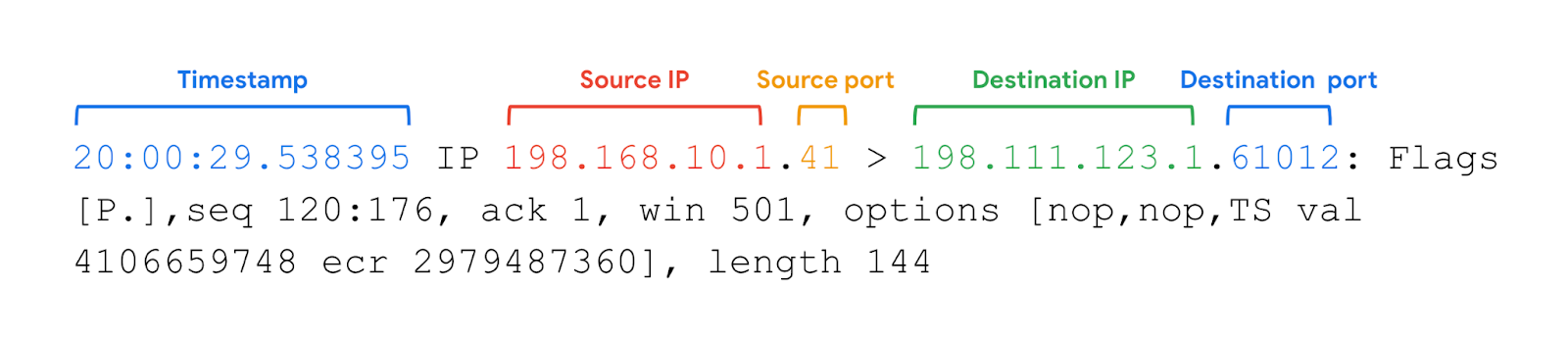
Analyzing network packets using tcpdump

**Tcpdump:** It is a command-line network protocol analyzer that is used to capture network traffic. This traffic can be saved to a packet capture (pcap)

General Syntax: **sudo tcpdump [-i interface] [option(s)] [expression(s)]**



1. Timestamp: The output begins with the timestamp, which starts with hours, minutes, seconds, and fractions of a second.
2. Source IP: The packet’s origin is provided by its source IP address.
3. Source port: This port number is where the packet originated.
4. Destination IP: The destination IP address is where the packet is being transmitted to.
5. Destination port: This port number is where the packet is being transmitted to.

To identify the interfaces in the system we check with **Sudo ifconfig** and determine the interfaces available for tcpdump we use **sudo tcpdump -D**

A computer screen shot of a black screen

Description automatically generated

To inspect network traffic of network interface

* -i eth0: Capture data specifically from the eth0 interface.
* -v: Display detailed packet data.
* -c5: Capture 5 packets of data.

A computer screen shot of a black screen

Description automatically generated

**To capture the data into a file**

**Command : sudo tcpdump -i eth0 -nn -c9 port 80 -w capture.pcap &**

* -i eth0: Capture data from the eth0 interface.
* -nn: Do not attempt to resolve IP addresses or ports to names.This is best practice from a security perspective, as the lookup data may not be valid. It also prevents malicious actors from being alerted to an investigation.
* -c9: Capture 9 packets of data and then exit.
* port 80: Filter only port 80 traffic. This is the default HTTP port.
* -w capture.pcap: Save the captured data to the named file.
* &: This is an instruction to the Bash shell to run the command in the background.

**To generate the HTTP Traffic we use “curl” command:**

**curl opensource.google.com** This is used like this to open a website, it generates some HTTP (TCP port 80) traffic that can be captured.

A screenshot of a computer screen

Description automatically generated