Lab 2: Wireshark to View Network Traffic

Overview:

Wireshark is an open-source network protocol analysis software program, widely considered the industry standard. A global organization of network specialists and software developers supports Wireshark and continues to make updates for new network technologies and encryption methods. Government agencies, corporations, non-profits, and educational institutions use Wireshark for troubleshooting and teaching purposes. There truly isn't a better way to learn low-level networking than to look at traffic under the Wireshark microscope.

You could think of a network packet analyser as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course). In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analysers available today. Here are some reasons people use Wireshark:

- Network administrators use it to troubleshoot network problems.
- Network security engineers use it to examine security problems.
- QA engineers use it to verify network applications.
- Developers use it to debug protocol implementations.
- People use it to learn network protocol internals.

How does Wireshark work?

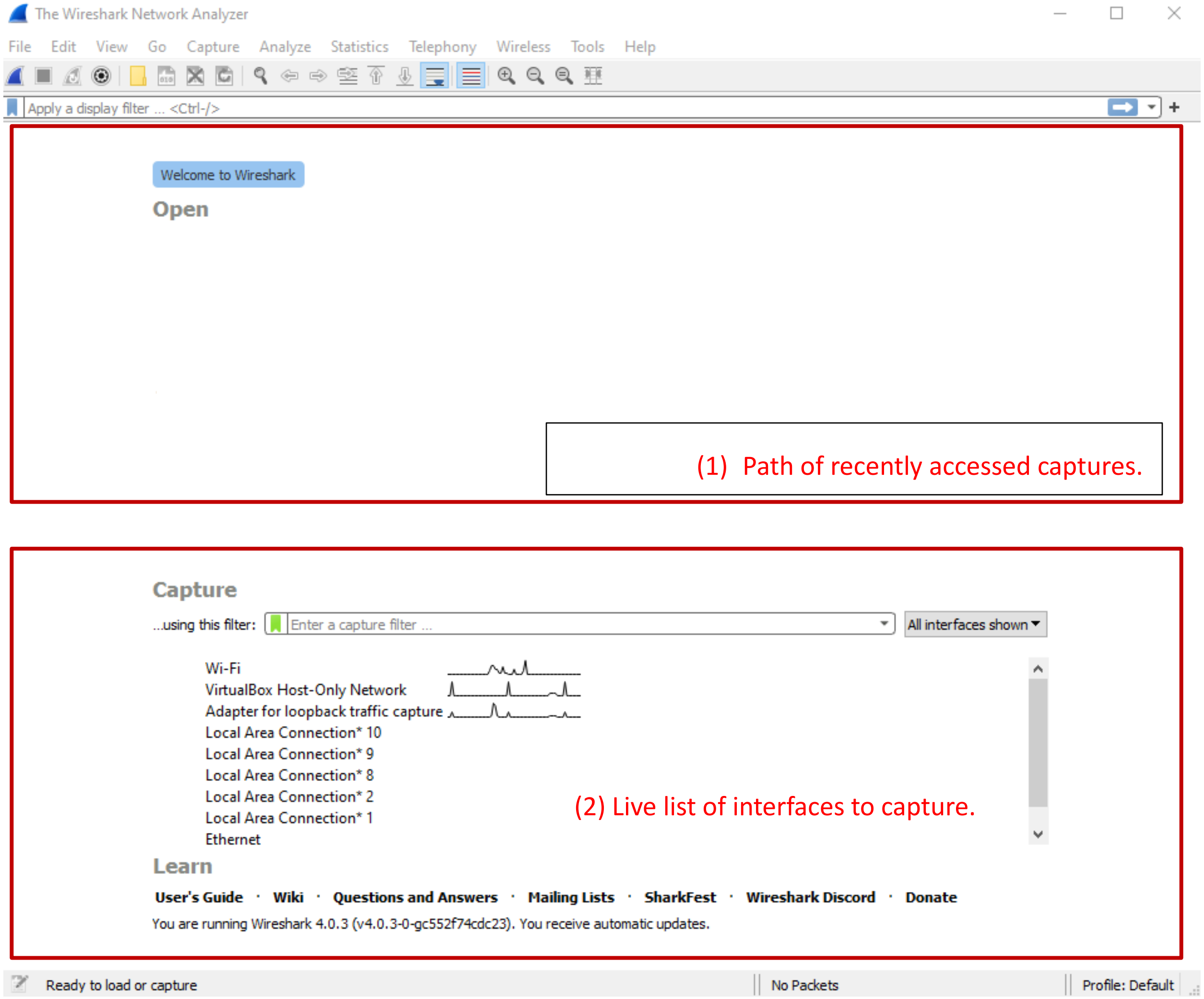
Wireshark is a packet sniffer and analysis tool. It captures network traffic from ethernet, Bluetooth, wireless (IEEE.802.11), token ring, and frame relay connections, among others, and stores that data for offline analysis. Wireshark allows you to filter the log before the capture starts or during analysis, so you can narrow down and zero in on what you're looking for in the network trace. For example, you can set a filter to see TCP traffic between two IP addresses, or you can set it only to show you the packets sent from one computer. The filters in Wireshark are one of the primary reasons it has become the standard tool for packet analysis.

Lab Objectives:

- Introduce and familiarize yourself with Wireshark.
- Use the tool to capture network traffic and basics of how to analyse the network traffic.
- Capture and analyse local ICMP data in network traffic, and how to locate the IP and MAC address information in the captured data.

Basics of Wireshark

The main page of Wireshark shows two main sections, as illustrated in Figure 1. If you have not opened any captures before, you won't see Figure 1(1).


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
(1) Path of recently accessed captures.
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Wi-Fi
VirtualBox Host-Only Network
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 2
Local Area Connection* 1
Ethernet
(2) Live list of interfaces to capture.
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Ready to load or capture
No Packets
Profile: Default

You are running Wireshark 4.0.3 (v4.0.3-0-gc552f74cdc23). You receive automatic updates.

Figure 1: Main page of Wireshar

The Capture Options button (highlighted in Figure 2), also accessible under the menu "Capture", opens the "Capture Interfaces" screen (Figure 3) and allows you to configure advanced options.

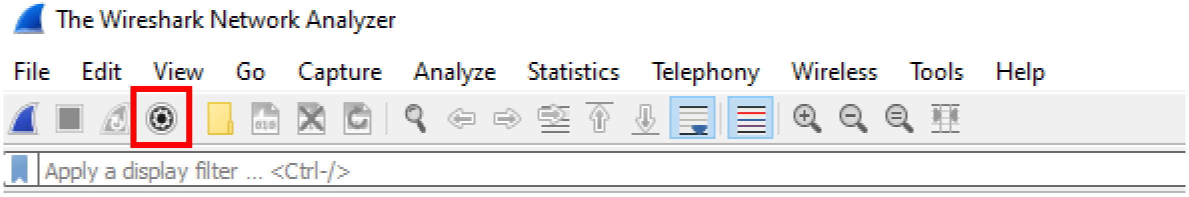

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

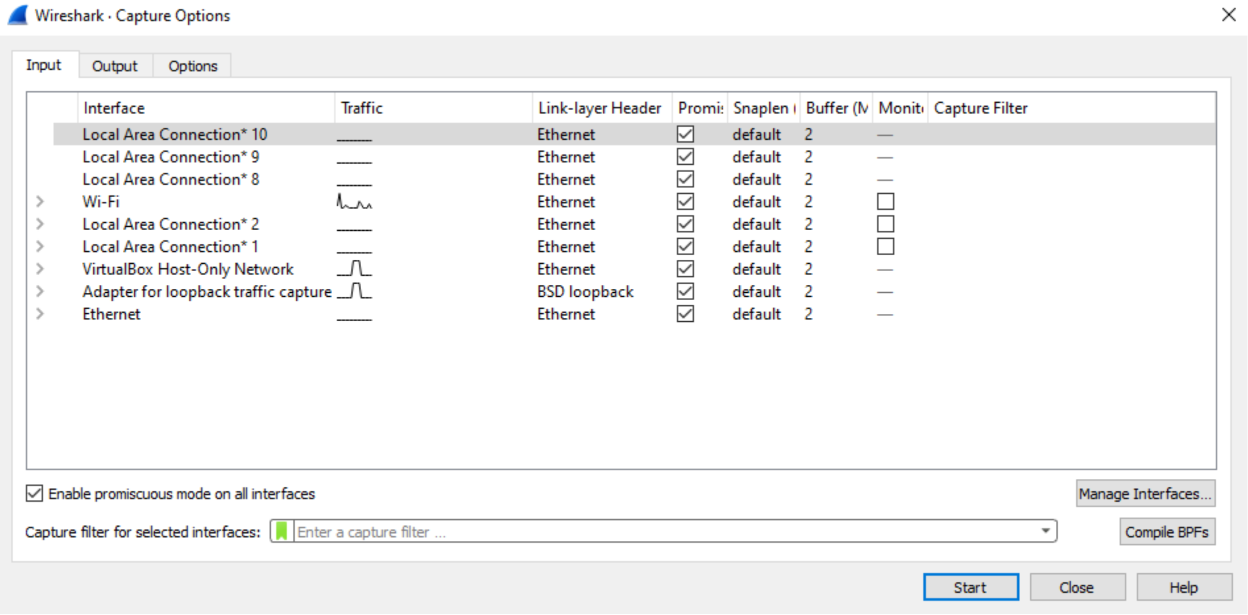
Figure 2: Capture Options button highlighted.

Capture options are distributed in 3 tabs (Input, Output and Options) and allow, e.g.:

- To determine the file where captured data will be written to.
- To resolve MAC addresses and DNS names.
- To limit the time or size of the capture.

The selection of these options helps to improve the performance of Wireshark capture. For example, you can adjust settings to avoid name-resolution issues, as they will otherwise slow down your capture system and generate large numbers of name queries. Time and size limits can also place limitations on unattended captures.

Explore the tabs.



Wireshark · Capture Options

	Interface	Traffic	Link-layer Header	Promi:	Snaplen (	Buffer (M	Monit	Capture Filter
	Local Area Connection* 10		Ethernet	☑	default	2	—	
	Local Area Connection* 9		Ethernet	☑	default	2	—	
	Local Area Connection* 8		Ethernet	☑	default	2	—	
>	Wi-Fi		Ethernet	☑	default	2	□	
>	Local Area Connection* 2		Ethernet	☑	default	2	□	
>	Local Area Connection* 1		Ethernet	☑	default	2	□	
>	VirtualBox Host-Only Network		Ethernet	☑	default	2	—	
>	Adapter for loopback traffic capture		BSD loopback	☑	default	2	—	
>	Ethernet		Ethernet	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

