TUTORIAL 1 - WIRESHARK

I. Purpose

- ✓ Understand the working protocol of Wireshark
- ✓ Know how to capture and filter Wireshark packets
- ✓ Understand Wireshark’s capture/filter syntax
- ✓ Analyze and understand Wireshark packets

II. Class Activities

1. Activity 1 (individual)

- Estimated Duration: 10 mins

Each of the class members downloads and installs Wireshark onto their computers and examines how to capture packets.

Use ipconfig to know IP configuration of their computers. Use net view to see computers in network and then ping that hostname to know address of that computer.

Dicussion 1

- Estimated Duration: 10 mins.

Students are expected to answer the following questions before Wireshark hand-ons:

- What is the physical network interface/virtual network interface?

- How to know which network interface needs to be used to capture packets?

- How does WireShark capture packets?

2. Activity 2 (individual)

- Estimated Duration: 20 mins

Each student carries out some networking activities related to ICMP, DNS, HTTP protocols using the Wireshark Guide available on the FIT portal and tries to capture these packets related to these activities and vice-versa.

Such as: How to capture HTTP traffic using Wireshark

a) Install Wireshark.

b) Open your Internet browser.
c) Clear your browser cache.
d) Open Wireshark
e) Click on "Capture > Interfaces". A pop up window will show up.
f) You probably want to capture traffic that goes through your ethernet driver. Click on the Start button to start capturing traffic via this interface.
g) Visit the URL that you wanted to capture the traffic from.
h) Go back to your Wireshark screen and press Ctrl + E to stop capturing

For ICMP and DNS students find themselves

Discussion 2

- Estimated Duration: 20 mins

After capturing, each is expected to answer the following questions:

- Identify characteristics of ICMP, DNS, HTTP, ARP, TCP packets as you see from capture packets.

- Identify capture/filter syntax of Wireshark

3. Reference

http://www.wireshark.org/docs/wsug_html_chunked/