COMP4621 Wireshark Labs: Getting Started

TA: Waheed GHALI

E-mail: wggghali@connect.ust.hk

Outline

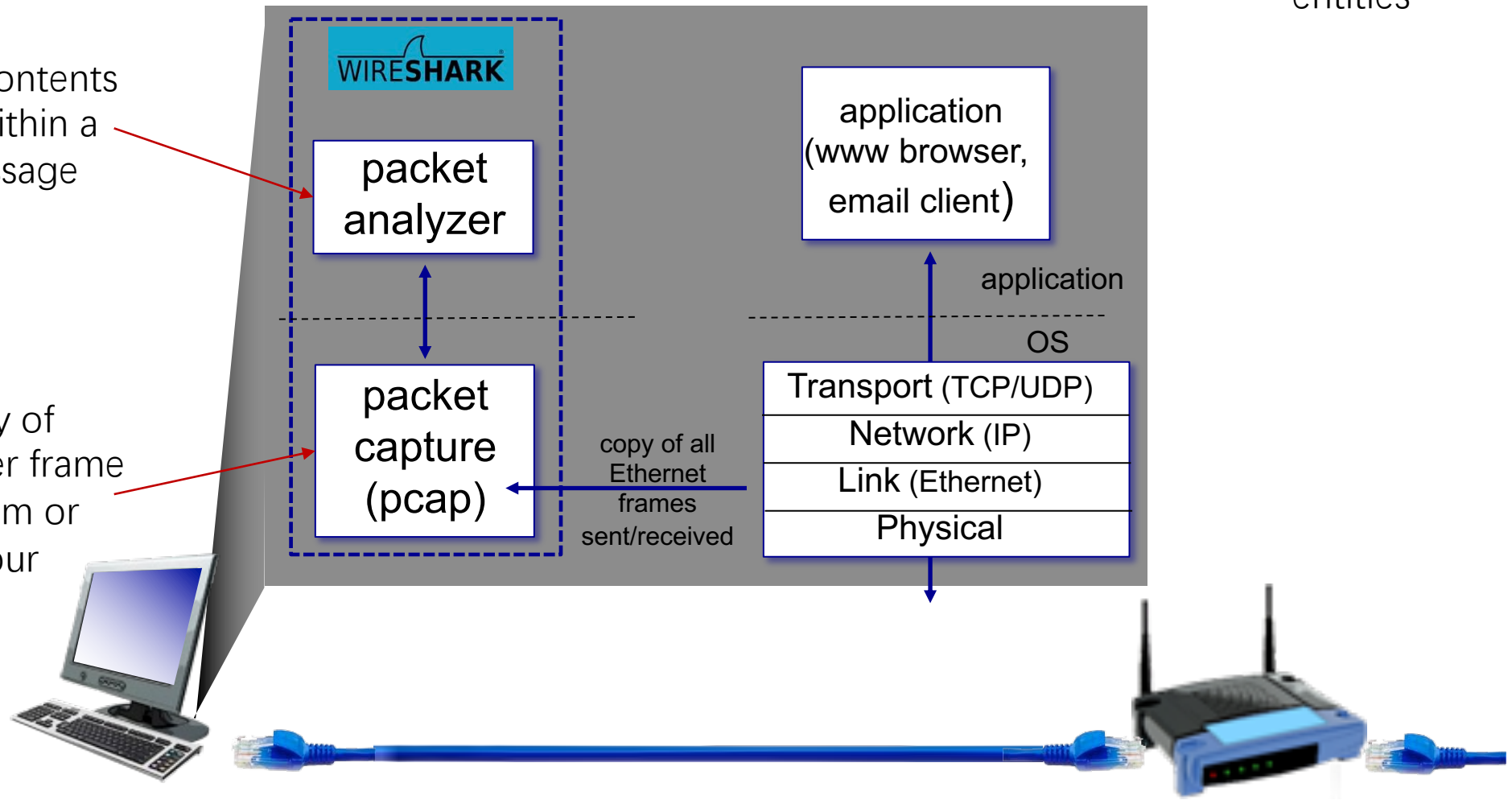
- Packet sniffer and Wireshark
- Downloading Wireshark
- Running Wireshark
- Test Run: Basic HTTP GET / response interaction

Packet sniffer and Wireshark

The basic tool for observing the messages exchanged between executing protocol entities

