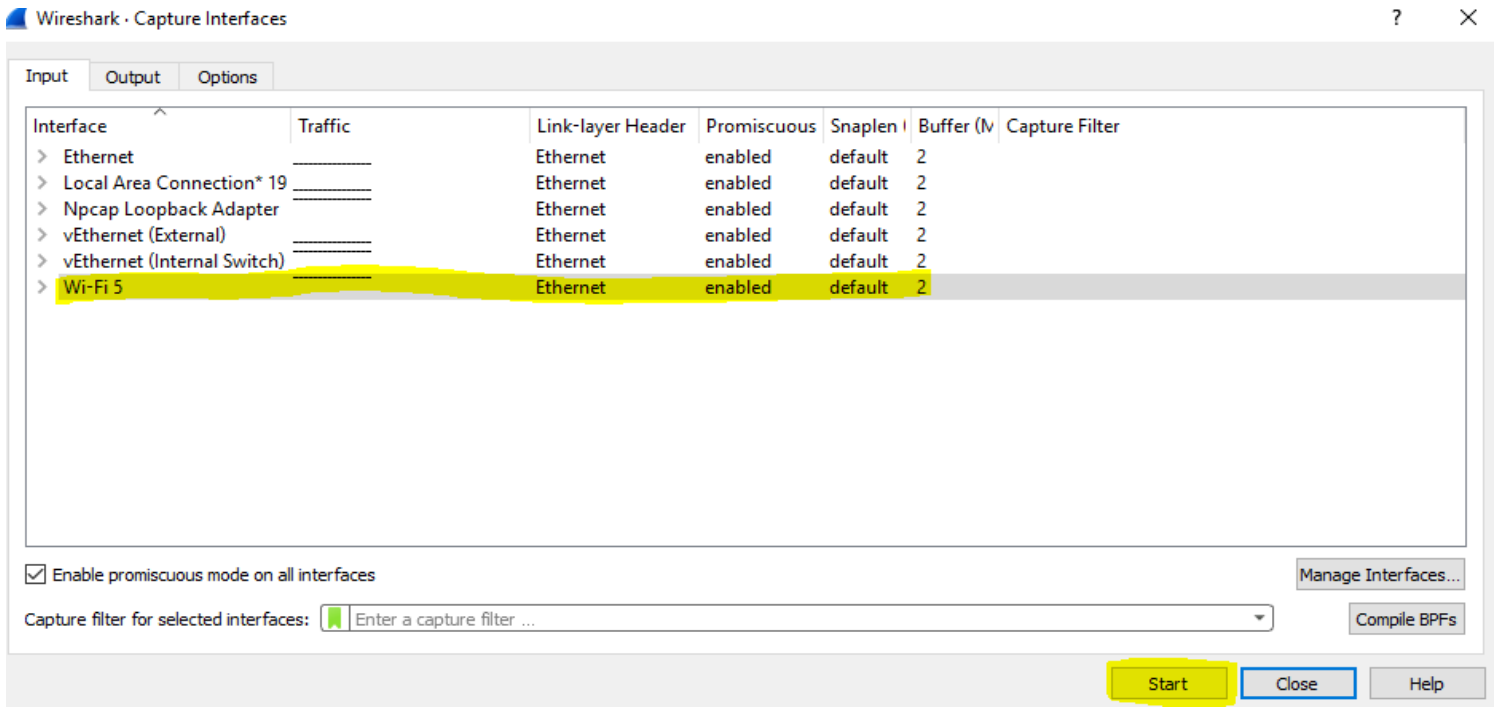
EXERCISE: DOWNLOAD AND INSTALL Wireshark

