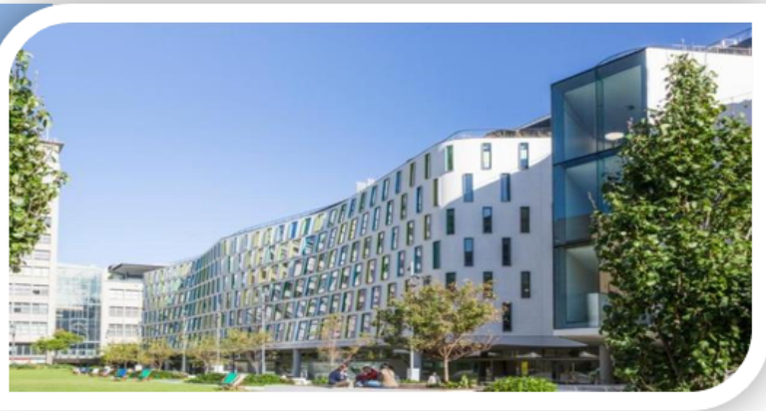
UNIVERSITY OF TECHNOLOGY, SYDNEY

IoT Security – Autumn 2024



Exploiting Unsecured Ports in IoT Devices through Packet Crafting

Manh Bui
DucManh.Bui@uts.edu.au

Objectives of Workshop

Part 1

- Using hping3 for Port Scanning

Part 2:

- Crafting Different Types of ICMP Messages

Part 3:

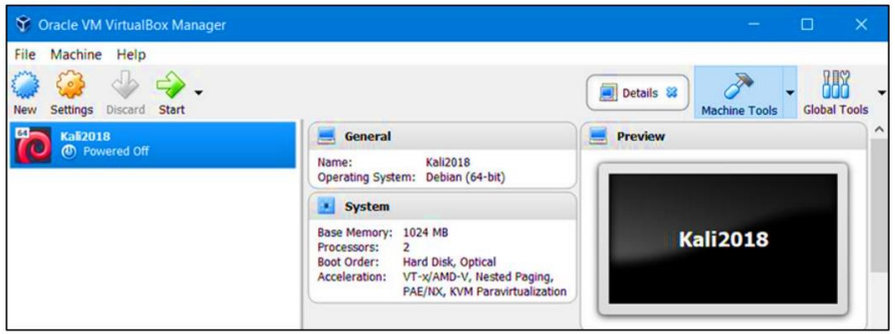
- Launching DoS Attacks

Required Resources

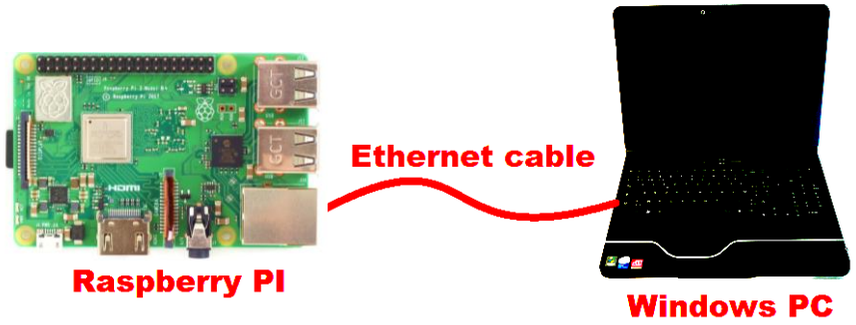
Part1: Raspberry Pi 3 Model B or later

Part2: 8GB Micro SD card (minimum required)

Part3: PC with IoTSec Kali VM



Part4: Network connectivity between PC and Raspberry Pi



DDoS/DoS attacks

How does cybercrime host the DDoS/DoS attacks?

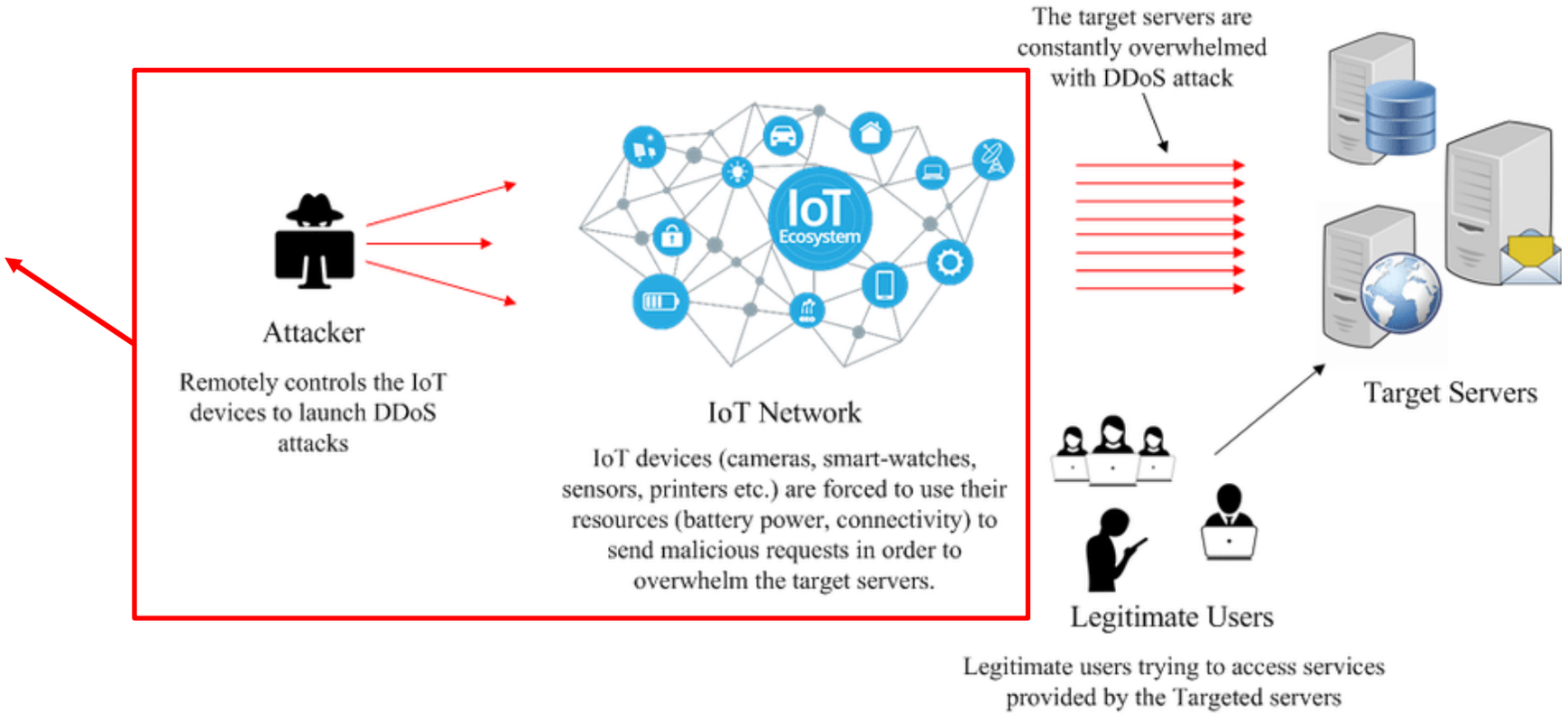


Figure 1: Example of DDoS attacks on IoT environment

Packet Crafting

- Packet crafting is the manual modification of network packets to manipulate or **exploit network behaviour.**
- Allow users to create packets with **any type of content** (length, payload,…)

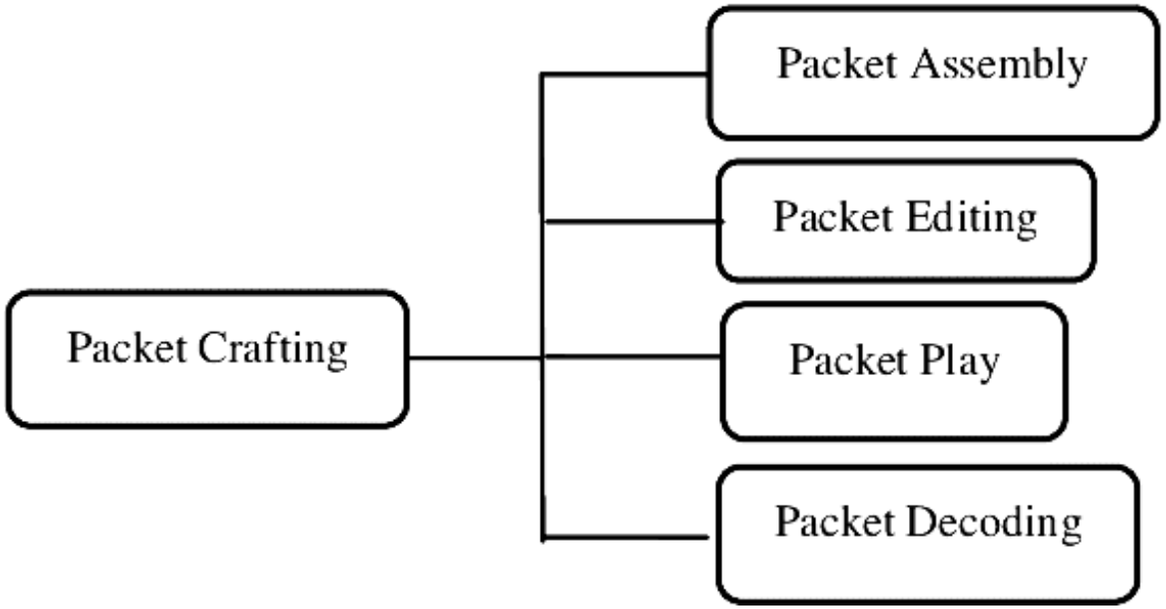


Figure 2: Stages of packet crafting

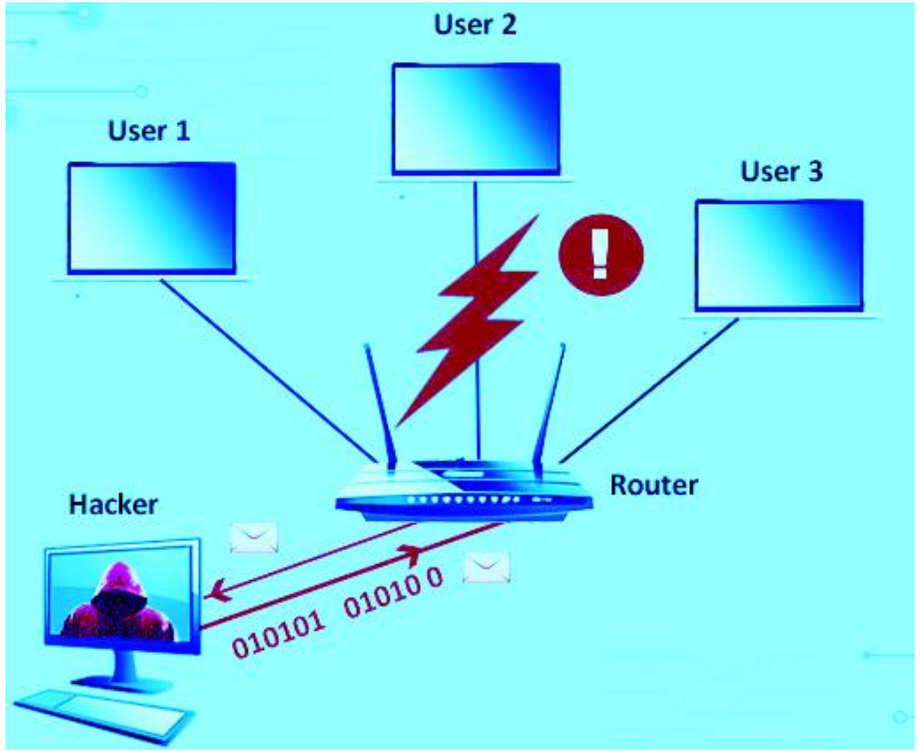
Packet Crafting Process

+----------------------+
Application or Script
+----------------------+

+----------------------+
Packet Crafting
+----------------------+

+----------------------+
Modified Packet
+----------------------+

+----------------------+
Sending the Packet
+----------------------+



Ref.

