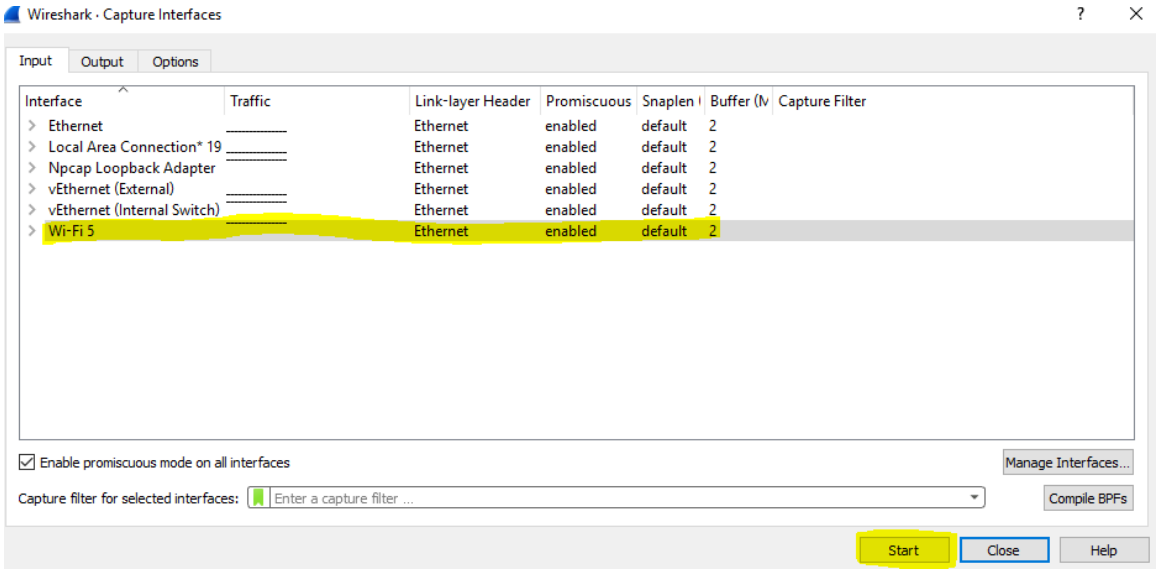
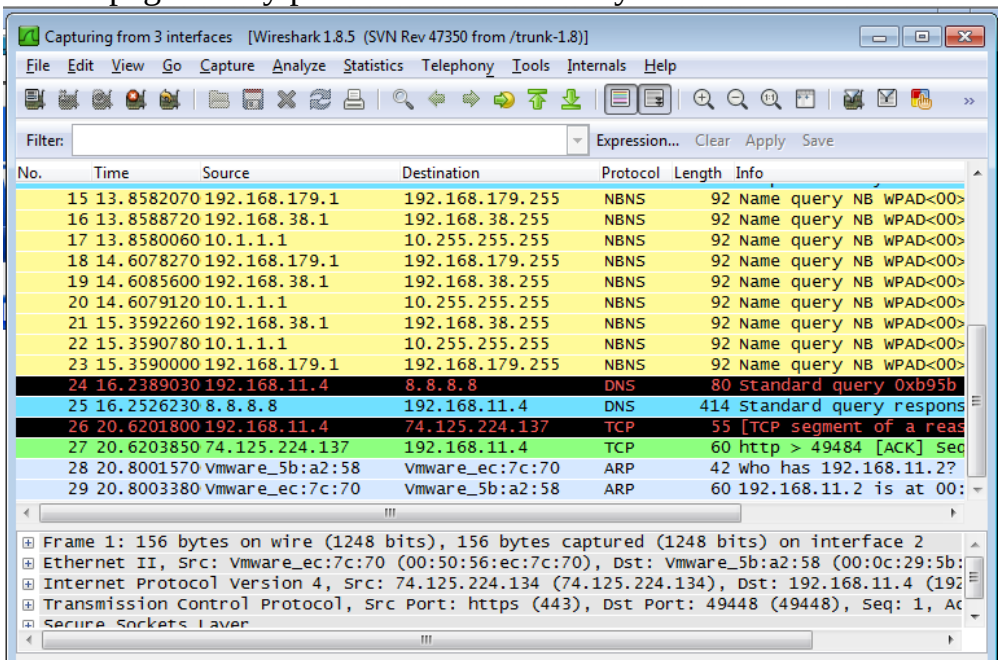
Exercise: Sniffing for key information using Wireshark

1. Click **Start**, **Wireshark**.
2. In Wireshark, click "**Capture**" Menu and **"Options"** and select the network interface (connected to internet).
3. Click the **Start** button.



4. You should see packets being captured and scrolling by, as shown below on this page. Every packet sent from or to your machine is shown here.



