# Overview

Install Wireshark and familiarize you with its operation.

# Process

The modules needed for install will be available via on the hades domain as part of the normal install/update/configure process.

On the hades.lab web server (lab302-web.hades.lab or lab302-repo.hades.lab {172.16.1.250 or 172.16.1.251}) you will find Wireshark information in the *wireshark* directory. There are two identical content manuals: one is a single giant web page, the other is in chunks (one subject matter at a time with the “next” and “back” buttons.

## Part 1: Install Wireshark

Install Wireshark from a root terminal using apt

1. Start the root terminal
2. Run the following command:
   1. apt-get install wireshark
3. Answer the default questions

\*\* Document the install from the terminal

## Part 2: Start Wireshark

It is your job to figure out how to start Wireshark.

Suggestions:

* Start it from a Terminal
* Start it from a Root Terminal
* Start it from Applications 🡪 Internet area

\*\* Comment on the differences and how they work differently

Figure out how to monitor network traffic in and out of your VM

Hints:

* You need to monitor an interface

\*\* Comment on using an interface

Start some network interactions while monitoring with Wireshark

Try:

* Use a Web Browser
* \*\* Ping
* Try a secure login:
  + ssh *userid*@*machineID*
    - Secure log on to the base work station
    - Use man to get the syntax
  + Try some commands and note they are being done on the base workstation
  + Log out of the ssh session
* Copy a small text file from your VM to the base workstation
  + Background:
    - rcp does a remote copy, scp does a secure remote copy
    - Use man to find the syntax to use them
  + Compare doing a remote copy (rcp) of a text file vs. a secure copy (scp)
    - Copy a small text file and monitor the data transmission with Wireshark.
      * Try the copy with rcp and monitor with Wireshark
        + Use man for the syntax
      * Next try a secure copy using scp:
        + copy the same small text file used for rcp
        + use *man* to figure out how scp can copy between your VM and the base workstation
      * \*\* Comment on how the system “helps” you.
    - Fix rcp
      * apt-get install rsh-client
      * update-alternatives
    - Do the copy again with rcp
      * \*\* Compare to the scp copy
  + Optional:
    - Try a copy from the base workstation to your VM

\*\* Show Wireshark data from the ping, rcp (fixed) and scp. Use a filter to isolate each item. Comment on and show that scp encrypts the test data. Explain what happened when you tried to use rcp the first time.

## Part 3: Capture interactions

### HTTP

With a fresh restart of Wireshark:

1. Open a browser
2. Browse lab302-web.hades.lab (172.16.1.250)
3. Use the filters to find:
   1. the original request (GET)
   2. the response (200 OK) with the data for the page
   3. Include screenshots of the above data

\*\* Clearly show the data for the GET and the 200 OK and data Response

### ARP and DHCP

With Wireshark running

1. Make sure DHCP is enabled on your VM
2. Set up filters for ARP and DHCP \*\*
3. Disconnect and reconnect your workstation from the network
4. Document the ARP and DHCP connection conversation \*\*
   1. Document only the relevant ARP and DHCP data

# Deliverable:

A report with

* A cover page
* An overview
* The items marked with \*\* above
* A summary