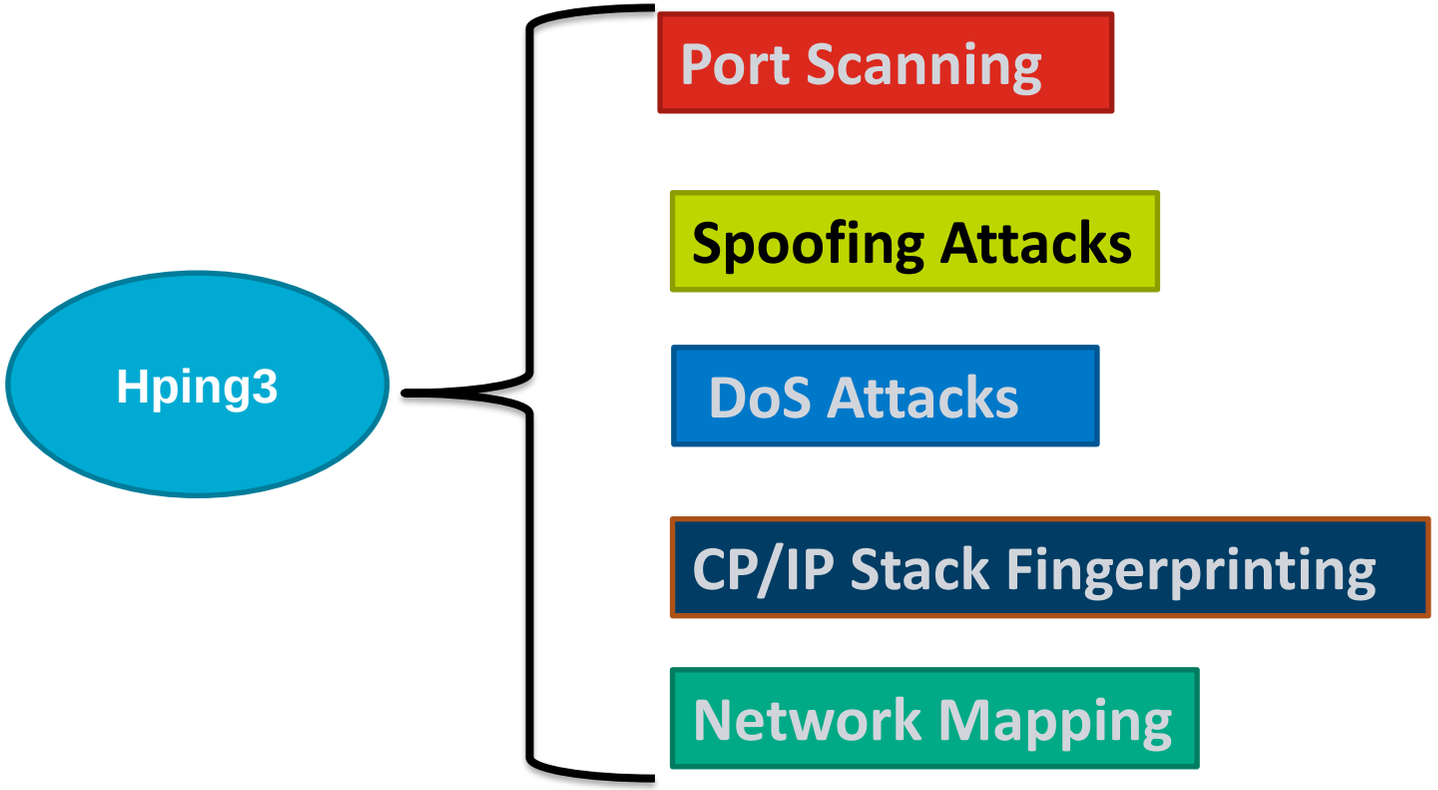
Hping3 Tools

- hping3 is a network tool able to send custom **ICMP/UDP/TCP** packets and to display target replies like ping does with **ICMP** replies.

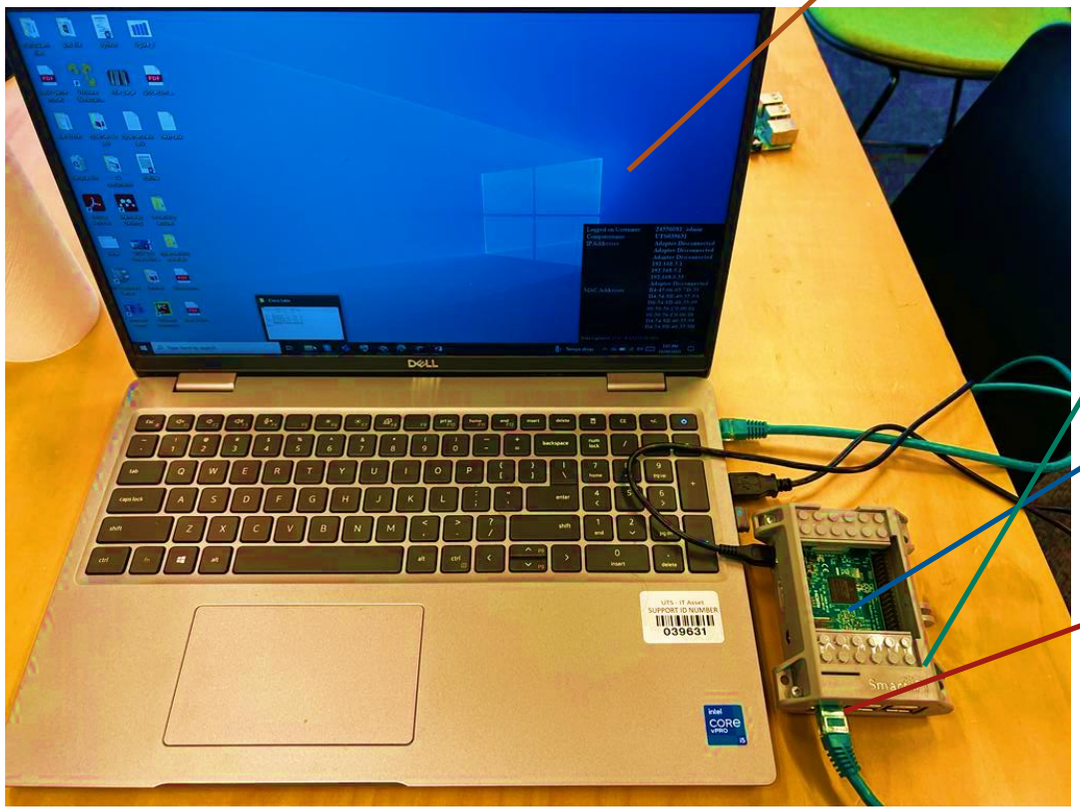
- Like Nmap, hping3 can use the TCP header flag fields **URG, ACK, PSH, RST, SYN**, and **FIN** to accomplish its scans.

- Using hping3, you can test firewall rules, perform (spoofed) port scanning, and test network performance using different protocols.

Hping3 Tools



Environment Setup



PC with IoTSec Kali VM

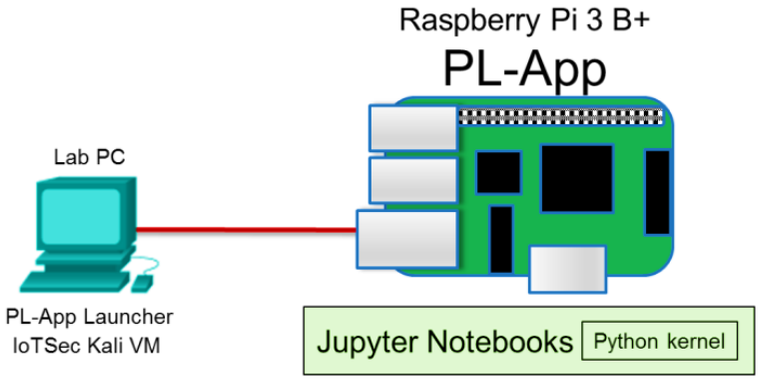
Sd card inserted

Raspberry Pi 3

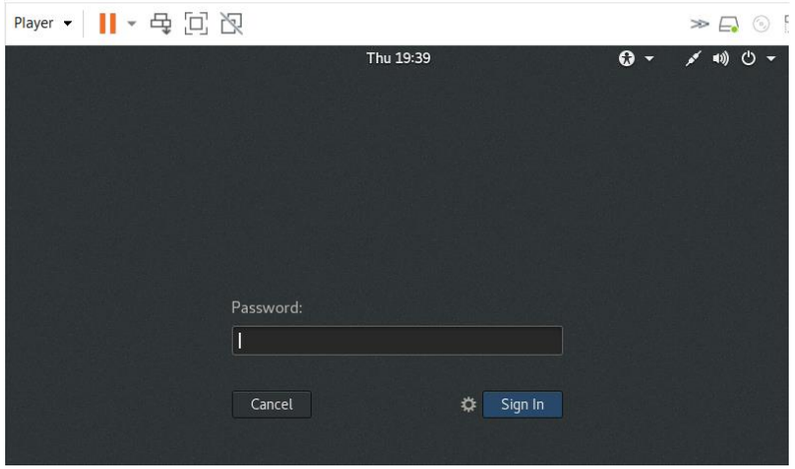
Network connectivity between PC and Raspberry Pi

Part 1: Hping3 for Port Scanning-Cont.

a. Set up the topology by connecting the Raspberry Pi to the PC.



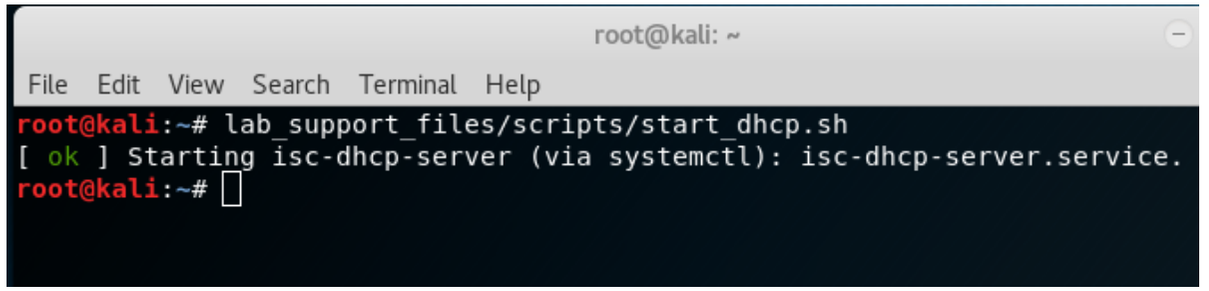
b. Start the IoTSec Kali VM and log in.



Part 1: Hping3 for Port Scanning-Cont.

