Ping Capture Procedure

This is the procedure I used to capture the ping data used in wireshark exercise.

Launch the windows command prompt. (You can do this by typing cmd in the windows start menu). We will use the command prompt to generate short bursts of traffic which we will analyze.

cmd

Figure 1: cmd

Launch wireshark. You can find it in the Start Menu.

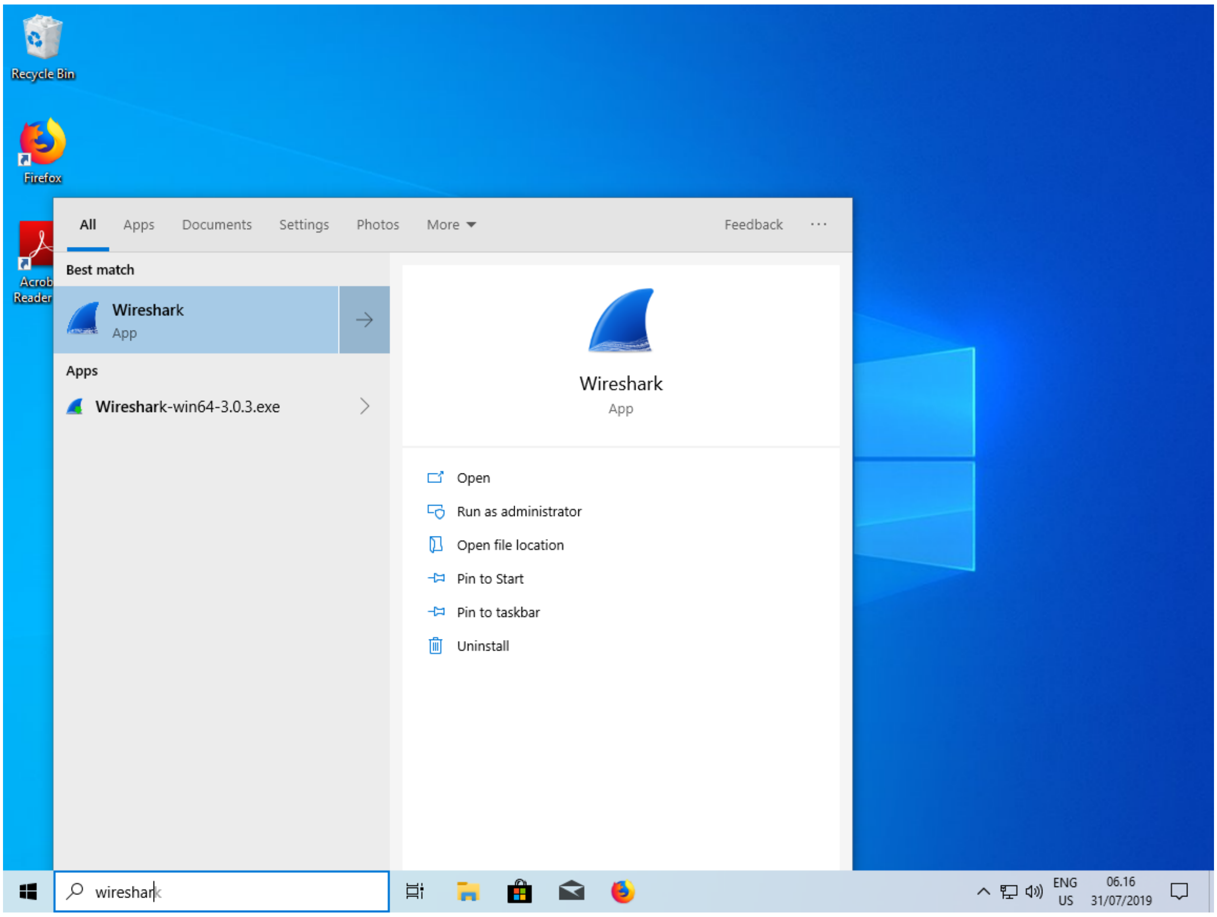
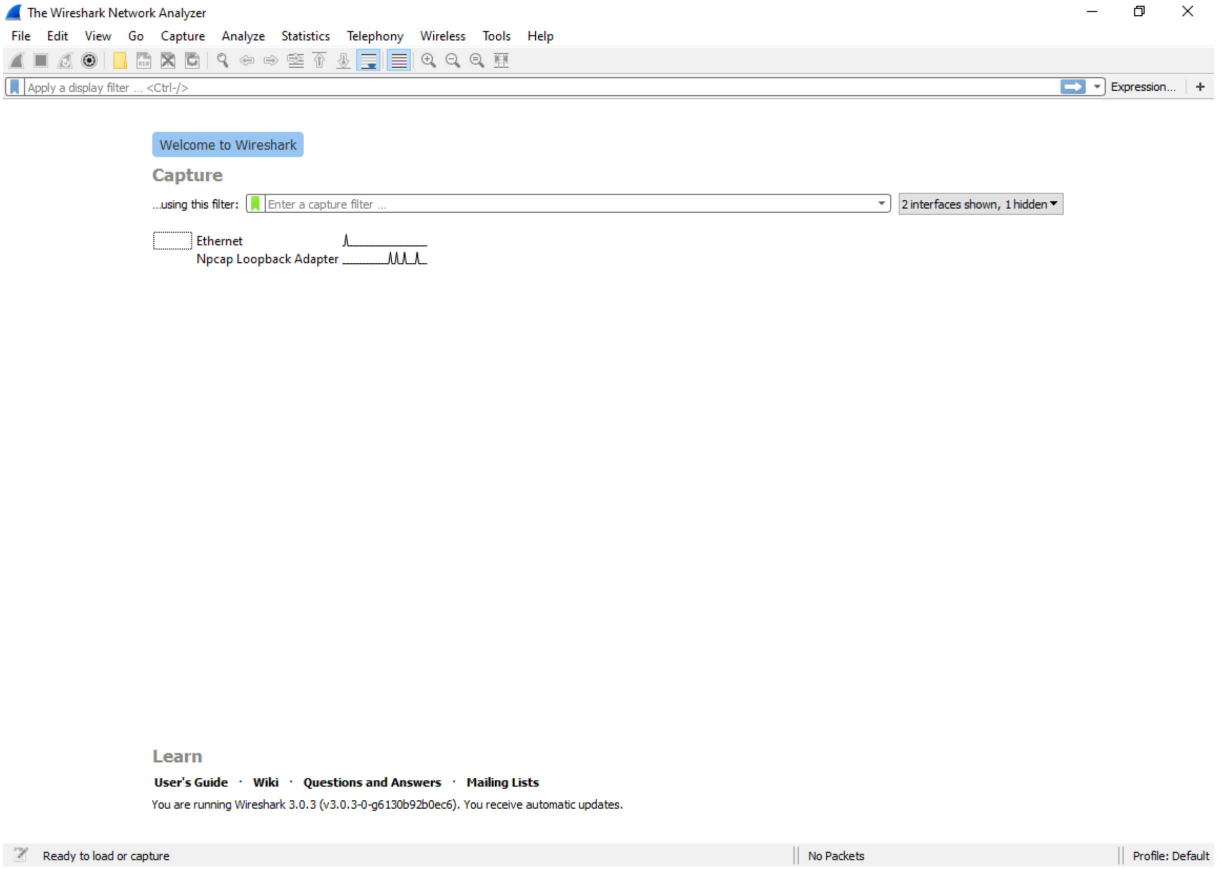


Figure 2: Launch Wireshark

After wireshark initializes you can see a list of network interfaces.

Depending on your hardware, there will probably be a wired ethernet and a wireless ethernet adapter (and may be a few other odds and ends).



