These are some common brute forcing tools:

* Aircrack-ng
* Hashcat
* John the Ripper
* Ophcrack
* THC Hydra

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 librarydesigned 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.

Tools for analyzing files:

* [**VirusTotal**](https://www.virustotal.com/gui/home) is a service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content. VirusTotal also offers additional services and tools for enterprise use. This reading focuses on the VirusTotal website, which is available for free and non-commercial use.
* [Jotti's malware scan](https://virusscan.jotti.org/) is a free service that lets you scan suspicious files with several antivirus programs. There are some limitations to the number of files that you can submit.
* [Urlscan.io](https://urlscan.io/) is a free service that scans and analyzes URLs and provides a detailed report summarizing the URL information.
* [MalwareBazaar](https://bazaar.abuse.ch/browse/) is a free repository for malware samples. Malware samples are a great source of threat intelligence that can be used for research purposes.