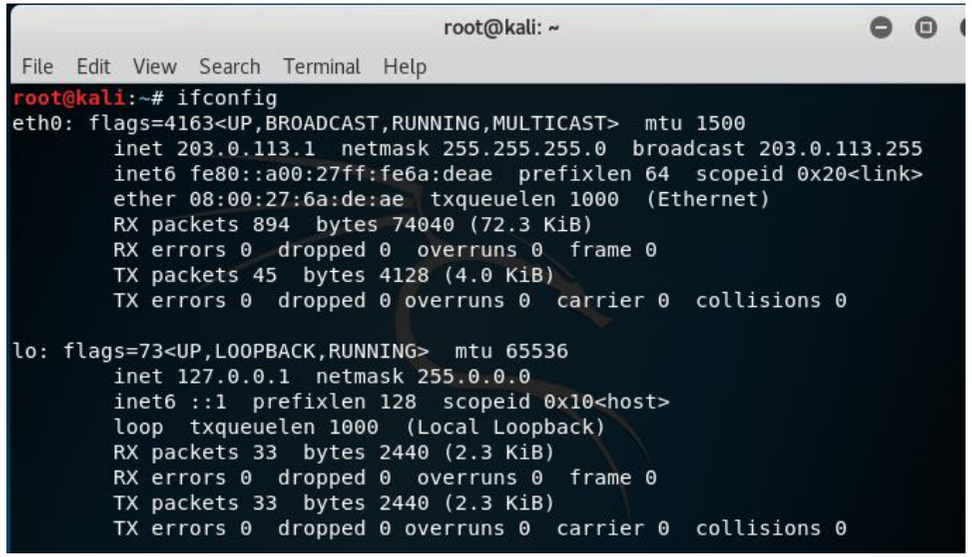
c. Open a terminal and start the DHCP server on the Kali VM.

root@kali:~#lab_support_files/scripts/start_dhcp.sh



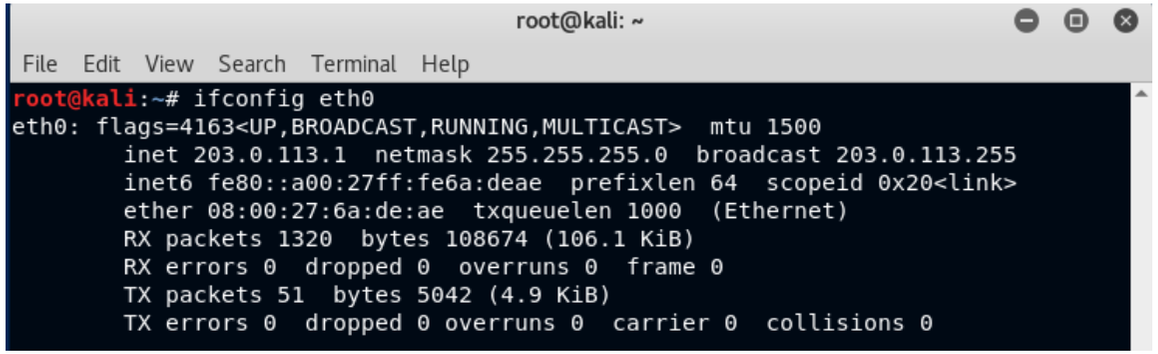
d. Verify that Kali VM is assigned an IP address on eth0.

root@kali:~# ifconfig

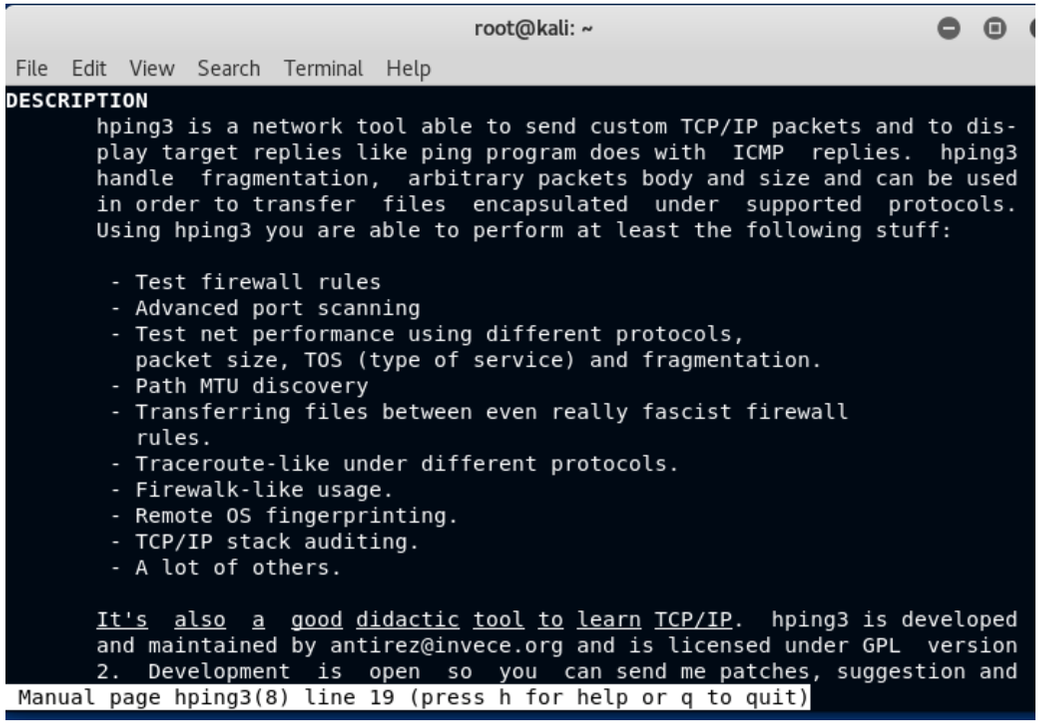


Part 1: Hping3 for Port Scanning-Cont.

e. Determine the IP address of your Raspberry Pi.



f. Open the man page for hping3 in Kali VM and review the features and options that are available in hping3.

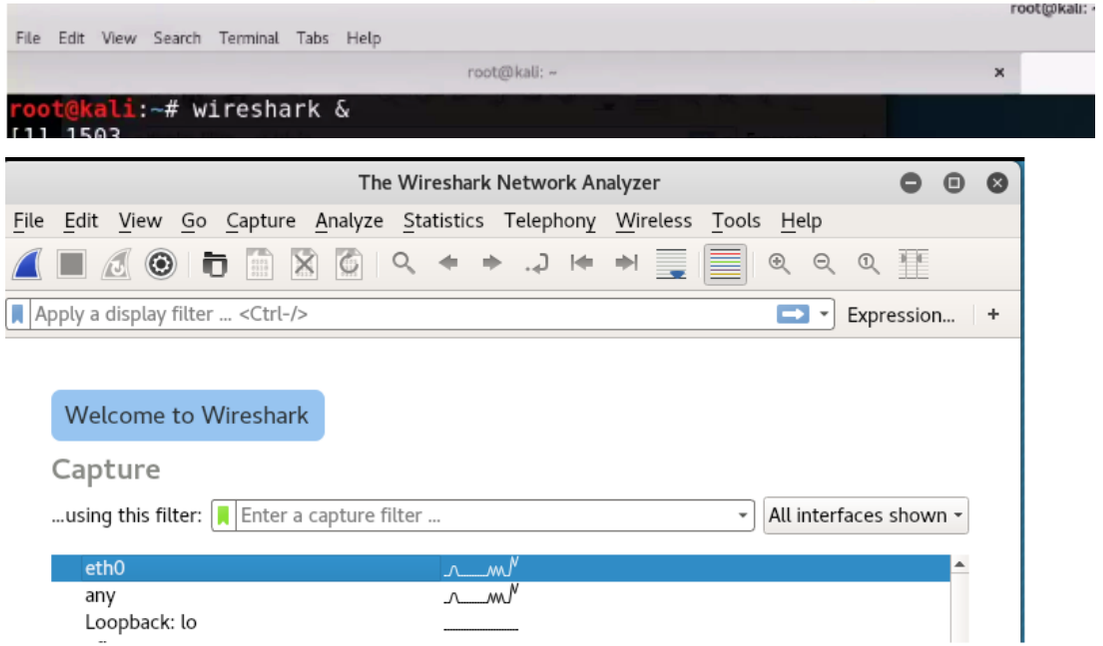


Part 1: Hping3 for Port Scanning-Cont.

g. In a Kali VM terminal, start Wireshark to monitor what hping3 is doing when we are scanning.

root@kali:~# wireshark

h. Select the **eth0** interface and click **Capture** to start capturing packets

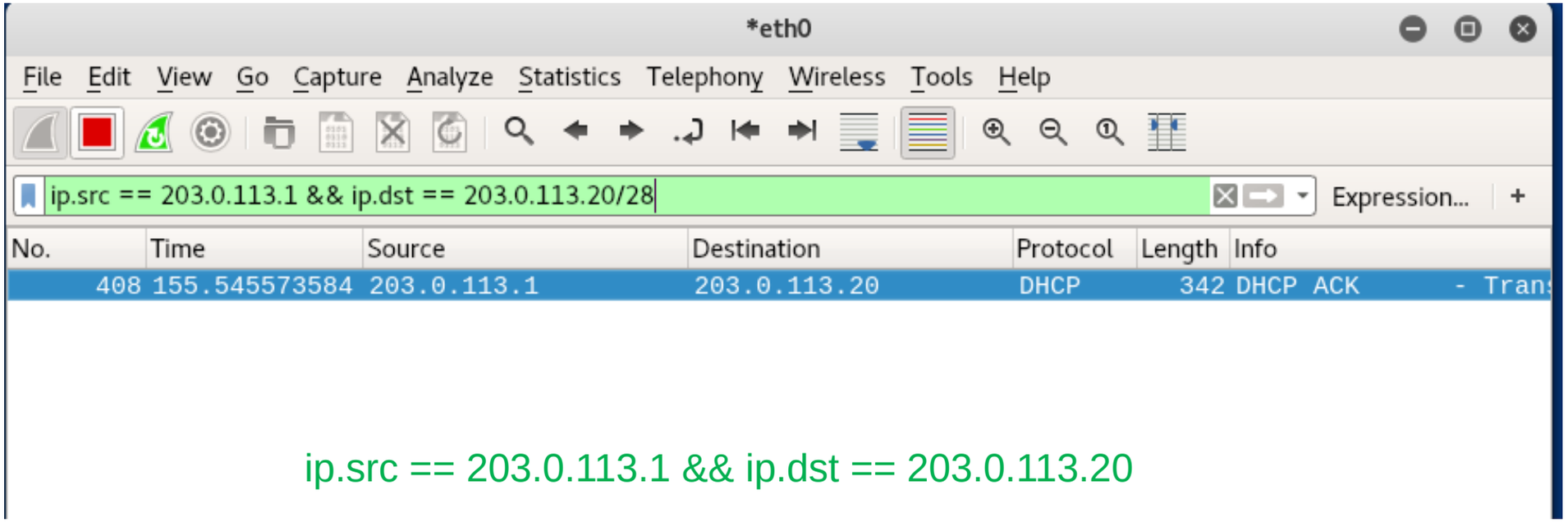


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	203.0.113.19	13.89.178.27	TCP	66	51114 → 443 [SYN] S
2	0.159836271	203.0.113.19	8.8.8.8	DNS	88	Standard query 0x24
3	0.159862131	203.0.113.19	8.8.8.8	DNS	88	Standard query 0x21
4	0.249637891	203.0.113.19	224.0.0.251	MDNS	80	Standard query 0x00
5	0.251119445	203.0.113.19	13.89.178.27	TCP	66	51115 → 443 [SYN] S
6	0.356348607	Raspberr_6d:7a:55	Broadcast	ARP	60	Who has 203.0.113.1
7	0.356373801	PcsCompu_6a:de:ae	Raspberr_6d:7a:55	ARP	42	203.0.113.1 is at 0
8	0.502444569	203.0.113.19	13.89.178.27	TCP	66	51116 → 443 [SYN] S
9	0.546608456	b4:45:06:65:7d:39	PcsCompu_6a:de:ae	ARP	60	Who has 203.0.113.1
10	0.546635831	PcsCompu_6a:de:ae	b4:45:06:65:7d:39	ARP	42	203.0.113.1 is at 0
11	0.750236510	203.0.113.19	13.89.178.27	TCP	66	51117 → 443 [SYN] S