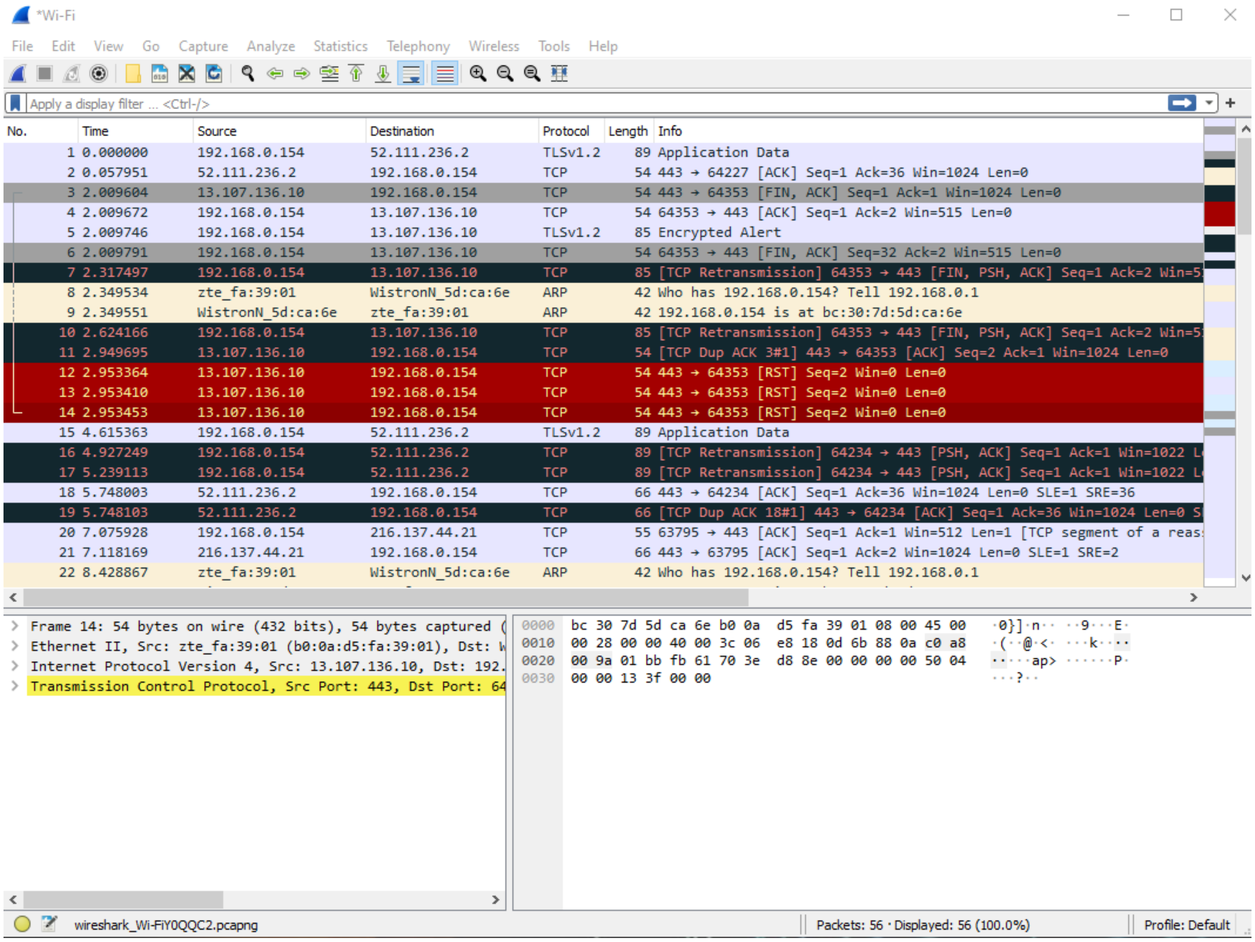
Capture filter for selected interfaces: Enter a capture filter ...

Figure 3: The Capture Interfaces screen.

Running a simple packet capture

Select one interface which is showing traffic, i.e., a wiggled line as you can see in Figure 1(2) for “Wireless Network Connection” and on Figure 3 – e.g., capture Ethernet traffic. If using the first option (main screen), just double-click on the relevant interface. If using the second option (capture interface screen), click on the **Start** button.

Wireshark screen will immediately begin filling up with traffic seen on the network interface, as illustrated in Figure 4.


*Wi-Fi
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
wireshark_Wi-FiY0QQC2.pcapng
Packets: 56 · Displayed: 56 (100.0%)
Profile: Default

```
No.    Time        Source              Destination         Protocol Length Info
     1 0.000000    192.168.0.154       52.111.236.2        TLSv1.2    89 Application Data
     2 0.057951    52.111.236.2        192.168.0.154       TCP        54 443 → 64227 [ACK] Seq=1 Ack=36 Win=1024 Len=0
     3 2.009604    13.107.136.10       192.168.0.154       TCP        54 443 → 64353 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
     4 2.009672    192.168.0.154       13.107.136.10       TCP        54 64353 → 443 [ACK] Seq=1 Ack=2 Win=515 Len=0
     5 2.009746    192.168.0.154       13.107.136.10       TLSv1.2    85 Encrypted Alert
     6 2.009791    192.168.0.154       13.107.136.10       TCP        54 64353 → 443 [FIN, ACK] Seq=32 Ack=2 Win=515 Len=0
     7 2.317497    192.168.0.154       13.107.136.10       TCP        85 [TCP Retransmission] 64353 → 443 [FIN, PSH, ACK] Seq=1 Ack=2 Win=5
     8 2.349534    zte_fa:39:01        WistronN_5d:ca:6e   ARP        42 Who has 192.168.0.154? Tell 192.168.0.1
     9 2.349551    WistronN_5d:ca:6e   zte_fa:39:01        ARP        42 192.168.0.154 is at bc:30:7d:5d:ca:6e
    10 2.624166    192.168.0.154       13.107.136.10       TCP        85 [TCP Retransmission] 64353 → 443 [FIN, PSH, ACK] Seq=1 Ack=2 Win=5
    11 2.949695    13.107.136.10       192.168.0.154       TCP        54 [TCP Dup ACK 3#1] 443 → 64353 [ACK] Seq=2 Ack=1 Win=1024 Len=0
    12 2.953364    13.107.136.10       192.168.0.154       TCP        54 443 → 64353 [RST] Seq=2 Win=0 Len=0
    13 2.953410    13.107.136.10       192.168.0.154       TCP        54 443 → 64353 [RST] Seq=2 Win=0 Len=0
    14 2.953453    13.107.136.10       192.168.0.154       TCP        54 443 → 64353 [RST] Seq=2 Win=0 Len=0
    15 4.615363    192.168.0.154       52.111.236.2        TLSv1.2    89 Application Data
    16 4.927249    192.168.0.154       52.111.236.2        TCP        89 [TCP Retransmission] 64234 → 443 [PSH, ACK] Seq=1 Ack=1 Win=1022 L
    17 5.239113    192.168.0.154       52.111.236.2        TCP        89 [TCP Retransmission] 64234 → 443 [PSH, ACK] Seq=1 Ack=1 Win=1022 L
    18 5.748003    52.111.236.2        192.168.0.154       TCP        66 443 → 64234 [ACK] Seq=1 Ack=36 Win=1024 Len=0 SLE=1 SRE=36
    19 5.748103    52.111.236.2        192.168.0.154       TCP        66 [TCP Dup ACK 18#1] 443 → 64234 [ACK] Seq=1 Ack=36 Win=1024 Len=0 S
    20 7.075928    192.168.0.154       216.137.44.21       TCP        55 63795 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reas
    21 7.118169    216.137.44.21       192.168.0.154       TCP        66 443 → 63795 [ACK] Seq=1 Ack=2 Win=1024 Len=0 SLE=1 SRE=2
    22 8.428867    zte_fa:39:01        WistronN_5d:ca:6e   ARP        42 Who has 192.168.0.154? Tell 192.168.0.1
```

```
> Frame 14: 54 bytes on wire (432 bits), 54 bytes captured (
> Ethernet II, Src: zte_fa:39:01 (b0:0a:d5:fa:39:01), Dst: W
> Internet Protocol Version 4, Src: 13.107.136.10, Dst: 192.
> Transmission Control Protocol, Src Port: 443, Dst Port: 64
```

```
0000  bc 30 7d 5d ca 6e b0 0a  d5 fa 39 01 08 00 45 00   ·0}]·n·· ··9···E·
0010  00 28 00 00 40 00 3c 06  e8 18 0d 6b 88 0a c0 a8   ·(··@·<· ···k····
0020  00 9a 01 bb fb 61 70 3e  d8 8e 00 00 00 00 50 04   ······ap> ······P·
0030  00 00 13 3f 00 00                                  ···?··
```

Figure 4: Live capture of packets on the selected interface.

Each line in the top pane of the Wireshark window corresponds to a single packet seen on the network. The default display shows:

- The time of the packet (relative to the initiation of the capture),
- The source and destination IP addresses,
- The protocol used and some information about the packet.

You can drill down and obtain more information by clicking on a row. This causes the bottom two window panes to fill with information:

- The middle pane contains drill-down details on the packet selected in the top frame.
- Clicking on Hex data in bottom half reveal varying levels of detail about each layer of information contained within the packet.

Select a packet, and examine its content across the top, middle and bottom panes.

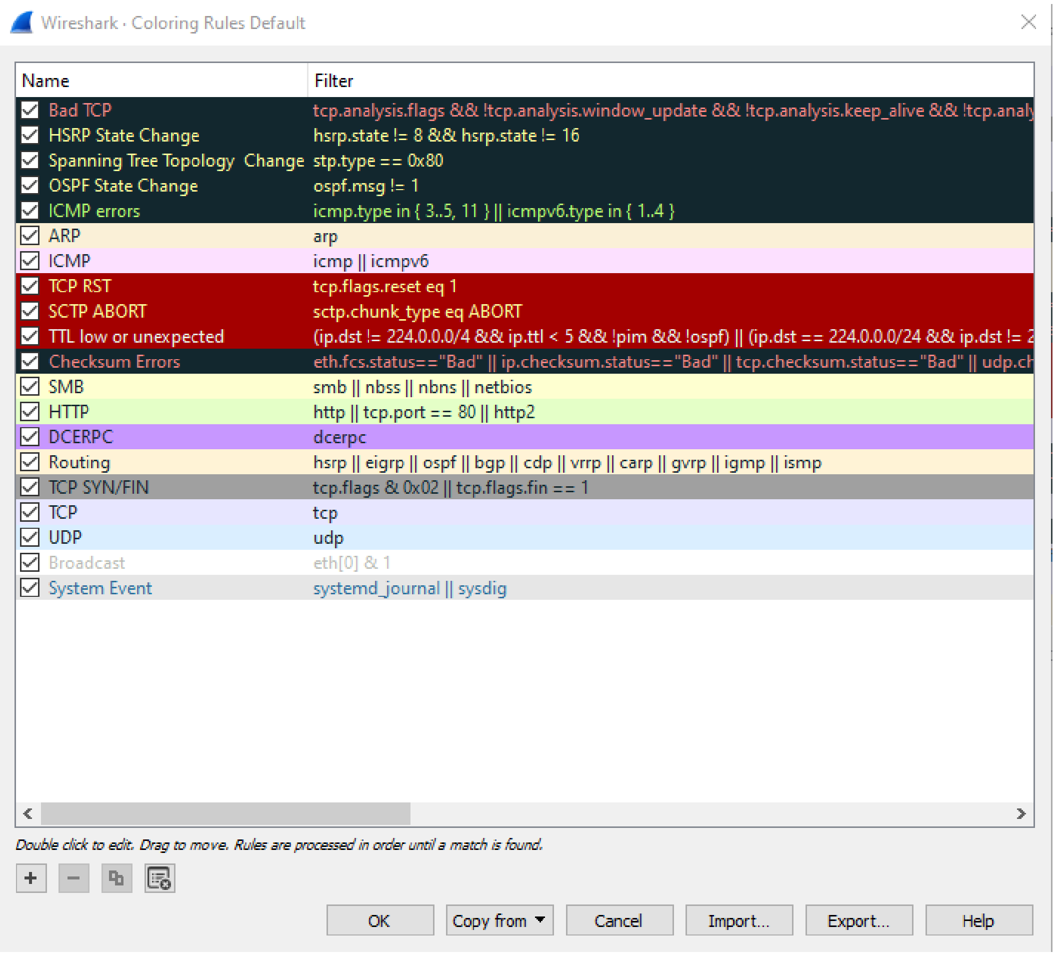
The following link contains useful information about setting up capture of network traffic. It starts with a warning – *you need to make sure you are allowed to capture packets from the network in the first place.*

https://wiki.wireshark.org/CaptureSetup

Wireshark coloring scheme

Color coding is helpful when analyzing packets with Wireshark. Notice in the capture you have done that each row is color-coded, according to different protocols.

Wireshark uses a complex coloring scheme (which you can customize). The default settings can be accessed via the **View menu** → **Coloring Rules**. The default scheme is shown in Figure 5.



Name	Filter
☑ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analy
☑ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
☑ Spanning Tree Topology Change	stp.type == 0x80
☑ OSPF State Change	ospf.msg != 1
☑ ICMP errors	icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }
☑ ARP	arp
☑ ICMP	icmp || icmpv6
☑ TCP RST	tcp.flags.reset eq 1
☑ SCTP ABORT	sctp.chunk_type eq ABORT
☑ TTL low or unexpected	(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 2
☑ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.ch
☑ SMB	smb || nbss || nbns || netbios
☑ HTTP	http || tcp.port == 80 || http2
☑ DCERPC	dcerpc
☑ Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
☑ TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1
☑ TCP	tcp
☑ UDP	udp
☑ Broadcast	eth[0] & 1
☑ System Event	systemd_journal || sysdig

Double click to edit. Drag to move. Rules are processed in order until a match is found.