STEP 1 : DOWNLOAD Wireshark FROM HERE

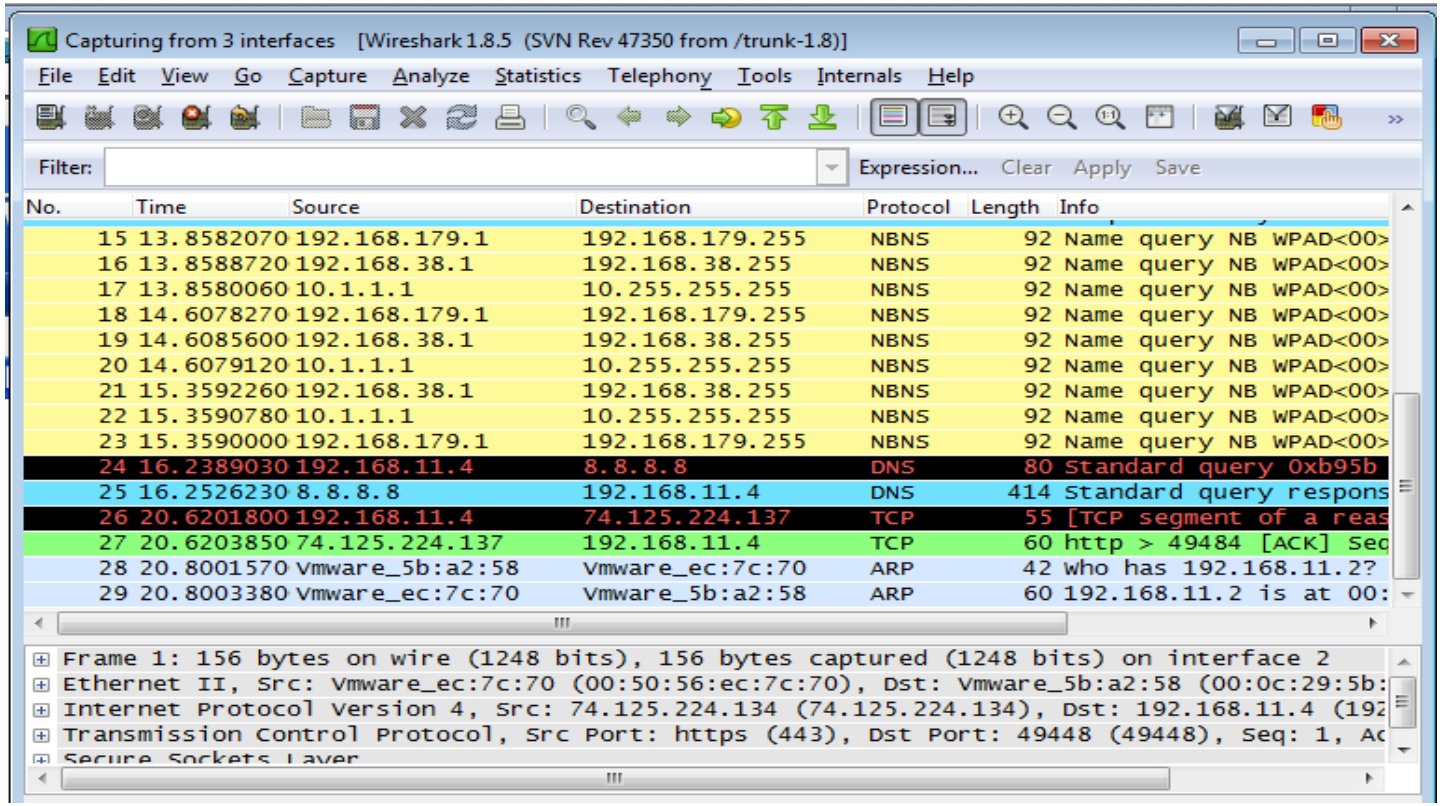
STEP 2: INSTALL THE Wireshark in Windows 7 VM.

STEP 3: In Wireshark, click "Capture" Menu and “Options” and select the network interface (connected to internet).

Click the Start button



STEP 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.



EXERCISE: Testing sniffing password using www.altoromutual.com

STEP 1 : Open a Web browser and go to http://www.altoromutual.com

STEP 2 : On the web page, click "Sign In". Enter a Username : Rehab 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.