Part 1: Hping3 for Port Scanning-Cont.

i. You may have captured network traffic that is not relevant to this lab. We are going to restrict the type and of packets we see by using a display filter

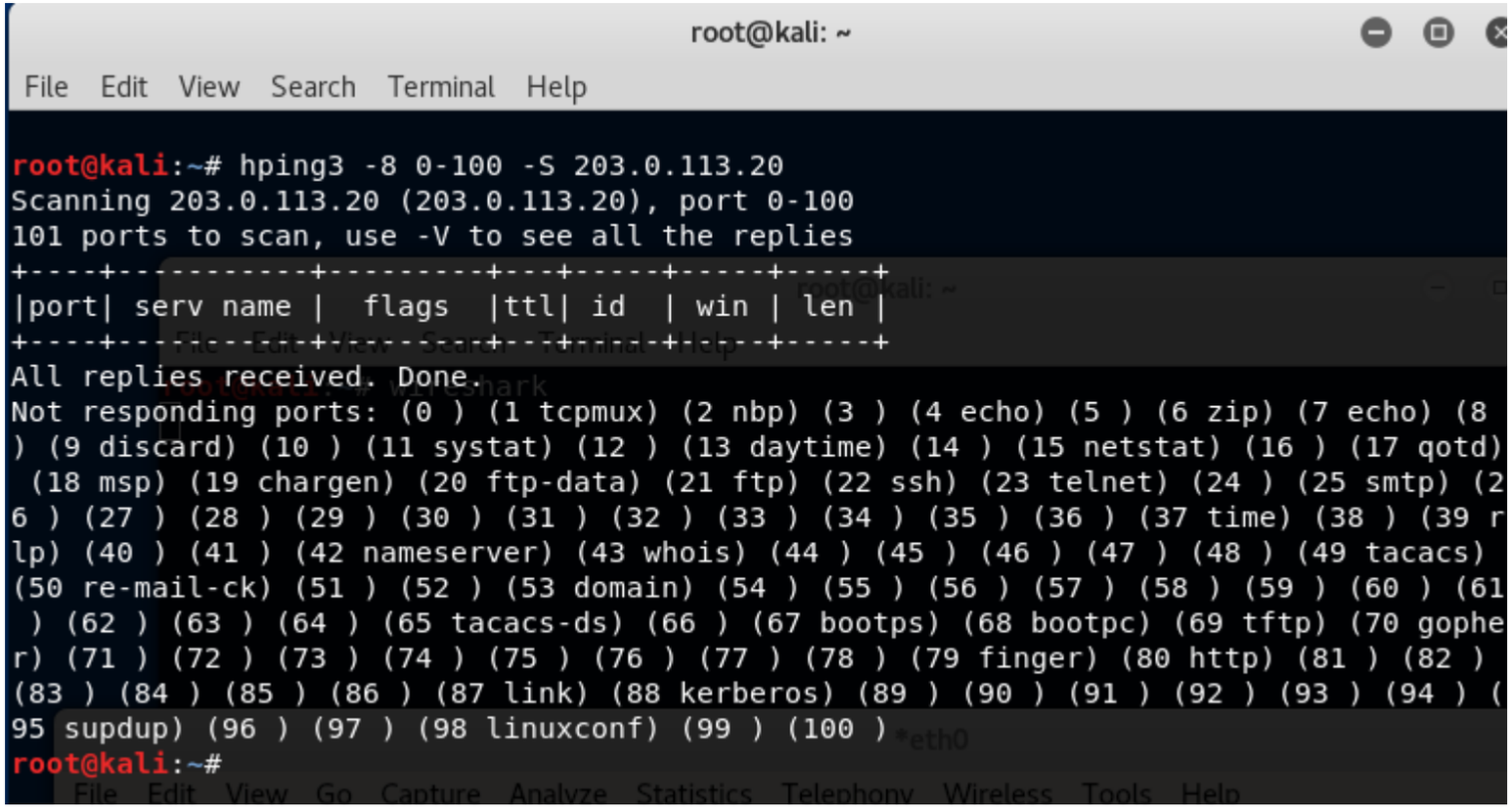
Apply the following filter in Wireshark using IP address of Kali VM as the source address and IP address of your Raspberry Pi as the destination address. In this example, 203.0.113.1 is IP address for Kali VM and 203.0.113.20 is the IP address of your Raspberry Pi.



Part 1: Hping3 for Port Scanning-Cont.

j. We will first craft packets to do a port scan against the IP address of your Raspberry Pi.

root@kali:~# hping3 -8 0-100 -S 203.0.113.20



Part 1: Hping3 for Port Scanning-Cont.

Refer to the Wireshark capture, the man pages, and other sources on the Internet. What do the options 8, 0-100 and -S do?

_____

_____

-8 signifies scan mode, 0-100 is the port range to be scanned and -S is sets the SYN flag in the scan.

What ports are shown as open?

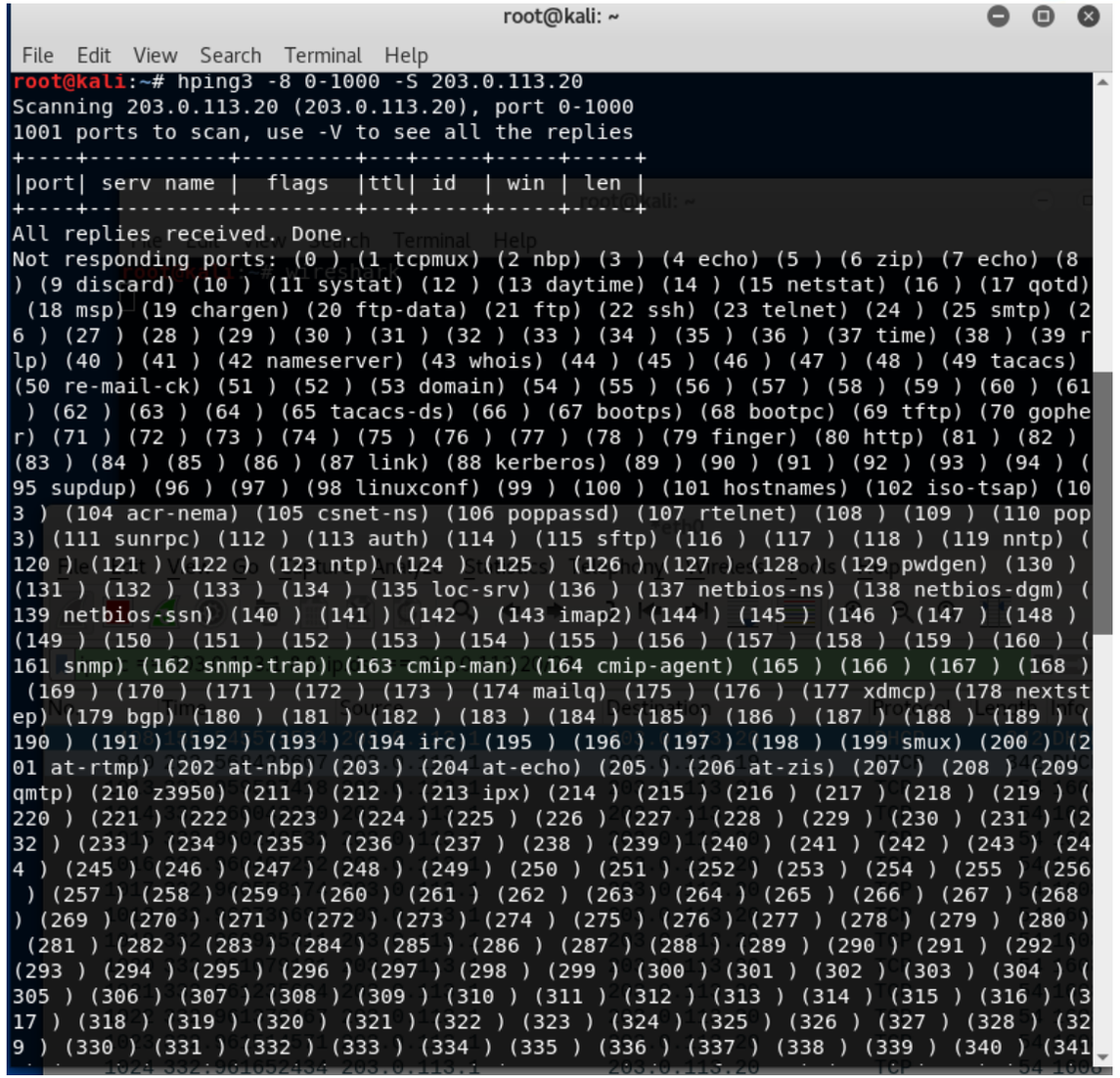
_____

Answers may vary. Ports 22 and 80 will be open at minimum.

Part 1: Hping3 for Port Scanning-Cont.

k. Expand your scan to include ports up to 1000.

root@kali:~# hping3 -8 0-1000 -S 203.0.113.20



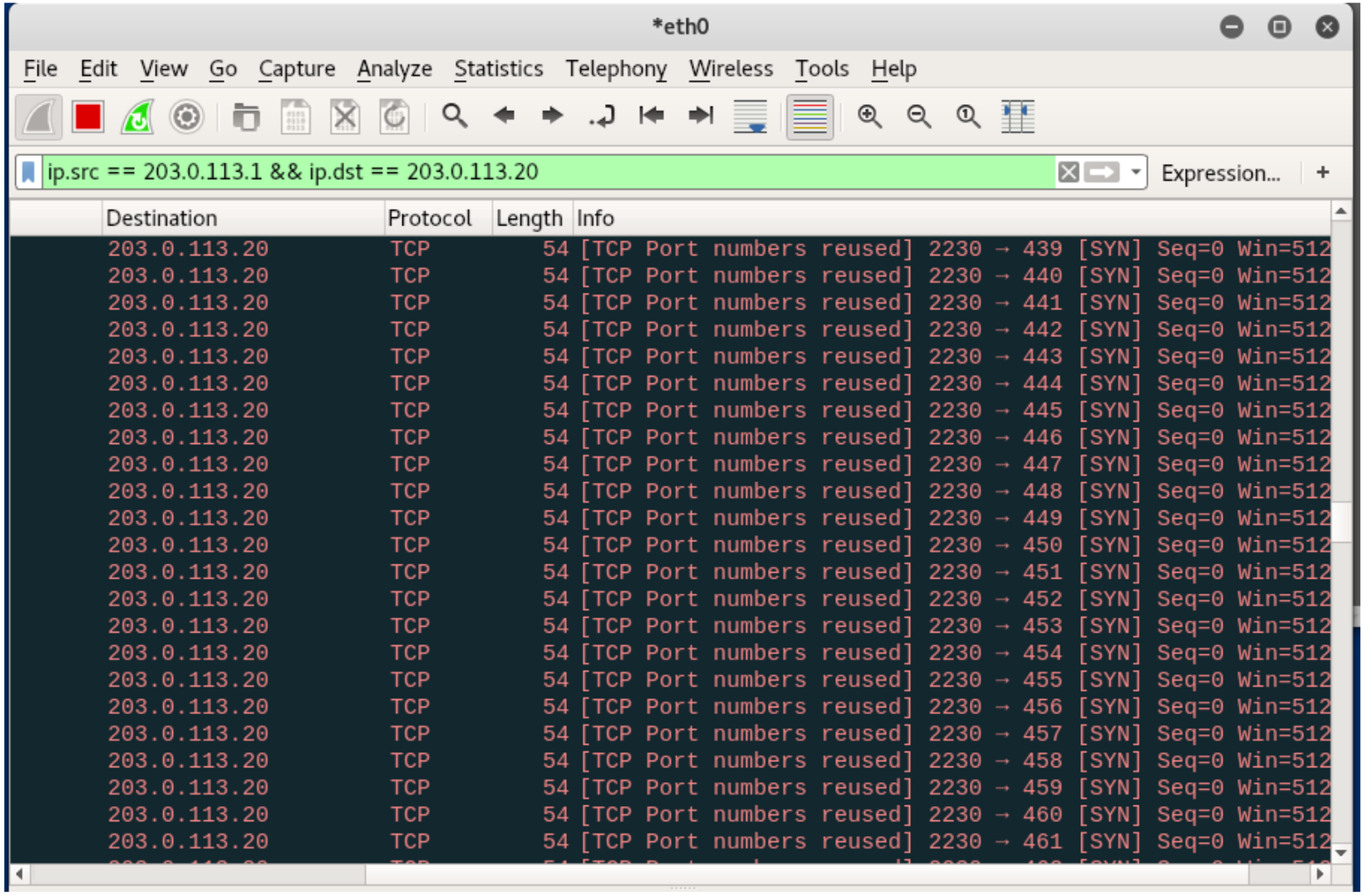
Part 1: Hping3 for Port Scanning-Cont.