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
2 interfaces shown, 1 hidden
Ethernet
Npcap Loopback Adapter
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.0.3 (v3.0.3-0-g6130b92b0ec6). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

Figure 3: First Screen

Select the interface you want to use. Correct interface depends on how you connect to the network. I will be using wired ethernet (as my workstation does not have a wireless interface).

Once you select the interface the capture icon on the top left will become clickable. The capture icon looks like a shark fin.

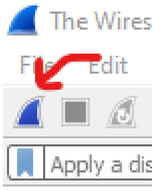


Figure 4: capture

After you click the capture button, switch to the command prompt and ping cbs.dk. Use the command below to stop capture after 3 ICMP packages.

```
ping -n 3 cbs.dk
```

As soon as the ping is over, click the red square on the top right corner to stop capture. We don't want to capture any other traffic (It can get confusing otherwise).

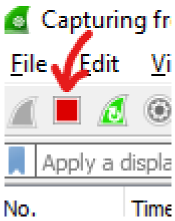
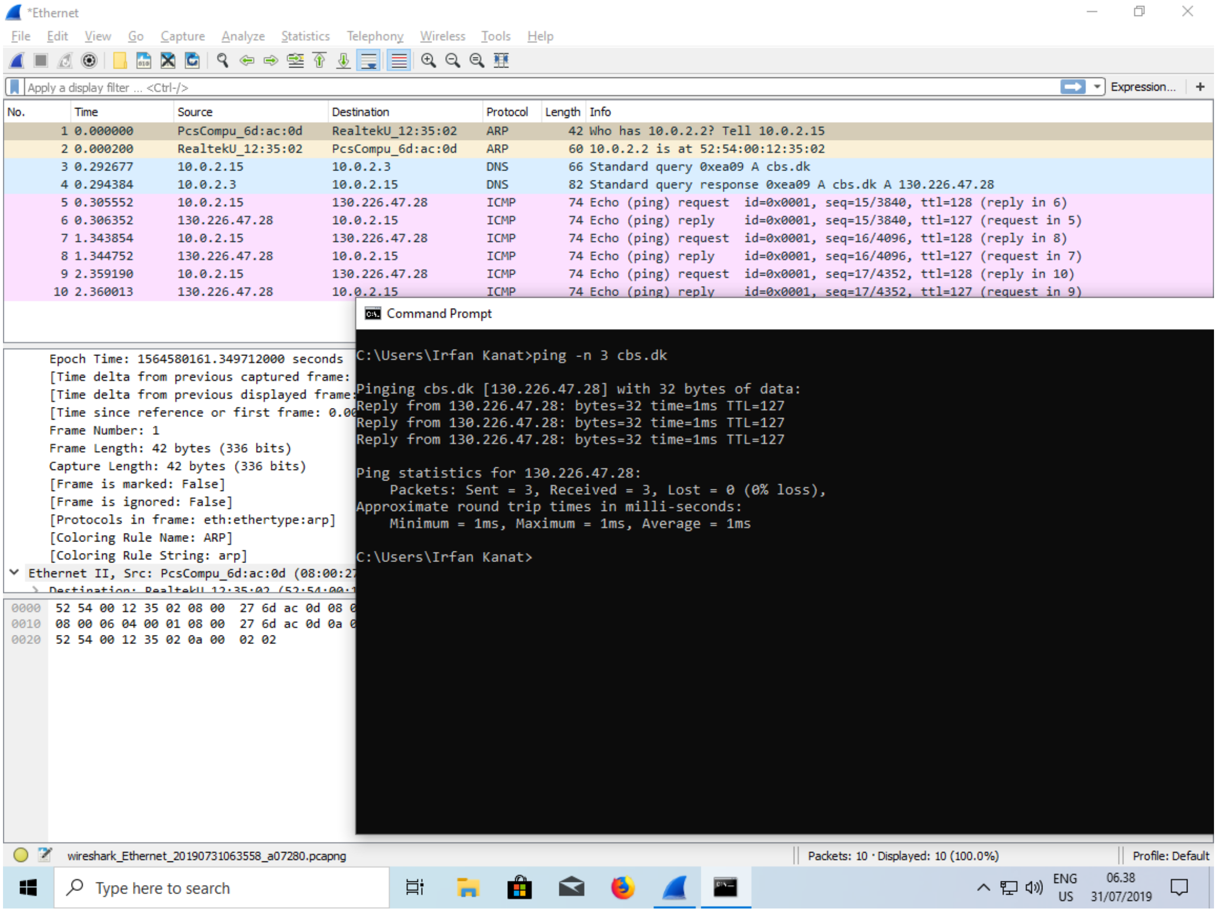