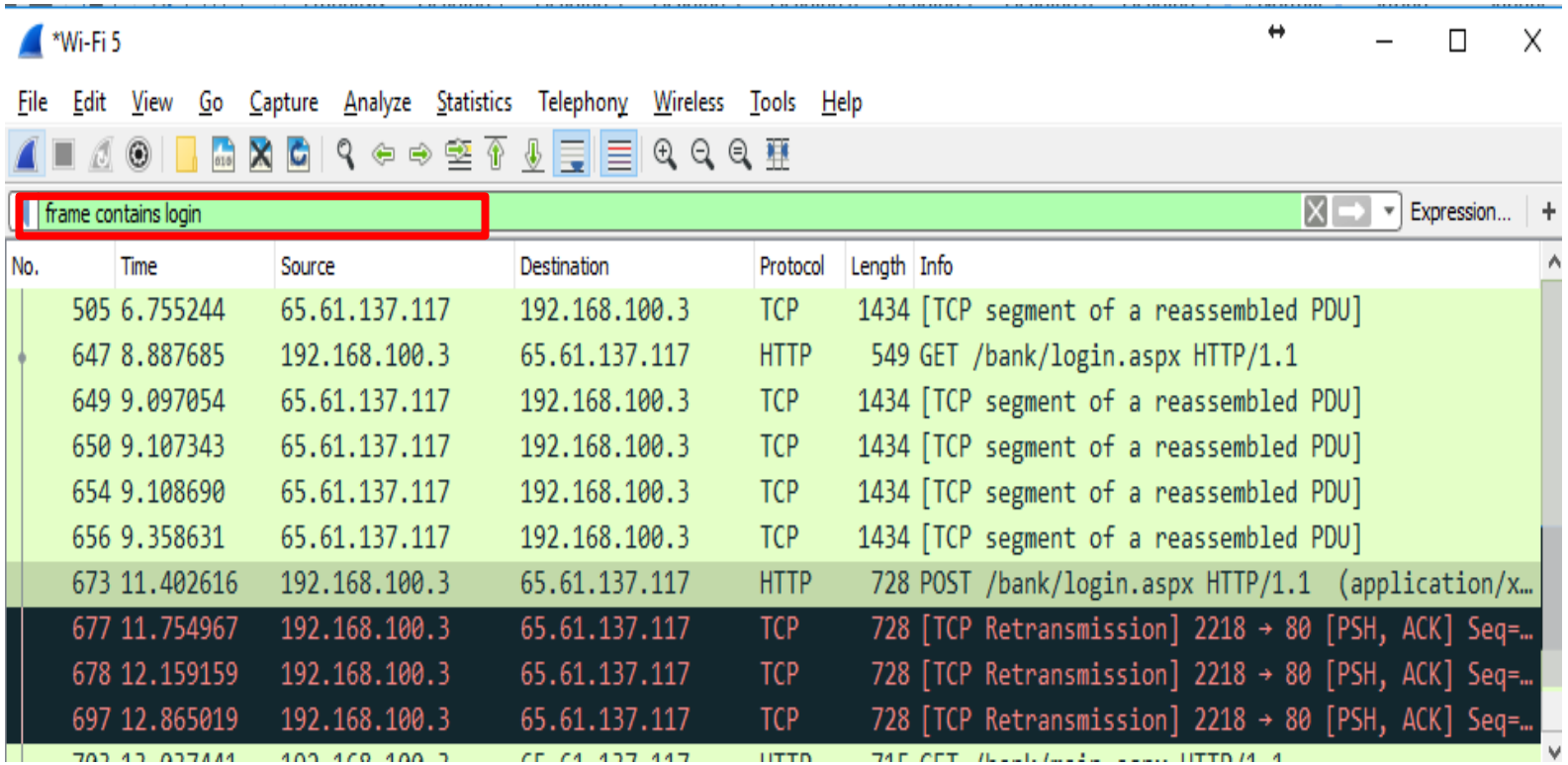
STEP 3 : Click the "Sign In" button.

STEP 4: Got o Wireshark and Stop the capture.