Did you find any additional ports?

No

What TCP flag was set in the shown in Wireshark?

SYN



Part 2: Crafting Different Types of ICMP Messages

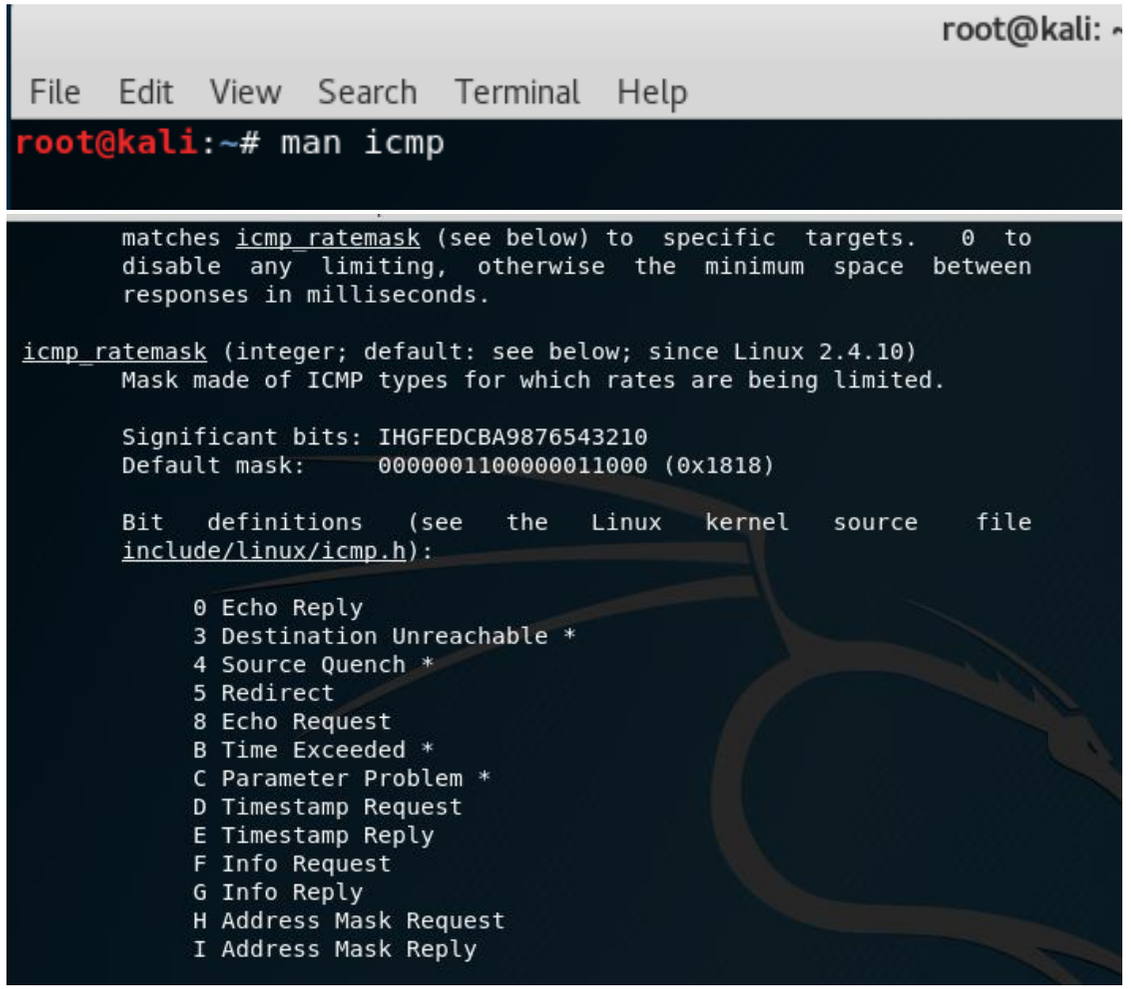
The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues.

Type	Code	Description
0 – Echo Reply	0	Echo reply
3 – Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation needed and DF flag set
	5	Source route failed
5 – Redirect Message	0	Redirect datagram for the Network
	1	Redirect datagram for the host
	2	Redirect datagram for the Type of Service and Network
	3	Redirect datagram for the Service and Host
8 – Echo Request	0	Echo request
9 – Router Advertisement	0	Use to discover the addresses of operational routers
10 – Router Solicitation	0	
11 – Time Exceeded	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12 – Parameter Problem	0	Pointer indicates error
	1	Missing required option
	2	Bad length
13 – Timestamp	0	Used for time synchronization
14 – Timestamp Reply	0	Reply to Timestamp message

Part 2: Crafting Different Types of ICMP Messages

a. Open the man page for ICMP in Kali VM and review the features and options that are available in ICMP.

root@kali:~# man icmp

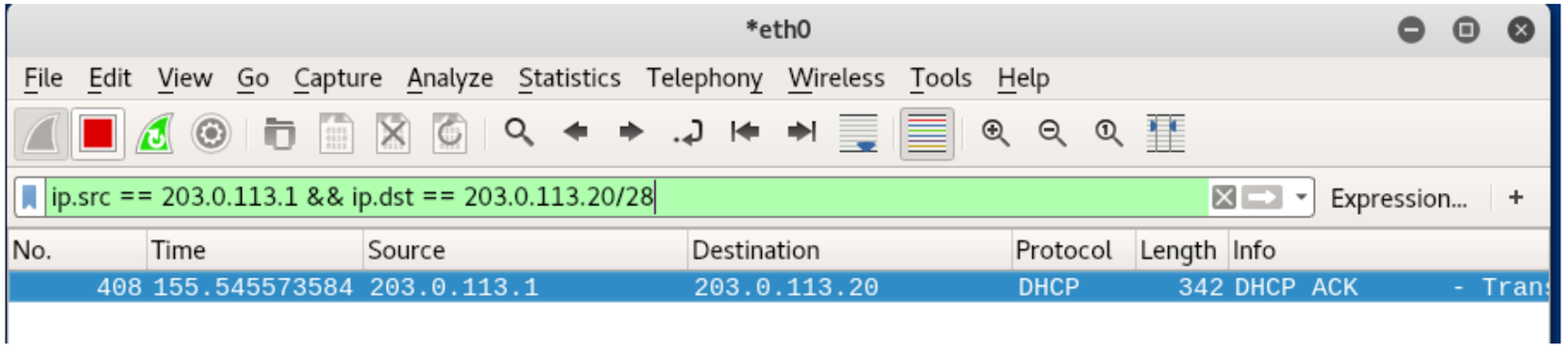


What is the RFC for ICMP?

RFC 792

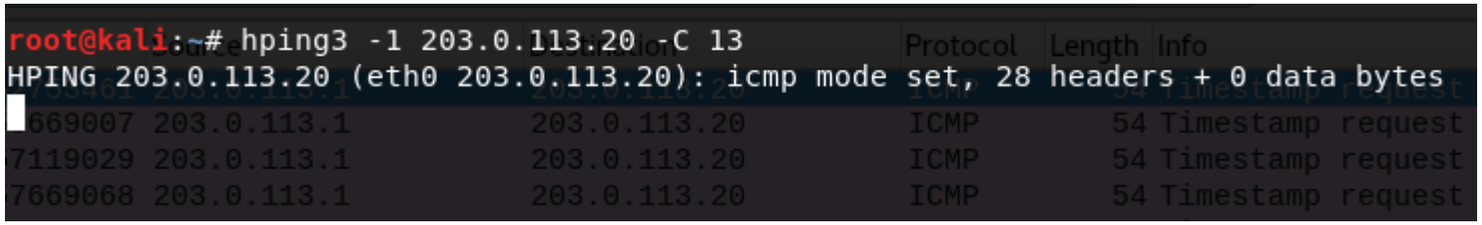
Part 2: Crafting Different Types of ICMP Messages

b. Start a new Wireshark capture. Click Continue without Saving when prompted to save the capture. Apply the same display filter as in the previous part.



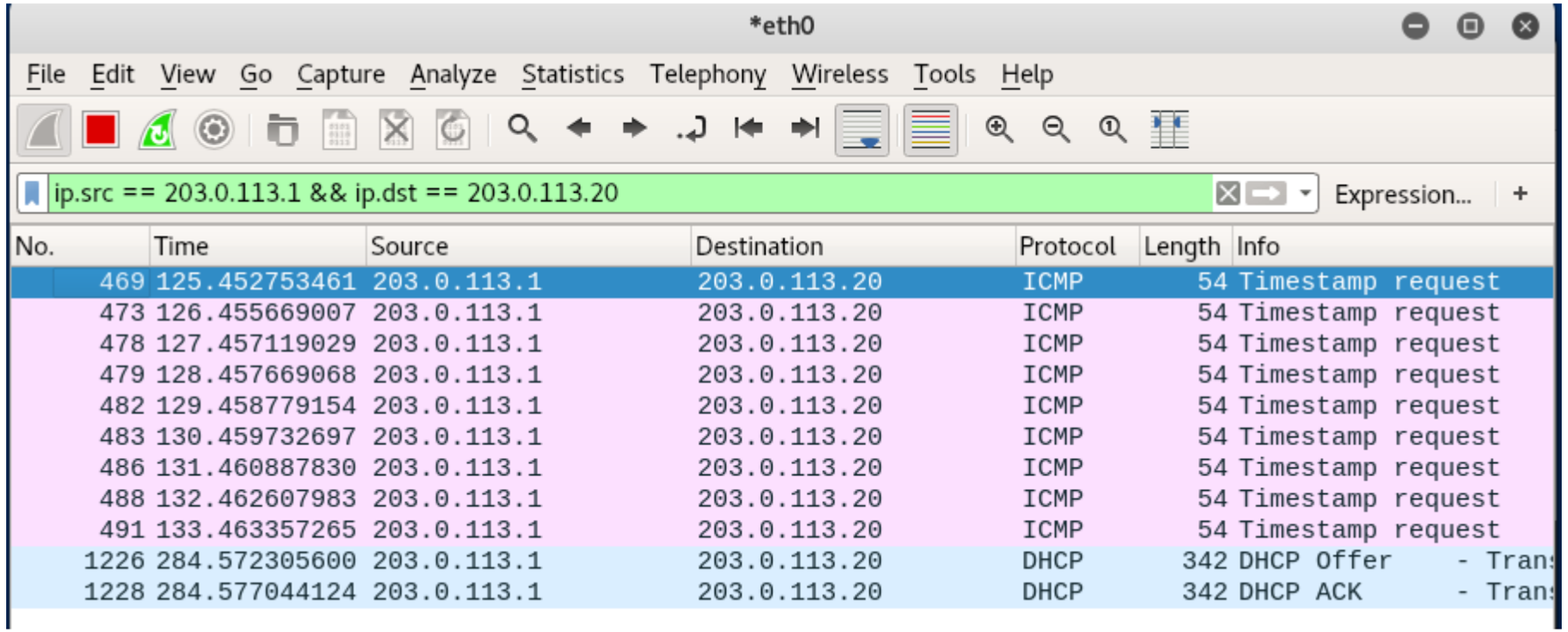
c. In the terminal, enter the hping3 command followed by -1 to scan in ICMP mode. Add the scan target IP address, and enter -C followed by 13 to indicate that ICMP type 13 timestamp request messages should be sent.

root@kali:~# hping3 -1 203.0.113.13 -C 13



Part 2: Crafting Different Types of ICMP Messages

d. Review the Wireshark results and confirm that the ICMP timestamp request packets were sent out. To stop the requests, press Ctrl-C in the Kali VM terminal.

