

Lab Assignment & Solution



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

Cybersecurity Professional Program
Computer Networking

Network Fundamentals

NET-02-LS1
Network Examination
with Wireshark

Note: Solutions for the instructor are shown inside the green box.



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?

The transport layer handles the coordination of data transfer between two network hosts: TCP and UDP.

- 2 In which layer of the OSI model do protocols like DNS, HTTP, and SSH operate?

Application Layer (7).

- 3 In which layer of OSI and TCP/IP models are source and destination logical addresses added to the packet?

OSI - Network Layer (3), TCP/IP - Internet Layer (3).

- 4 In which layer of OSI and TCP/IP are source and destination physical addresses added to the frame?

OSI - Data Link Layer (2), TCP/IP - Network Access (1).

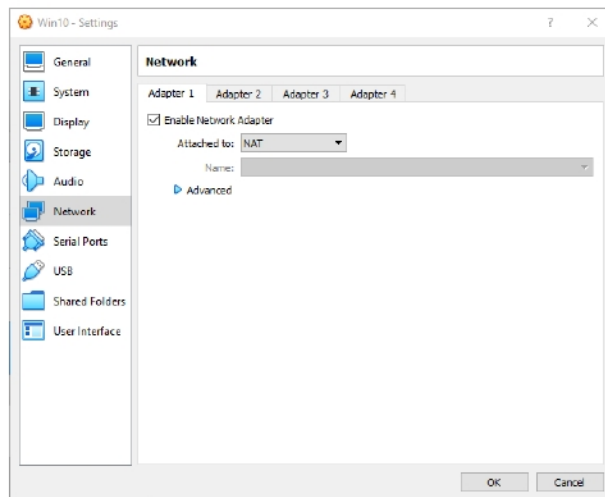
- 5 What does UDP do with corrupted or out-of-order packets?

Nothing, the destination discards corrupted packets.

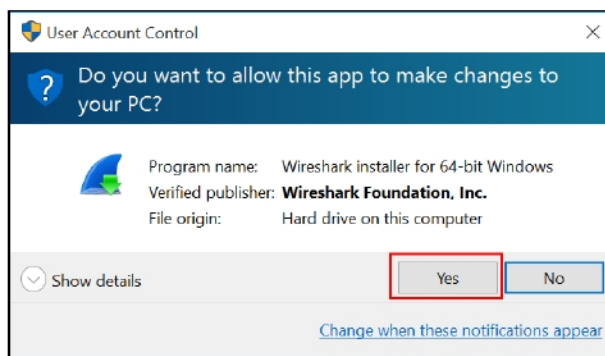
Lab Task 2: Wireshark Installation

In this task, we will install Wireshark.

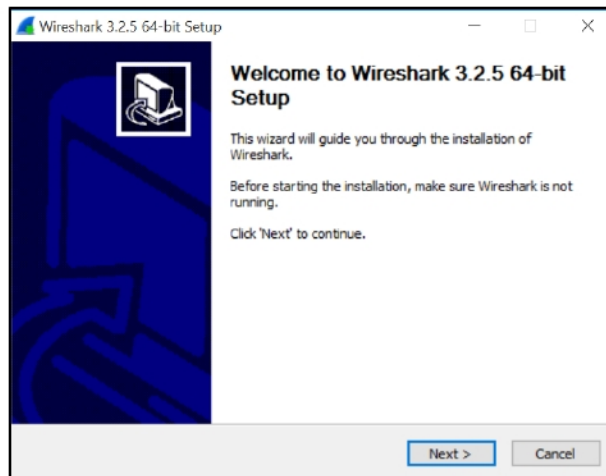
- 1 Before you start, make sure your Windows 10 virtual machine's NIC is configured to NAT.



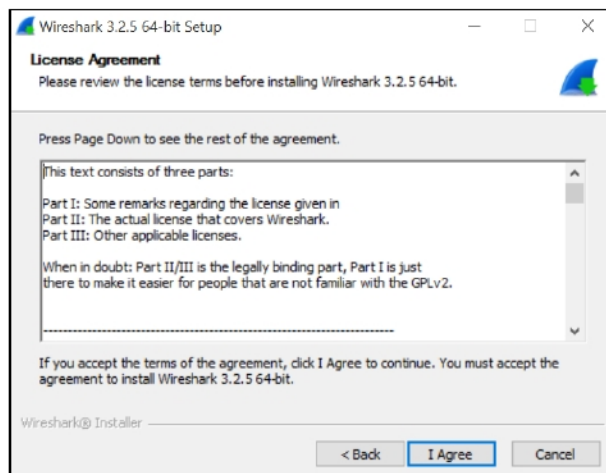
- 2 Use the provided Wireshark installation file to install the software. Double-click the file to start the installation.
- 3 If a message regarding “User Account Control” appears, click “Yes”.



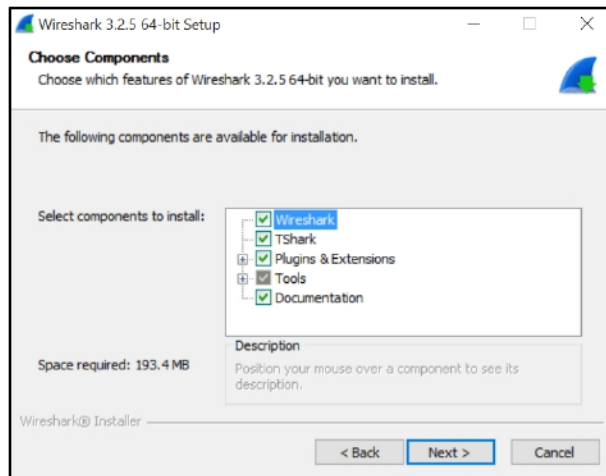
- 4 Click Next in the first setup page to begin.



