**PRACTICAL-5**

**AIM:** Understand basic networking concept using Wireshark. Use of different Wireshark Display Filters.

**PRACTICAL/THEORY**:

* Wire shark is a free and open source packet analyser.
* It is used for network troubleshooting, analysis, software and communications protocol development, and education.

**USAGE:**

* Network administrators use it to troubleshoot network problems
* Network security engineers use it to examine security problems

**FEATURES:**

* Live capture and offline analysis
* Live capture and offline analysis
* The most powerful display filters in the industry
* Coloring rules can be applied to the packet list for quick, intuitive analysis
* Output can be exported to XML, PostScript®, CSV, or plain text

**PROS and CONS**:

**PROS:**

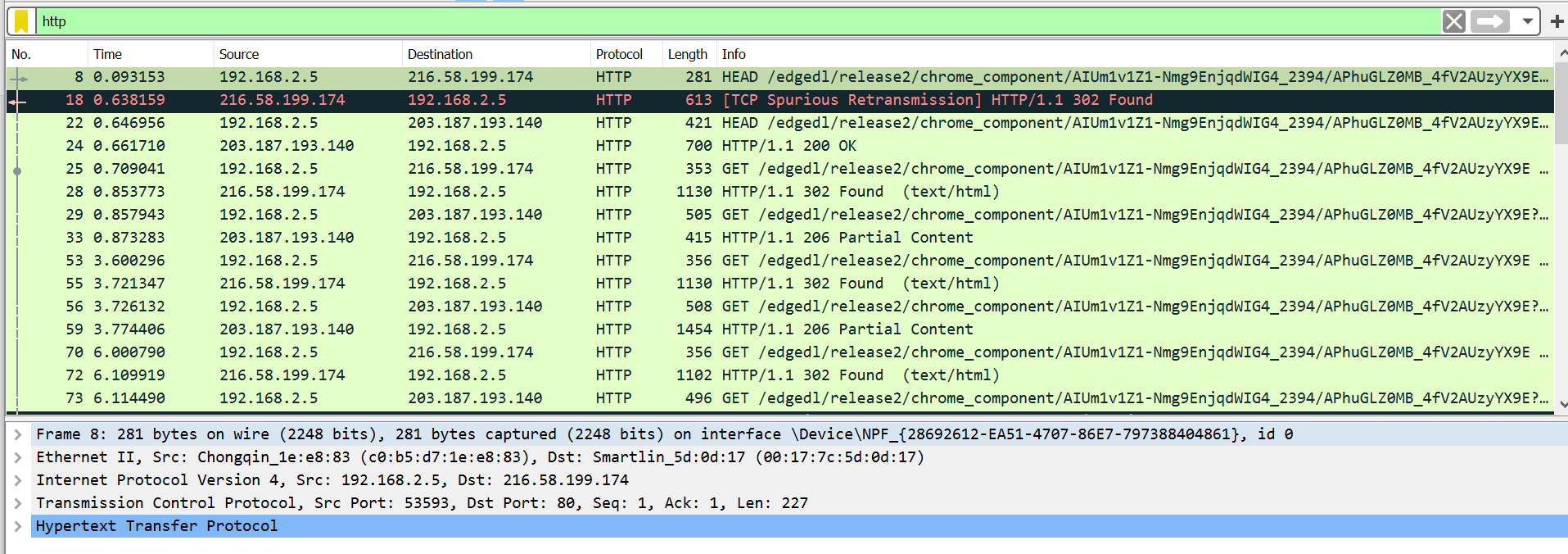
* Captures all kinds of packet data in network traffic
* Save & restore captured packed data
* Show errors and issues in levels below the HTTP protocol

