

Lab Assignment



Copyright © 1996-2020 HackerU Ltd.
All Rights Reserved.

Cybersecurity Professional Program
Computer Networking

Network Fundamentals

NET-02-L1
Network Examination
with Wireshark

Lab Objective

The objective of this lab is to learn how to use Wireshark and how computers encapsulate and send data.

Lab Mission

The mission of this lab is to capture various types of network traffic, and analyze the data.

Lab Duration

30-60 minutes

Requirements

- Knowledge of the TCP/IP model and data encapsulation.
- Knowledge of basic Wireshark filters.

Resources

- Environment & Tools
 - Windows 10 VM
 - Web browser
 - Internet connection
- Extra Lab Files
 - Wireshark is 4.0.3.exe

Lab Task 1: OSI & TCP/IP

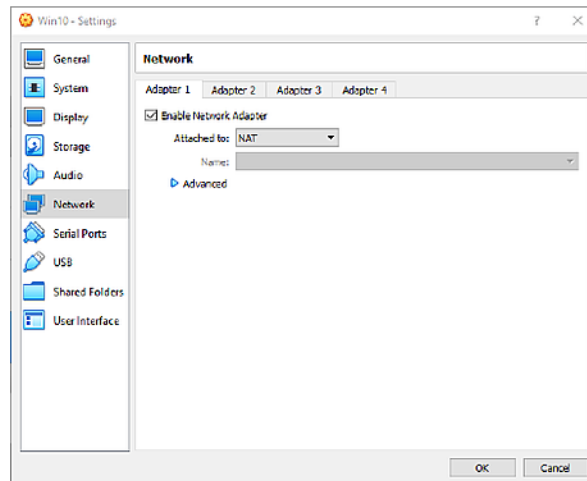
This task will review OSI & TCP/IP information previously learned.

- 1** What is the primary role of the Transport Layer and which are the two most common corresponding protocols?
- 2** In which layer of the OSI model do protocols like DNS, HTTP, and SSH operate?
- 3** In which layer of OSI and TCP/IP models are source and destination logical addresses added to the packet?
- 4** In which layer of OSI and TCP/IP are source and destination physical addresses added to the frame?
- 5** What does UDP do with corrupted or out-of-order packets?

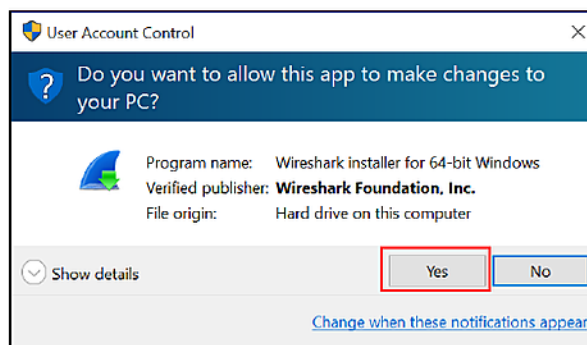
Lab Task 2:Wireshark Installation

In this task, we will install Wireshark.

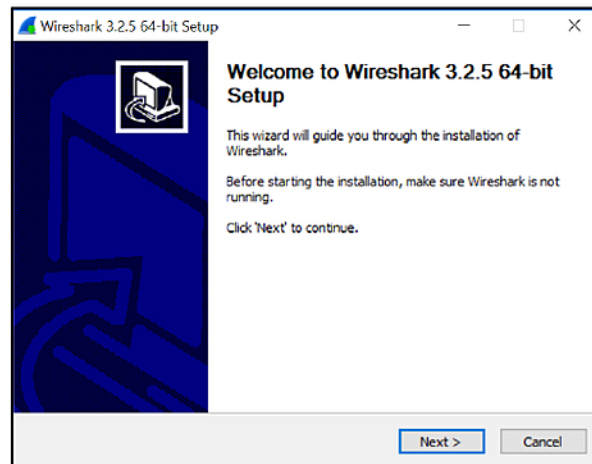
- 1 Before you start, make sure your Windows 10 virtual machine's NIC is configured to NAT.