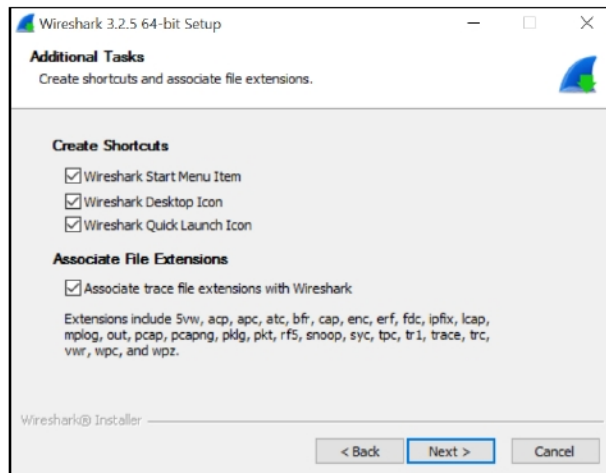
- 5 In the next page, click "I Agree", for the license agreement.



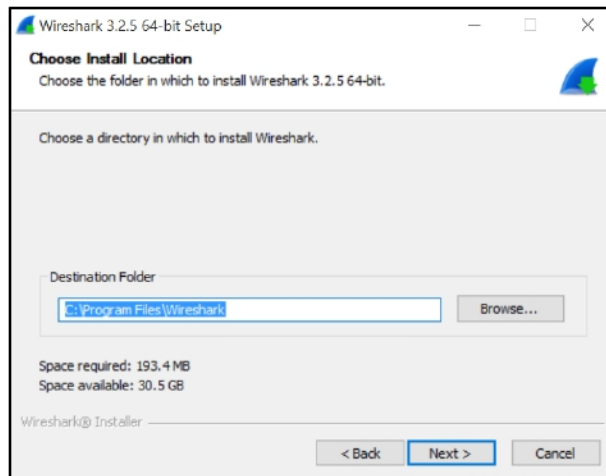
- 6 In the next page, make sure all the components are selected, and click “Next”.



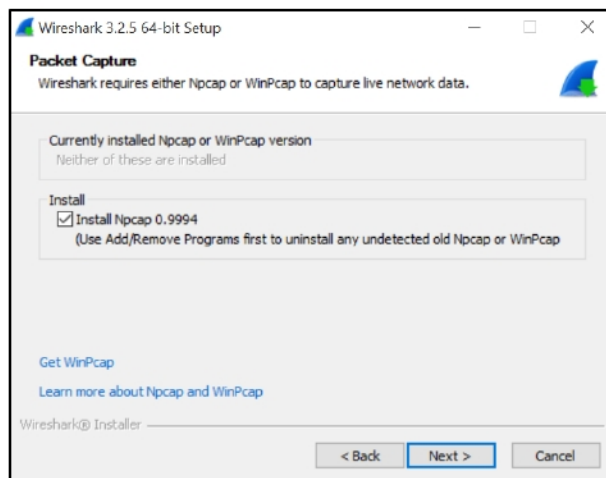
- 7 In the next page, make sure all the options are selected, and click “Next”.



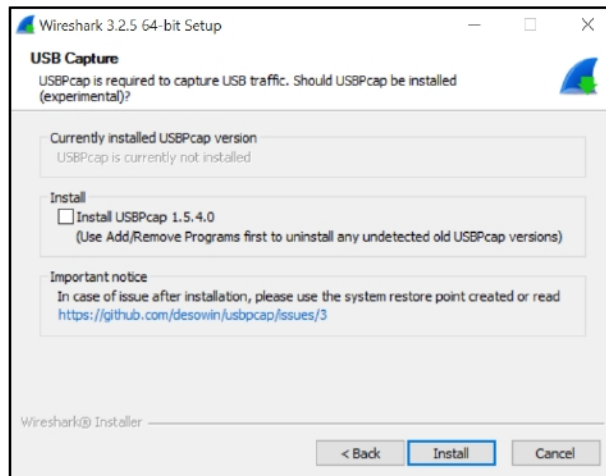
- 8 In the next page, select the installation destination folder, and click “Next”.



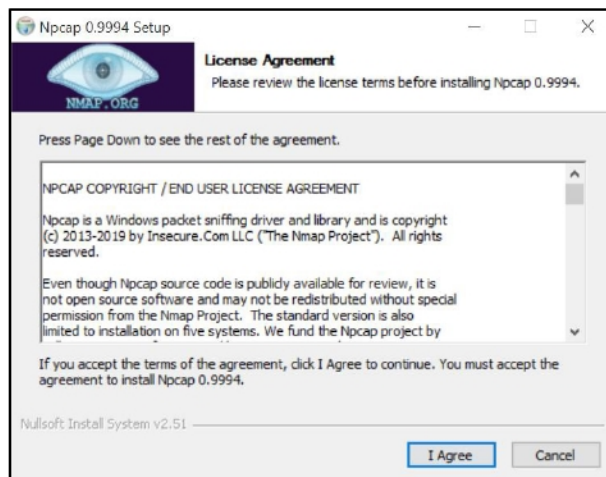
- 9 In the next page, make sure “Install Npcap 0.9994” is selected, and click “Next”.