**CONS:**

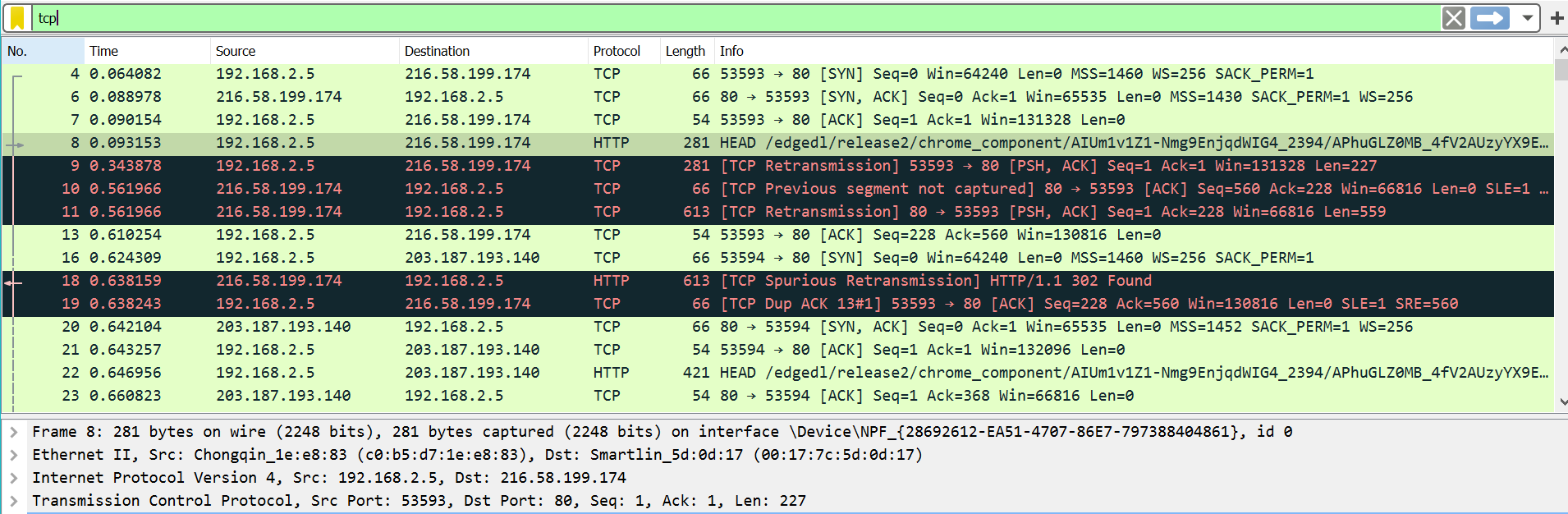
* Can't modify or manipulate things/data on the network (only records data)
* A better interface would be nice - it's functional as-is, but it could use some polish

**DIFFERENT FILTERS:**

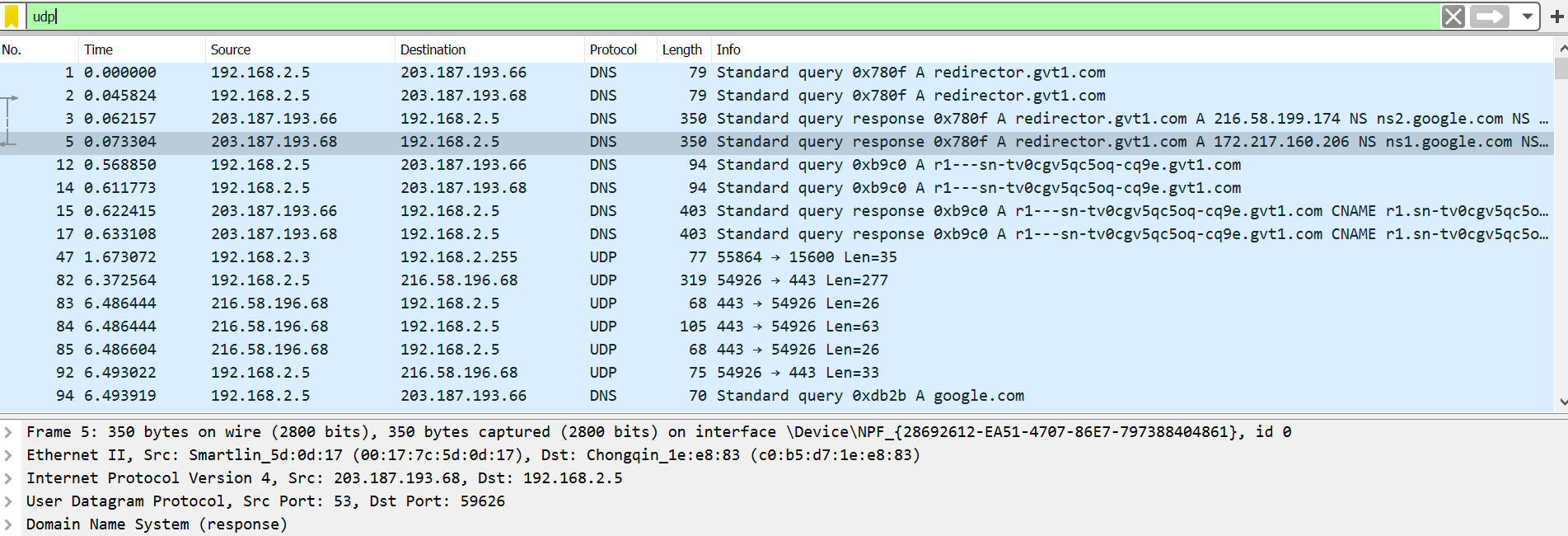
## HTTP:



## TCP:



## UDP:



**CONCLUSION:**

* By performing the above practical, we got to know about basics of Wireshark and different filters that can be used for capturing and for analysis