WIRESHARK

The first think that comes to my mind when I listen the sentence “Network Monitoring (Traffic and Performance)” is to switch my operating system to kali linux .In kali linux we find the wireshark installed by default.

Wireshark: Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible (Link: https://www.wireshark.org/docs/wsug_html/#ChIntroWhatIs).

To start this we need to know about the network interfaces present in our System.

Through cmd: (Mostly we try to enable or disable Wi-Fi adapter),eth0-ethernet,eth1-Wifi

ifconfig/all

netsh interface shoe interface

netsh interface ip show interface

netsh mbn show interface

disabling :

netsh interface set interface "YOUR-ADAPTER-NAME" disable

enabling:

netsh interface set interface "YOUR-ADAPTER-NAME" enable

Required network interfaces are enabled, Then we proceed.

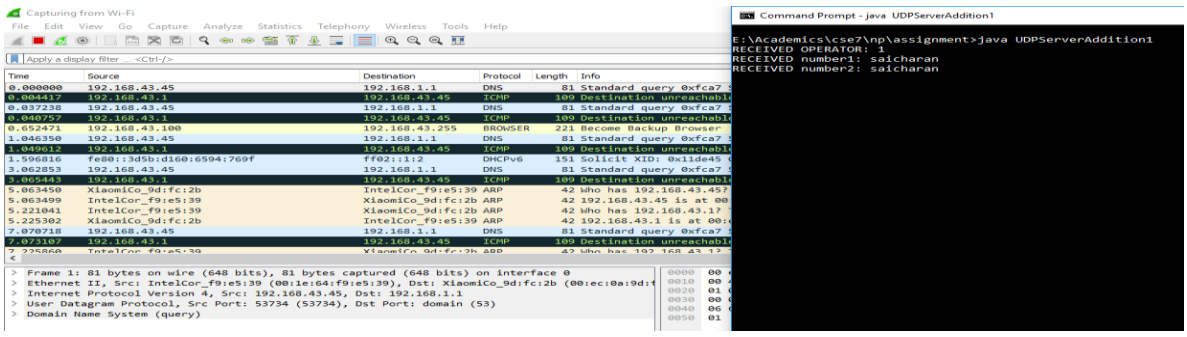
I will take the Example of ASSN-I-15115060.pdf. Here we run the Client in one system and server in other system. Client connect the server by using IP address.

We take another System named (USEDROPPER).Here all the system connect to same network. We start the application named wireshark and select the Wi-Fi adapter to listen the Network.

The following are some of the functionalites Wireshark provides:

- **Available for *UNIX* and *Windows*.**
- ***Capture* live packet data from a network interface.**
- ***Open* files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.**
- ***Import* packets from text files containing hex dumps of packet data.**
- **Display packets with *very detailed protocol information*.**
- ***Save* packet data captured.**
- ***Export* some or all packets in a number of capture file formats.**
- ***Filter packets* on many criteria.**
- ***Search* for packets on many criteria.**
- ***Colorize* packet display based on filters.**
- **Create various *statistics*.**

Then Automatically So ARP, UDP, DNS, HTTP…packets starts listing out: (Click below image for full view)



We will be having 3 section in this.They are: **(1)** Packet List: List of Packet flow in Network ,it contain following columns like: Time, Source, destination, Protocol, length, Info **(2)** Packet Details: Complete detailed information including data in a selected packet **(3)** Packet Bytes: look of the packet converted into byte format. Click the Image:

This is the main menu look in wireshark interface.

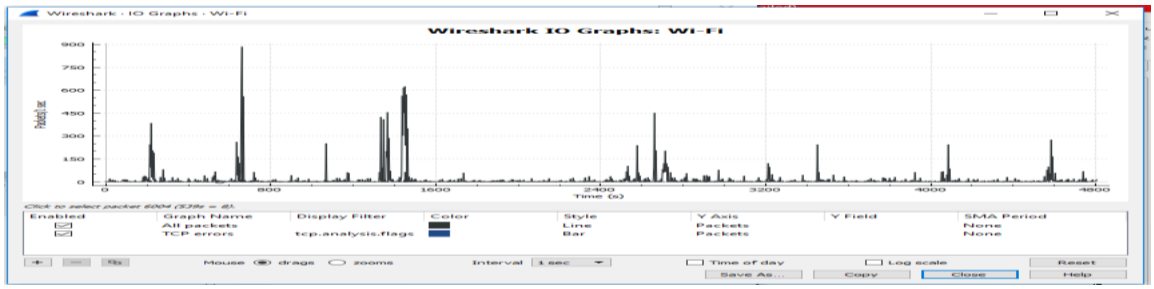
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

In Capture we have capture filters, start and stop buttons. In Analyze we have Display filters (code sheet link: https://drive.google.com/open?id=17UcFcK7u_qEa4vrUNyr03FxDBLIKrSDy), Decode as, follow functions(used to separate the conversation between to clients)

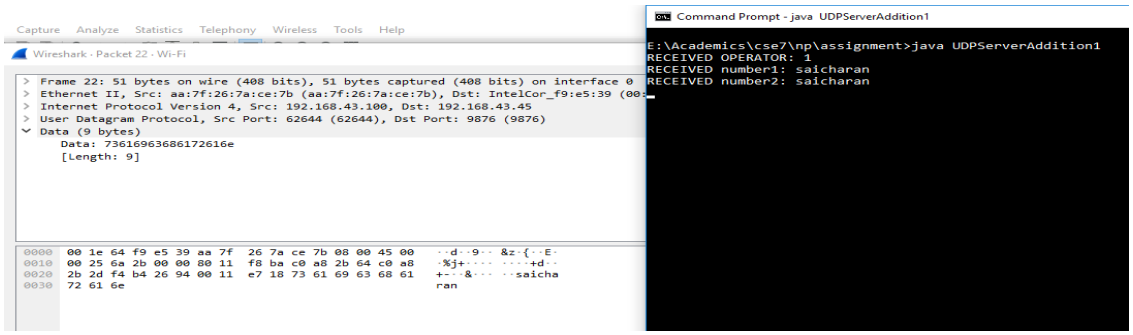
In statistics section where we have follow graphs: Click below image:

it actually gives us a clear picture of how SYN,ack signals,handshaking works and how the packets are exchanging between different ip's.(Visual TraceRoute : Traceroute graphically)

In statistics section we have IO graphs: Click below image:



We can actually sniffing the packets and decode it to see the message content: Message after decoding is seen as follows:



Message which is sent is sniffed by USESDOPPER and message is seen and understood if at all it is not encrypted.(above images can be clicked to view properly)