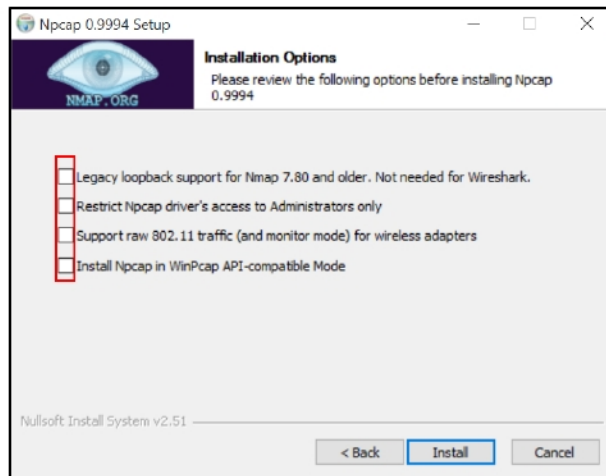
- 10** In the next page, click “Install” without changing anything. The installation will begin.



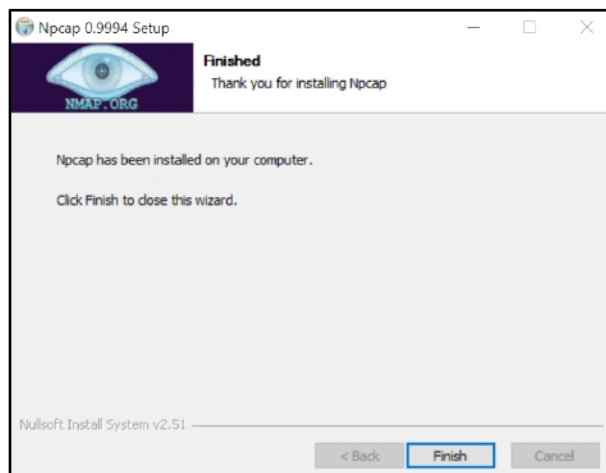
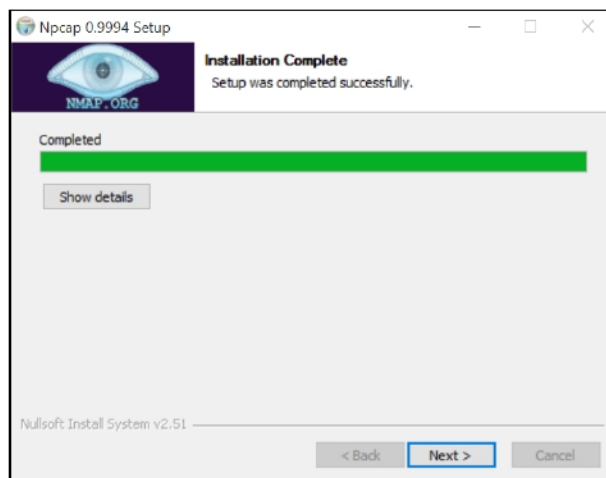
- 11** When the installation process ends, click “I Agree” for the Npcap setup license agreement.



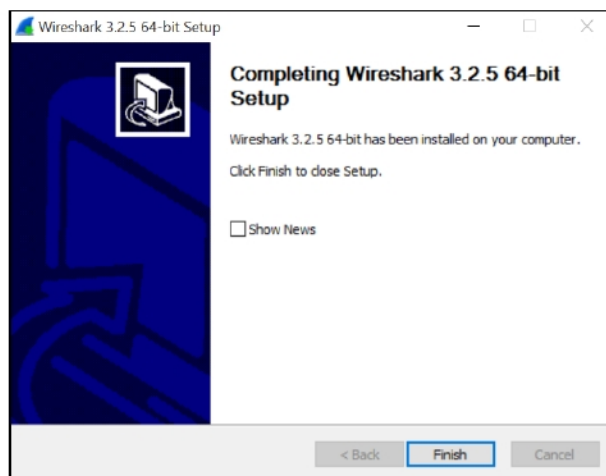
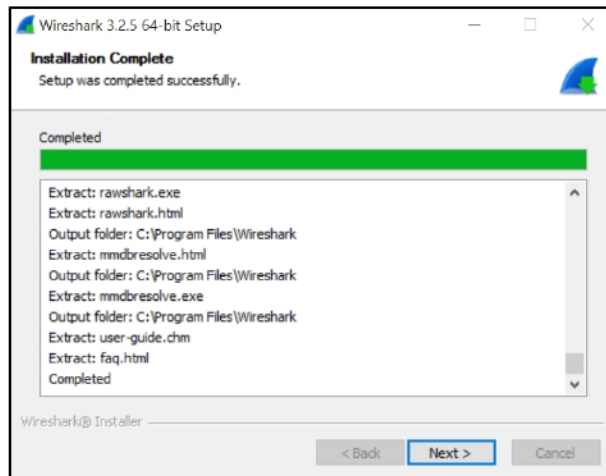
12 In the next page, leave all the options unselected and click “Install”.



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”.

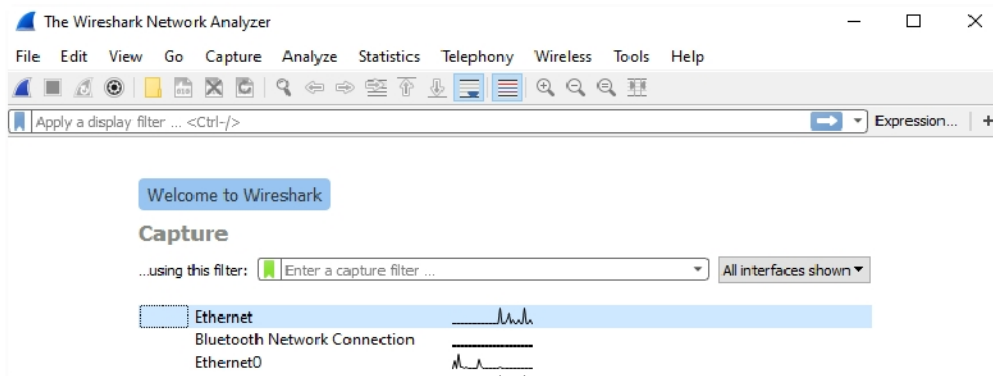


Lab Task 3: Use Wireshark to Examine Live Network Traffic

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.