Figure 5: Default packet colour scheme used by Wireshark.

Stop capturing live packets is possible via the red button (2nd highlighted in Figure 6). To restart the current capture, use the green button (3rd highlighted in Figure 6). All these options are also available via the **Capture** menu.

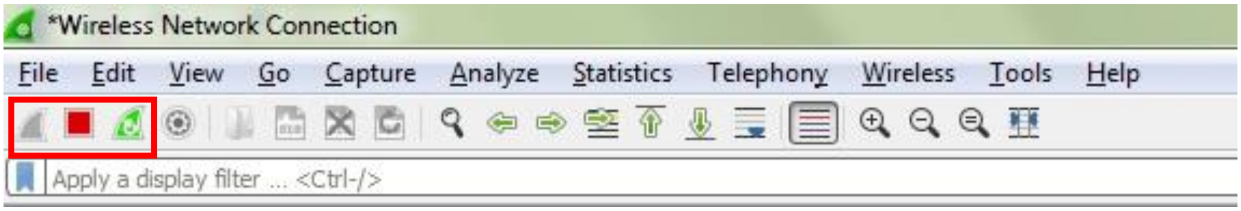

*Wireless Network Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Figure 6: Manipulating captures – Start, Stop and Restart, respectively.

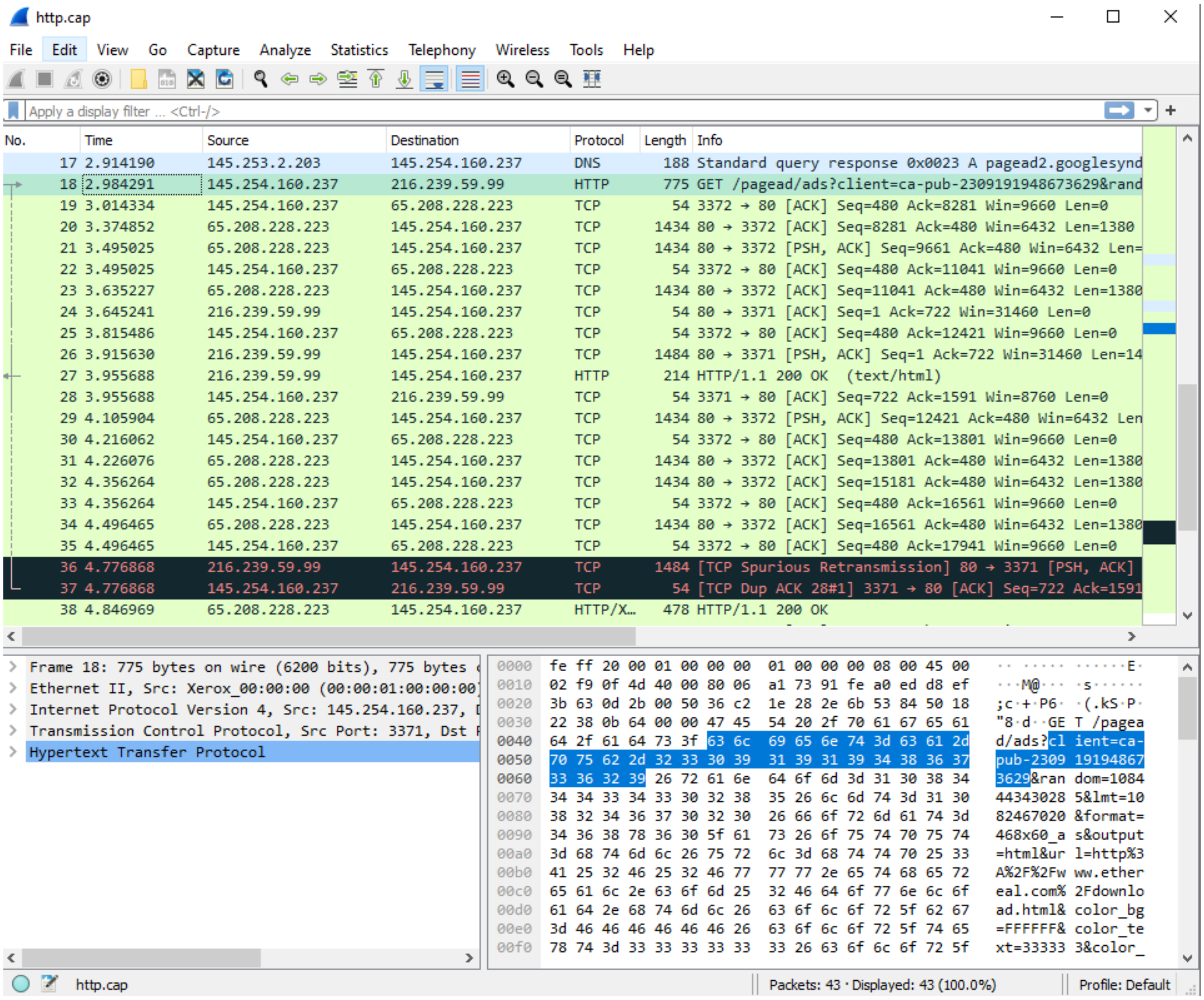
If you stop a capture, and either want to start a new one or restart the same capture, Wireshark will ask if you want to save the captured packages or not.

Make sure you stop the live capture without saving.

Packet display filtering

Download the Wireshark capture file **http.cap** available on Moodle, this should be already downloaded when you downloaded the file: http://wiki.wireshark.org/SampleCaptures

Open the **http.cap** file, you will see the saved packets as shown in Figure 7.


http.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time      Source           Destination      Protocol Length Info
     17 2.914190  145.253.2.203    145.254.160.237  DNS       188 Standard query response 0x0023 A pagead2.googlesynd
     18 2.984291  145.254.160.237  216.239.59.99    HTTP      775 GET /pagead/ads?client=ca-pub-2309191948673629&rand
     19 3.014334  145.254.160.237  65.208.228.223   TCP        54 3372 → 80 [ACK] Seq=480 Ack=8281 Win=9660 Len=0
     20 3.374852  65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [ACK] Seq=8281 Ack=480 Win=6432 Len=1380
     21 3.495025  65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [PSH, ACK] Seq=9661 Ack=480 Win=6432 Len=
     22 3.495025  145.254.160.237  65.208.228.223   TCP        54 3372 → 80 [ACK] Seq=480 Ack=11041 Win=9660 Len=0
     23 3.635227  65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [ACK] Seq=11041 Ack=480 Win=6432 Len=1380
     24 3.645241  216.239.59.99    145.254.160.237  TCP        54 80 → 3371 [ACK] Seq=1 Ack=722 Win=31460 Len=0
     25 3.815486  145.254.160.237  65.208.228.223   TCP        54 3372 → 80 [ACK] Seq=480 Ack=12421 Win=9660 Len=0
     26 3.915630  216.239.59.99    145.254.160.237  TCP      1484 80 → 3371 [PSH, ACK] Seq=1 Ack=722 Win=31460 Len=14
     27 3.955688  216.239.59.99    145.254.160.237  HTTP      214 HTTP/1.1 200 OK  (text/html)
     28 3.955688  145.254.160.237  216.239.59.99    TCP        54 3371 → 80 [ACK] Seq=722 Ack=1591 Win=8760 Len=0
     29 4.105904  65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [PSH, ACK] Seq=12421 Ack=480 Win=6432 Len
     30 4.216062  145.254.160.237  65.208.228.223   TCP        54 3372 → 80 [ACK] Seq=480 Ack=13801 Win=9660 Len=0
     31 4.226076  65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [ACK] Seq=13801 Ack=480 Win=6432 Len=1380
     32 4.356264  65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [ACK] Seq=15181 Ack=480 Win=6432 Len=1380
     33 4.356264  145.254.160.237  65.208.228.223   TCP        54 3372 → 80 [ACK] Seq=480 Ack=16561 Win=9660 Len=0
     34 4.496465  65.208.228.223   145.254.160.237  TCP      1434 80 → 3372 [ACK] Seq=16561 Ack=480 Win=6432 Len=1380
     35 4.496465  145.254.160.237  65.208.228.223   TCP        54 3372 → 80 [ACK] Seq=480 Ack=17941 Win=9660 Len=0
     36 4.776868  216.239.59.99    145.254.160.237  TCP      1484 [TCP Spurious Retransmission] 80 → 3371 [PSH, ACK]
     37 4.776868  145.254.160.237  216.239.59.99    TCP        54 [TCP Dup ACK 28#1] 3371 → 80 [ACK] Seq=722 Ack=1591
     38 4.846969  65.208.228.223   145.254.160.237  HTTP/X…   478 HTTP/1.1 200 OK
```

```
> Frame 18: 775 bytes on wire (6200 bits), 775 bytes c
> Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00)
> Internet Protocol Version 4, Src: 145.254.160.237, [
> Transmission Control Protocol, Src Port: 3371, Dst F
> Hypertext Transfer Protocol
```