Testing sniffing password using www.altoromutual.com

1. Open a Web browser and go to http://www.altoromutual.com
2. On the web page, click "**Sign In**". Enter a Username : jsmith and Password : Demo123

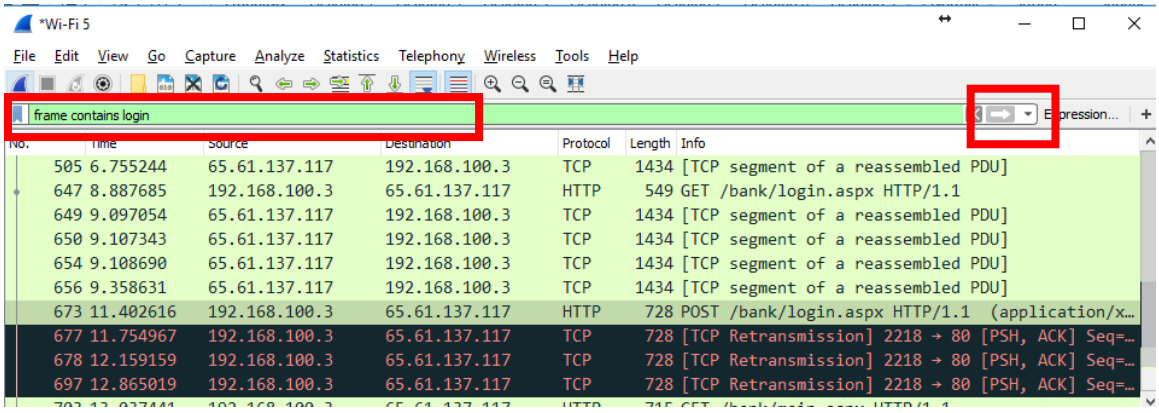
   If you get an error message, it's a normal behavior, we are just testing if we can sniff for passwords using Wireshark packets capture.

3. Click the "**Sign In**" button.
4. Goto Wireshark and **Stop** the capture.

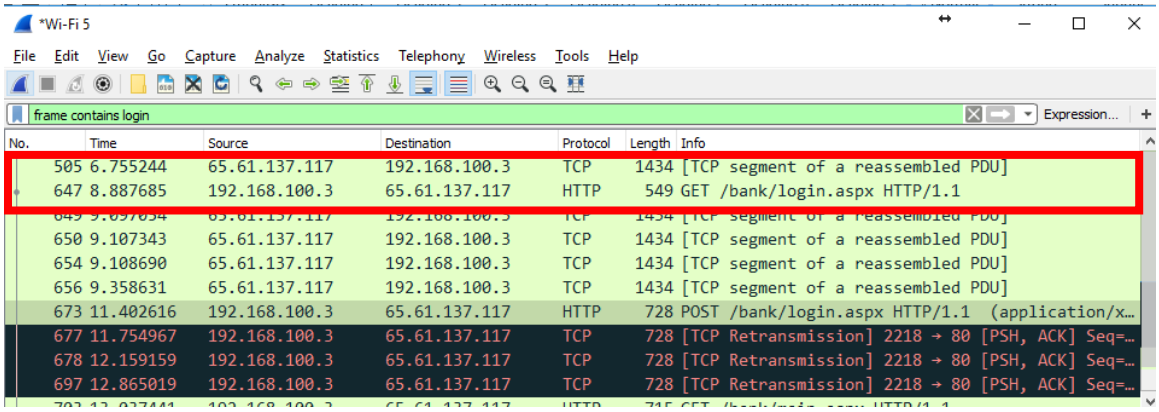
Observing the Password in Wireshark

1. In the Wireshark window, box, in the Filter bar, type this filter, as shown below:

frame contains login then press Apply



2. Explore the data packet to see if details of the login can be found



Starting Another Packet Capture

3. From the Wireshark menu bar, click **Capture**, **Start**.
   A Message pops up asking "Do you want to save the captured packets before starting a new capture?" Click "**Continue without saving**".

Using a Secure Password Transmission

1. In a Web browser, go to **mail.ksu.edu.sa**
2. Enter a Username of **YOURNAME** (using your own name, not the literal string "YOURNAME", and a **YOUR PASSWORD** of , as shown below.
3. Click the "**Sign in**" button.
4. In the Wireshark window, box, click Capture, Stop.
5. Try locating the login details.

Points to ponder:

Possible reason why Wireshark failed to find the login information for the **mail.ksu.edu.sa** login sequence.

Filters to be used with WireShark:

ip.addr==x.x.x.x
Display packets sent or received from to ip x.x.x.x.x
ip.src==x.x.x.x
Display packets sent from ip x.x.x.x
ip.dst==x.x.x.x
Display all packets received to ip x.x.x.x
tcp.port==x.x.x.x
Display all TCP packets sent or received from or to port no x.x.x.x
tcp.srcport==x.x.x.x
Display all TCP packets sent from port no x.x.x.x (as source port)
tcp.dstport==x.x.x.x
Display all TCP packets received to port no x.x.x.x (as destination port)
udp.port==x.x.x.x
Display all UDP packets sent or received from or to port no x.x.x.x
udp.srcport==x.x.x.x
Display all UDP packets sent from port no x.x.x.x (as source port)
udp.dstport==x.x.x.x
Display all UDP packets received to port no x.x.x.x (as destination port)
tcp.stream==x.x OR tcp.stream eq x.x
Display all TCP conversation/stream no x.x
udp.stream==x.x OR udp.stream eq x.x
Display all UDP conversation/stream no x.x
http.request
Display all POST or GET request from web server.
tcp.flags.syn==1
Display all TCP packets that SYN flags are set
tcp.flags.ack==1
Display all TCP packets that ACK flags are set
TCP
Display all TCP packets
UDP
Display all UDP packets
SNMP
Display all SNMP packets
OSPF
Display all OSPF packets
ARP
Display all ARP packets
DSN
Display all DNS packets
Udp.dstport==53
To display DNS requests

Udp.srcport==53

DNS replay

ICMP

Display all ICMP packets

Icmp.type==8

Display all ICMP packets of type request

Icmp.type==0