

# how to read a tcpdump

idk if this is correct but from my research this is what I've figured out

An example TCP dump looks like this:

Timestamp source IP > destination IP.protocol : flags [TCP flags], seq sequence numbers, ack acknowledgement number, win window size, options [TCP options], length payload length : payload

Here's an actual example:

12:14:35.783589 IP ip.your.machine.port > domain.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1

Here's a breakdown of the example:

12:14:35.783589 IP ip.your.machine.24365 > domain.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1

**12:14:35.783589**: The timestamp of when the packet was captured.

**IP**: The protocol of the packet. In this case, it's IP.

**ip.your.machine**: The source IP address.

**> domain.com.http**: The destination IP address and the protocol (HTTP in this case).

**Flags [P.]**: The TCP flags for this packet. "P." stands for PSH (Push) and ACK (Acknowledgment).

**seq 1:74**: The sequence number for this packet. This packet is sending bytes 1 through 74.

**ack 1**: The acknowledgement field. This is the next sequence number that the sender of the ACK is expecting. It's the sequence number plus the segment length received in the last packet.

**win 512**: The window size, indicating the number of bytes that can be received before needing to send an acknowledgment.

**options [nop,nop,TS val 3302576859 ecr 3302576859]**: The TCP options for this packet. It includes two No-Operation (nop) options and a Timestamp (TS) option with value (val) 3302576859 and echo reply (ecr) 3302576859.

**length 73**: The length of the payload (in bytes).

**HTTP: GET / HTTP/1.1**: The payload itself, which is an HTTP GET request in this case.

## TCP Flag codes include:

Flags [S] - SYN: Synchronization sequence numbers to initiate a connection

Flags [F] - FIN: Finish, used to close a connection

Flags [P] - PSH: Push function is utilized

Flags [R] - RST: Reset the connection

Flags [.] - ACK: Acknowledgment

## Options Include:

**nop**: No Operation. It's used for alignment purposes and doesn't carry any information.

**TS val 3302576859**: This is the Timestamp value. It's the value of the sender's timestamp clock when this segment was sent.

**ecr 3302576859**: This is the Echo Reply timestamp. It's the timestamp value that was received in the TSval field of the segment being acknowledged.

---

Revision #4

Created 3 July 2023 08:09:19 by naruzkurai

Updated 3 July 2023 10:29:21 by naruzkurai