```
0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00   ·· ····· ······E·
0010  02 f9 0f 4d 40 00 80 06  a1 73 91 fe a0 ed d8 ef   ···M@··· ·s······
0020  3b 63 0d 2b 00 50 36 c2  1e 28 2e 6b 53 84 50 18   ;c·+·P6· ·(.kS·P·
0030  22 38 0b 64 00 00 47 45  54 20 2f 70 61 67 65 61   "8·d··GE T /pagea
0040  64 2f 61 64 73 3f 63 6c  69 65 6e 74 3d 63 61 2d   d/ads?cl ient=ca-
0050  70 75 62 2d 32 33 30 39  31 39 31 39 34 38 36 37   pub-2309 19194867
0060  33 36 32 39 26 72 61 6e  64 6f 6d 3d 31 30 38 34   3629&ran dom=1084
0070  34 34 33 34 33 30 32 38  35 26 6c 6d 74 3d 31 30   44343028 5&lmt=10
0080  38 32 34 36 37 30 32 30  26 66 6f 72 6d 61 74 3d   82467020 &format=
0090  34 36 38 78 36 30 5f 61  73 26 6f 75 74 70 75 74   468x60_a s&output
00a0  3d 68 74 6d 6c 26 75 72  6c 3d 68 74 74 70 25 33   =html&ur l=http%3
00b0  41 25 32 46 25 32 46 77  77 77 2e 65 74 68 65 72   A%2F%2Fw ww.ether
00c0  65 61 6c 2e 63 6f 6d 25  32 46 64 6f 77 6e 6c 6f   eal.com% 2Fdownlo
00d0  61 64 2e 68 74 6d 6c 26  63 6f 6c 6f 72 5f 62 67   ad.html& color_bg
00e0  3d 46 46 46 46 46 46 26  63 6f 6c 6f 72 5f 74 65   =FFFFFF& color_te
00f0  78 74 3d 33 33 33 33 33  33 26 63 6f 6c 6f 72 5f   xt=33333 3&color_
```

Figure 7: Capture file http.cap open on Wireshark

It is important to create filters that show only packets according to a filtering rule to facilitate the analysis of a given capture. This will isolate the particular exchange or the analysis of a specific protocol. For that, we use the **Filter** section in the top bar, highlighted in Figure 8.

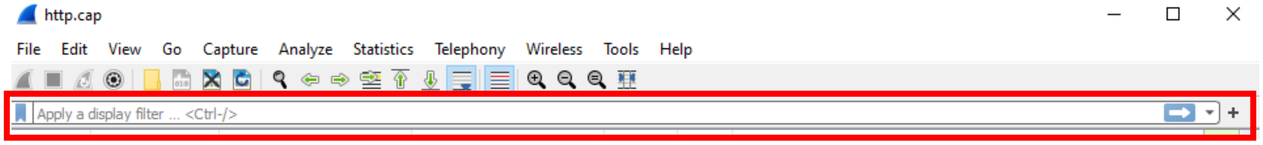

http.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Figure 8: Feature which allow filtering packets for display purposes.

You can create filtering rules. A rule is based on the different packet header fields for known protocols.

- Type the rule **http** (under "*Apply a display filter*") and either click on the (blue) forward arrow on the right or just press **Enter**.
  The number of packets displayed will reduce from 43 to 4.

Click on the “X” (red) button that appears before the arrow to remove the filtering rule.

- Type the rule **ip.dst==145.254.160.237** and press **Enter**.
  The number of packets displayed will reduce from 43 to 23.
  Remove the filtering rule.

You can create multiple combined filtering rules using the following operators:

  - **&&** (AND)
  - **||** (OR)
  - **!** (NOT)

For example, if we want all packets with an IP destination equal to 145.254.160.237 and with a source or destination port different from 80:

- Type the rule **ip.dst == 145.254.160.237 && !tcp.port == 80** and press **Enter**.
  The number of packets displayed will reduce from 43 to 1.
  Remove the filtering rule.

Read more about *Display Filtering* and examples in:

https://wiki.wireshark.org/DisplayFilters

You can also provide some description for the filter from “+” button, highlighted in Figure 9 to describe the functionality and why the filter is created.

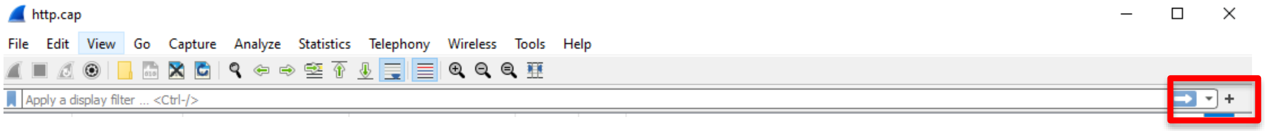


Figure 9: Provide description to the filter using “+” button.

The http.cap file is no longer needed, so close it.

Analysing local ICMP traffic

In this part, you will ping another PC on the LAN (illustrated in Figure 10) and capture **ICMP requests and replies** using Wireshark. You will also look inside the packets captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

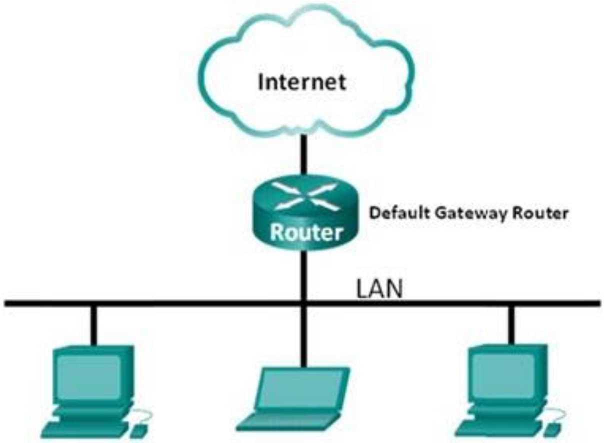
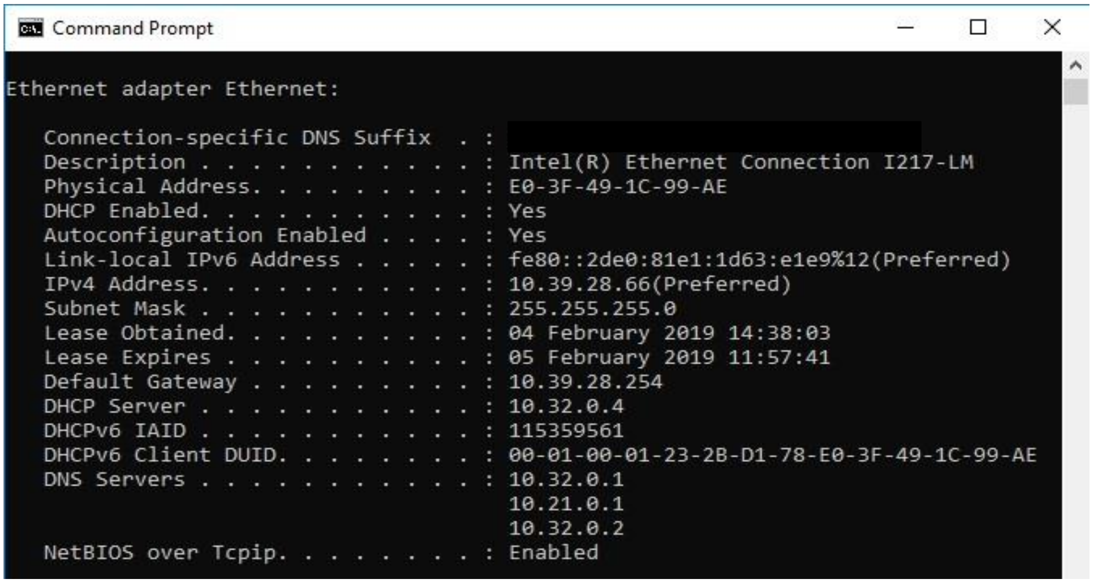


Figure 10: Typical LAN topology.

Step 1: Retrieve your PC's interface addresses.

For this lab, you will need to retrieve your PC's IP address and its network interface card (NIC) physical address, also called the MAC address.

a. Open a command prompt window: **Start → cmd (select *Command Prompt*)**
b. Type **ipconfig /all**, and then press **Enter**.
c. Note your PC interface's IP address and MAC (physical) address, as shown in Figure 11.



```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : [redacted]
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection I217-LM
   Physical Address. . . . . . . . . : E0-3F-49-1C-99-AE
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2de0:81e1:1d63:e1e9%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.39.28.66(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 04 February 2019 14:38:03
   Lease Expires . . . . . . . . . . : 05 February 2019 11:57:41
   Default Gateway . . . . . . . . . : 10.39.28.254
   DHCP Server . . . . . . . . . . . : 10.32.0.4
   DHCPv6 IAID . . . . . . . . . . . : 115359561
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-2B-D1-78-E0-3F-49-1C-99-AE
   DNS Servers . . . . . . . . . . . : 10.32.0.1
                                       10.21.0.1
                                       10.32.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Figure 11: Output of command ipconfig /all

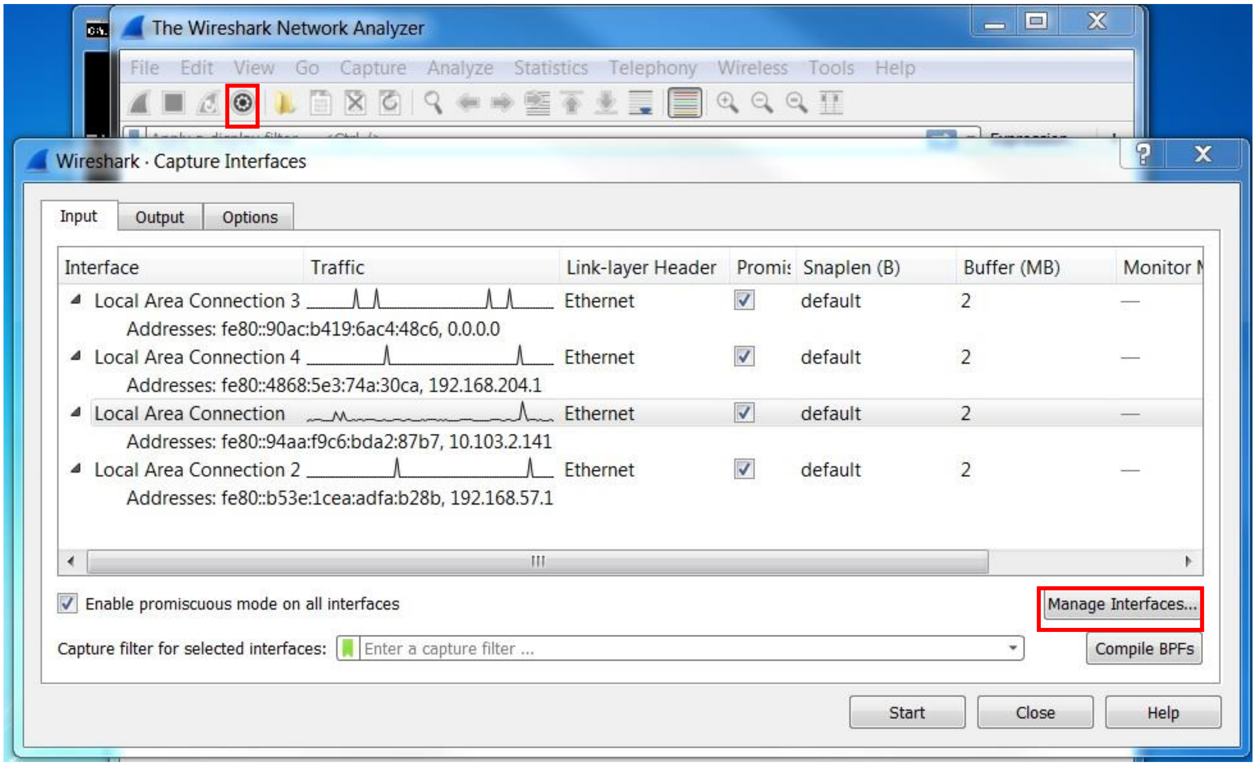
d. Ask a colleague for him/her PC’s IP address and provide your PC’s IP address to him/her. Do not provide your MAC address at this time.

Step 2: Start Wireshark and begin capturing data.

a. On your PC, **launch Wireshark**.

b. After Wireshark starts, click on the **Capture Interfaces** (round icon highlighted in Figure 12).
Several LAN connections may appear. When multiple interfaces are listed and you are unsure which interface to capture, proceed to the next step (2c).

c. Expand each arrow beside the interfaces to see details, see Figure 12.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Capture Interfaces
Input
Output
Options
Manage Interfaces...
Compile BPFs
Start
Close
Help

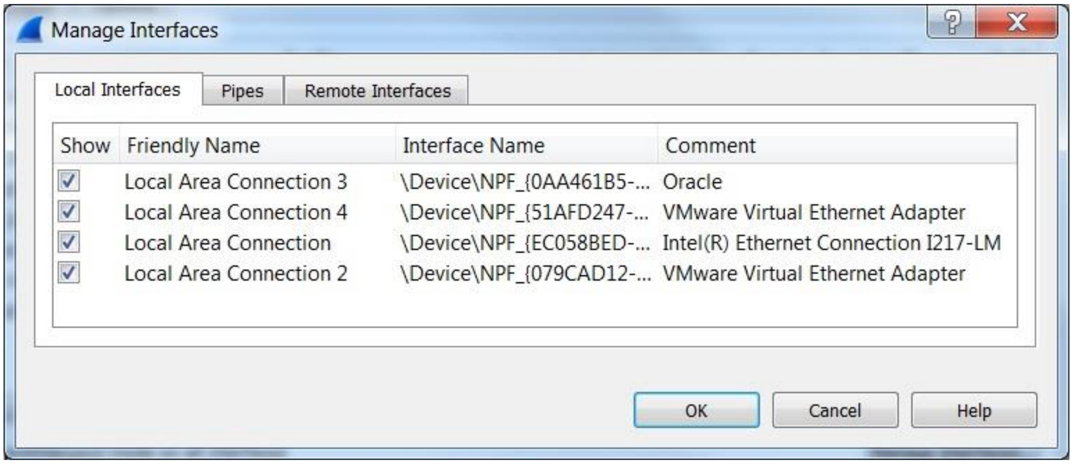
Interface	Traffic	Link-layer Header	Promis	Snaplen (B)	Buffer (MB)	Monitor M
Local Area Connection 3		Ethernet	☑	default	2	—
Addresses: fe80::90ac:b419:6ac4:48c6, 0.0.0.0						
Local Area Connection 4		Ethernet	☑	default	2	—
Addresses: fe80::4868:5e3:74a:30ca, 192.168.204.1						
Local Area Connection		Ethernet	☑	default	2	—
Addresses: fe80::94aa:f9c6:bda2:87b7, 10.103.2.141						
Local Area Connection 2		Ethernet	☑	default	2	—
Addresses: fe80::b53e:1cea:adfa:b28b, 192.168.57.1						

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Figure 12: Selecting an interface to capture.

