SE375 - Laboratory Assignment 06

Introduction to Wireshark

Part 1: Demonstration

In the first hour, we will investigate the capabilities of Wireshark in a top-down manner.

- Capturing with Wireshark and Color Codes

  Open Wireshark, start capturing the Ethernet interface.

  Color codes: By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.

- Filters, Syntax, Boolean Logic

  Important: Capture filter versus display filter. Capture filter applied on before starting to capture. Display filter is applied after starting to capture.

  Filters are just combinations of Boolean expressions

- Application Layer through HTTP example

  Browse to homes.ieu.edu.tr

  `http.host == homes.ieu.edu.tr` (http) Everything is easily observable.

  Browse to ieu.edu.tr

  `http.host == ieu.edu.tr` (https) No packets can be observed after the first request. Secure connection established. Need additional tools to follow through. Even observed the contents will be encrypted.

- TCP through conversation filter in Transport Layer

  `http.host == homes.ieu.edu.tr` then right-click>>Follow>>TCP stream on a packet

  http uses TCP as its Transport Layer protocol (reliable connection)

- Another Application Layer example through DNS (uses UDP as Transport Layer)

  `http.host == homes.ieu.edu.tr || dns.qry.name == homes.ieu.edu.tr`

  observe that DNS query resolves homes.ieu.edu.tr to its IP address. (10.0.0.5)

  DNS uses UDP as its Transport Layer protocol (unreliable connection)

  Browse to 10.0.0.5 to be assured.

- Network Layer through IP

  Enter `ipconfig -all` into command line and acquire your IP and also IP of school's DNS.

  Use ping command to send a Hello message to school's DNS
  `ip.src == YOUR_IP && ip.dst == DNS_IP` (captures all traffic from you to DNS)

  ping uses ICMP protocol over IP, filter through icmp

  `ip.src == YOUR_IP && ip.dst == DNS_IP && icmp` (from you to DNS, requests)

  `ip.dst == YOUR_IP && ip.src == DNS_IP && icmp` (from DNS to you, replies)

  `(ip.dst == YOUR_IP && ip.src == DNS_IP) || (ip.src == YOUR_IP && ip.dst == DNS_IP)`

  (All traffic between these two computers)

- Network Layer through ARP (only observable in Local Area Network) Apply `arp` filter

  Simply we have the IP of the target and want to know its MAC address (physical address of the computer). Observe that IPs appearing after filtering are local ones

  Distinctions between request and reply

  `arp.opcode == request`

  `arp.opcode == reply`

  Why do we have many requests rather than replies? (because arp is broadcasted but only needs replies to specific computers not to all)

- Data-link layer through Ethernet

  Enter `ipconfig -all` into command line and acquire your MAC address.

  Distinctions between Unicast (one-to-one), Broadcast (one-to-all), Multicast (one-to-many)

  Note: Broadcast is also a way of multicasting.

  `ff:ff:ff:ff:ff:ff` is a virtual MAC address reserved for broadcasting

  `eth.dst==ff:ff:ff:ff:ff:ff (broadcast only)`

  `(eth.dst[0] & 1) (multicast only)`

  `!(eth.dst[0] & 1) (unicast only)`

  `(eth.dst[0] & 1) && eth.dst!=ff:ff:ff:ff:ff:ff (multicast but not broadcast)`

  Tell the difference between `&` (bit-wise `and` operator) and `&&` (logical and operator)

Part 2: Assignment

Modify one of your existing Word Count programs to acquire the files to be parsed through HTTP requests sent to

- `http://homes.ieu.edu.tr/culudagli/files/SE375/Week06/r8-train-all-terms.txt`
- `http://homes.ieu.edu.tr/culudagli/files/SE375/Week06/r8-test-all-terms.txt`
- `http://homes.ieu.edu.tr/culudagli/files/SE375/Week06/r52-train-all-terms.txt`
- `http://homes.ieu.edu.tr/culudagli/files/SE375/Week06/r52-test-all-terms.txt`

Modify your argument passing to include the first argument as the link where the files reside. Then, the rest defines the filenames as usual. Use Wireshark to debug your HTTP requests.

Note: Although this assignment is still building on top of the Word Count assignments, it is actually independent.