# Step-By-Step Instructions

Follow the instructions and fill in the sections to complete the activity.

### Step 1: Access  the template

To use the template for this course item, click the following link and select *Use Template*.

Access the template (Diagram template)

### Step 2: Conduct online research

To begin, conduct online research to learn more about tcpdump and Wireshark. You can begin by using the official Wireshark documentation and tcpdump documentation:

- tcpdump - Resources and documentation
- Wireshark - Official user guide

You can also perform an internet search to find resources that explain how these tools work. Try searching for information using these terms:

- *Wireshark features and functionalities*
- *tcpdump features and functionalities*
- *comparison between tcpdump and Wireshark*

Be sure to critically evaluate the search results and select reliable and authoritative sources such as official documentation, reputable cybersecurity websites, or technical forums that provide accurate and factual information about the tools.
Explore these resources to gather information on tcpdump and Wireshark and focus on understanding the different features and functionalities that each tool has.

Consider these questions to help you compare the two tools:

- What software or equipment is required to access and use the tool? Is the tool open-source or proprietary?
- What type of user interface or layout does the tool use?
- How do security analysts typically use the tool? What are the recommended usage scenarios for each tool?
- How does the tool handle capturing, analyzing, and filtering network traffic?
- Are there any limitations or considerations for using this tool?

### Step 3: Fill in the diagram

After you've completed your research on Wireshark and tcpdump, fill out the template and include at least two features for each tool. These could be related to the tool's capabilities, the type of analysis they perform, contrasting features, user interfaces, usage scenarios, and any other notable distinctions. Then, include three similarities between tcpdump and Wireshark.

## What to Include in Your Response

Be sure to address the following elements in your completed activity:

- At least 2 differences between Wireshark and tcpdump
- At least 3 similarities between Wireshark and tcpdump