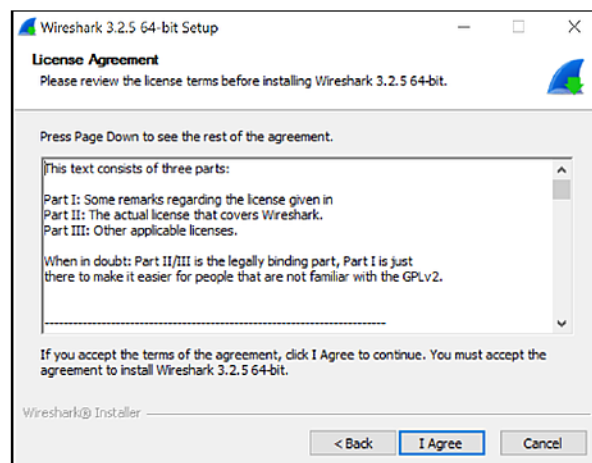
- 2 Use the provided Wireshark installation file to install the software. Double-click the file to start the installation.
- 3 If a message regarding "User Account Control" appears, click "Yes".



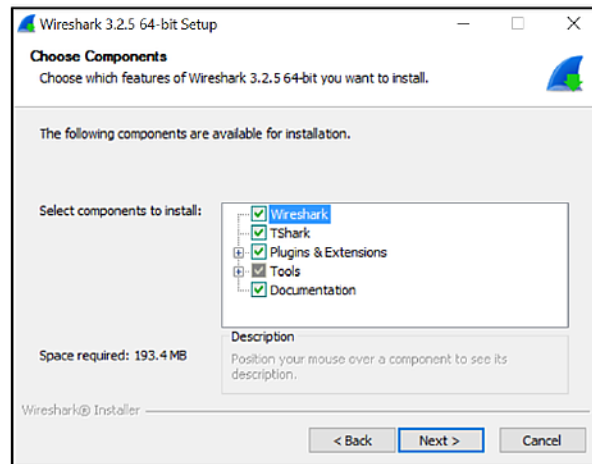
- 4 Click Next in the first setup page to begin.



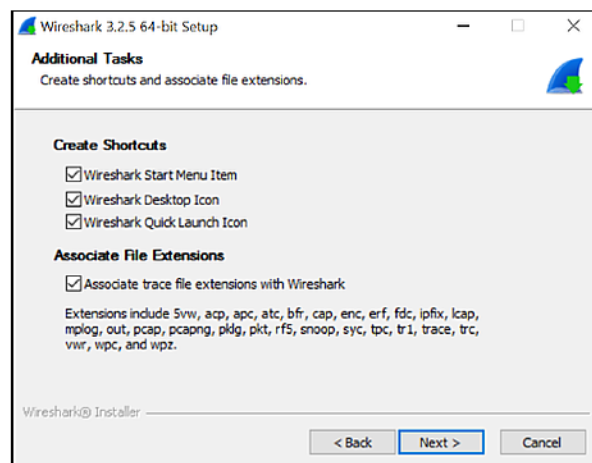
- 5 In the next page, click "I Agree", for the license agreement.



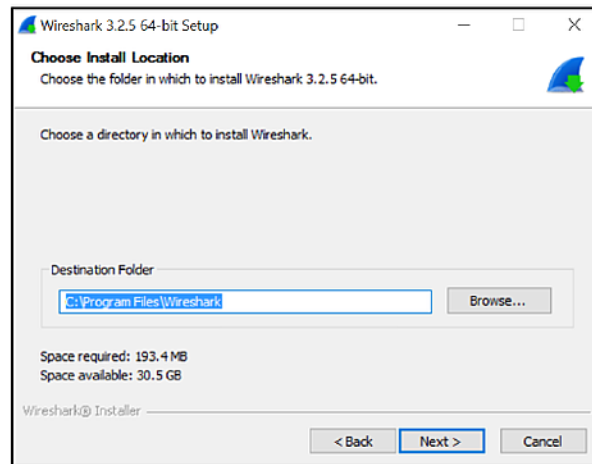
- 6 In the next page, make sure all the components are selected, and click “Next”.



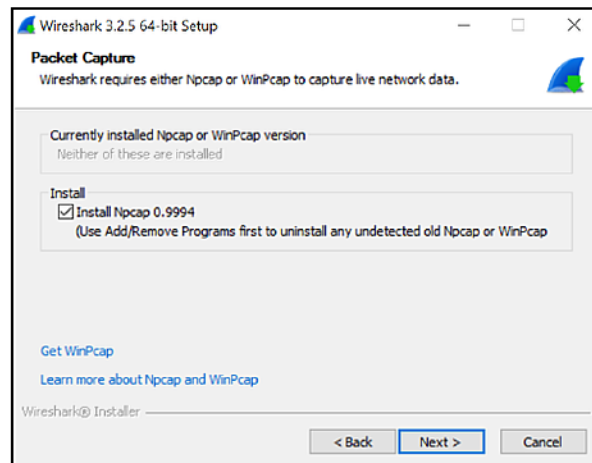
- 7 In the next page, make sure all the options are selected, and click “Next”.