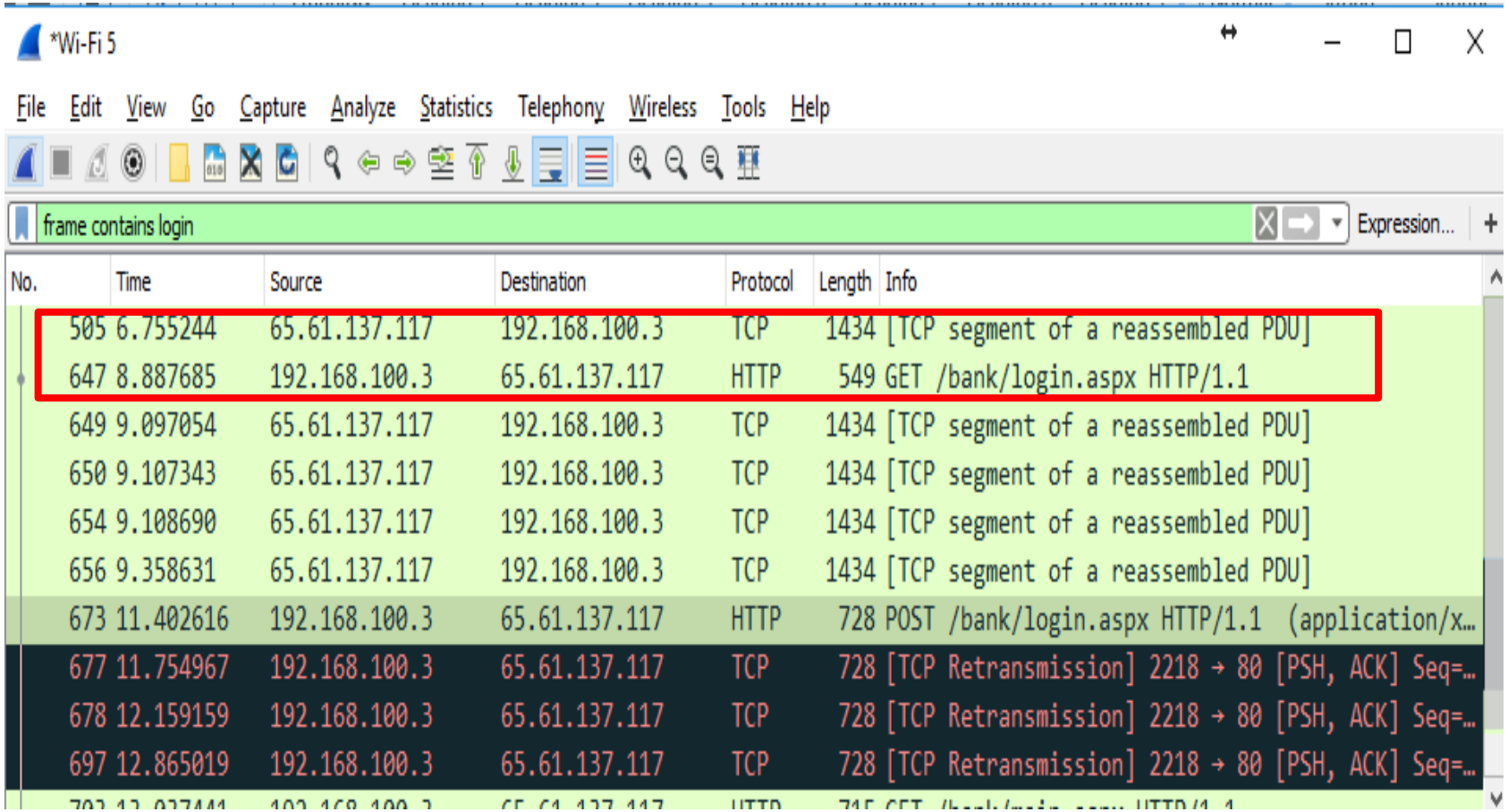
EXERCISE: Observing the Password in Wireshark

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



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".

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.

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

EXERCISE: Filters to be used with WIRESHARK

To display packets sent or received from to ip x.x.x.x.x
ip.addr==x.x.x.x
To display packets sent from ip x.x.x.x
ip.src==x.x.x.x
To display all packets received to ip x.x.x.x
ip.dst==x.x.x.x
To display all TCP packets sent or received from or to port no x.x.x.x
tcp.port==x.x.x.x
To display all TCP packets sent from port no x.x.x.x (as source port)
tcp.srcport==x.x.x.x
To display all TCP packets received to port no x.x.x.x (as destination port)
tcp.dstport==x.x.x.x
To display all UDP packets sent or received from or to port no x.x.x.x
udp.port==x.x.x.x

EXERCISE: Filters to be used with WIRESHARK

To display all UDP packets sent from port no x.x.x.x (as source port)
udp.srcport==x.x.x.x
To display all UDP packets received to port no x.x.x.x (as destination port)
udp.dstport==x.x.x.x
To display all TCP conversation/stream no x.x
tcp.stream==x.x OR tcp.stream eq x.x
To display all UDP conversation/stream no x.x
udp.stream==x.x OR udp.stream eq x.x
To display all POST or GET request from web server.
http.request
To display all TCP packets that SYN flags are set
tcp.flags.syn==1

EXERCISE: Filters to be used with WIRESHARK

Display all TCP packets that ACK flags are set
tcp.flags.ack==1
Display all TCP packets
tcp
Display all UDP packets
udp
Display all SNMP packets
snmp
Display all OSPF packets
ospf
Display all ARP packets
arp
Display all DNS packets (requests and replies)
dns

EXERCISE: Filters to be used with WIRESHARK

To display only DNS requests

udp.dstport==53

To display only DNS reply

udp.srcport==53

To display all ICMP packets (ping requests and ping replies)

icmp

To display only ICMP requests (ping requests)

icmp.type==8

To display only ICMP replies (ping replies)

icmp.type==0