Lab 01

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

HTTP, TCP and DNS.

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?
(By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began.
To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

```
   1889 22:07:55.130160 172.31.98.151    128.119.245.12    HTTP     569 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   1895 22:07:55.422149 128.119.245.12   172.31.98.151     HTTP     492 HTTP/1.1 200 OK  (text/html)
```

According to the screenshot, the time interval between the HTTP GET message and HTTP OK message is
55.422149 - 55.130160 = 0.291989s

3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

The Internet address of the gaia.cs.umass.edu is: 128.199.245.12
The Internet address of my computer is: 172.31.98.151

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.

The screenshot of HTTP GET message:

```
No.     Time              Source                Destination           Protocol Length Info
   1889 22:07:55.130160   172.31.98.151         128.119.245.12        HTTP     569    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1
Frame 1889: 569 bytes on wire (4552 bits), 569 bytes captured (4552 bits) on interface \Device\NPF_{185BC2D4-588F-4111-8BE5-6B56836A739C}, id
0
Ethernet II, Src: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10), Dst: ArubaaHe_cd:eb:28 (6c:f3:7f:cd:eb:28)
Internet Protocol Version 4, Src: 172.31.98.151, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52609, Dst Port: 80, Seq: 1, Ack: 1, Len: 515
Hypertext Transfer Protocol
```

The screenshot of HTTP OK message:

```
No.     Time              Source                Destination           Protocol Length Info
   1895 22:07:55.422149   128.119.245.12        172.31.98.151         HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 1895: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{185BC2D4-588F-4111-8BE5-6B56836A739C}, id
0
Ethernet II, Src: ArubaaHe_cd:eb:28 (6c:f3:7f:cd:eb:28), Dst: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.31.98.151
Transmission Control Protocol, Src Port: 80, Dst Port: 52609, Seq: 1, Ack: 516, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```

5. Look for Wireshark alternatives. Choose 2 of them: install and play around with the tools. List out the main features of the alternative tools. Compare those tools with Wireshark: pros and cons, unique features compare to Wireshark.

❖ **tcpdump**

- Features:
  - Command-line packet analyzer.
  - Captures and displays network packets.
  - Supports packet filtering using Berkeley Packet Filter (BPF) syntax.
  - Works on various platforms, including Linux, macOS, and Windows.
  - Lightweight and efficient.
- Comparison with Wireshark: Pros:
  - Lightweight and does not require a graphical user interface.
  - Works well for quick captures and analysis on command line.
  - No need for installation, as it is usually pre-installed on UNIX-based systems.
- Cons:
  - Lacks the advanced GUI interface and extensive analysis features of Wireshark.
  - Limited functionality when it comes to deep packet inspection and extensive protocol decoding.
  - Requires some familiarity with command-line usage.

❖ **Tshark:**

- Features:
  - Command-line version of Wireshark.
  - Offers similar capabilities to Wireshark for capturing, analyzing, and filtering network packets.
  - Supports various file formats, including pcap, pcapng, and ERF.
  - Works on multiple platforms.
- Comparison with Wireshark: Pros:
  - Lightweight and efficient, similar to tcpdump.
  - Allows you to perform packet analysis and filtering via command-line interface.
  - Suitable for scripting and automation purposes.
- Cons:
  - Lacks the user-friendly graphical interface provided by Wireshark.
  - May require some familiarity with command-line usage and Tshark syntax.
  - Advanced analysis features and customization options may not be as comprehensive as Wireshark.

⇒ It's important to note that both tcpdump and Tshark are powerful tools but are primarily command-line driven and may have a steeper learning curve compared to Wireshark's GUI-based approach. However, they offer lightweight alternatives for quick captures and analysis, especially in environments where a graphical interface is not available or necessary.