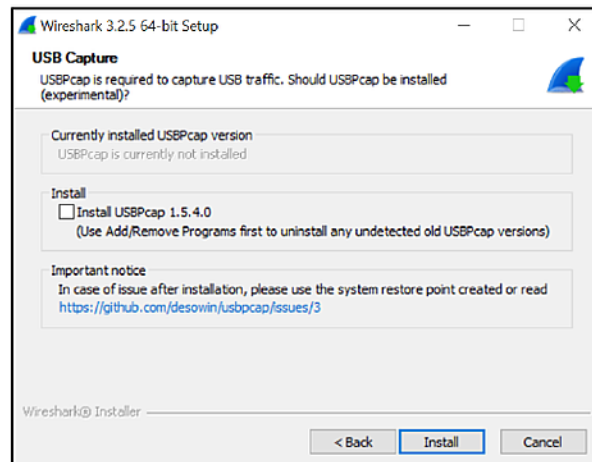
- 8 In the next page, select the installation destination folder, and click “Next”.



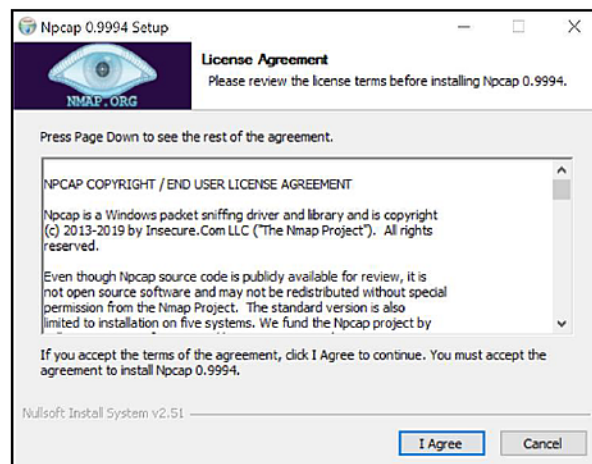
- 9 In the next page, make sure “Install Npcap 0.9994” is selected, and click “Next”.



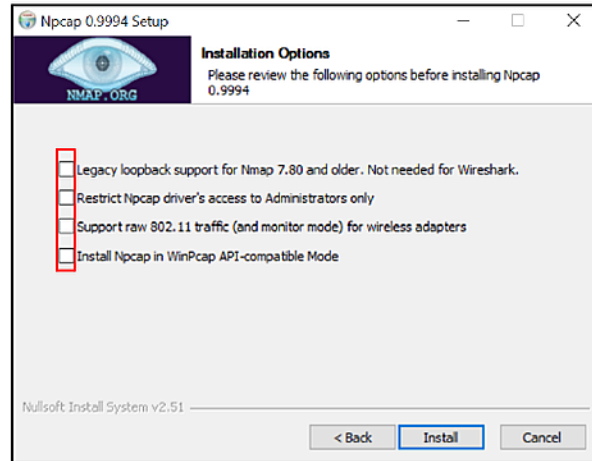
- 10** In the next page, click “Install” without changing anything. The installation will begin.



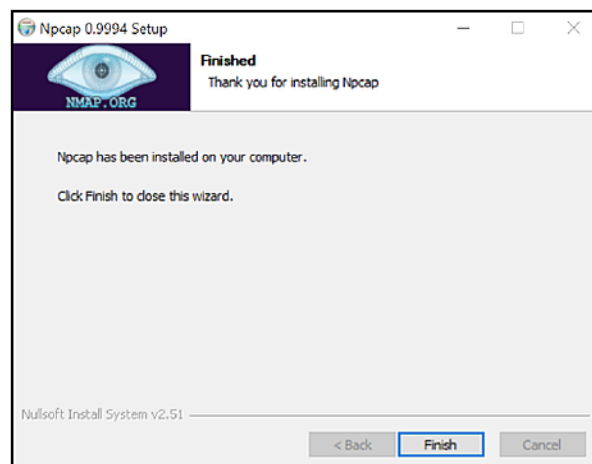
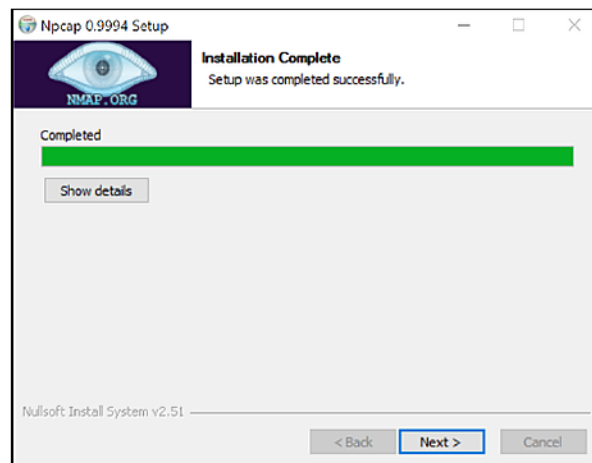
- 11** When the installation process ends, click “I Agree” for the Npcap setup license agreement.