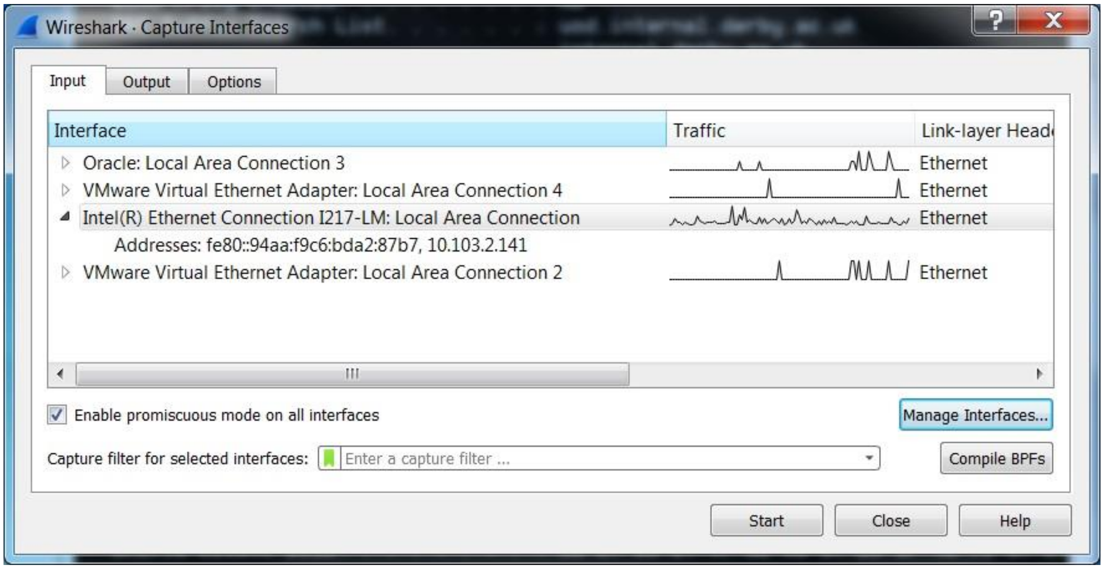
d. Click on the **Manage Interfaces** button (also highlighted in Figure 12) to see further details as illustrated in Figure 13.



Show	Friendly Name	Interface Name	Comment
☑	Local Area Connection 3	\Device\NPF_{0AA461B5-...	Oracle
☑	Local Area Connection 4	\Device\NPF_{51AFD247-...	VMware Virtual Ethernet Adapter
☑	Local Area Connection	\Device\NPF_{EC058BED-...	Intel(R) Ethernet Connection I217-LM
☑	Local Area Connection 2	\Device\NPF_{079CAD12-...	VMware Virtual Ethernet Adapter

Figure 13: Manage Interfaces screen.

e. Go back to the Capture Interfaces screen. If you click “Cancel”, you simply go back to the Capture Interface screen as it was displayed previously. If you click “OK”, the Capture Interfaces screen will display the list of interfaces with updates names, as shown in Figure 14.



Wireshark · Capture Interfaces

Input | Output | Options

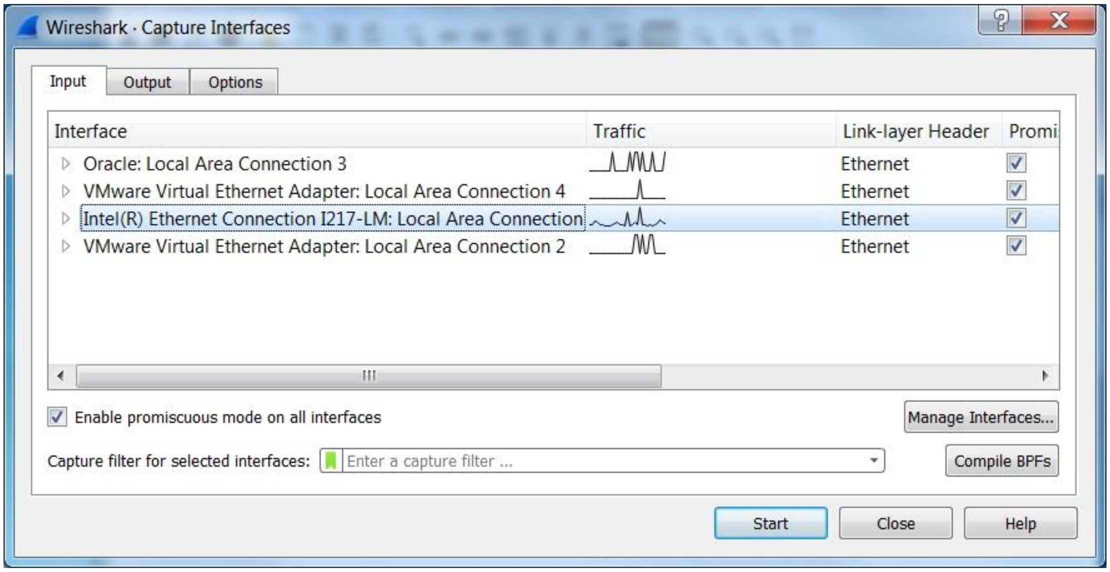
Interface	Traffic	Link-layer Head
Oracle: Local Area Connection 3		Ethernet
VMware Virtual Ethernet Adapter: Local Area Connection 4		Ethernet
Intel(R) Ethernet Connection I217-LM: Local Area Connection Addresses: fe80::94aa:f9c6:bda2:87b7, 10.103.2.141		Ethernet
VMware Virtual Ethernet Adapter: Local Area Connection 2		Ethernet

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Figure 14: Updated interface names.

f. Identify the interface related to the IP address of your PC.
g. Select the correct interface, as illustrated in Figure 15.
h. Click **Start** to initiate the data capture.



Wireshark · Capture Interfaces

Input | Output | Options

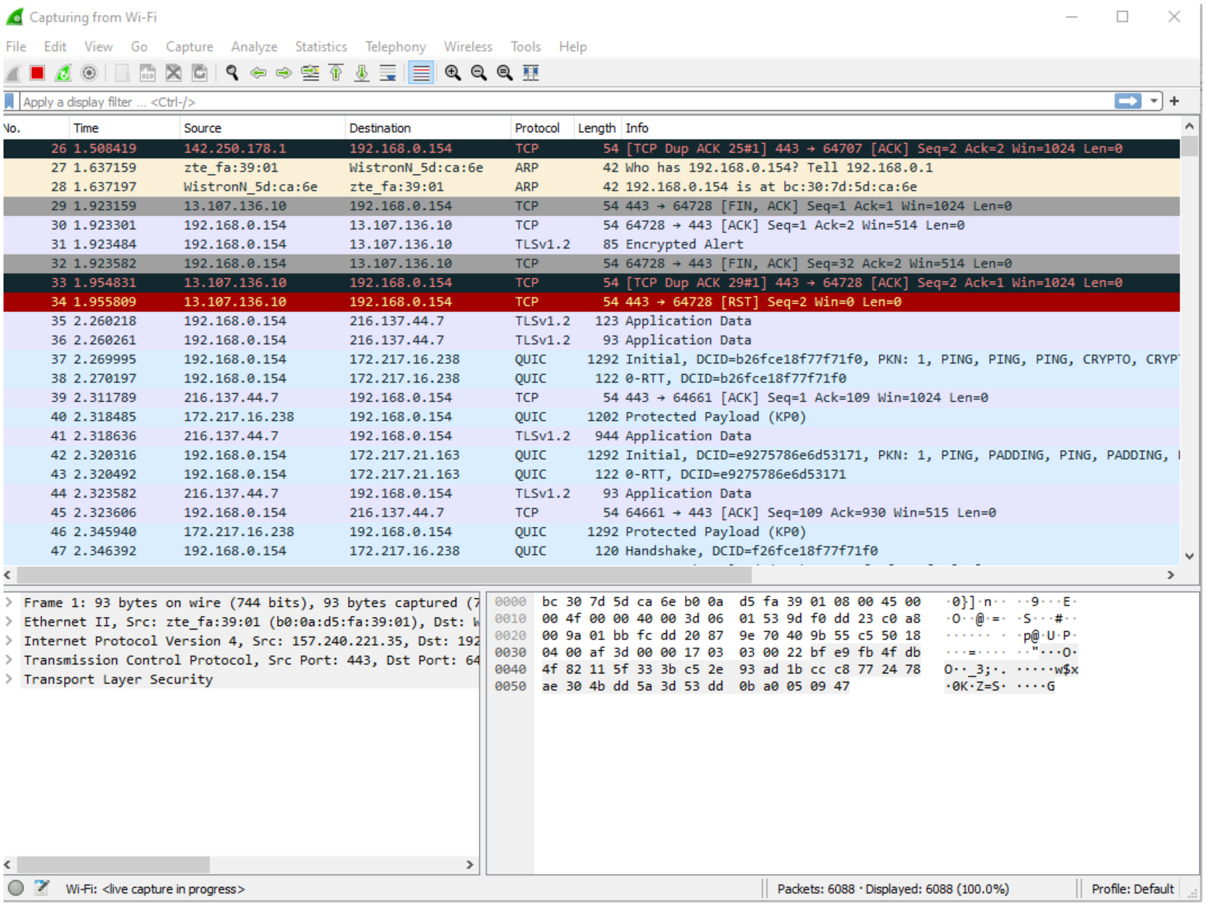
Interface	Traffic	Link-layer Header	Promi
Oracle: Local Area Connection 3		Ethernet	☑
VMware Virtual Ethernet Adapter: Local Area Connection 4		Ethernet	☑
Intel(R) Ethernet Connection I217-LM: Local Area Connection		Ethernet	☑
VMware Virtual Ethernet Adapter: Local Area Connection 2		Ethernet	☑

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Figure 15: Interface selected for start of data capture.

Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol, as shown in Figure 16.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time       Source              Destination        Protocol  Length Info
     26 1.508419   142.250.178.1       192.168.0.154      TCP         54 [TCP Dup ACK 25#1] 443 → 64707 [ACK] Seq=2 Ack=2 Win=1024 Len=0
     27 1.637159   zte_fa:39:01        WistronN_5d:ca:6e  ARP         42 Who has 192.168.0.154? Tell 192.168.0.1
     28 1.637197   WistronN_5d:ca:6e   zte_fa:39:01       ARP         42 192.168.0.154 is at bc:30:7d:5d:ca:6e
     29 1.923159   13.107.136.10       192.168.0.154      TCP         54 443 → 64728 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
     30 1.923301   192.168.0.154       13.107.136.10      TCP         54 64728 → 443 [ACK] Seq=1 Ack=2 Win=514 Len=0
     31 1.923484   192.168.0.154       13.107.136.10      TLSv1.2     85 Encrypted Alert
     32 1.923582   192.168.0.154       13.107.136.10      TCP         54 64728 → 443 [FIN, ACK] Seq=32 Ack=2 Win=514 Len=0
     33 1.954831   13.107.136.10       192.168.0.154      TCP         54 [TCP Dup ACK 29#1] 443 → 64728 [ACK] Seq=2 Ack=1 Win=1024 Len=0
     34 1.955809   13.107.136.10       192.168.0.154      TCP         54 443 → 64728 [RST] Seq=2 Win=0 Len=0
     35 2.260218   192.168.0.154       216.137.44.7       TLSv1.2    123 Application Data
     36 2.260261   192.168.0.154       216.137.44.7       TLSv1.2     93 Application Data
     37 2.269995   192.168.0.154       172.217.16.238     QUIC      1292 Initial, DCID=b26fce18f77f71f0, PKN: 1, PING, PING, PING, CRYPTO, CRYP
     38 2.270197   192.168.0.154       172.217.16.238     QUIC       122 0-RTT, DCID=b26fce18f77f71f0
     39 2.311789   216.137.44.7        192.168.0.154      TCP         54 443 → 64661 [ACK] Seq=1 Ack=109 Win=1024 Len=0
     40 2.318485   172.217.16.238      192.168.0.154      QUIC      1202 Protected Payload (KP0)
     41 2.318636   216.137.44.7        192.168.0.154      TLSv1.2    944 Application Data
     42 2.320316   192.168.0.154       172.217.21.163     QUIC      1292 Initial, DCID=e9275786e6d53171, PKN: 1, PING, PADDING, PING, PADDING,
     43 2.320492   192.168.0.154       172.217.21.163     QUIC       122 0-RTT, DCID=e9275786e6d53171
     44 2.323582   216.137.44.7        192.168.0.154      TLSv1.2     93 Application Data
     45 2.323606   192.168.0.154       216.137.44.7       TCP         54 64661 → 443 [ACK] Seq=109 Ack=930 Win=515 Len=0
     46 2.345940   172.217.16.238      192.168.0.154      QUIC      1292 Protected Payload (KP0)
     47 2.346392   192.168.0.154       172.217.16.238     QUIC       120 Handshake, DCID=f26fce18f77f71f0
```

