

**HANOI UNIVERSITY**

**Faculty of Information Technology**

**CNE – Tutorial Guide**

**Week 3**

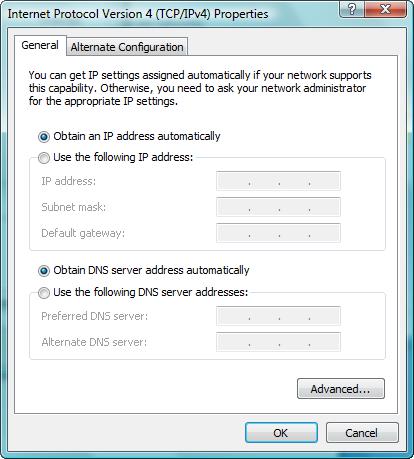
Network traffic analysis by ***Wireshark***

# Wireshark is The world's most popular network protocol analyzer.

Please download Wireshark at: <https://www.wireshark.org/>

1. DHCP Analysis

1. Set the NIC to obtain an IP from DHCP



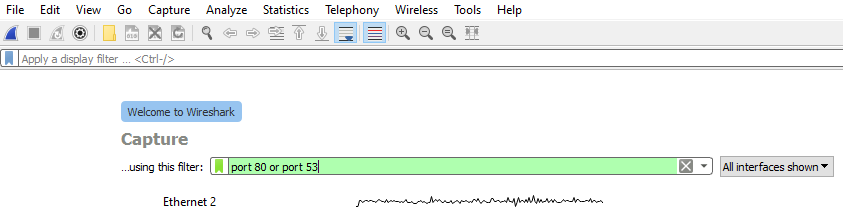
1. Start Wireshark
2. Plug off the network cable
3. Start capturing with Wireshark
4. Plug in the network cable

Page 1 Tutorial 3 – Network Traffic Analysis by Wireshark

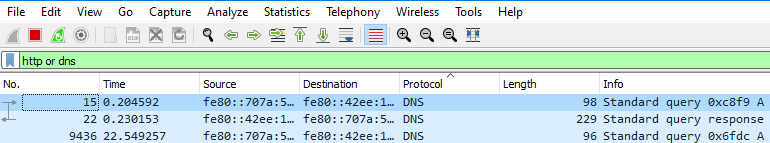
* 1. Look at Wireshark and describe the network traffic (IP, service)



1. Web Connection Analysis
   1. Start Wireshark
   2. Edit **Capture Filter** (right after when you open Wireshark) to capture only http and dns packets:



**Or Capture all** traffics in/out and then enter criteria for **Display Filter**  to display only http and dns packets:



* 1. Open this website: [**www.google.com**](http://www.google.com) **/** [**https://lms.fit.hanu.vn**](https://lms.fit.hanu.vn) **/** [**https://hanu.vn**](https://hanu.vn)
  2. Look at Wireshark and describe network traffic (Service, IP)

1. Ping Analysis
   1. Start Wireshark
   2. Edit Capture Filter to capture only icmp, icmpv6, http and dns packets
   3. Start Capture in Wireshark
   4. Ping [**www.google.com**](http://www.google.com) **/** [**https://lms.fit.hanu.vn**](https://lms.fit.hanu.vn) **/** [**https://hanu.vn**](https://hanu.vn)
   5. Look at Wireshark and describe network traffic (Service, IP)

IV. Tracert Analysis

1. Start Wireshark
2. Edit Capture Filter to capture only icmp, icmpv6, http and dns packets
3. Start Capture in Wireshark
4. Tracert [**www.google.com**](http://www.google.com) **/** [**https://lms.fit.hanu.vn**](https://lms.fit.hanu.vn) **/** [**https://hanu.vn**](https://hanu.vn)
5. Look at Wireshark and describe network traffic (Service, IP

Page 2 Tutorial 3 – Network Traffic Analysis by Wireshark