Advanced Filters

Wireshark Filters

» **What is a filter?**

- Used to limit what appears in the Packets List pane

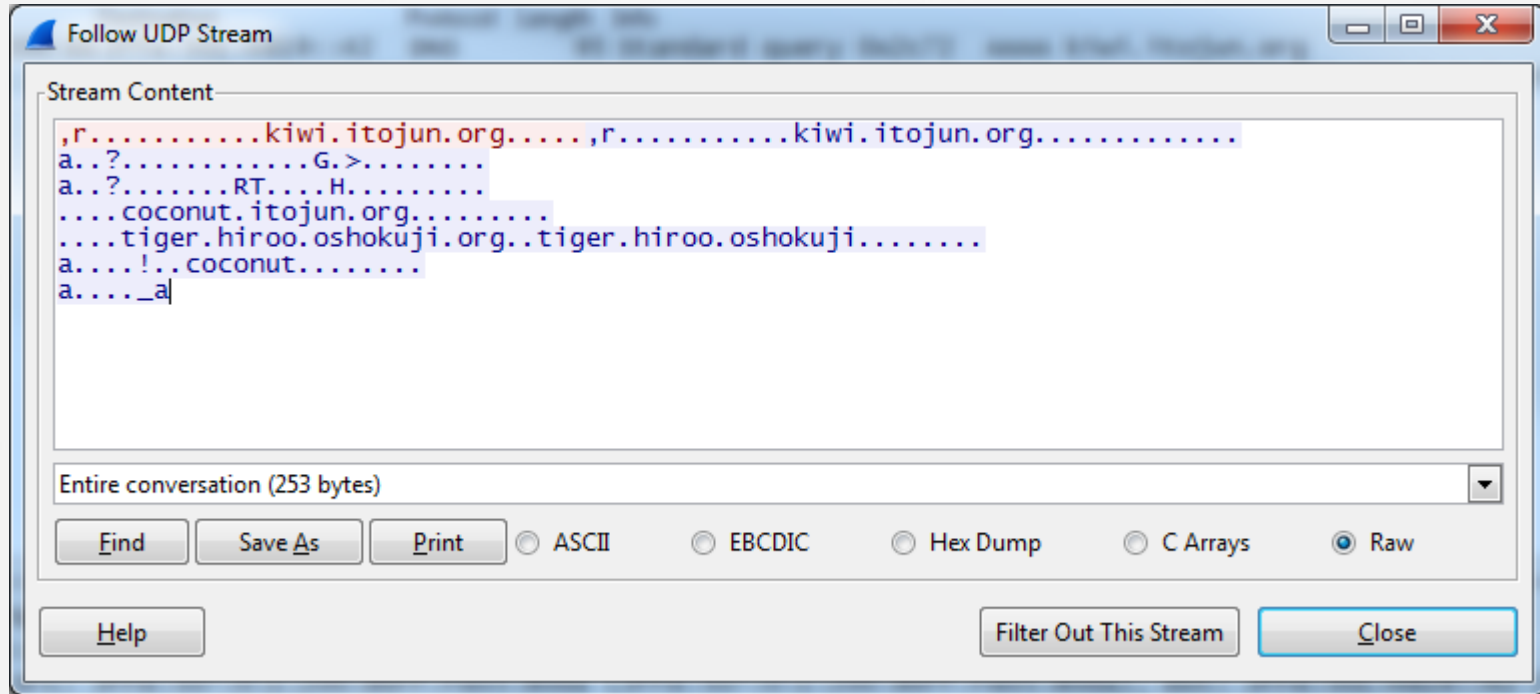» **Wireshark filters are used to**

- Aid in troubleshooting efforts
- Refine the view
- Assist with only collecting only what you need
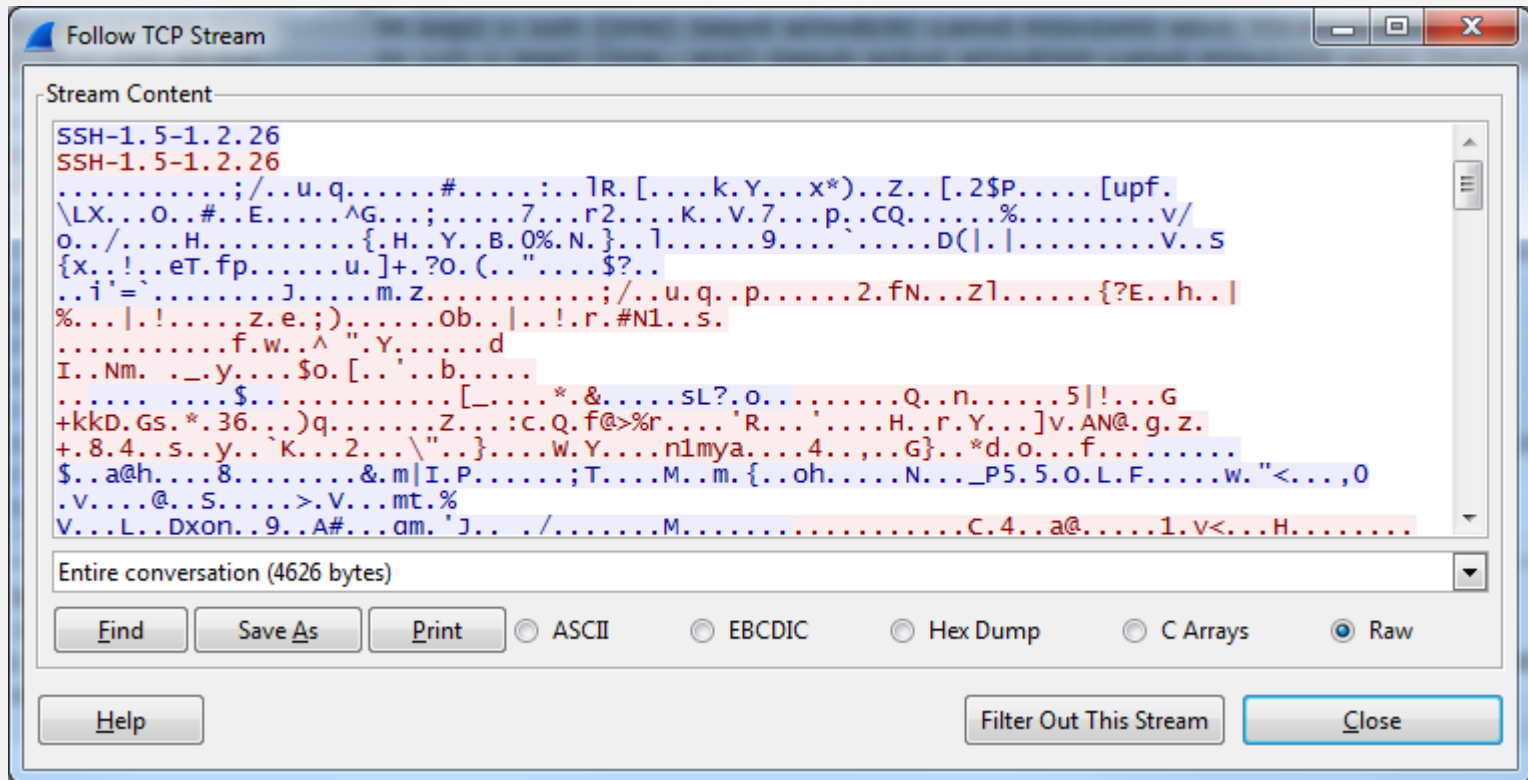
Wireshark Advanced Filters

» **Filter types**

- Capture and display
- Streams (TCP and UDP)
- Macros
- Conversation filters
- Others

Configuring an Advanced Filter

Configuring a Capture Filter

Wireshark Filters

» **Troubleshooting with filters**

- Streamline viewable traffic to find exactly what you need

- Remove anything that could cause confusion

- Give the analyst a clearer view of the root cause data

Questions?