```
> Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (7
> Ethernet II, Src: zte_fa:39:01 (b0:0a:d5:fa:39:01), Dst: W
> Internet Protocol Version 4, Src: 157.240.221.35, Dst: 192
> Transmission Control Protocol, Src Port: 443, Dst Port: 64
> Transport Layer Security
```

```
0000  bc 30 7d 5d ca 6e b0 0a  d5 fa 39 01 08 00 45 00   ·0}]·n·· ··9···E·
0010  00 4f 00 00 40 00 3d 06  01 53 9d f0 dd 23 c0 a8   ·O··@·=· ·S···#··
0020  00 9a 01 bb fc dd 20 87  9e 70 40 9b 55 c5 50 18   ······ · ·p@·U·P·
0030  04 00 af 3d 00 00 17 03  03 00 22 bf e9 fb 4f db   ···=···· ··"···O·
0040  4f 82 11 5f 33 3b c5 2e  93 ad 1b cc c8 77 24 78   O··_3;·. ·····w$x
0050  ae 30 4b dd 5a 3d 53 dd  0b a0 05 09 47            ·0K·Z=S· ····G
```

Wi-Fi: <live capture in progress>

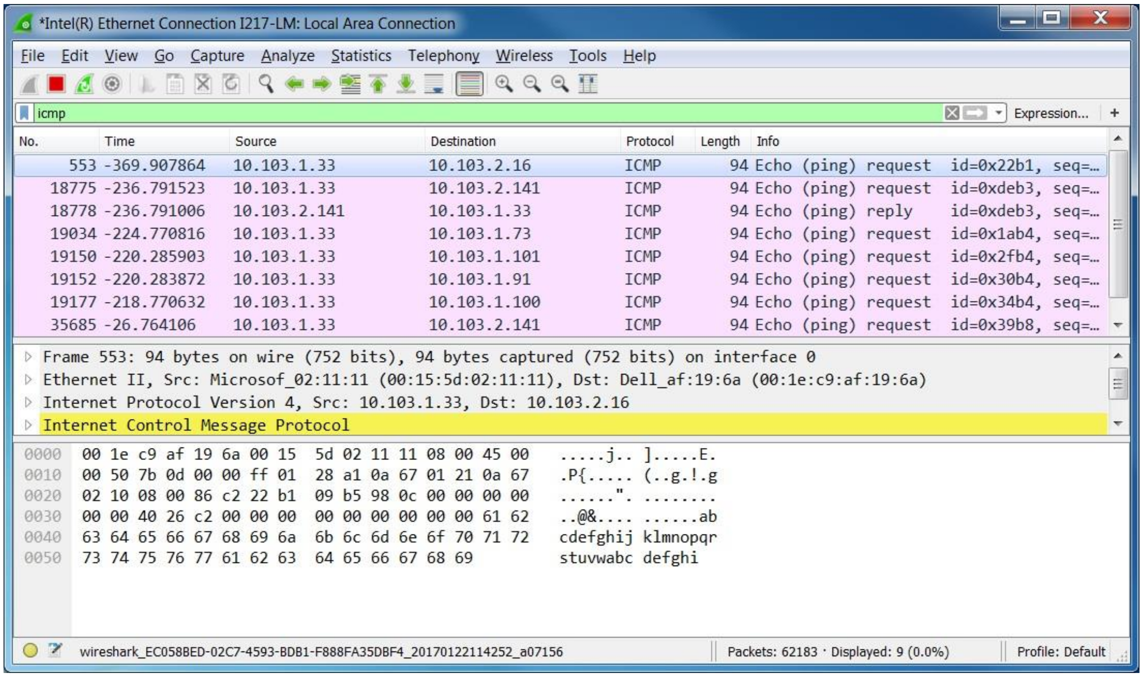
Packets: 6088 · Displayed: 6088 (100.0%)

Profile: Default

Figure 16: Live capture of the selected interface.

This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN.

Since we are only interested in displaying ICMP (ping) PDUs, you should apply a filter as discussed in part I of this tutorial. This filtering is illustrated in Figure 17.


*Intel(R) Ethernet Connection I217-LM: Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

icmp

No.	Time	Source	Destination	Protocol	Length	Info
553	-369.907864	10.103.1.33	10.103.2.16	ICMP	94	Echo (ping) request id=0x22b1, seq=…
18775	-236.791523	10.103.1.33	10.103.2.141	ICMP	94	Echo (ping) request id=0xdeb3, seq=…
18778	-236.791006	10.103.2.141	10.103.1.33	ICMP	94	Echo (ping) reply id=0xdeb3, seq=…
19034	-224.770816	10.103.1.33	10.103.1.73	ICMP	94	Echo (ping) request id=0x1ab4, seq=…
19150	-220.285903	10.103.1.33	10.103.1.101	ICMP	94	Echo (ping) request id=0x2fb4, seq=…
19152	-220.283872	10.103.1.33	10.103.1.91	ICMP	94	Echo (ping) request id=0x30b4, seq=…
19177	-218.770632	10.103.1.33	10.103.1.100	ICMP	94	Echo (ping) request id=0x34b4, seq=…
35685	-26.764106	10.103.1.33	10.103.2.141	ICMP	94	Echo (ping) request id=0x39b8, seq=…

```
▷ Frame 553: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
▷ Ethernet II, Src: Microsof_02:11:11 (00:15:5d:02:11:11), Dst: Dell_af:19:6a (00:1e:c9:af:19:6a)
▷ Internet Protocol Version 4, Src: 10.103.1.33, Dst: 10.103.2.16
▷ Internet Control Message Protocol
```

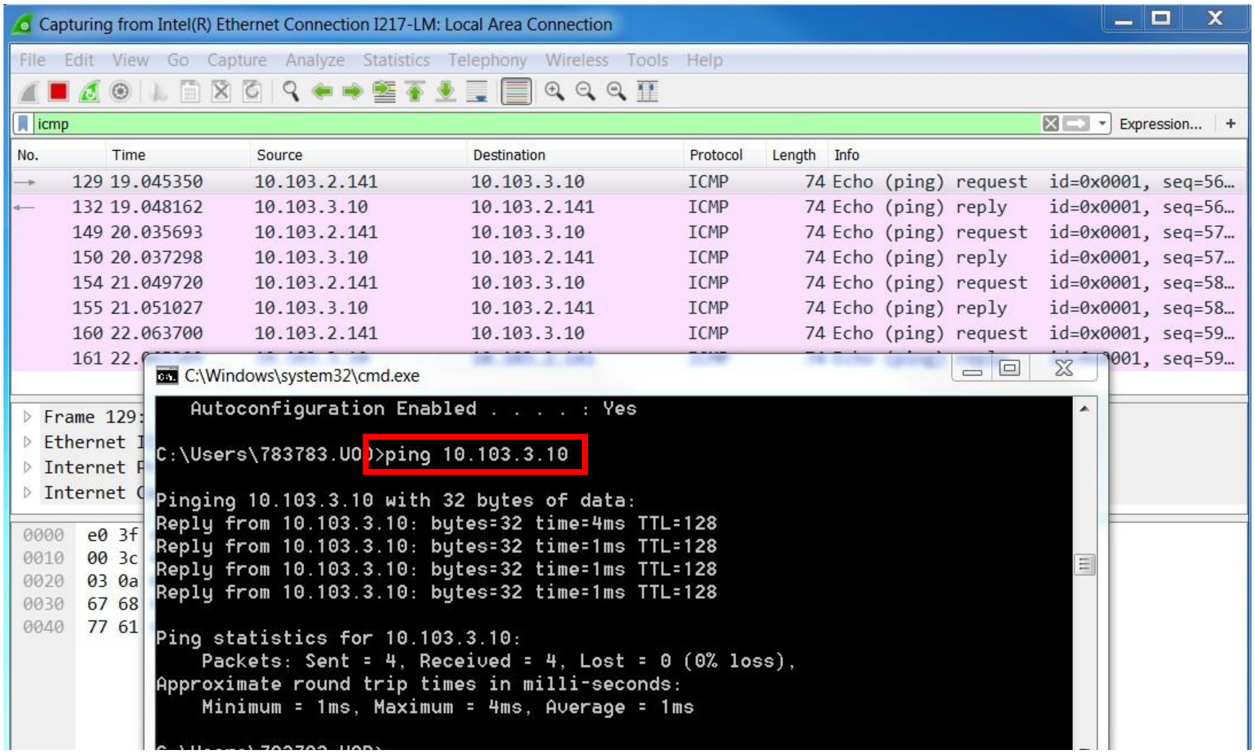
```
0000  00 1e c9 af 19 6a 00 15  5d 02 11 11 08 00 45 00   .....j.. ].....E.
0010  00 50 7b 0d 00 00 ff 01  28 a1 0a 67 01 21 0a 67   .P{..... (..g.!.g
0020  02 10 08 00 86 c2 22 b1  09 b5 98 0c 00 00 00 00   ......". ........
0030  00 00 40 26 c2 00 00 00  00 00 00 00 00 00 61 62   ..@&.... ......ab
0040  63 64 65 66 67 68 69 6a  6b 6c 6d 6e 6f 70 71 72   cdefghij klmnopqr
0050  73 74 75 76 77 61 62 63  64 65 66 67 68 69         stuvwabc defghi
```

wireshark_EC058BED-02C7-4593-BDB1-F888FA35DBF4_20170122114252_a07156 | Packets: 62183 · Displayed: 9 (0.0%) | Profile: Default

Figure 17: Data capture filtered to shown only ICMP PDUs.

This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Make sure you go to the last packet captured – you can do that in two ways: via the **Go** menu or using the key combination **Ctrl+End**.

a. Bring forward the command prompt window that you opened earlier and ping the IP address that you received from a colleague – refer to Figure 18.
   Notice that you start seeing data related to this ping appearing in the top window of Wireshark again.



Capturing from Intel(R) Ethernet Connection I217-LM: Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression…
+
C:\Windows\system32\cmd.exe

```
No.   Time         Source          Destination     Protocol  Length  Info
  129 19.045350    10.103.2.141    10.103.3.10     ICMP        74 Echo (ping) request  id=0x0001, seq=56…
  132 19.048162    10.103.3.10     10.103.2.141    ICMP        74 Echo (ping) reply    id=0x0001, seq=56…
  149 20.035693    10.103.2.141    10.103.3.10     ICMP        74 Echo (ping) request  id=0x0001, seq=57…
  150 20.037298    10.103.3.10     10.103.2.141    ICMP        74 Echo (ping) reply    id=0x0001, seq=57…
  154 21.049720    10.103.2.141    10.103.3.10     ICMP        74 Echo (ping) request  id=0x0001, seq=58…
  155 21.051027    10.103.3.10     10.103.2.141    ICMP        74 Echo (ping) reply    id=0x0001, seq=58…
  160 22.063700    10.103.2.141    10.103.3.10     ICMP        74 Echo (ping) request  id=0x0001, seq=59…
  161 22.                                                                             001, seq=59…
```

```
▷ Frame 129:
▷ Ethernet I
▷ Internet P
▷ Internet C

0000  e0 3f
0010  00 3c
0020  03 0a
0030  67 68
0040  77 61
```

```
   Autoconfiguration Enabled . . . . : Yes

C:\Users\783783.UOD>ping 10.103.3.10

Pinging 10.103.3.10 with 32 bytes of data:
Reply from 10.103.3.10: bytes=32 time=4ms TTL=128
Reply from 10.103.3.10: bytes=32 time=1ms TTL=128
Reply from 10.103.3.10: bytes=32 time=1ms TTL=128
Reply from 10.103.3.10: bytes=32 time=1ms TTL=128

