How to Wireshark

```
Who am I?
https://www.linkedin.com/in/propatriavigilans/
https://raymondrizzo.com
```

Download Wireshark

https://www.wireshark.org/download.html

The download will recommend the right edition and platform for you, but you can choose whatever edition you prefer or need for a different platform.

Documentation

Documentation is available at the same location.

There will also be an offline copy installed with Wireshark.

Integrity Checking

Press `Ctrl+j` to see your downloads, go to the containing folder, right click, and scan the file for viruses. (Windows 11 users may need to click `Show more options` first).

ALWAYS Scan downloaded files with your local anti-malware program, even if you trust them.

Do not assume that a scanned file is safe

Check the signatures file, in the Verify Downloads section of the previous website. Copy the SHA256 SUM from the version that you downloaded, and paste it into a txt document.

In the location bar above the explorer file area, type `powershell` and hit enter. When PowerShell is loaded, run the following commandlet:

```
PS C:\Users\[User-Name]\Downloads> Get-FileHash .\Wireshark-[Whichever-version-you-downloaded]
```

You can use `tab` to complete the filename once you've typed enough characters to make it distinct enough.

Compare the hash here to the one that you previously noted.

Installation

Do not install this on a production server without having a maintenance window scheduled. You could be required to reboot!

1. Run the downloaded installer.
2. Verify that the `Verified Publisher` in your UAC warning is `Sysdig, Inc.`.

3. Press `Yes` to continue if correct.
4. Click `Next`.
5. I suggest reading the licensing information before clicking `Noted`, as the GPL has given us some great things.
6. The only component that I feel is optional here is TShark. Feel free to deselect it if you will never be using the terminal to capture traffic on this machine, then click `Next`.
7. Your preference for shortcut locations and file associations (I highly suggest leaving the defaults), then click `Next`.
8. Your preference for a destination folder, then click `Next`.
9. If you are only viewing captures, you don't need to install Npcap. Odds are you will be capturing traffic, so leave it default and click `Next`.
10. It goes way beyond this topic. Short story is that you don't need USBPcap. Click `Next`.
11. Unless you're planning on doing wireless troubleshooting (better you than me) or have a security policy that restricts who can capture packets, click through the remainder and accept the defaults.

Capture Devices

You will see every connected interface that is available on your PC, but not all of them will be in use.

If you are unsure of the correct adapter to use, you can get an overview of the network traffic in the graph to the right of the interface name.

If you select an interface with no traffic, you will be notified that nothing was captured upon stopping and will be able to select a new interface.

If you received data but still selected the wrong interface, you will need to click File > Close to be able to select a different interface.

Time Display

When working with people from other time zones, you will want to both be working with UTC Time of Day, or notify each other of the time offset. This will keep you in sync.

- View > Time Display Format
  - Date and Time of Day (`Ctrl+Shift+1`)
  - UTC Date and Time of Day (`Ctrl+Shift+8`)

By default you are going to be using "Date and Time of Day".

You may also shift the time displayed locally to adjust for your local time difference.

If a packet was captured at 8:00am on the East Coast, a PC on the West Coast would show the same packet as arriving at 5:00am. To shift the packet time:

- Edit > Time Shift (`Ctrl+Shift+T`)
- Add/Remove time
  - Central = -1:00:00 > `Apply`
  - *Time shifts are cumulative.*
  - Central = -1:00:00 > `Apply` x3 or -3:00:00 > `Apply`

Be sure to undo all shifts before closing this window.

Filters

Capture filters

Capture filters and display filters are frustratingly different in Wireshark. But it is good to have at least a base understanding of capture filters, as this is going to be your primary tool for reducing the amount of traffic that you're going to collect.

The most common capture filters that you will use are host, network, transport protocol (with or without specifying a port range).

- host 192.168.0.1
- net 192.168.0.0/24
- udp
- udp portrange 6000-7000 || udp port 5060

Display Filters

The most common display filters that you will use are protocol, source/destination, and port based.

- sip || rtp
- rtp.ssrc == 2143629653
- ip.src == xxx.xxx.xxx.xxx
- ip.dst == xxx.xxx.xxx.xxx
- ip.addr == xxx.xxx.xxx.xxx

Saving Filtered Data

Once you've identified the important information and filtered on it, you can export only that information. If you're not sure of what is important, just make sure that you're using a ring buffer to keep your files sizes small.