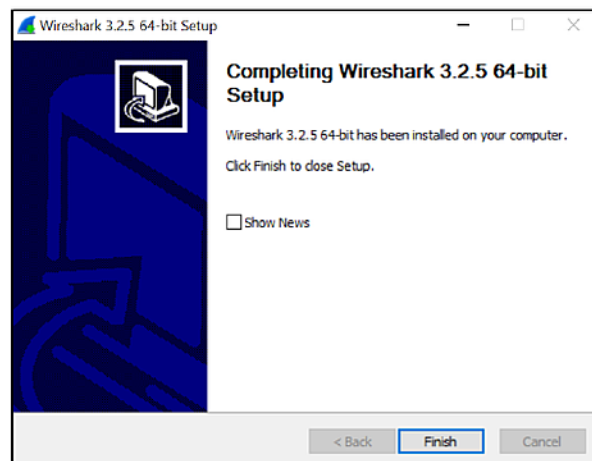
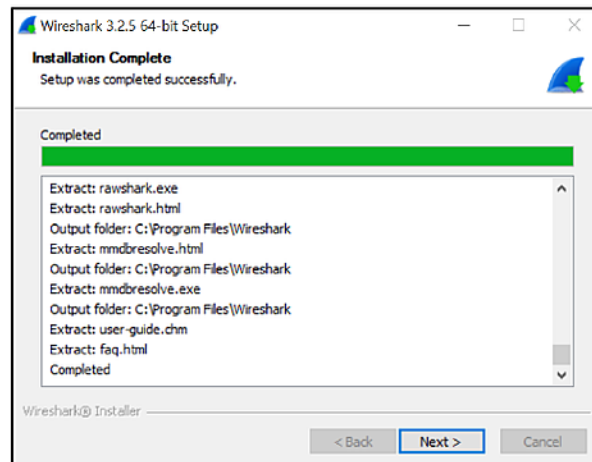
12 In the next page, leave all the options unselected and click “Install”.



13 When the installation ends, click “Next”, and in the next window, click “Finish”.
The Wireshark installation process will continue.



- 14 When the installation ends, click “Next”, and in the next window, click “Finish” without selecting “Show News”.

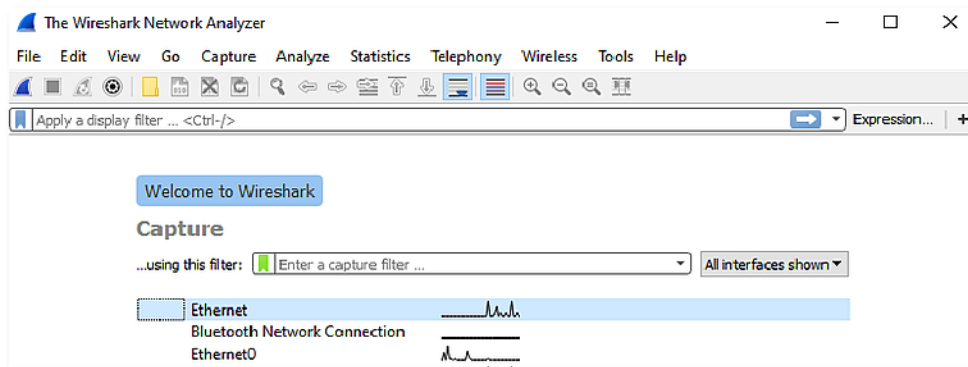


Lab Task 3: Use Wireshark to Examine Live Network Traffic

In this task, we will install Wireshark and become familiar with the interface.

