NCCIC

National Cybersecurity and Communications Integration Center

WAKE UP AND SMELL THE PACKETS

What is Wireshark?

Wireshark is a protocol analyzer. It understands many protocols and supports capturing, sorting, filtering, and analysis of network traffic.

Why Use Wireshark?

Analyzing network traffic with Wireshark can help an administrator find misconfigurations, identify performance issues, and detect malicious communications.

Download and Install

Wireshark is freely available for download at https://wireshark.org

Use Wireshark

Load a Capture File or Capture Live Traffic

- File ➡ Open ➡ Select capture file (.pcap)
- OR: Capture ➡ Options ➡ select Interface
- Click Start

Generate Statistics

- Statistics ➡ Protocol Hierarchy
- Statistics ➡ Conversations
- Statistics ➡ Endpoints

Compare the results to your network diagram. A quick reference of protocols can be found at:

https://wiki.wireshark.org/ProtocolReference

Focus On A Single Conversation

Right-click on a TCP/UDP packet and select:

- Follow TCP/UDP Stream

This opens a window that displays the full conversation and allows export of content in various formats.

Display Filters

Almost any field can be applied as a display filter. To view only conversations involving a specific IP:

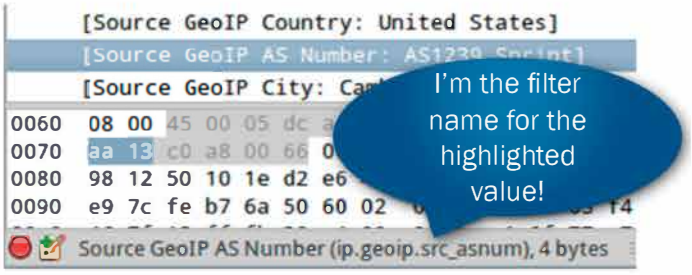
- ip.addr == x.x.x.x

Alternatively, to filter out a specific IP:

- !(ip.addr == x.x.x.x)

To specify a source or destination IP address, use ip.src or ip.dst, respectively, in place of ip.addr.

Filter names are shown in the bottom left corner of the display filter.



Many more display filters are available. For a full listing, see: https://wireshark.org/docs/dfref

For examples of how to use display filters, see:

https://wiki.wireshark.org/DisplayFilters

Custom Columns

Any display filter can be used to create custom columns in the packet list:

- Edit ➡ Preferences ➡ Appearance ➡ Columns
- Click "+"
- For Title, enter a name for the column
- Change the Field type to "Custom"
- For "Field Name," enter the display filter

Time Display Format and Name Resolution

To change the Time column display:

- View ➡ Time Display Format

To toggle Name Resolution of IP addresses:

- View ➡ Name Resolution

Find Strings

Case-insensitive:

- Edit ➡ Find Packet ➡ String

Case-sensitive:

- Display Filter: "frame contains _____"

Automate File Extraction

To extract files from the packet capture:

- File ➡ Export Objects ➡ HTTP
- Select files and click Save As

ASN Lookup and IP Address Geolocation

Free BGP Autonomous System Number (ASN) ownership and IP geolocation lookups are available through databases downloaded from MaxMind. To automate updates to the databases, install geoipupdate (Mac OS X), geoip-bin (Ubuntu), or manually pull the "Binary/gzip" version from:

https://dev.maxmind.com/geoip/legacy/geolite

Configure Wireshark to use MaxMind data:

- Edit ➡ Preferences ➡ Name Resolution
- GeoIP database directories ➡ Edit
- Click "+"
- Enter path to directory of MaxMind .dat files

More details at:
https://wiki.wireshark.org/HowToUseGeoIP

Limitations Of And Complements To Wireshark

Wireshark is not an Intrusion Detection System (IDS) and does not handle large volumes of traffic well. Also, full packet capture (PCAP) can be done more efficiently from the command line using tools such as **Tshark** or **tcpdump**.

If you need to merge or divide PCAP files that are too large to be opened in Wireshark, try command line tools **editcap**, **mergecap**, or **tcpslice**. If the storage/processing requirements are too great for full PCAP analysis, consider a free platform such as **Bro** (https://www.bro.org) to collect network metadata. Bro logs can be easily pushed into a Security Information and Event Management **(SIEM)** tool such as Splunk or an ELK stack (ElasticSearch, LogStash, Kibana) for long-term correlation and analysis. Free threat intelligence feeds for Bro are at: https://intel.criticalstack.com.

Snort (https://snort.org) and **Suricata** (https://suricata-ids.org) are also free IDS/IPSs; the SecurityOnion (https://securityonion.net) Linux distribution includes these and many other tools for network security monitoring. DigitalBond's Quickdraw SCADA Snort signatures are available at: https://www.digitalbond.com/tools/quickdraw.

Incident Response

If you believe your ICS/SCADA network is compromised, please contact the NCCIC Hunt and Incident Response Team (HIRT).

To report a Cyber Incident, email the (24x7) Service Desk at NCCICCustomerService@us-cert.gov.

About NCCIC

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

http://www.dhs.gov/national-cybersecurity-communications-integration-center