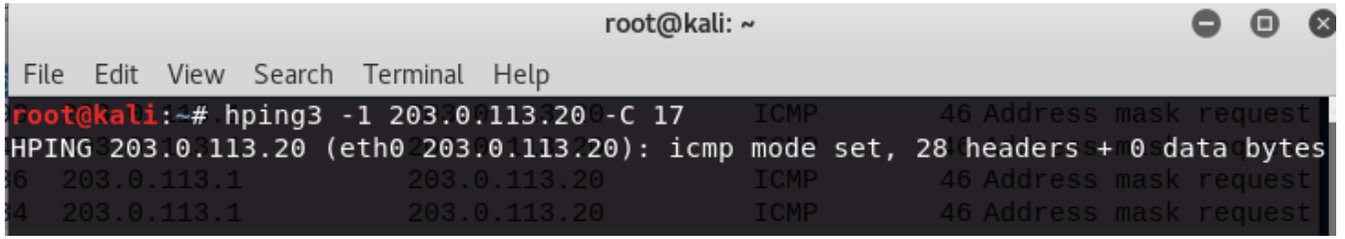


e. Start a new Wireshark capture. Click Continue without Saving when prompted to save the capture

Part 2: Crafting Different Types of ICMP Messages

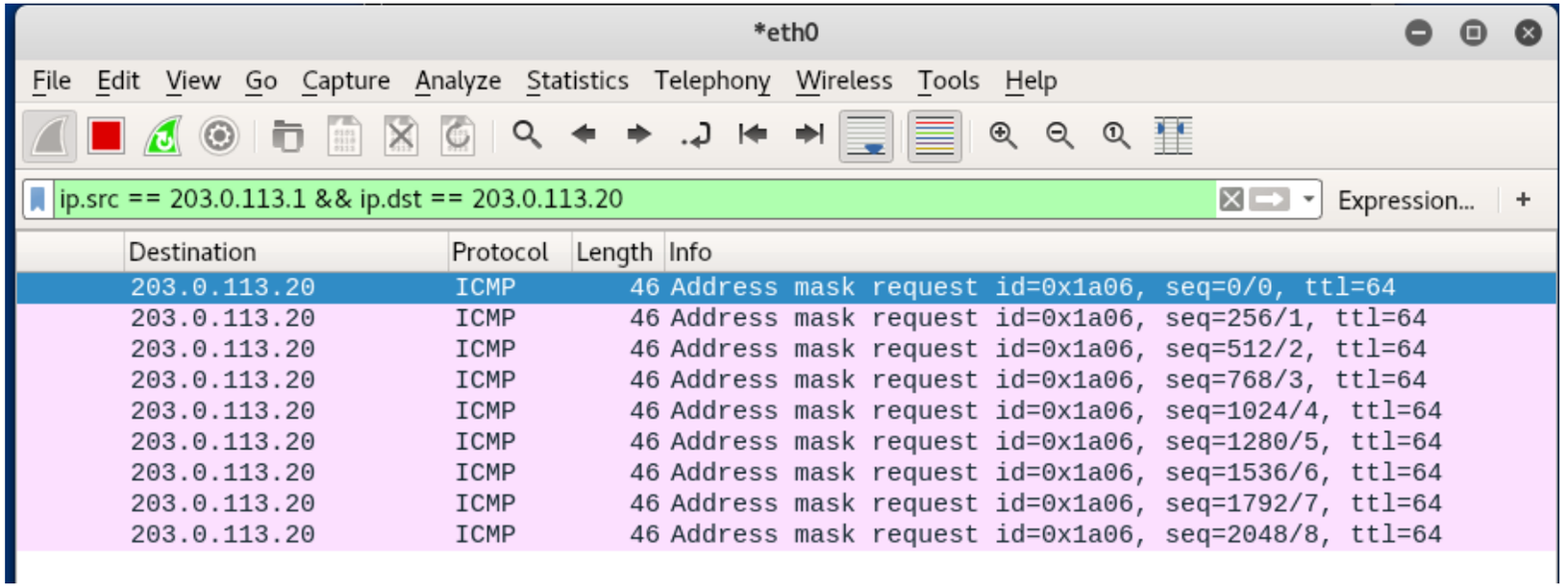
f. Apply the following filter in Wireshark using IP address of Kali VM as the source address and IP address of your Raspberry Pi as the destination address

ip.src == 203.0.113.1 && ip.dst == 203.0.113.13



g. Repeat the hping3 command above, but this time send ICMP code 17.

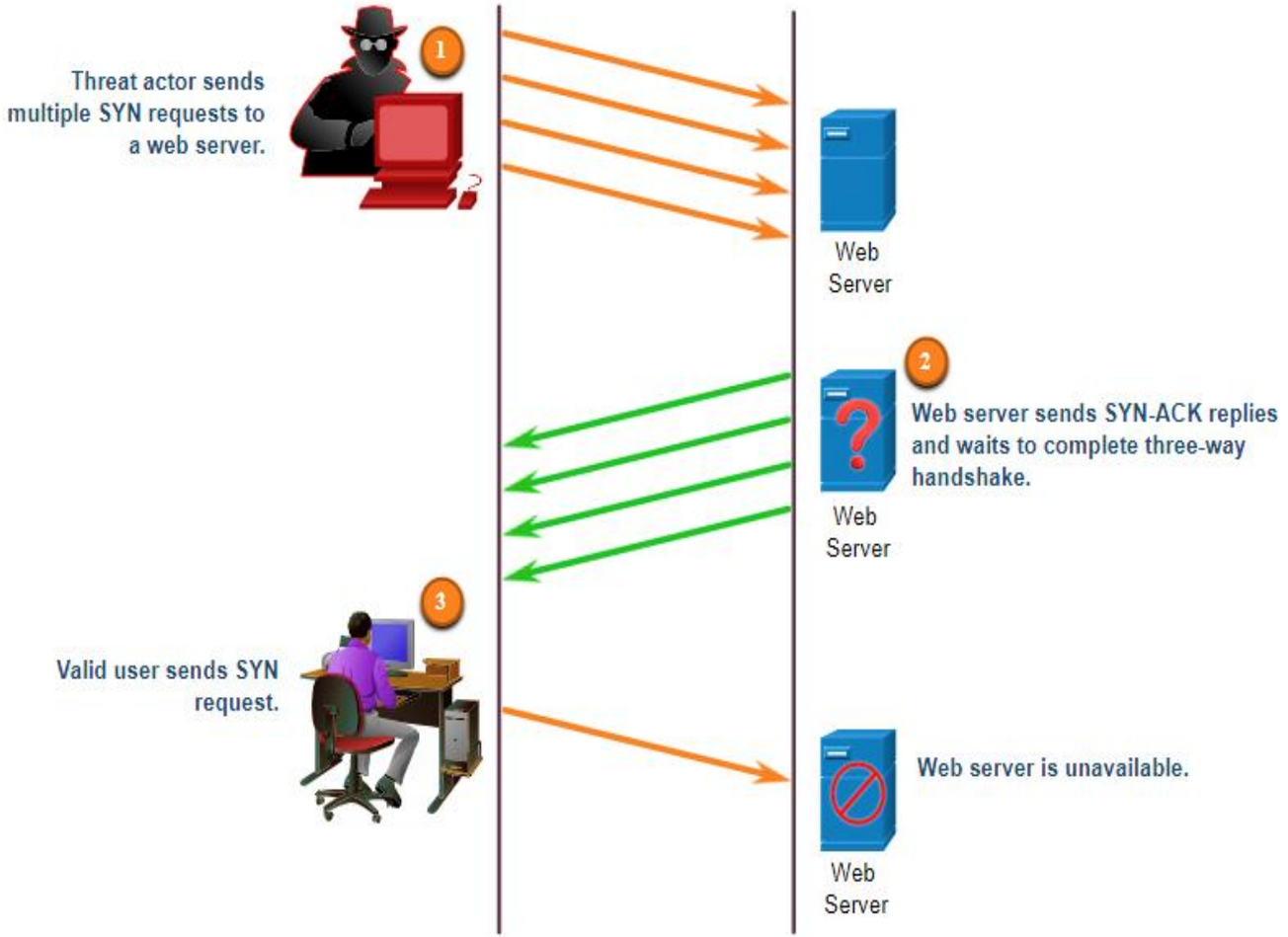
h. Review the Wireshark results. Which ICMP message was sent?



Part 3: Launching DoS Attacks

- The goal of a DoS attack is to make the **website or service unavailable** to its users, often resulting in loss of revenue, damage to reputation, and inconvenience to customers.
- There are several different types of DoS attacks, including:
  - **SYN Flood Attack**: Sends a large number of SYN requests to a server, causing it to be unable to handle any new requests.
  - **UDP Flood Attack**: Sends a large number of User Datagram Protocol (UDP) packets to a server, overwhelming its ability to process the requests.
  - **Ping of Death**: Sends an oversized packet to a server, causing it to crash or become unresponsive.
  - **Smurf Attack:** Sends a large number of ICMP packets to a network, causing all devices on the network to become unresponsive.
  - **Slowloris Attack:** Sends a large number of incomplete requests to a server, keeping the server busy and preventing it from serving legitimate requests.

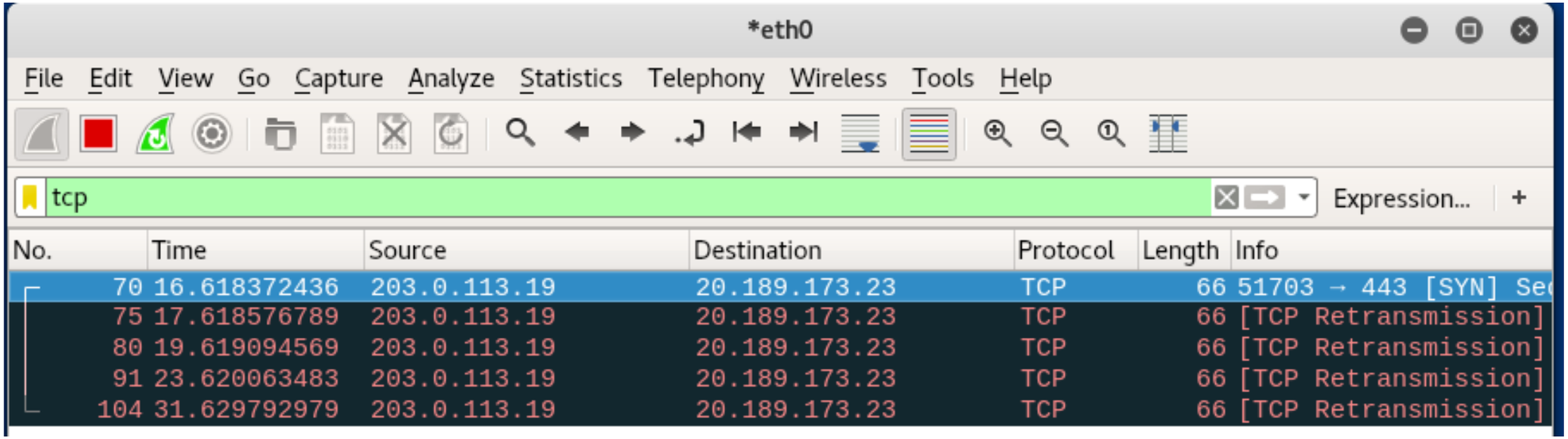
Part 3: Launching DoS Attacks-Cont.