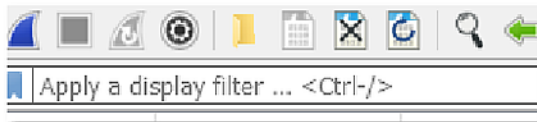
Part 1 – Learn about the Wireshark Dashboard

- 1 Choose the network adapter in use, and who you want to view data on.
The graph shows which interface is active.





2 Dashboard View:

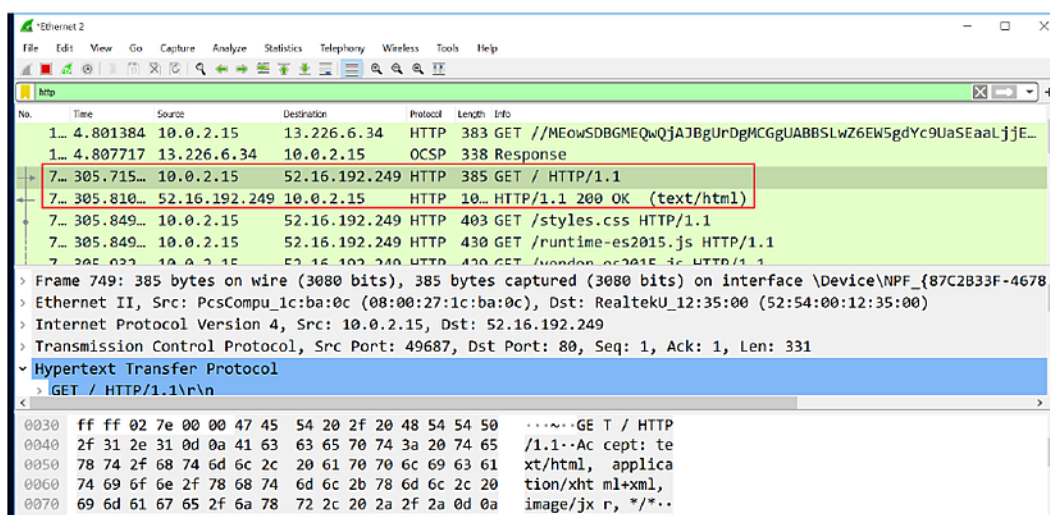
- a) The top screen or bar contains the program's tools, such as preferences, settings, and the search bar.



- b) The windows in the middle show the live network traffic on the network card (adapter). Data is presented as frames.
- c) The screen at the bottom displays information for a selected frame.

Part 2 – Examine Live Network Traffic



- 3 Start capturing the network by clicking the Wireshark icon .
- 4 Open a web browser (recommended: Edge or Firefox).
- 5 Browse to <http://juice-shop.herokuapp.com/#/> and immediately after the web page is loaded, click the stop button .
- 6 Take a closer look at a client requesting a web page from a server. Use the search bar to display only the HTTP packets.



- 7 Click the GET HTTP packet sent from the local PC to the server.
- 8 Click each header to view the encapsulated data (logical ports, IP, and MAC address).
- 9 Document the following details:
 - a) What are the logical port source and destination?
 - b) What are the logical source and destination addresses?
 - c) What are the physical source and destination addresses?

Lab Task 4: Capture Network Traffic to a File and Analyze it

In this task, we will capture packet data and save it to our disk. We will then open the saved file and look for specific data using filters.

- 1 Click the Wireshark icon  to start capturing.
- 2 Open the CMD and send a ping to 8.8.8.8
- 3 Browse to <http://hack-yourself-first.com/>
- 4 Stop capturing using the stop button .
- 5 Click File and then Save as. Name the file **capture1** and save it in the Desktop folder.
- 6 Close Wireshark.
- 7 Double-click capture1.pcap to open the file.
- 8 Using the appropriate display filter, display only the DNS packets.
Note: if you fail to find the query, flush the DNS cache with the command **ipconfig /flushdns** and repeat steps 3-8.
- 9 Document the following details:
 - a) Which Layer 4 protocol is used to encapsulate the Layer 4 header.
 - b) What are the source and destination logical ports?
 - c) What is the default DNS server configured on your machine, according to the Layer 3 header?
- 10 Which filter will display all packets sent to port 53?
- 11 Using the appropriate display filter, display only the Ping packets.
- 12 Document the following details:
 - a) How many requests and replays are shown?
 - b) Why doesn't ICMP have a logical port number listed in the packet capture?
- 13 Which filter will display all packets sent to the 8.8.8.8 host?