Ping statistics for 10.103.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 1ms
```

Figure 18: Pinging a colleague's PC and viewing ICMP packets.

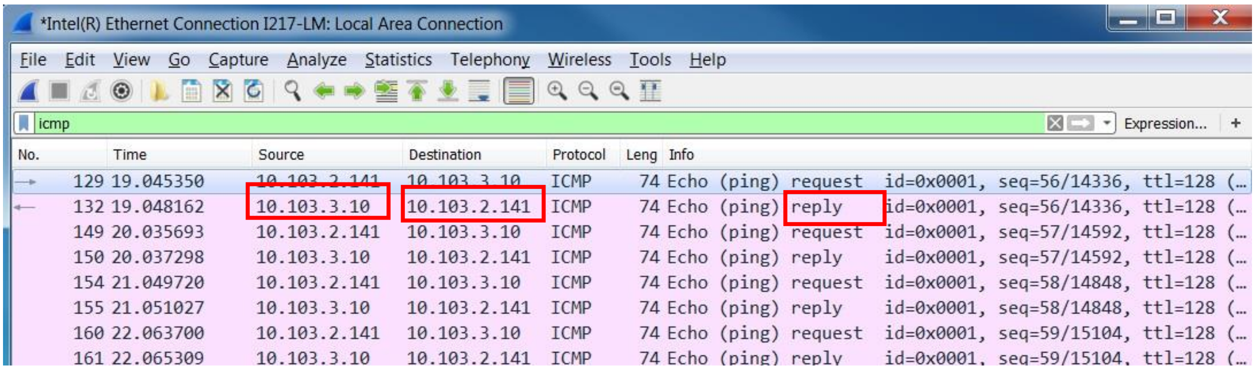
b. Stop capturing data by clicking the **Stop Capture** (red) icon.

Step 3: Examine the captured data.

In Step 3, examine the data that was generated by the ping requests to your colleague’s PC and respective replies. As you know, Wireshark data is displayed in three sections:

1. The **top section** displays the list of PDU frames captured with a summary of the IP packet information listed.
2. The **bottom left section** lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers.
3. The **bottom right section** displays the raw data of each layer. The raw data is displayed in both hexadecimal and ASCII formats.

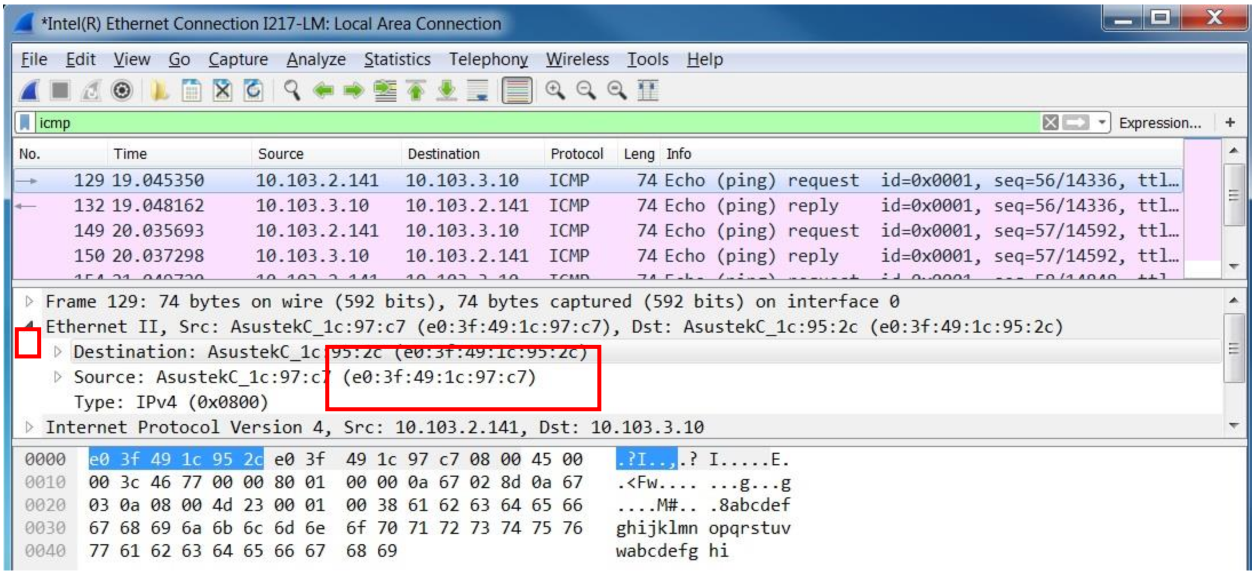
a. Click on an ICMP request PDU frame in the top section of Wireshark. Notice that the *Source* column has your PC's IP address, and the *Destination* contains the IP address of the colleague's PC you pinged. Refer to Figure 19.


*Intel(R) Ethernet Connection I217-LM: Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
+

```
No.     Time        Source         Destination    Protocol Leng Info
  129 19.045350    10.103.2.141   10.103.3.10    ICMP     74 Echo (ping) request  id=0x0001, seq=56/14336, ttl=128 (…
  132 19.048162    10.103.3.10    10.103.2.141   ICMP     74 Echo (ping) reply    id=0x0001, seq=56/14336, ttl=128 (…
  149 20.035693    10.103.2.141   10.103.3.10    ICMP     74 Echo (ping) request  id=0x0001, seq=57/14592, ttl=128 (…
  150 20.037298    10.103.3.10    10.103.2.141   ICMP     74 Echo (ping) reply    id=0x0001, seq=57/14592, ttl=128 (…
  154 21.049720    10.103.2.141   10.103.3.10    ICMP     74 Echo (ping) request  id=0x0001, seq=58/14848, ttl=128 (…
  155 21.051027    10.103.3.10    10.103.2.141   ICMP     74 Echo (ping) reply    id=0x0001, seq=58/14848, ttl=128 (…
  160 22.063700    10.103.2.141   10.103.3.10    ICMP     74 Echo (ping) request  id=0x0001, seq=59/15104, ttl=128 (…
  161 22.065309    10.103.3.10    10.103.2.141   ICMP     74 Echo (ping) reply    id=0x0001, seq=59/15104, ttl=128 (…
```

Figure 19: Analysing ICMP requests in the top section of Wireshark.

b. With this PDU frame still selected in the top section, navigate to the **bottom left section**. Click the **right arrow** of the Ethernet II row (highlighted in Figure 20) to view the Destination and Source MAC addresses (see Figure 20).


*Intel(R) Ethernet Connection I217-LM: Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
+

```
No.     Time        Source         Destination    Protocol Leng Info
  129 19.045350    10.103.2.141   10.103.3.10    ICMP     74 Echo (ping) request  id=0x0001, seq=56/14336, ttl…
  132 19.048162    10.103.3.10    10.103.2.141   ICMP     74 Echo (ping) reply    id=0x0001, seq=56/14336, ttl…
  149 20.035693    10.103.2.141   10.103.3.10    ICMP     74 Echo (ping) request  id=0x0001, seq=57/14592, ttl…
  150 20.037298    10.103.3.10    10.103.2.141   ICMP     74 Echo (ping) reply    id=0x0001, seq=57/14592, ttl…
```

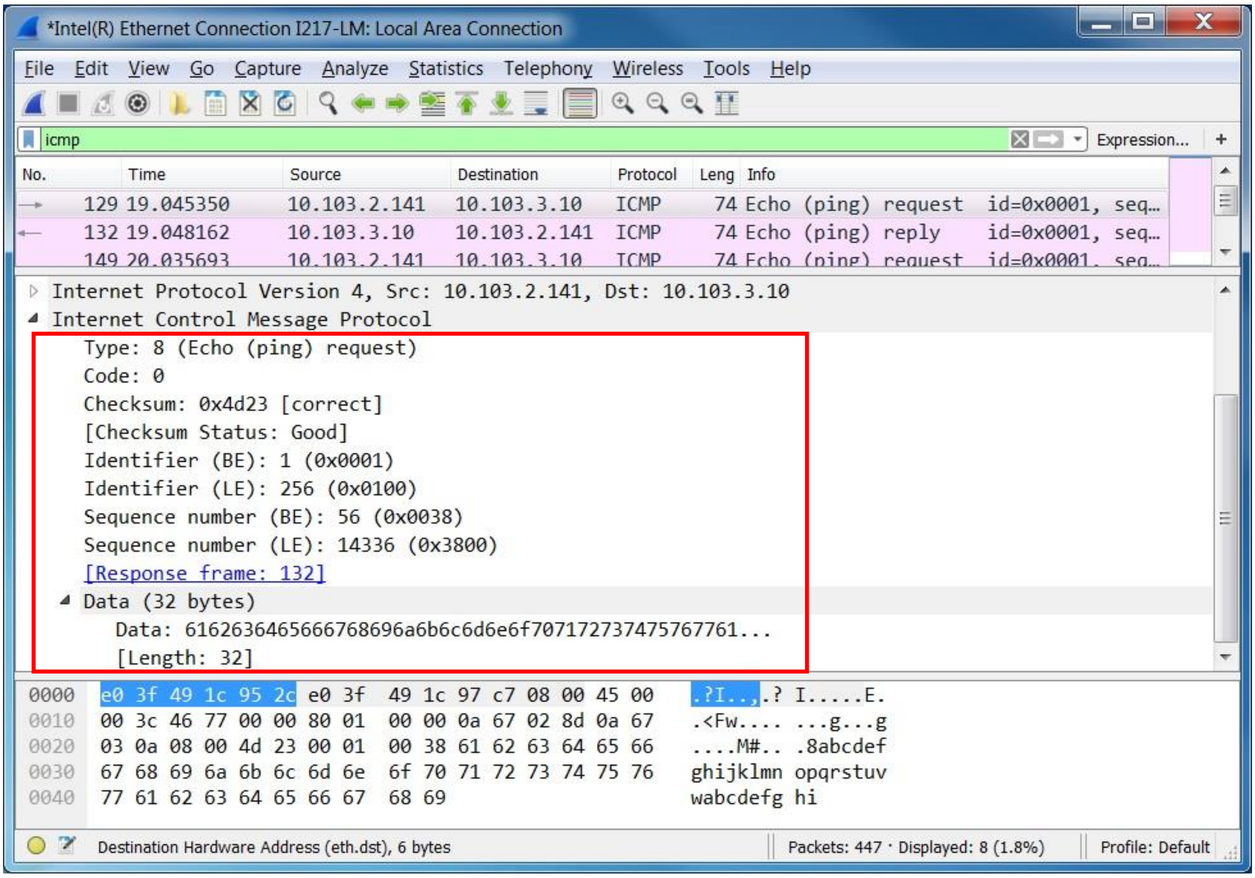
```
▷ Frame 129: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
◢ Ethernet II, Src: AsustekC_1c:97:c7 (e0:3f:49:1c:97:c7), Dst: AsustekC_1c:95:2c (e0:3f:49:1c:95:2c)
  ▷ Destination: AsustekC_1c:95:2c (e0:3f:49:1c:95:2c)
  ▷ Source: AsustekC_1c:97:c7 (e0:3f:49:1c:97:c7)
    Type: IPv4 (0x0800)
▷ Internet Protocol Version 4, Src: 10.103.2.141, Dst: 10.103.3.10
```

```
0000  e0 3f 49 1c 95 2c e0 3f  49 1c 97 c7 08 00 45 00   .?I..,.? I.....E.
0010  00 3c 46 77 00 00 80 01  00 00 0a 67 02 8d 0a 67   .<Fw.... ...g...g
0020  03 0a 08 00 4d 23 00 01  00 38 61 62 63 64 65 66   ....M#.. .8abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Figure 20: PDU information for the ICMP request selected on the top part of the screen.

- Does the Source MAC address match your PC's interface?
- Does the Destination MAC address match the MAC address that of your colleague's?
- How is the MAC address of the pinged PC obtained by your PC?

Note: As you can see on the captured ICMP request/reply, ICMP data is encapsulated inside an IPv4 packet PDU (IPv4 header) which is then encapsulated in an Ethernet II frame PDU (Ethernet II header) for transmission on the LAN, as seen in the lecture. Figure 21 illustrates the encapsulation and the ICMP data/payload.


