Interpret network communications with packets

If a packet capture is like intercepting an envelope in the mail, then packet analysis is like reading the letter inside of the envelope.
Let's discuss how analyzing packets can help us interpret and understand network communications.

As you may know, networks are noisy.
There's an enormous volume of communications happening between devices at any given time.
And because of this, packet captures can contain large amounts of network communications, making analysis challenging and time-consuming.

As a security professional, you'll be working against the clock to protect networks and computer systems from potential attacks.
You may analyze network evidence in the form of packet captures to identify indicators of compromise.
Having the ability to filter network traffic using packet sniffers to gather relevant information is an essential skill to have.
For example, let's say that you were tasked with analyzing a packet capture to find any indication of data exfiltration.
How would you go about this?

Using a network analyzer tool, you can filter the packet capture to sort packets.
This can help you quickly identify an event associated with data exfiltration, like large amounts of data leaving a database.
There are many other filters you can apply to packet captures to find the information you need to support an investigation efficiently.

Examples of network analyzer tools include tcpdump and Wireshark.
tcpdump is accessed through a command line while Wireshark has a graphical user interface, or GUI.
Both tools are useful for security analysts, and soon you'll have the opportunity to explore both.

Before we begin using these tools, let's explore packet fields in detail, specifically, IP headers.
Meet you there.

Revision #1
Created 2023-09-10 06:34:21 UTC by naruzkurai
Updated 2023-11-01 01:10:46 UTC by naruzkurai