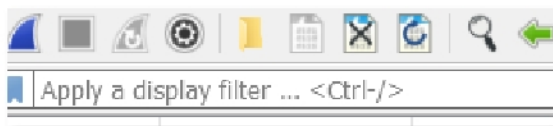


Note: The answers in this section were taken from a lab environment.

Since you are working in a different network environment, some of the answers may be different.



2 Dashboard View:

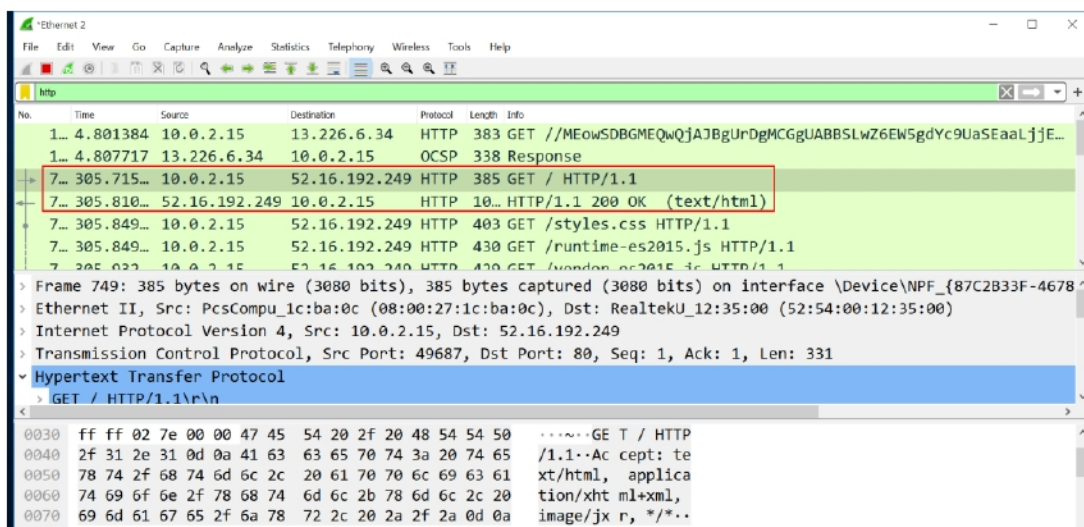
- a) The top screen or bar contains the program's tools, such as preferences, settings, and the search bar.



- 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.

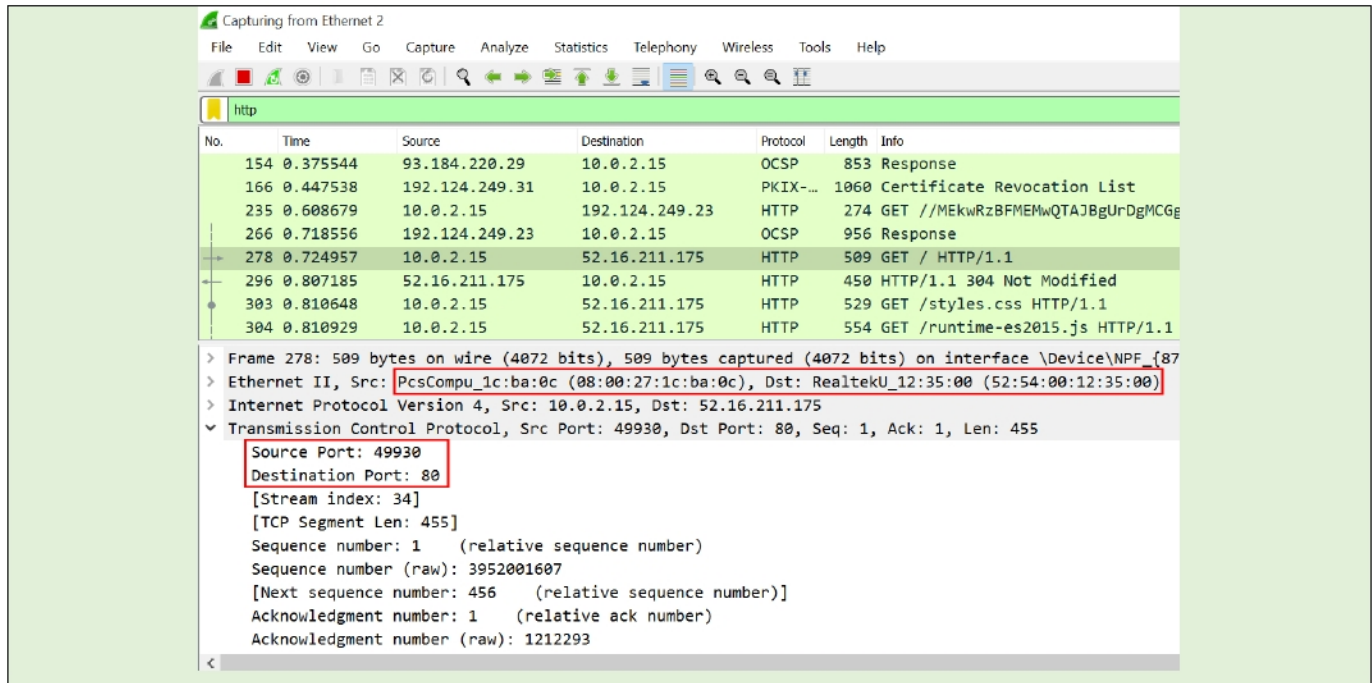
The image shows a Wireshark packet capture window titled "Capturing from Ethernet 2". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. A packet list table is displayed with the following columns: No., Time, Source, Destination, Protocol, Length, and Info.

