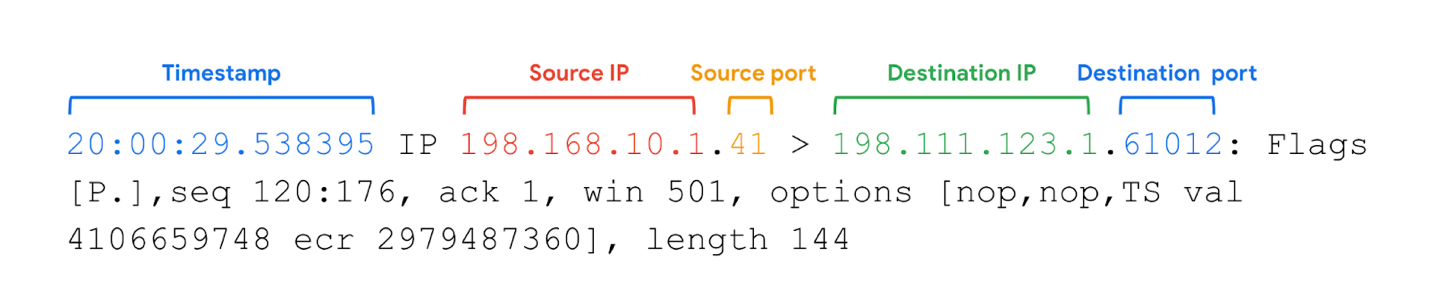
**tcpdump**

**tcpdump** is a command-line network protocol analyzer. It is popular, lightweight–meaning it uses little memory and has a low CPU usage–and uses the open-source libpcap library. tcpdump is text based, meaning all commands in tcpdump are executed in the terminal. It can also be installed on other Unix-based operating systems, such as macOS®. It is preinstalled on many Linux distributions.

tcpdump provides a brief packet analysis and converts key information about network traffic into formats easily read by humans. It prints information about each packet directly into your terminal. tcpdump also displays the source IP address, destination IP addresses, and the port numbers being used in the communications.

**Interpreting output**

tcpdump prints the output of the command as the sniffed packets in the command line, and optionally to a log file, after a command is executed. The output of a packet capture contains many pieces of important information about the network traffic.



Some information you receive from a packet capture includes:

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

**Note:** By default, tcpdump will attempt to resolve host addresses to hostnames. It'll also replace port numbers with commonly associated services that use these ports.

# Read tcpdump logs

A **network protocol analyzer**, sometimes called a packet sniffer or a packet analyzer, is a tool designed to capture and analyze data traffic within a network. They are commonly used as investigative tools to monitor networks and identify suspicious activity. There are a wide variety of network protocol analyzers available, but some of the most common analyzers  include:

* SolarWinds NetFlow Traffic Analyzer
* ManageEngine OpManager
* Azure Network Watcher
* Wireshark
* tcpdump

This reading will focus exclusively on tcpdump, though you can apply what you learn here to many of the other network protocol analyzers you'll use as a cybersecurity analyst to defend against any network intrusions. In an upcoming activity, you’ll review a tcpdump data traffic log and identify a DoS attack to practice these skills.