- File > Export Specified Packets

Ring Buffers

You're probably going to be emailing these files to someone, but even if you aren't, you don't want to be opening large files on (typically under-powered) company laptops. Ring buffers will create X amount of files at a certain file size, and overwrite them in a cyclical manner to keep overall disk use down.

Considering this, you probably want to write to non solid state media.

Before starting a capture to a ring buffer, start a standard capture and verify that you're seeing the traffic that you are expecting. If you do not see what you want, you are probably on the wrong VLAN, port, or using the wrong capture interface.

- Capture > Options (`Ctrl+K`)
    - Input Tab
        - Select the capture device that you've previously identified
    - Output Tab

        - These days, you can probably keep the default setting of pcapng. If someone didn't update their software in the last five-ish years, it's on them...
        - Browse to a location to save the files, and enter a good name.
        - I prefer the following format [Customer-Name]_[Issue-Description].pcapng
    - Select "Create a new file automatically..."
    - Select the second checkbox, and set the value to 10 megabytes
    - Select "Use a ring buffer" and set the value to the amount of space you are able to use on the local disk (in MB) divided by 10.
        - You want to ensure that this selected amount of files will be enough to not overwrite potentially valuable data, but not take up all of your remaining disk space.
    - Click Start to begin the capture, and wait for some good data.

Everyone has their own naming convention, even if it's just the default, but I'm going on record for the following Recommendation: **[Customer-Name]_[Issue-Description]_[File-Number]_*[Date-Time]*.pcapng**

Once the problem has been identified, you can stop the capture and open the associated capture file that relates to the timeframe, [Date-Time], when the issue occurred.

For context, you may need to combine the previous or next capture in sequence by merging the files.

Merge Files

1. Open first .pcap or .pcapng file.
2. File > Merge

- Select file to merge.

The default setting of "Merge packets chronologically" interleaves the packets where it is easier (most logical) to read them.

Call Flows

- Telephony > VoIP Calls > Select Call
- Flow Sequence: Displays a cradle-to-grave view of all events in the call.
- Prepare Filter: Filters view to only show relevant SIP and RTP packets for a specific call.
- Play Streams: Listen to both (hopefully) audio streams.

SIP

Before we start, here is a brief example of a best-case SIP call flow. Your milage may vary, as you may see Delayed Offer messages when dealing with different SIP clients.

Direction	Message	Description
->	INVITE SDP	Initial call setup from initiating device
<-	100 Trying	SIP Server call progress response
<-	180 Session Progress SDP	The remote client has been contacted and has provided SDP information

Direction	Message	Description
<-	200 OK SDP	The remote client as acknowledged the initial invite
->	ACK	The local client has acknowledged the SDP information and the call is initiated
<-	RTP	
->	RTP	
->	Bye	The local client terminates the call
<-	200 OK	The remote client has acknowledged the call termination

- *Telephony > SIP Flows*
    - This will generally provide you the same information that you can find in VoIP calls.
- *Telephony > SIP Statistics*
    - This will provide you a count of each SIP message that was found in your capture, along with call setup times.

You generally want to make sure you are seeing very few 4xx, 5xx, and some 6xx messages, as they are indicators of call processing problems.

RTP

RTP Packets can be combined based on the Synchronization Source Identifier.

Synchronization source (SSRC): This 32-bit number uniquely identifies each RTP stream.

Wireshark Filter: rtp.ssrc == 0x7fc53155

Your filter can be the *hexadecimal* or *decimal value*

- Telephony > RTP > RTP Stream Analysis:
    - The two most important columns are Delta and Jitter:
    - Delta: This is the measurement of the time (in milliseconds) between the current and previous packets in the individual RTP stream, which includes the size of the payload of the CODEC.
    - Jitter: Variation of the timing between packets.
    - Max Jitter: This is what you want to keep an eye out for. Your devices should have a Jitter Buffer that will be able to accommodate for the maximum jitter that you experience in transmission, while not being too large as to cause a noticeable delay.
    - Lost: Some codecs handle packet loss better than others. Research Forward Error Correction (FEC) for more information.

Maximum Latency Recommendations

- One Way Latency: 150ms
- Round Trip Latency: 300ms
- Jitter: Less than 30ms (you may need to manually specify a jitter buffer).

- Packet Loss: Less than 1% (based on g711).

Less is always better.