No.	Time	Source	Destination	Protocol	Length	Info
154	0.375544	93.184.220.29	10.0.2.15	OCSP	853	Response
166	0.447538	192.124.249.31	10.0.2.15	PKIX-...	1060	Certificate Revocation Lis
235	0.608679	10.0.2.15	192.124.249.23	HTTP	274	GET //MEkWRzBFMEMwQTAJBgU
266	0.718556	192.124.249.23	10.0.2.15	OCSP	956	Response
278	0.724957	10.0.2.15	52.16.211.175	HTTP	509	GET / HTTP/1.1
296	0.807185	52.16.211.175	10.0.2.15	HTTP	450	HTTP/1.1 304 Not Modified
303	0.810648	10.0.2.15	52.16.211.175	HTTP	529	GET /styles.css HTTP/1.1
304	0.810929	10.0.2.15	52.16.211.175	HTTP	554	GET /runtime-es2015.js HT

Packet 278 is selected and expanded, showing the Hypertext Transfer Protocol details. The request line is "GET / HTTP/1.1\r\n". The "Cookie" field contains "cookieconsent status=dismiss\r\n". The "Full request URI" is highlighted as "http://juice-shop.herokuapp.com/".

```
GET / HTTP/1.1\r\nAccept: text/html, application/xhtml+xml, image/jxr, */*\r\nAccept-Language: en-US\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)\r\nAccept-Encoding: gzip, deflate\r\nHost: juice-shop.herokuapp.com\r\nIf-Modified-Since: Tue, 21 Jul 2020 20:01:20 GMT\r\nIf-None-Match: W/"785-17372f75b4a"\r\nConnection: Keep-Alive\r\nCookie: cookieconsent status=dismiss\r\n\r\n[Full request URI: http://juice-shop.herokuapp.com/]
```

- 8 Click each header to view the encapsulated data (logical ports, IP, and MAC address).



Wireshark packet capture showing an HTTP GET request. The packet list shows frame 278 selected. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol headers. The TCP header shows Source Port: 49930 and Destination Port: 80.

No.	Time	Source	Destination	Protocol	Length	Info
154	0.375544	93.184.220.29	10.0.2.15	OCSP	853	Response
166	0.447538	192.124.249.31	10.0.2.15	PKIX...	1060	Certificate Revocation List
235	0.608679	10.0.2.15	192.124.249.23	HTTP	274	GET //MEKwRzBFMEwQTAJBgUrDgMCGg
266	0.718556	192.124.249.23	10.0.2.15	OCSP	956	Response
278	0.724957	10.0.2.15	52.16.211.175	HTTP	509	GET / HTTP/1.1
296	0.807185	52.16.211.175	10.0.2.15	HTTP	450	HTTP/1.1 304 Not Modified
303	0.810648	10.0.2.15	52.16.211.175	HTTP	529	GET /styles.css HTTP/1.1
304	0.810929	10.0.2.15	52.16.211.175	HTTP	554	GET /runtime-es2015.js HTTP/1.1

Frame 278: 509 bytes on wire (4072 bits), 509 bytes captured (4072 bits) on interface \Device\NPF_{87...}

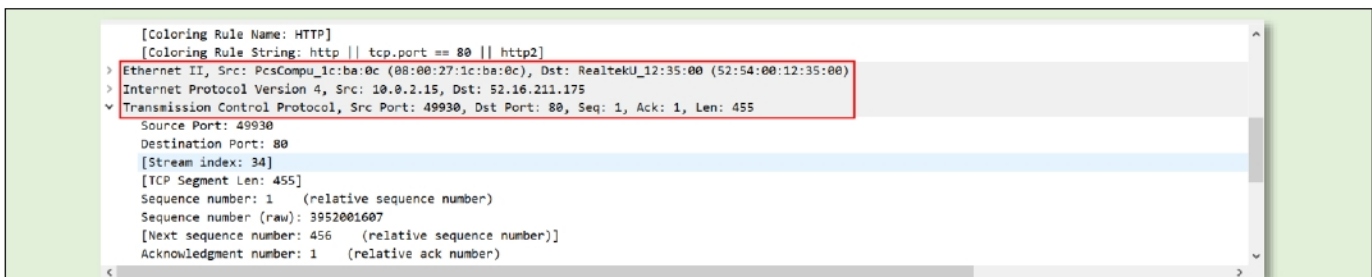
Ethernet II, Src: PcsCompu_1c:ba:0c (08:00:27:1c:ba:0c), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 52.16.211.175

Transmission Control Protocol, Src Port: 49930, Dst Port: 80, Seq: 1, Ack: 1, Len: 455

Source Port: 49930
Destination Port: 80
[Stream index: 34]
[TCP Segment Len: 455]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 3952001607
[Next sequence number: 456 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 1212293

- 9 Document the following details:
- What are the logical port source and destination?
 - What are the logical source and destination addresses?
 - What are the physical source and destination addresses?



Wireshark packet capture showing an HTTP GET request. The packet list shows frame 278 selected. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol headers. The TCP header shows Source Port: 49930 and Destination Port: 80.

