Learn more about packet captures

The role of security analysts involves monitoring and analyzing network traffic flows. One way to do this is by generating packet captures and then analyzing the captured traffic to identify unusual activity on a network.

Previously, you explored the fundamentals of networks. Throughout this section, you'll refer to your foundation in networking to better understand network traffic flows. In this reading, you'll learn about the three main aspects of network analysis: packets, network protocol analyzers, and packet captures.

Packets

Previously in the program, you learned that a **data packet** is a basic unit of information that travels from one device to another within a network. Detecting network intrusions begins at the packet level. That's because packets form the basis of information exchange over a network. Each time you perform an activity on the internet—like visiting a website—packets are sent and received between your computer and the website's server. These packets are what help transmit information through a network. For example, when uploading an image to a website, the data gets broken up into multiple packets, which then get routed to the intended destination and reassembled upon delivery.

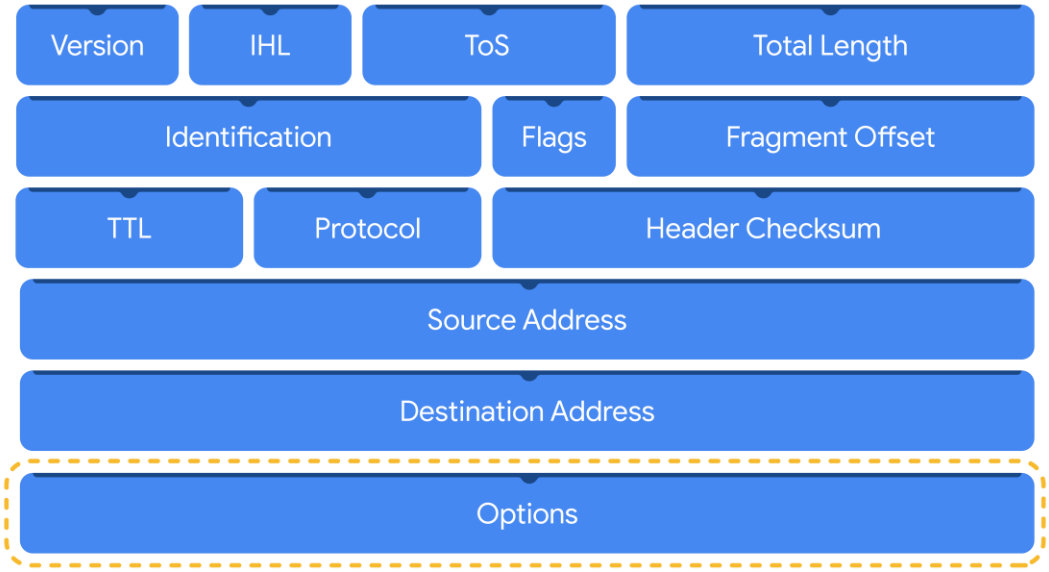
In cybersecurity, packets provide valuable information that helps add context to events during investigations. Understanding the transfer of information through packets will not only help you develop insight on network activity, it will also help you identify abnormalities and better defend networks from attacks.

Packets contain three components: the header, the payload, and the footer. Here's a description of each of these components.

Header

Packets begin with the most essential component: the header. Packets can have several headers depending on the protocols used such as an Ethernet header, an IP header, a TCP header, and more. Headers provide information that's used to route packets to their destination. This includes information about the source and destination IP addresses, packet length, protocol, packet identification numbers, and more.

Here is an IPv4 header with the information it provides:



Payload

The payload component directly follows the header and contains the actual data being delivered. Think back to the example of uploading an image to a website; the payload of this packet would be the image itself.

Footer

The footer, also known as the trailer, is located at the end of a packet. The Ethernet protocol uses footers to provide error-checking information to determine if data has been corrupted. In addition, Ethernet network packets that are analyzed might not display footer information due to network configurations.

Note: Most protocols, such as the Internet Protocol (IP), *do not* use footers.