Part 3: Launching DoS Attacks-Cont.

Hping3 can launch DoS attacks against ports you found previously in this lab. Using hping3 for this purpose is a good way to test how a network will react to various types of DoS attacks.

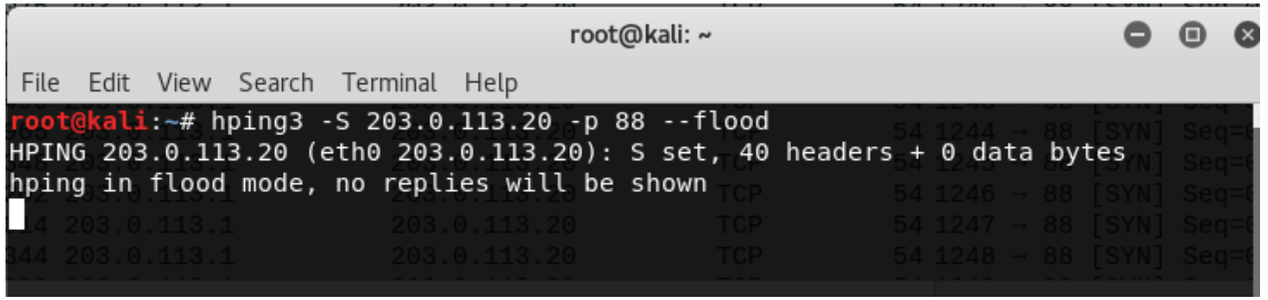
a. Start a new Wireshark capture. Click Continue without Saving when you are prompted to save the capture. To see two-way TCP traffic from between the Kali VM or the Raspberry Pi, enter only tcp as a display filter.



Part 3: Launching DoS Attacks-Cont.

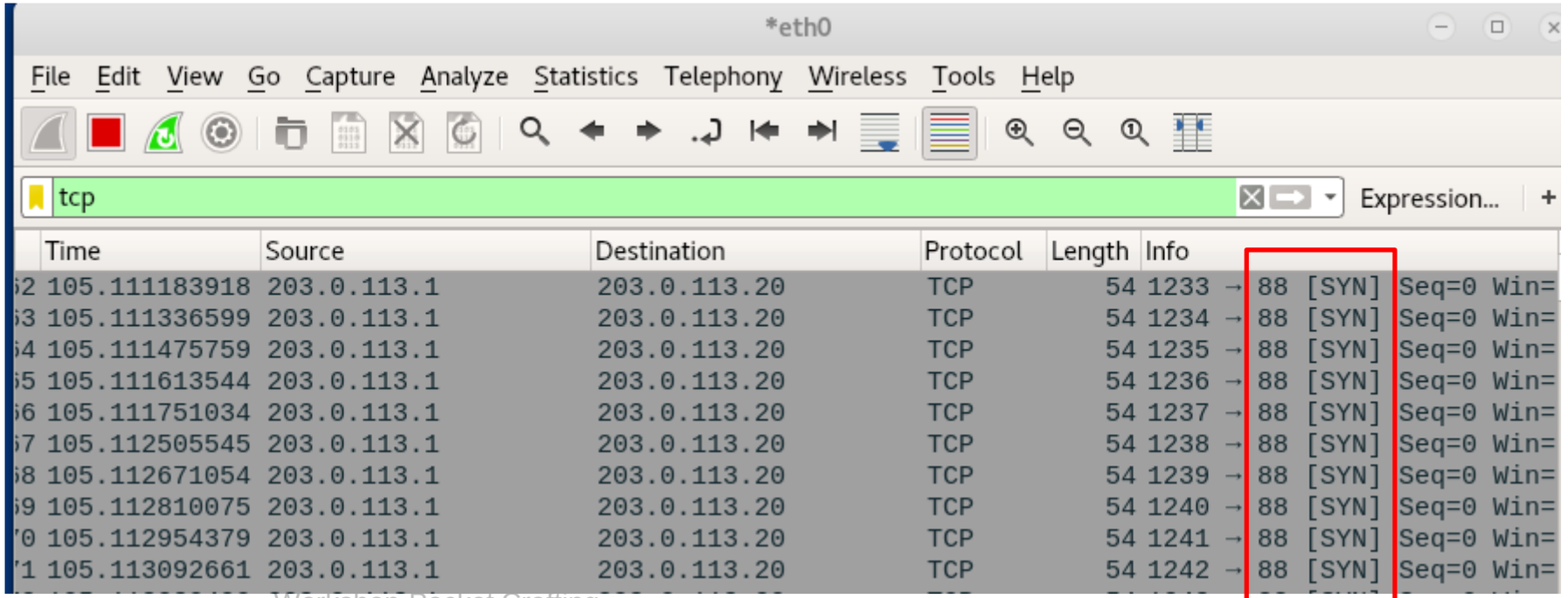
b. In the Kali VM terminal, enter the hping3 command to send a DoS attack

root@kali:~# hping3 -S 203.0.113.13 -p 88 --flood



Looking at Wireshark and the hping3 documentation, what type of TCP messages were sent in this DoS attack? What was the destination TCP port of the attack?

DoS SYN flood against port 88

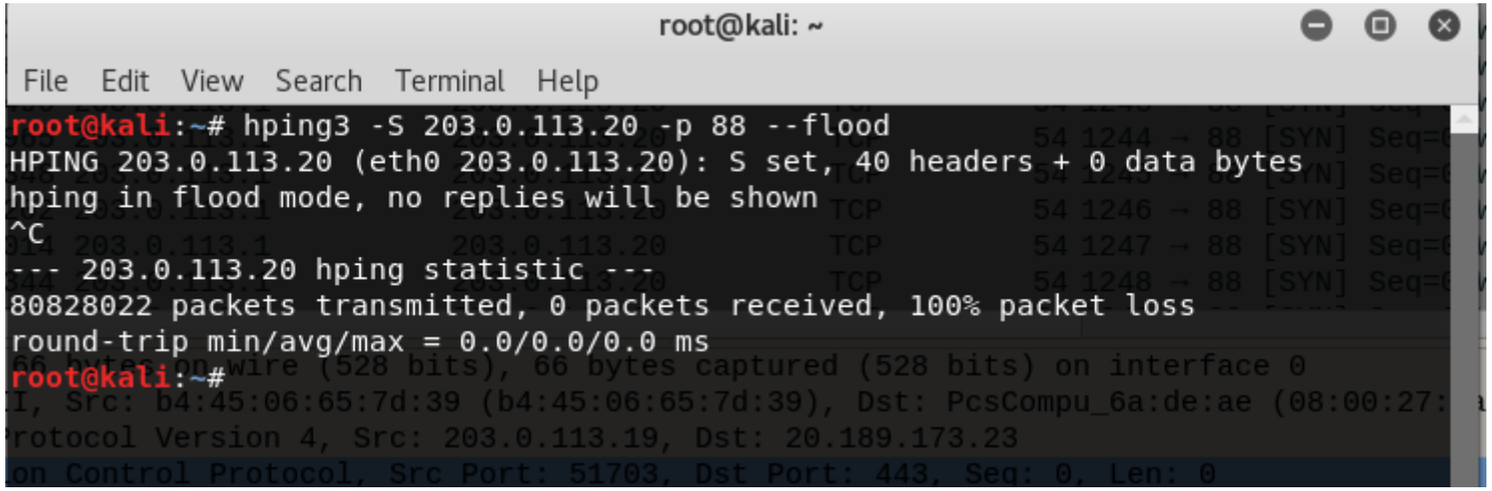


Part 3: Launching DoS Attacks-Cont.

Look at the source ports that hping3 uses to conduct the DoS flood. How does this scan assign source TCP ports?

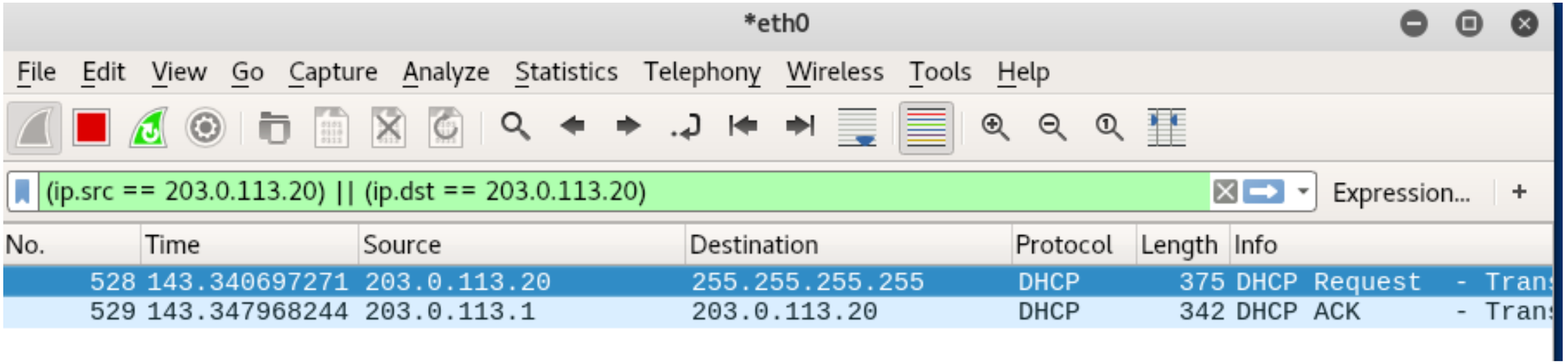
It starts at a random port and increments the source port number in each packet.

c. Press Ctrl-C to stop the flood



Part 3: Launching DoS Attacks-Cont.

d. Start a new Wireshark capture. Click Continue without Saving when prompted to save the capture. Display only traffic that has source or destination IP addresses that match the IP address of the Raspberry Pi. (Hint: Edit the ip.src and ip.dest display filter to both use the IP address of the Raspberry Pi. Instead of the && operator, use the || (or) operator.