No.	Time	Source	Destination	Protocol	Length	Info
154	0.375544	93.184.220.29	10.0.2.15	OCSP	853	Response
166	0.447538	192.124.249.31	10.0.2.15	PKIX...	1060	Certificate Revocation List
235	0.608679	10.0.2.15	192.124.249.23	HTTP	274	GET //MEKwRzBFMEwQTAJBgUrDgMCGg
266	0.718556	192.124.249.23	10.0.2.15	OCSP	956	Response
278	0.724957	10.0.2.15	52.16.211.175	HTTP	509	GET / HTTP/1.1
296	0.807185	52.16.211.175	10.0.2.15	HTTP	450	HTTP/1.1 304 Not Modified
303	0.810648	10.0.2.15	52.16.211.175	HTTP	529	GET /styles.css HTTP/1.1
304	0.810929	10.0.2.15	52.16.211.175	HTTP	554	GET /runtime-es2015.js HTTP/1.1

Frame 278: 509 bytes on wire (4072 bits), 509 bytes captured (4072 bits) on interface \Device\NPF_{87...}

Ethernet II, Src: PcsCompu_1c:ba:0c (08:00:27:1c:ba:0c), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 52.16.211.175

Transmission Control Protocol, Src Port: 49930, Dst Port: 80, Seq: 1, Ack: 1, Len: 455

Source Port: 49930
Destination Port: 80
[Stream index: 34]
[TCP Segment Len: 455]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 3952001607
[Next sequence number: 456 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 1212293

Protocol Layer 4: TCP

Source Port: 49930 (usually selected randomly from the dynamic port range).

Destination Port: 80 (used by HTTP for web page transfer).

Flag: We can understand by observing the flags that this is the first packet of the TCP 3-way handshake process.


```

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 52.16.211.175
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 495
  Identification: 0x5c50 (23632)
  > Flags: 0x4000, Don't fragment
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.0.2.15
  Destination: 52.16.211.175

```

Layer 3 protocol: IPv4

Source address: 10.0.2.15 (local machine)

Destination address: 52.16.211.175 (Juice shop hosting server)

```

[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: PcsCompu_1c:ba:0c (08:00:27:1c:ba:0c), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
  > Destination: RealtekU_12:35:00 (52:54:00:12:35:00)
  > Source: PcsCompu_1c:ba:0c (08:00:27:1c:ba:0c)
  Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 10.0.2.15, Dst: 52.16.211.175
  > Transmission Control Protocol, Src Port: 49930, Dst Port: 80, Seq: 1, Ack: 1, Len: 455
    Source Port: 49930
    Destination Port: 80
    [Stream index: 34]
    [TCP Segment Len: 455]
    Sequence number: 1 (relative sequence number)
    Sequence number (raw): 3952001607

```

Layer 2 protocol: Ethernet

Source address: 08:00:27:1c:ba:0c (local machine)

Destination address: 52:54:00:12:35:00

```


> Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_1c:ba:0c (08:00:27:1c:ba:0c)
> Internet Protocol Version 4, Src: 52.16.211.175, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 80, Dst Port: 49930, Seq: 1, Ack: 456, Len: 396
> Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
  Server: Cowboy\r\n
  Content-Length: 0\r\n
  Connection: keep-alive\r\n
  Access-Control-Allow-Origin: *\r\n
  X-Content-Type-Options: nosniff\r\n
  X-Frame-Options: SAMEORIGIN\r\n
  Feature-Policy: payment 'self'\r\n
  Accept-Ranges: bytes\r\n
  Cache-Control: public, max-age=0\r\n
  Last-Modified: Tue, 21 Jul 2020 20:01:20 GMT\r\n
  Etag: W/"785-17372f75bda"\r\n
  Date: Wed, 22 Jul 2020 09:17:32 GMT\r\n
  Via: 1.1 vegur\r\n
  \r\n
  [HTTP response 1/3]
  [Time since request: 0.082228000 seconds]
  [Request in frame: 278]

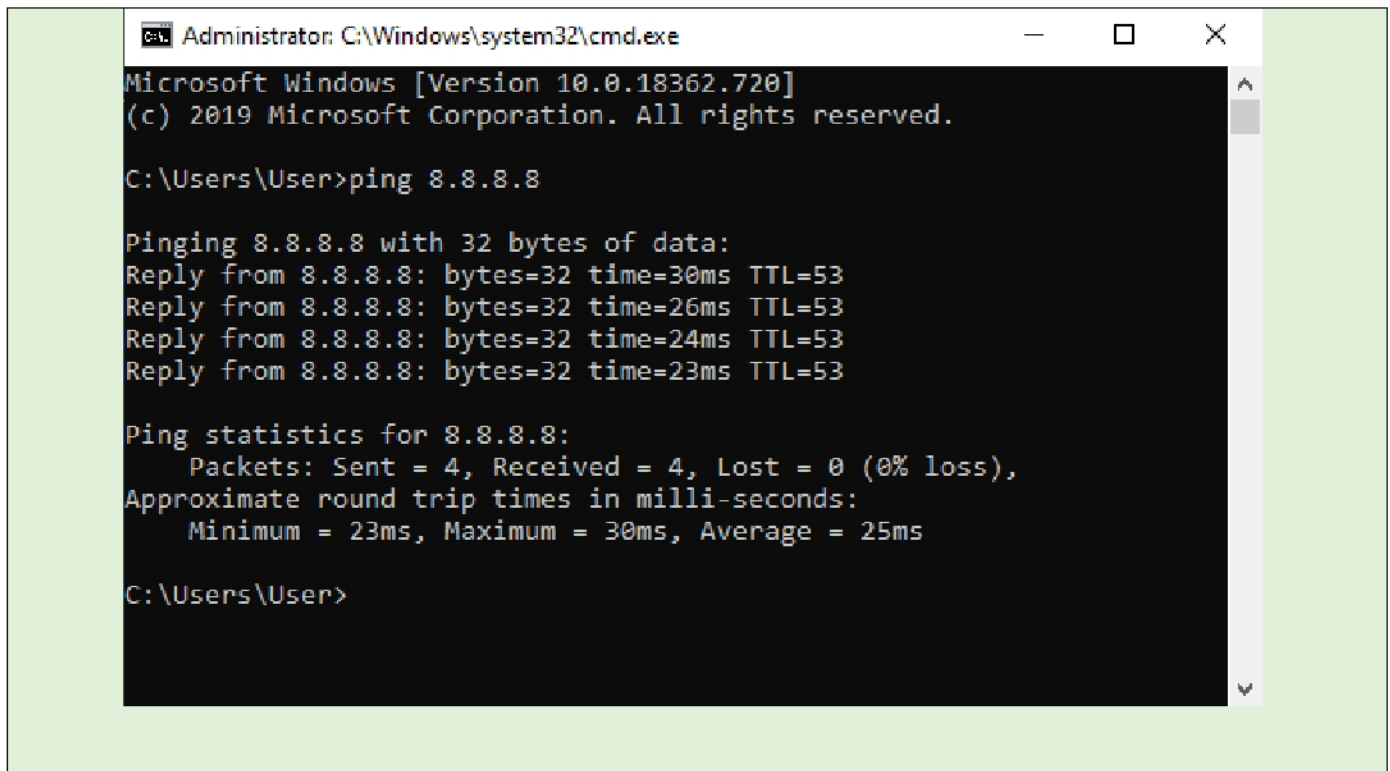
```