*Intel(R) Ethernet Connection I217-LM: Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...

```
No.    Time       Source        Destination   Protocol Leng Info
129 19.045350  10.103.2.141  10.103.3.10   ICMP     74 Echo (ping) request  id=0x0001, seq…
132 19.048162  10.103.3.10   10.103.2.141  ICMP     74 Echo (ping) reply    id=0x0001, seq…
149 20.035693  10.103.2.141  10.103.3.10   ICMP     74 Echo (ping) request  id=0x0001, seq…
```

```
▷ Internet Protocol Version 4, Src: 10.103.2.141, Dst: 10.103.3.10
◢ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d23 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 56 (0x0038)
    Sequence number (LE): 14336 (0x3800)
    [Response frame: 132]
  ◢ Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677761...
      [Length: 32]
```

```
0000  e0 3f 49 1c 95 2c e0 3f  49 1c 97 c7 08 00 45 00   .?I..,.? I.....E.
0010  00 3c 46 77 00 00 80 01  00 00 0a 67 02 8d 0a 67   .<Fw.... ...g...g
0020  03 0a 08 00 4d 23 00 01  00 38 61 62 63 64 65 66   ....M#.. .8abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Destination Hardware Address (eth.dst), 6 bytes | Packets: 447 · Displayed: 8 (1.8%) | Profile: Default

Figure 21: Content of the encapsulated ICMP data/payload.

If you want, you can save this capture via the **File** → **Save As** option from the menu or simply close it without saving via **File** → **Close, Continue without Saving.**

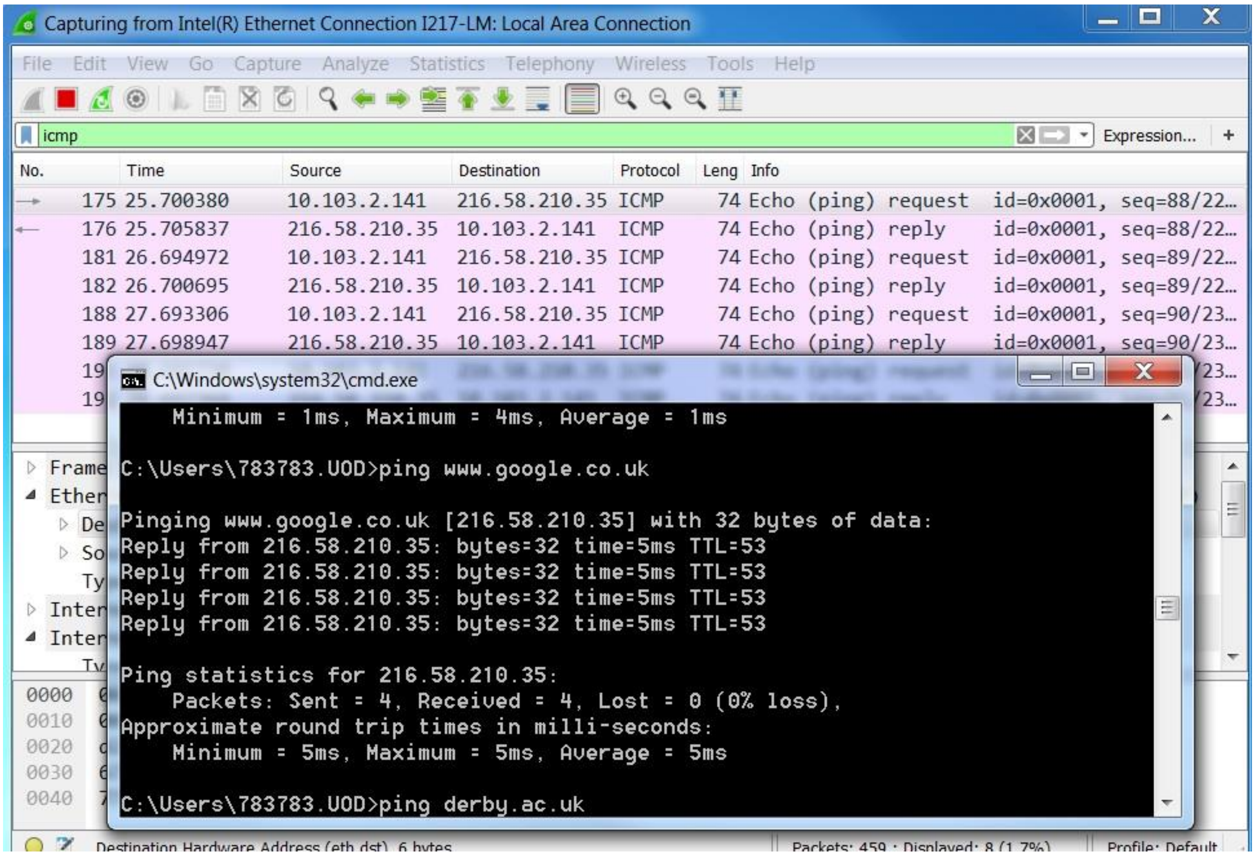
Analysing remote ICMP traffic ping

You will now ping remote hosts (hosts not on the LAN) and examine the generated data from those pings. You will then determine what is different about this data from the data examined for the local ping.

Step 1: Start capturing data on interface.

a. Click on the **Capture Interfaces** icon to bring up the list of interfaces again.
b. Make sure you select the LAN interface, and then click **Start**.
c. With the capture active, ping the following three website URLs – please note that you should ping the first, wait for a few replies, then the second and so on. Just pressing **Enter**, will cause a new command prompt to appear. Figure 22 illustrates the process.
   - www.google.co.uk
   - www.warwick.ac.uk
   - www.bbc.co.uk

You can stop capturing data by clicking on the (red) **Stop Capture** icon when you are done.


Capturing from Intel(R) Ethernet Connection I217-LM: Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
C:\Windows\system32\cmd.exe

```
No.   Time        Source         Destination    Protocol Leng Info
  175 25.700380   10.103.2.141   216.58.210.35  ICMP       74 Echo (ping) request  id=0x0001, seq=88/22…
  176 25.705837   216.58.210.35  10.103.2.141   ICMP       74 Echo (ping) reply    id=0x0001, seq=88/22…
  181 26.694972   10.103.2.141   216.58.210.35  ICMP       74 Echo (ping) request  id=0x0001, seq=89/22…
  182 26.700695   216.58.210.35  10.103.2.141   ICMP       74 Echo (ping) reply    id=0x0001, seq=89/22…
  188 27.693306   10.103.2.141   216.58.210.35  ICMP       74 Echo (ping) request  id=0x0001, seq=90/23…
  189 27.698947   216.58.210.35  10.103.2.141   ICMP       74 Echo (ping) reply    id=0x0001, seq=90/23…
```

```
    Minimum = 1ms, Maximum = 4ms, Average = 1ms

C:\Users\783783.UOD>ping www.google.co.uk

Pinging www.google.co.uk [216.58.210.35] with 32 bytes of data:
Reply from 216.58.210.35: bytes=32 time=5ms TTL=53
Reply from 216.58.210.35: bytes=32 time=5ms TTL=53
Reply from 216.58.210.35: bytes=32 time=5ms TTL=53
Reply from 216.58.210.35: bytes=32 time=5ms TTL=53

Ping statistics for 216.58.210.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms

C:\Users\783783.UOD>ping derby.ac.uk
```

Destination Hardware Address (eth.dst), 6 bytes | Packets: 459 · Displayed: 8 (1.7%) | Profile: Default

Figure 22: Pinging website URLs and viewing ICMP data in Wireshark.

Step 2: Examining and analyzing the data from the remote hosts.

Review the captured data in Wireshark. When you ping the URLs listed, notice that the Domain Name Server (DNS) translates each URL to an IP address. Therefore, it will be helpful to remove the "icmp" filter to see the packets related to the *DNS query* and the *DNS query response* for each URL. Figure 23 illustrates the removal of the filter and a DNS query.

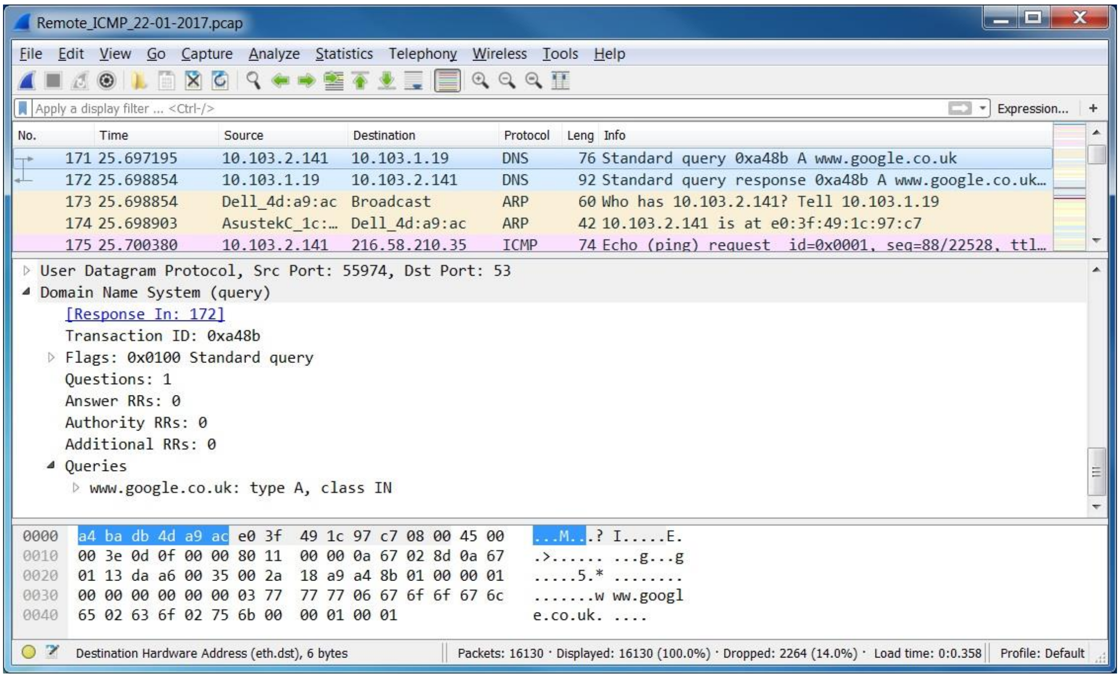
Tip: It might be helpful to use filter "**dns**" first and then "**icmp**".

Make note of the IP address corresponding to each URL you pinged and recover their corresponding MAC addresses.

www.google.co.uk - IP: MAC:
www.warwick.ac.uk - IP: MAC:
www.bbc.co.uk - IP: MAC:

- What is significant about this information?

- How does this information differ from the local ping information you obtained before?



Remote_ICMP_22-01-2017.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

No.	Time	Source	Destination	Protocol	Leng	Info
171	25.697195	10.103.2.141	10.103.1.19	DNS	76	Standard query 0xa48b A www.google.co.uk
172	25.698854	10.103.1.19	10.103.2.141	DNS	92	Standard query response 0xa48b A www.google.co.uk…
173	25.698854	Dell_4d:a9:ac	Broadcast	ARP	60	Who has 10.103.2.141? Tell 10.103.1.19
174	25.698903	AsustekC_1c:…	Dell_4d:a9:ac	ARP	42	10.103.2.141 is at e0:3f:49:1c:97:c7
175	25.700380	10.103.2.141	216.58.210.35	ICMP	74	Echo (ping) request id=0x0001, seq=88/22528, ttl…

```
▷ User Datagram Protocol, Src Port: 55974, Dst Port: 53
◢ Domain Name System (query)
    [Response In: 172]
    Transaction ID: 0xa48b
  ▷ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ◢ Queries
    ▷ www.google.co.uk: type A, class IN
```

```
0000  a4 ba db 4d a9 ac e0 3f  49 1c 97 c7 08 00 45 00   ...M...? I.....E.
0010  00 3e 0d 0f 00 00 80 11  00 00 0a 67 02 8d 0a 67   .>...... ...g...g
0020  01 13 da a6 00 35 00 2a  18 a9 a4 8b 01 00 00 01   .....5.* ........
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   .......w ww.googl
0040  65 02 63 6f 02 75 6b 00  00 01 00 01              e.co.uk. ....
```

Destination Hardware Address (eth.dst), 6 bytes | Packets: 16130 · Displayed: 16130 (100.0%) · Dropped: 2264 (14.0%) · Load time: 0:0.358 | Profile: Default

Figure 23: DNS query related to one of the URLs.

- Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

  Read this link for further information about remote ICMP request/reply:

  https://en.wikiversity.org/wiki/Wireshark/IPv4_remote

Homework (Optional)

Using safe and private VMs, play the role of both the attacker and the network administrator to capture and analyse network traffic to investigate an unauthorized access attempt on a computer within the network. Present and interpret the result.

References

- Wireshark website https://www.wireshark.org/
- Cisco Networking academy: Lab - Using Wireshark to View Network Traffic (*** updated for version 2.x GUI).