 Win=512
6	0.000064934	192.168.1.100	192.168.1.100	TCP	54	35352 → 0 [SYN] Seq=0 Win=512
7	0.000075587	192.168.1.100	192.168.1.100	TCP	54	35353 → 0 [SYN] Seq=0 Win=512
8	0.000087378	192.168.1.100	192.168.1.100	TCP	54	35354 → 0 [SYN] Seq=0 Win=512

Terminal Output:

```
hping3 192.168.1.100 -i 10000 -S -C
hping in flood mode, no replies will be shown
^C
--- 192.168.1.100 hping statistic ---
224283 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:/home/kali#
```