Response packet: Note that the source and destination addresses switched places.

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




```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\User>ping 8.8.8.8

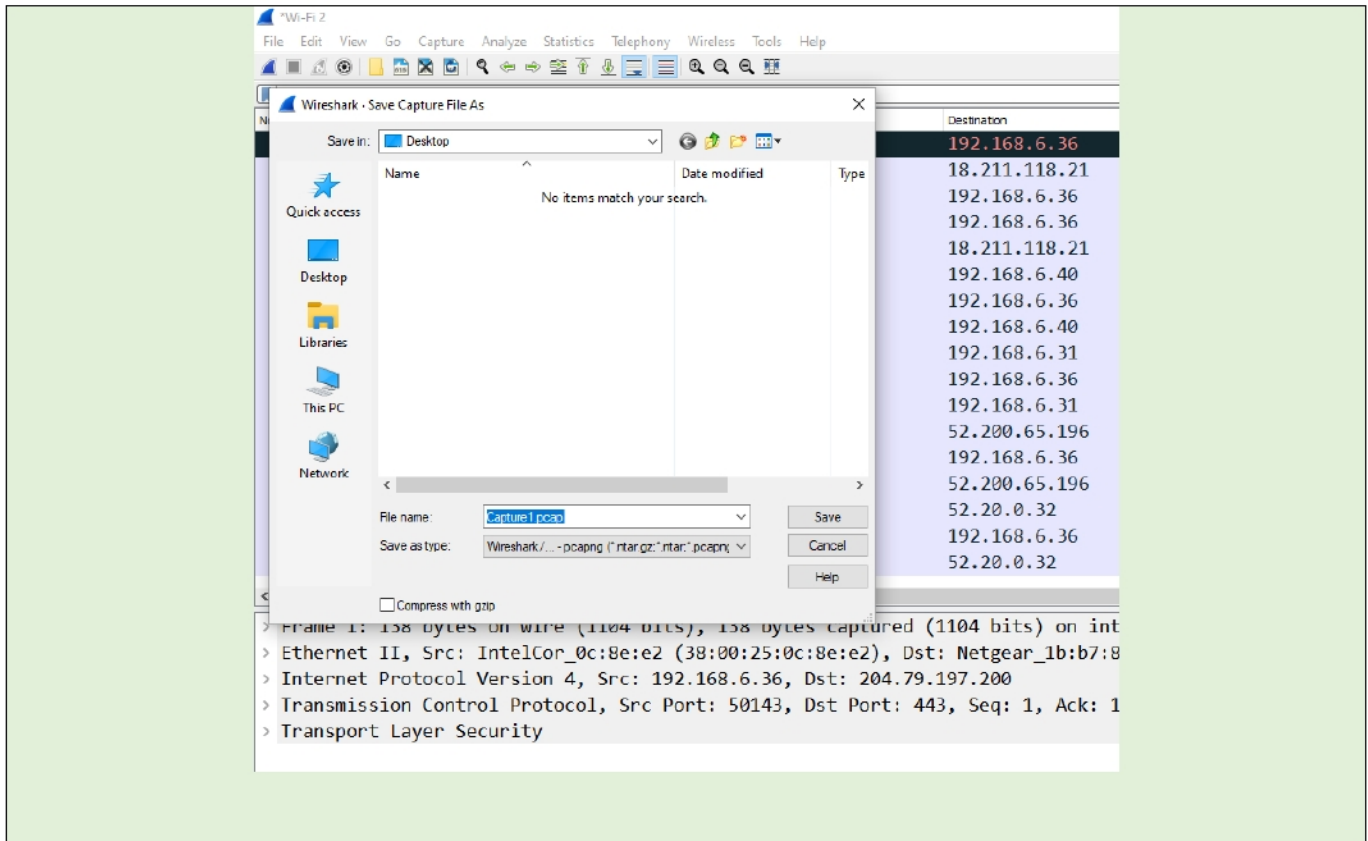
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=30ms TTL=53
Reply from 8.8.8.8: bytes=32 time=26ms TTL=53
Reply from 8.8.8.8: bytes=32 time=24ms TTL=53
Reply from 8.8.8.8: bytes=32 time=23ms TTL=53

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 30ms, Average = 25ms

C:\Users\User>
```

- 3 Browse to <http://hack-yourself-first.com/>
- 4 Stop capturing using the stop button .