Display the contents of all fields within a protocol message

Receive a copy of every link-layer frame that is sent from or received by your computer

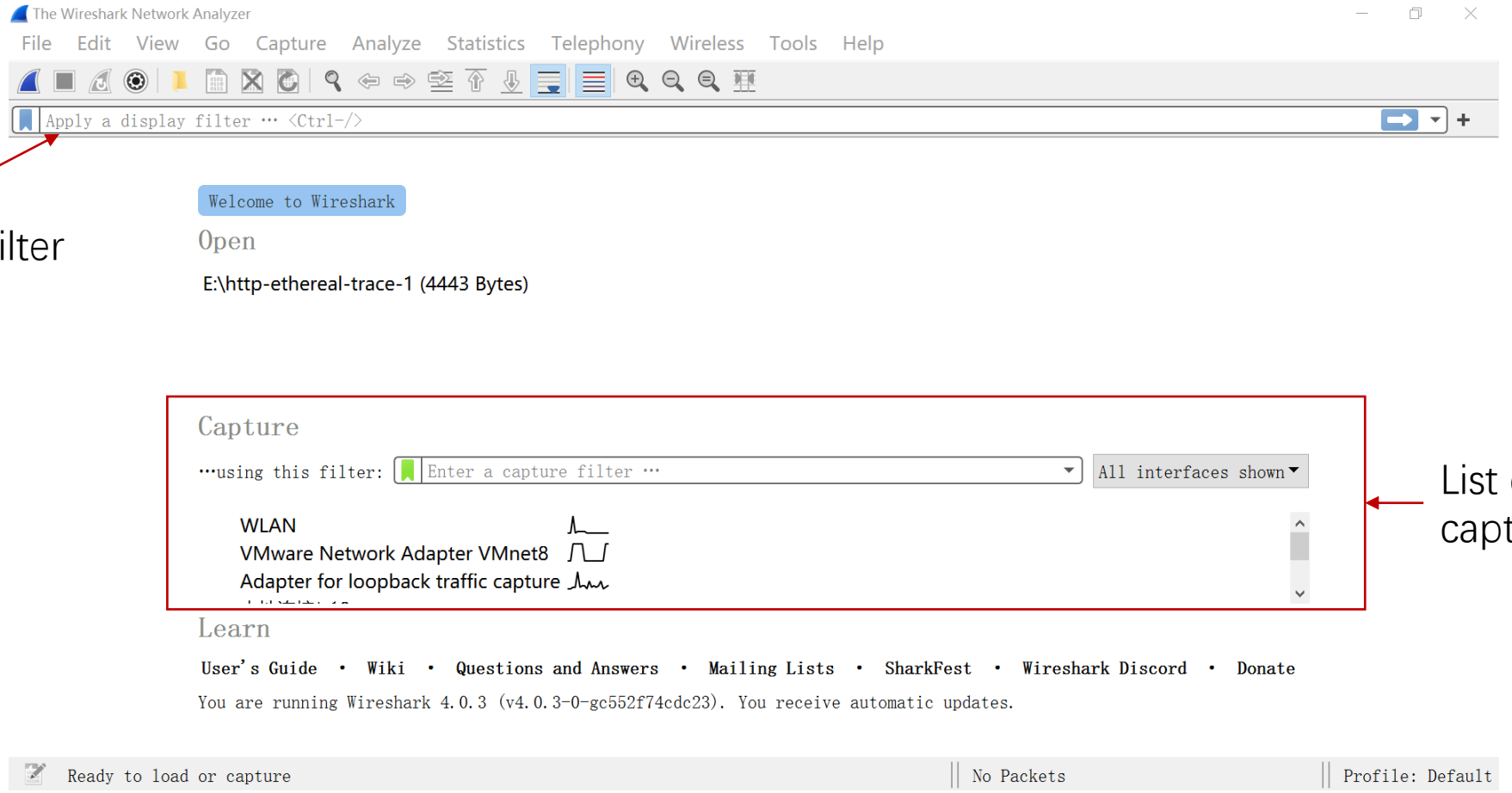


Downloading Wireshark

- http://www.wireshark.org/download.html

- Other useful pages
  - user-guide: http://www.wireshark.org/docs/wsug_html_chunked/
  - man pages: http://www.wireshark.org/docs/man-pages/
  - FAQ: http://www.wireshark.org/faq.html