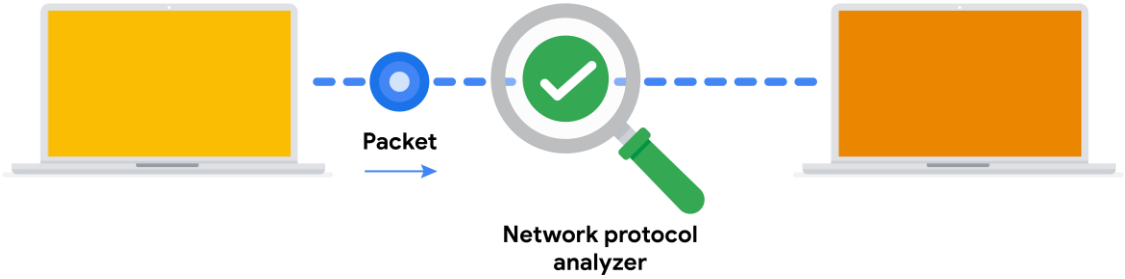
Network protocol analyzers

Network protocol analyzers (packet sniffers) are tools designed to capture and analyze data traffic within a network. Examples of network protocol analyzers include tcpdump, Wireshark, and TShark.

Beyond their use in security as an investigative tool used to monitor networks and identify suspicious activity, network protocol analyzers can be used to collect network statistics, such as bandwidth or speed, and troubleshoot network performance issues, like slowdowns.

Network protocol analyzers can also be used for malicious purposes. For example, malicious actors can use network protocol analyzers to capture packets containing sensitive data, such as account login information.

Here’s a network diagram illustrating how packets get transmitted from a sender to the receiver. A network protocol analyzer is placed in the middle of the communications to capture the data packets that travel over the wire.



How network protocol analyzers work

Network protocol analyzers use both software and hardware capabilities to capture network traffic and display it for security analysts to examine and analyze. Here's how:

1. First, packets must be collected from the network via the **Network Interface Card (NIC)**, which is hardware that connects computers to a network, like a router. NICs receive and transmit network traffic, but by default they only listen to network traffic that's addressed to them. To capture all network traffic that is sent over the network, a NIC must be switched to a mode that has access to all visible network data packets. In wireless interfaces this is often referred to as monitoring mode, and in other systems it may be called promiscuous mode. This mode enables the NIC to have access to all visible network data packets, but it won't help analysts access all packets across a network. A network protocol analyzer must be positioned in an appropriate network segment to access all traffic between different hosts.
2. The network protocol analyzer collects the network traffic in raw binary format. Binary format consists of 0s and 1s and is not as easy for humans to interpret. The network protocol analyzer takes the binary and converts it so that it's displayed in a human-readable format, so analysts can easily read and understand the information.

Capturing packets

Packet sniffing is the practice of capturing and inspecting data packets across a network. A **packet capture (p-cap)** is a file containing data packets intercepted from an interface or network. Packet captures can be viewed and further analyzed using network protocol analyzers. For example, you can filter packet captures to only display information that's most relevant to your investigation, such as packets sent from a specific IP address.

Note: Using network protocol analyzers to intercept and examine private network communications without permission is considered illegal in many places.

P-cap files can come in many formats depending on the packet capture library that's used. Each format has different uses and network tools may use or support specific packet capture file formats by default. You should be familiar with the following libraries and formats:

1. **Libpcap** is a packet capture library designed to be used by Unix-like systems, like Linux and MacOS®. Tools like tcpdump use Libpcap as the default packet capture file format.
2. **WinPcap** is an open-source packet capture library designed for devices running Windows operating systems. It's considered an older file format and isn't predominantly used.
3. **Npcap** is a library designed by the port scanning tool Nmap that is commonly used in Windows operating systems.
4. **PCAPng** is a modern file format that can simultaneously capture packets and store data. Its ability to do both explains the "ng," which stands for "next generation."

Pro tip: Analyzing your home network can be a good way to practice using these tools.

Key takeaways

Network protocol analyzers are helpful investigative tools that provide you with insight into the activity happening on a network. As an analyst, you'll use network protocol analyzer tools to view and analyze packet capture files to better understand network communications and defend against intrusions.

Resources for more information

This Infosec article describes the risks of packet crafting, a technique used to test a network's structure.