Figure 5: Stop Capture

This is how it should look like during the capture:



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+
Command Prompt
Type here to search
ENG
US
06.38
31/07/2019

```
No.    Time      Source             Destination        Protocol  Length Info
     1 0.000000  PcsCompu_6d:ac:0d  RealtekU_12:35:02  ARP          42 Who has 10.0.2.2? Tell 10.0.2.15
     2 0.000200  RealtekU_12:35:02  PcsCompu_6d:ac:0d  ARP          60 10.0.2.2 is at 52:54:00:12:35:02
     3 0.292677  10.0.2.15          10.0.2.3           DNS          66 Standard query 0xea09 A cbs.dk
     4 0.294384  10.0.2.3           10.0.2.15          DNS          82 Standard query response 0xea09 A cbs.dk A 130.226.47.28
     5 0.305552  10.0.2.15          130.226.47.28      ICMP         74 Echo (ping) request  id=0x0001, seq=15/3840, ttl=128 (reply in 6)
     6 0.306352  130.226.47.28      10.0.2.15          ICMP         74 Echo (ping) reply    id=0x0001, seq=15/3840, ttl=127 (request in 5)
     7 1.343854  10.0.2.15          130.226.47.28      ICMP         74 Echo (ping) request  id=0x0001, seq=16/4096, ttl=128 (reply in 8)
     8 1.344752  130.226.47.28      10.0.2.15          ICMP         74 Echo (ping) reply    id=0x0001, seq=16/4096, ttl=127 (request in 7)
     9 2.359190  10.0.2.15          130.226.47.28      ICMP         74 Echo (ping) request  id=0x0001, seq=17/4352, ttl=128 (reply in 10)
    10 2.360013  130.226.47.28      10.0.2.15          ICMP         74 Echo (ping) reply    id=0x0001, seq=17/4352, ttl=127 (request in 9)
```

```
    Epoch Time: 1564580161.349712000 seconds
    [Time delta from previous captured frame:
    [Time delta from previous displayed frame:
    [Time since reference or first frame: 0.00
    Frame Number: 1
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
v Ethernet II, Src: PcsCompu_6d:ac:0d (08:00:27
  > Destination: RealtekU_12:35:02 (52:54:00:1
```

```
0000  52 54 00 12 35 02 08 00  27 6d ac 0d 08 0
0010  08 00 06 04 00 01 08 00  27 6d ac 0d 0a 0
0020  52 54 00 12 35 02 0a 00  02 02
```

```
C:\Users\Irfan Kanat>ping -n 3 cbs.dk

Pinging cbs.dk [130.226.47.28] with 32 bytes of data:
Reply from 130.226.47.28: bytes=32 time=1ms TTL=127
Reply from 130.226.47.28: bytes=32 time=1ms TTL=127
Reply from 130.226.47.28: bytes=32 time=1ms TTL=127

Ping statistics for 130.226.47.28:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Irfan Kanat>
```

wireshark_Ethernet_20190731063558_a07280.pcapng | Packets: 10 · Displayed: 10 (100.0%) | Profile: Default

Figure 6: During Capture