Running Wireshark



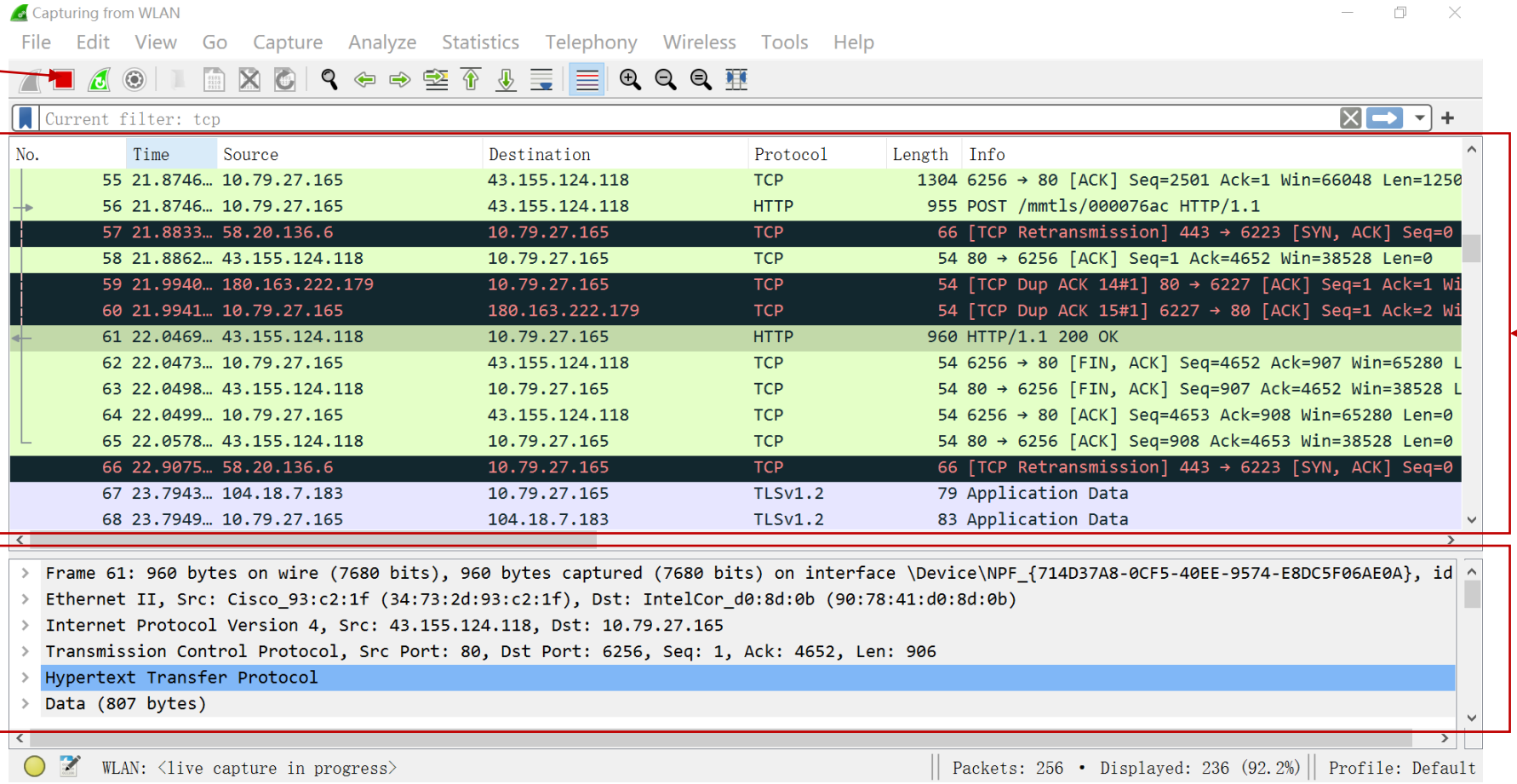
Packet display filter

List of interfaces to capture packets from

startup screen

Running Wireshark

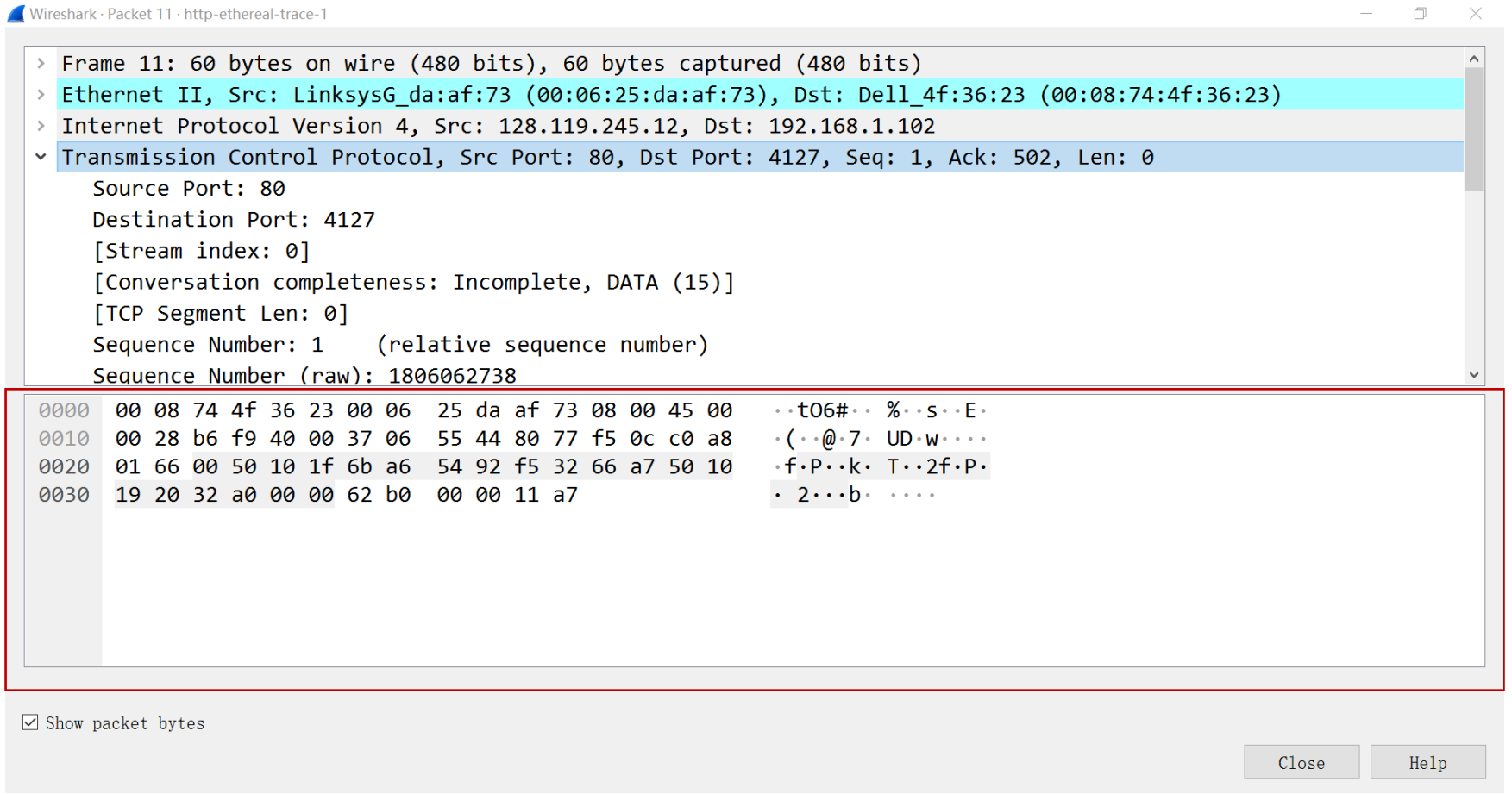
Stop capturing packets



List of captured packets

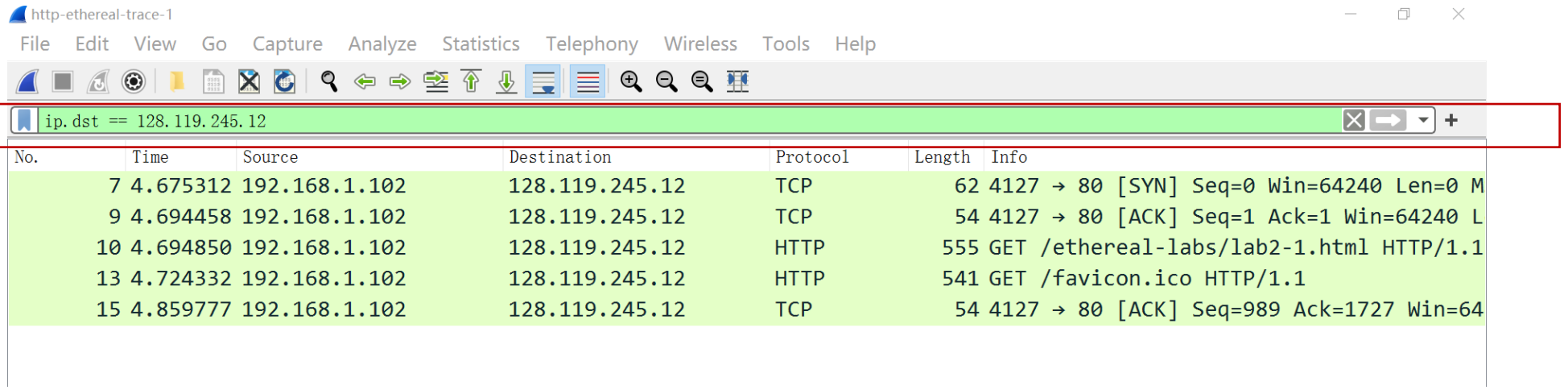
details of selected packet header

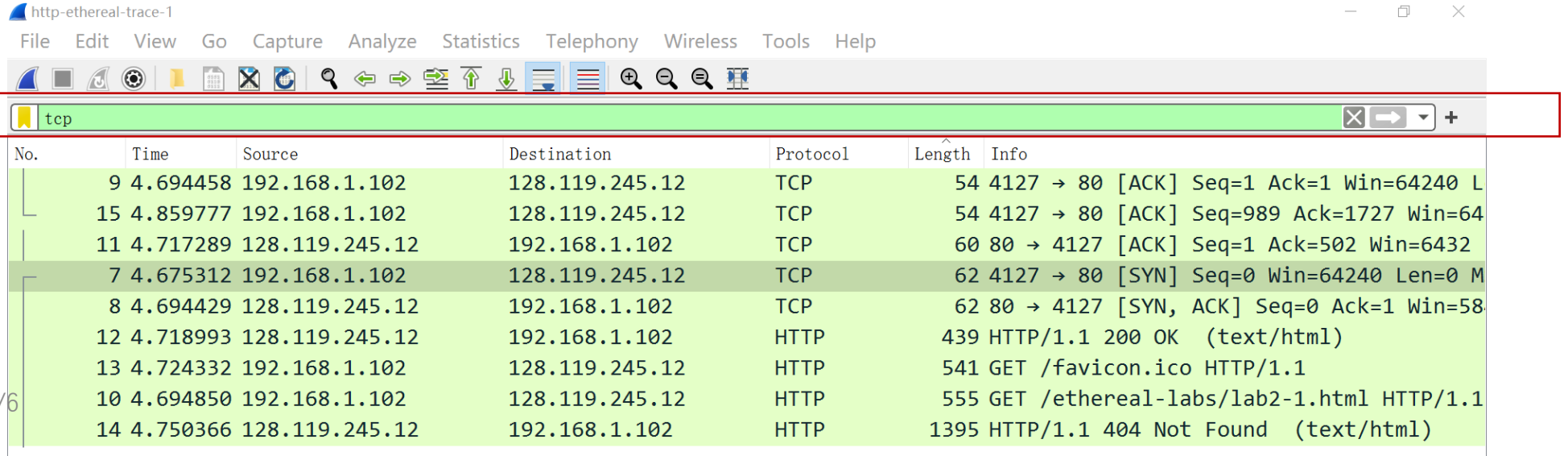
Running Wireshark



Packet-contents window