Part 3: Launching DoS Attacks-Cont.

e. In the Kali VM terminal, enter the hping3 command to send a DoS Land Attack. This attack sends a packet with the same source IP/port combination as the destination IP/port. In other words, the source IP address is "spoofed" by replacing the Kali VM address another value in the packets

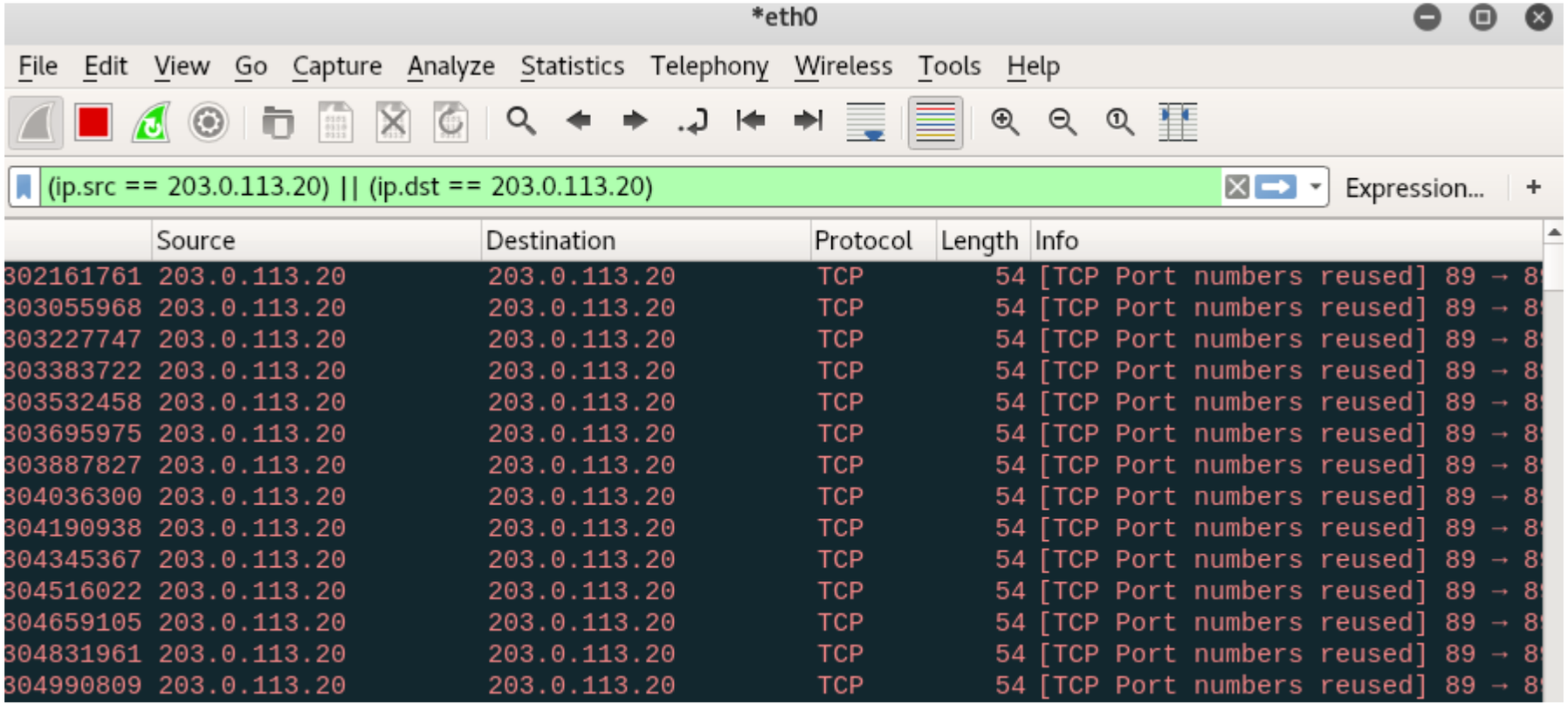
root@kali:~# hping3 -S 203.0.113.13 -a 203.0.113.13 -k -s 89 -p 89 --flood

```
root@kali:~# hping3 -S 203.0.113.20 -a 203.0.113.20 -k -s 89 -p 89 --flood
HPING 203.0.113.20 (eth0 203.0.113.20): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Compare this scan with the SYN flood that you just ran. How were source ports used in this scan? What info does Wireshark report about the packets?

The source port is specified for the scan and it does’t increment. Wirehark reports that TCP port numbers are reused

Part 3: Launching DoS Attacks-Cont.

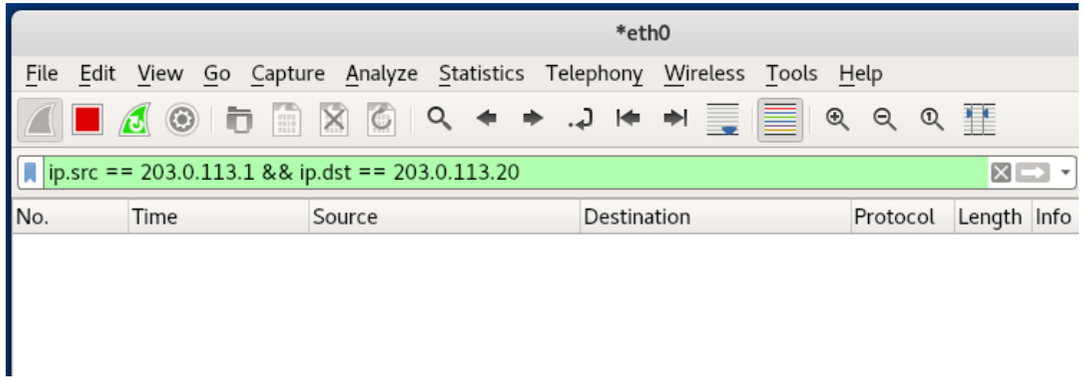


f. Press Ctrl-C to stop the flood

```
root@kali:~# hping3 -S 203.0.113.20 -a 203.0.113.20 -k -s 89 -p 89 --flood
HPING 203.0.113.20 (eth0 203.0.113.20): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 203.0.113.20 hping statistic ---
51940870 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

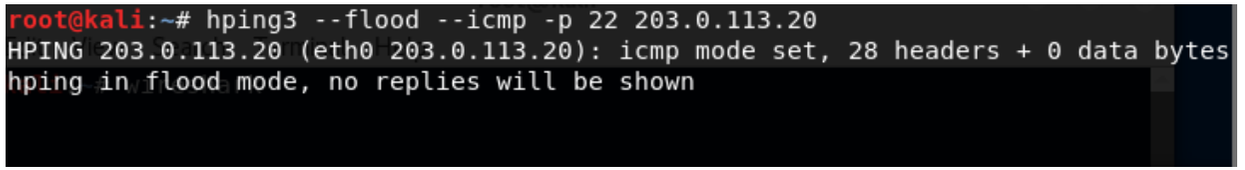
Part 3: Launching DoS Attacks-Cont.

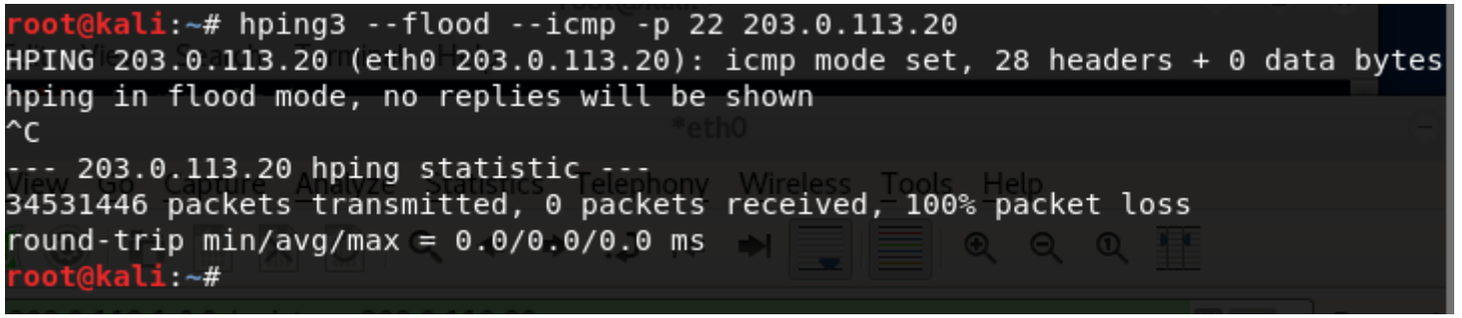
g. Start a new Wireshark capture. Click Continue without Saving when prompted to save the capture. Apply the display filter that specifies the Kali VM as the source and the Raspberry Pi as the destination, as was done previously in this lab.



h. In the Kali VM terminal, enter the hping3 command to send a flood attack

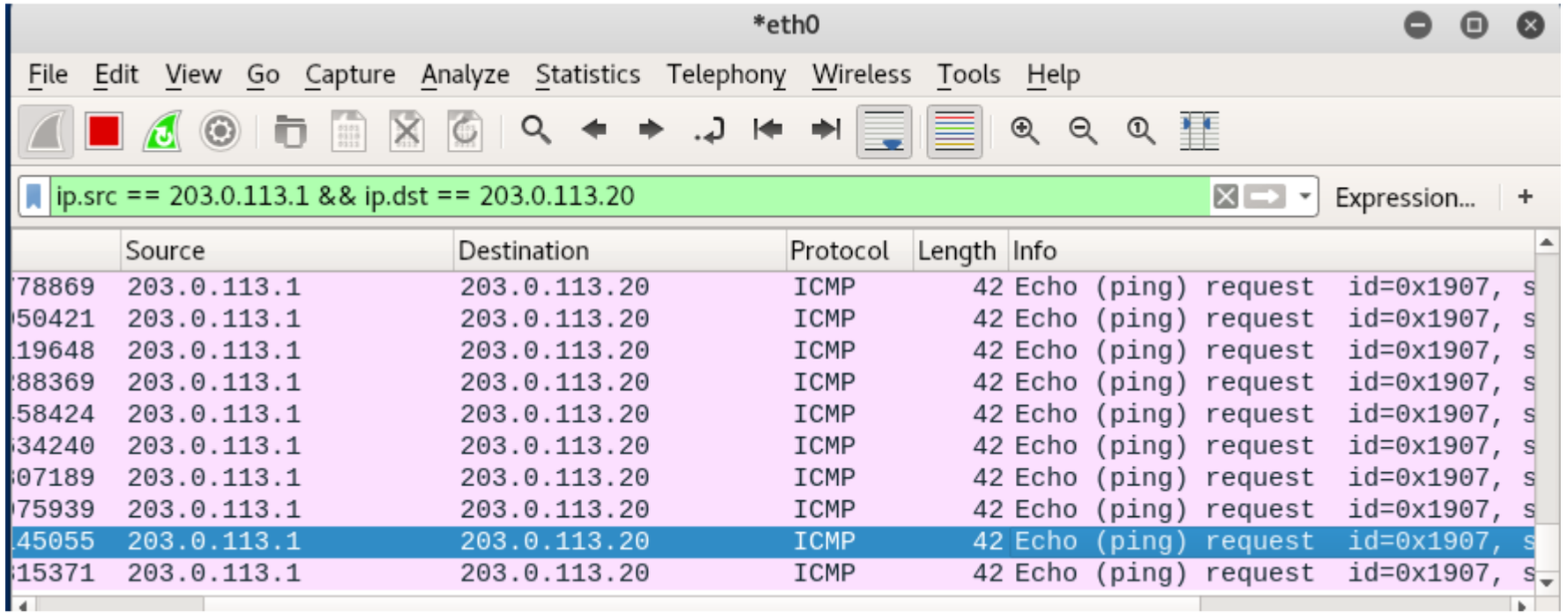
root@kali:~# hping3 --flood –-icmp -p 22 203.0.113.13





Part 3: Launching DoS Attacks-Cont.

Look at Wireshark what type of ICMP messages are you seeing?



Type 8 echo request

i. Press Ctrl-C to stop the flood.

Part 3: Launching DoS Attacks-Cont.

j. Complete the following table for the hping3 options that you used in this lab. Use the hping3 man page or other information resources.

Option	Name	Description
-8	scan mode	scans a range of TCP ports on the target host address provided
-S	set SYN flag	sets the SYN flag in the TCP header of the packets to be sent
-1	ICMP mode	sends ICMP echo request packet(s) unless another type of packet has been specified
-C	icmptype	used to set the ICMP packet type
--flood	N/A	send packets as fast as possible without waiting for replies
-a	spoof hostname	set a fake IP source address
-p	destport	specify destination TCP port
-s	baseport	specify TCP source port, or port at which to start a scan in which the port number is increased for each packet sent
-k	keep	retains the specified source port instead of incrementing it with each packet that is sent.

References

1. Hping3 Usage Example

https://www.kali.org/tools/hping3/

2. What is ICMP? | Internet Control Message Protocol

https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/

3. DDos-attack-tool

https://github.com/topics/ddos-attack-tool

4. What is a denial-of-service attack?

https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/


Questions
?
?
Answers
?