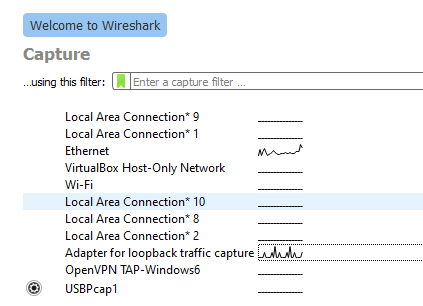
NOTE: I am not expecting a high mark on this lab, I do not know most of the information that this lab is asking me to display. The answers I have provided are a combination of the small amount of knowledge I have, (lots of) google, and guess work. Please keep this in mind and hopefully you don’t think I am a COMPLETE idiot. (only a partial one)

1.2

1.3 – ethernet and Adapter for loopback capture

2.2 – Its not the best way to capture traffic because it captures ALL network traffic, not just the one we are looking for

2.3.1 – 64 frames

2.3.2 – SSDP (I know this comes from a browser but I don’t have one open so IDK where its coming from)

2.3.3 – 192.168.0.1

2.3.4 – TCP

2.3.5 – The conversation coming from a browser

2.3.6 – It comes from a non certified IP so we cant trust it as it may be spoofed

3.1.1 – 10.162.101.197

3.1.2 – Because that is the only ARP request that got a response

3.1.3 – Cisco\_cb:49:02

3.1.4 – 113

3.2.1 – 10.162.101.197

3.2.2 – that the user is connecting to a website called [www.goal.com](http://www.goal.com)

3.2.3 – A three way handshake is happening so the host machine can establish a connection to the server

3.2.4 – It is a response to a certificate request on line 469

3.2.5 – A security protocol to exchange the encryption key so the encrypted data that is sent can be read (only by the intended recipient)

3.3.1 – A failed connection between two computers (perhaps a ddos attack)

3.3.1 – All the failed TCP requests

3.3.3 – Another user in the same home network because the IP addresses are near identical

3.4.1 – It appears to be an ARP scan/sweep, where someone (usually an attacker) is checking every IP address in a network sequentially to find out what responds

3.4.2 – because there is an overwhelming number of ARP requests that are sequential

3.4.3 – 10.162.101.67

3.5.1 – It appears to be an attacker attempting to connect to a server using SSH by trying a bunch of different keys

3.5.2 – 10.162.101.207