Running Wireshark

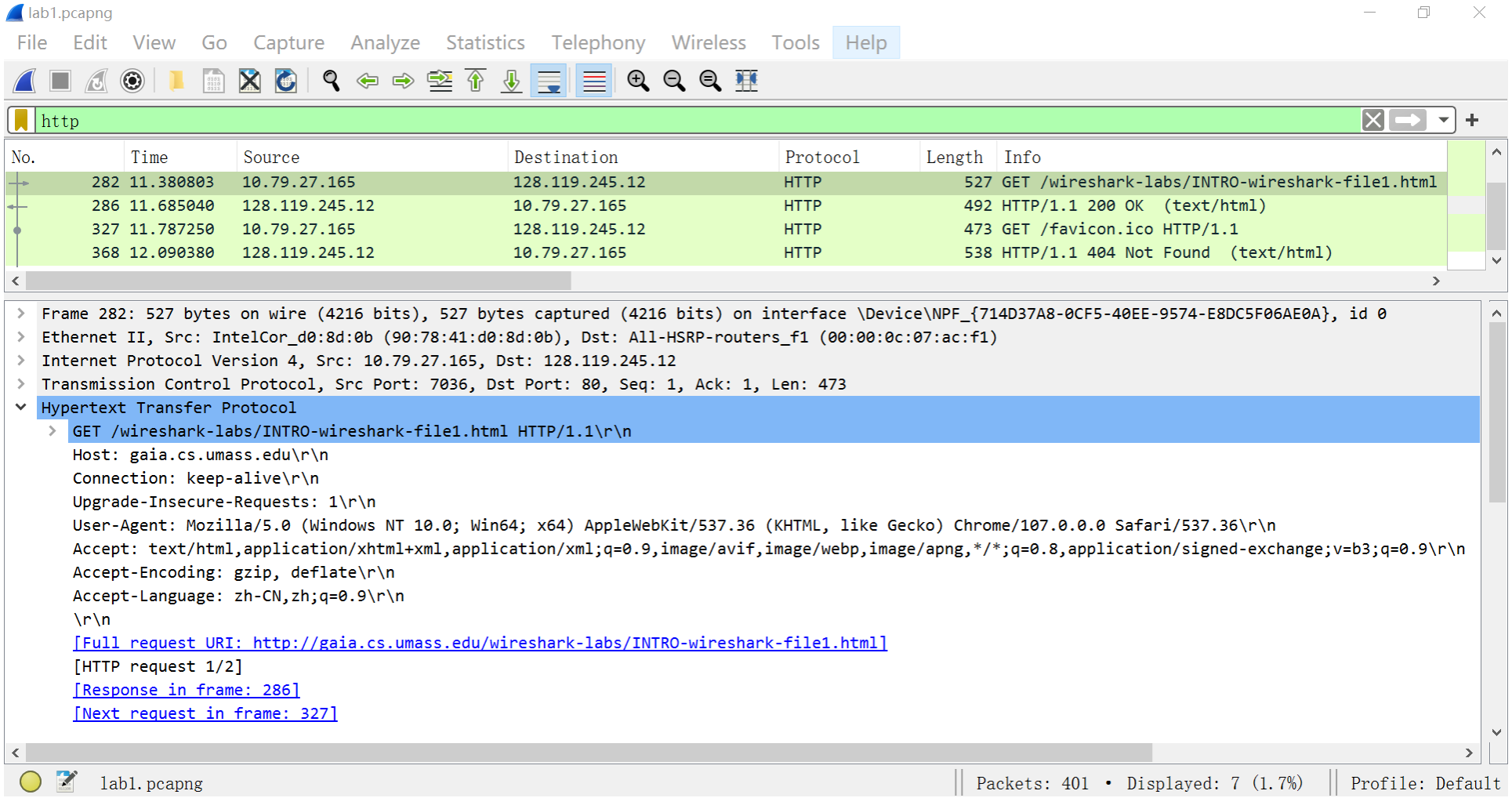




Test Run: Basic HTTP GET / response interaction

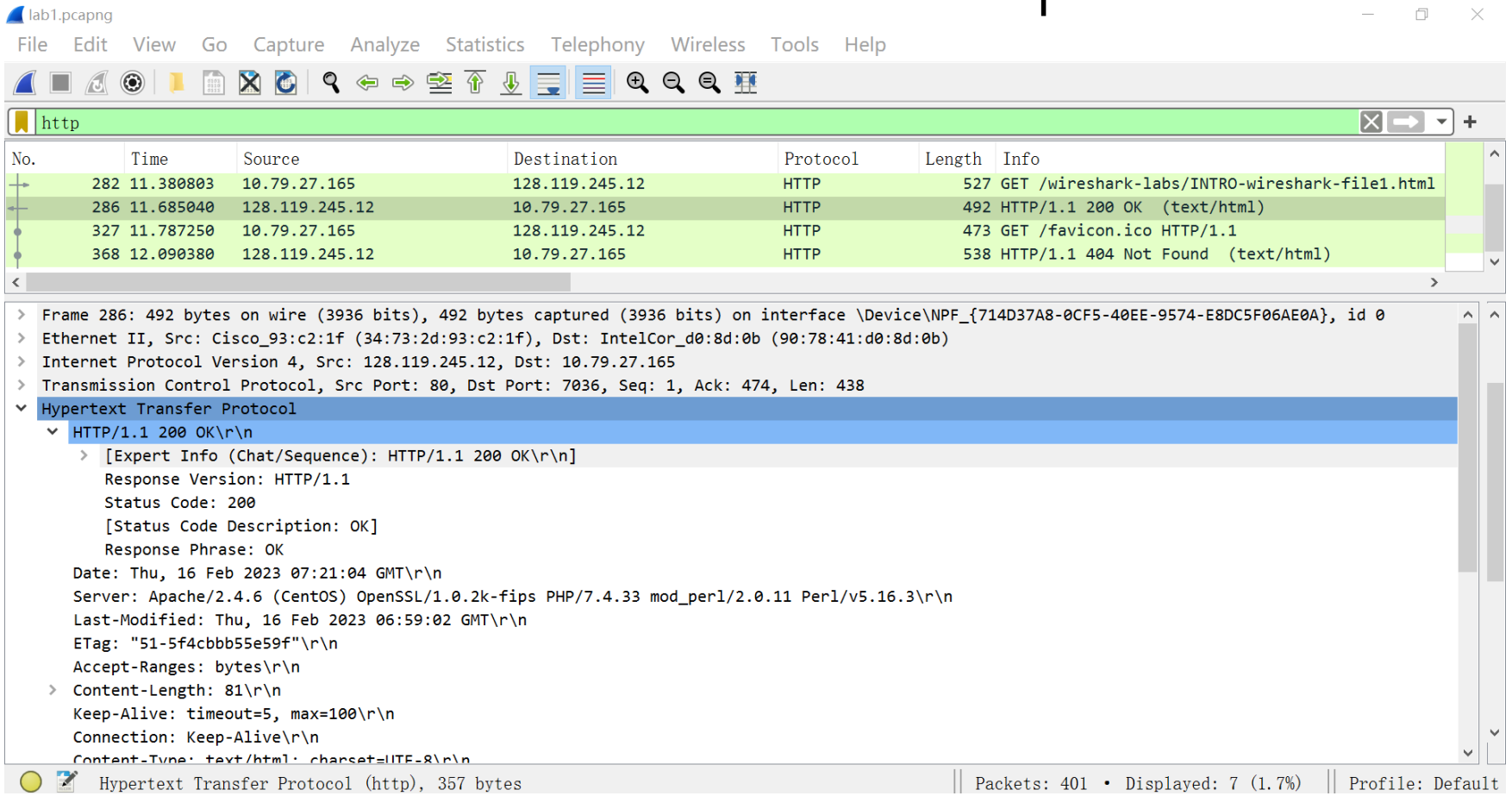
1. Start up your web browser
2. Open the Wireshark packet sniffer
3. Select your interface and begin Wireshark packet capture
4. Enter the following in your web browser:
   http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
5. After your browser has displayed the INTRO-wireshark-file1.html page, stop the Wireshark packet capture
6. Type ‘http’ in the display filter window

Test Run: Basic HTTP GET / response interaction



HTTP GET message

Test Run: Basic HTTP GET / response interaction




```
Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations.  You've downloaded the file lab2-1.html!\n
    </html>\n
```

HTTP response message

Conclusion

- Packet sniffer and Wireshark
  - packet capture library
  - packet analyzer
- Downloading Wireshark
- Running Wireshark
  - Start the Wireshark
  - Select the interface and begin Wireshark packet capture
  - Stop the Wireshark packet capture
  - Use the display filter to filter the packets displayed

Lab Exercise

- What is the **IP address** of the gaia.cs.umass.edu? What is the **IP address** of your computer?
- Use the display filter to find the **HTTP** packets where the **destination IP address** is the IP address of the gaia.cs.umass.edu.
- Use the display filter to find the **TCP** packets where the **source IP address** is the IP address of the gaia.cs.umass.edu and the **destination IP address** is the IP address of your computer.

- Hint
  - https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html