- Click File and then Save as. Name the file **capture1** and save it in the Desktop folder.



- Close Wireshark.
- Double-click capture1.pcap to open the file.
- 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.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.234844	10.0.2.15	8.8.8.8	DNS	72	Standard query 0x0dc9 A www.bing.com
3	0.311586	8.8.8.8	10.0.2.15	DNS	193	Standard query response 0x0dc9 A www.bing.com CNAME a-0001.a-afden...
59	1.202924	10.0.2.15	162.159.27.72	DNS	139	Dynamic update 0x11bd SOA Cyber.com CNAME AAAA A 10.0.2.15
60	1.259667	162.159.27.72	10.0.2.15	DNS	69	Unknown operation (8) response 0x11bd Not implemented SOA Cyber.com
2...	29.109166	10.0.2.15	8.8.8.8	DNS	84	Standard query 0x5a3e A hack-yourself-first.com
3...	29.178947	8.8.8.8	10.0.2.15	DNS	157	Standard query response 0x5a3e No such name A hack-yourself-first...
3...	36.128947	10.0.2.15	8.8.8.8	DNS	83	Standard query 0xd68c A hack-yourself-first.com
3...	36.220372	8.8.8.8	10.0.2.15	DNS	99	Standard query response 0xd68c A hack-yourself-first.com A 104.42...
3...	36.769431	10.0.2.15	8.8.8.8	DNS	77	Standard query 0x99de A urs.microsoft.com

```

COMMANDO 22/07/2020 13:45:20.38
C:\Windows\system32\ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

```

- 9 Document the following details:
- Which Layer 4 protocol is used to encapsulate the Layer 4 header.
 - What are the source and destination logical ports?
 - What is the default DNS server configured on your machine, according to the Layer 3 header?

```

> Frame 729: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{87C2
> Ethernet II, Src: PcsCompu_1c:ba:0c (08:00:27:1c:ba:0c), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 61464, Dst Port: 53
  Source Port: 61464
  Destination Port: 53
  Length: 50
  Checksum: 0x1c62 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 13]
> [Timestamps]

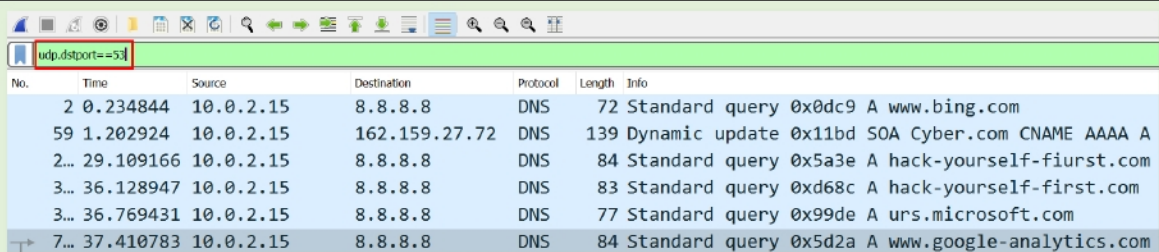
```

Layer 4 protocol: UDP

Source port: 61464

Destination port: 53

- 10 Which filter will display all packets sent to port 53?



No.	Time	Source	Destination	Protocol	Length	Info
2	0.234844	10.0.2.15	8.8.8.8	DNS	72	Standard query 0x0dc9 A www.bing.com
59	1.202924	10.0.2.15	162.159.27.72	DNS	139	Dynamic update 0x11bd SOA Cyber.com CNAME AAAA A
2...	29.109166	10.0.2.15	8.8.8.8	DNS	84	Standard query 0x5a3e A hack-yourself-fiurst.com
3...	36.128947	10.0.2.15	8.8.8.8	DNS	83	Standard query 0xd68c A hack-yourself-first.com
3...	36.769431	10.0.2.15	8.8.8.8	DNS	77	Standard query 0x99de A urs.microsoft.com
7...	37.410783	10.0.2.15	8.8.8.8	DNS	84	Standard query 0x5d2a A www.google-analytics.com

11 Using the appropriate display filter, display only the Ping packets.

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
40	0.486646	10.0.2.15	8.8.8.8	ICMP	213	Destination unreachable
84	8.714769	10.0.2.15	8.8.8.8	ICMP	74	Echo (ping) request
85	8.783218	8.8.8.8	10.0.2.15	ICMP	74	Echo (ping) reply
87	9.734447	10.0.2.15	8.8.8.8	ICMP	74	Echo (ping) request
88	9.802806	8.8.8.8	10.0.2.15	ICMP	74	Echo (ping) reply
89	10.749410	10.0.2.15	8.8.8.8	ICMP	74	Echo (ping) request

12 Document the following details:

- How many requests and replies are shown?
- Why doesn't ICMP have a logical port number listed in the packet capture?

Request Packets: 4

Reply Packets: 4

ICMP is a Layer 3 protocol, meaning it does not have a logical port. To verify this, you can view the header of the packet, and note that there is no Layer 4 header.

13 Which filter will display all packets sent to the 8.8.8.8 host?

ip.dst==8.8.8.8						
No.	Time	Source	Destination	Protocol	L	
12	0.165509	10.0.2.15	8.8.8.8	DNS		
35	0.249834	10.0.2.15	8.8.8.8	DNS		
40	0.486646	10.0.2.15	8.8.8.8	ICMP		
82	8.313399	10.0.2.15	8.8.8.8	DNS		
84	8.714769	10.0.2.15	8.8.8.8	ICMP		
87	9.734447	10.0.2.15	8.8.8.8	ICMP		