Packet Analysis with Wireshark

Step 1 Starting Capture (Interface selection & baseline)

The picture can't be displayed.

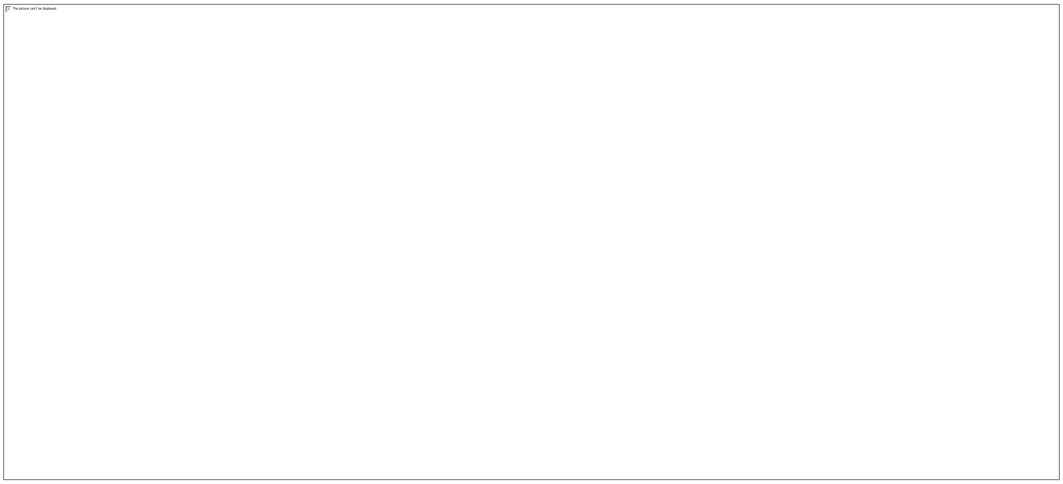
In other to login as root user to get direct access to the network I used Sudo wireshark.

Step 2 Start capturing Packets

The picture can't be displayed.

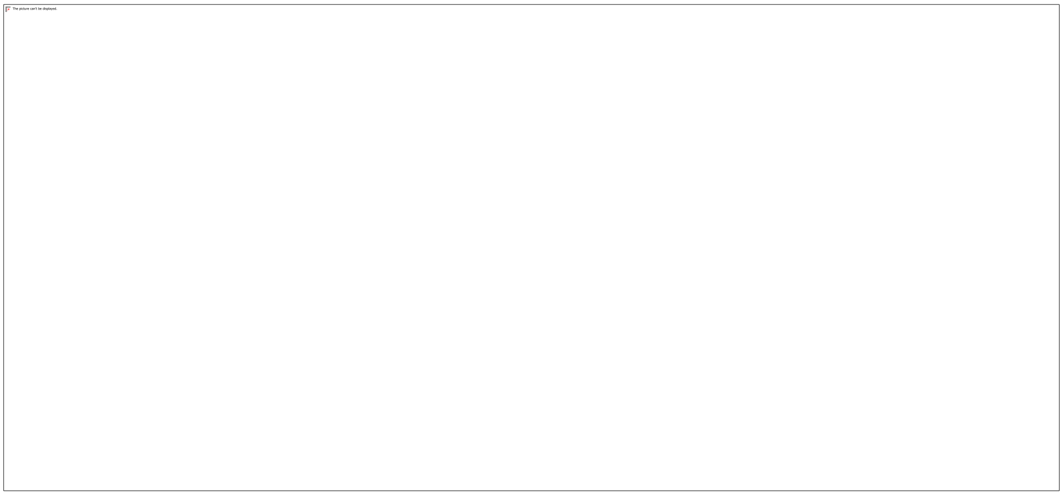
I started capturing packets from my network by clicking on the blue shark fin on the top left of the wireshark GUI interface

Step 3 Load up a website using HTTP unsecure port



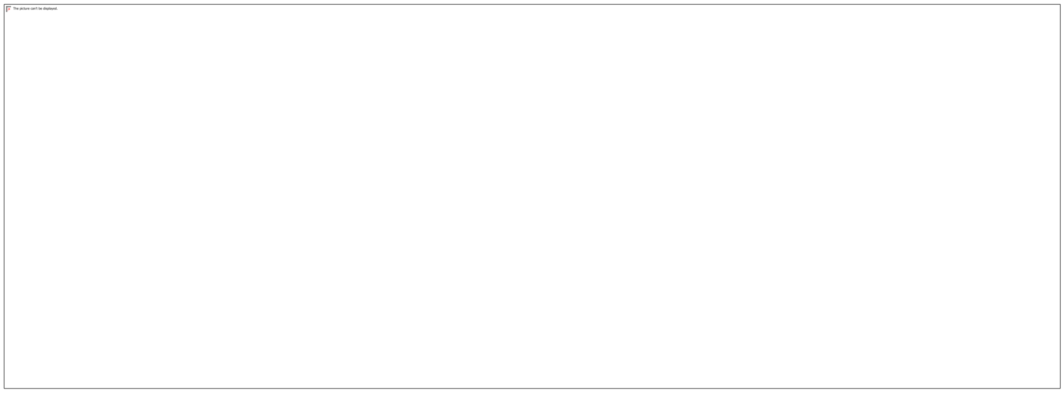
In other to get HTTP traffic from my network I load up a website using unsecure HTTP port 80

Step 4 Analyzing HTTP traffic



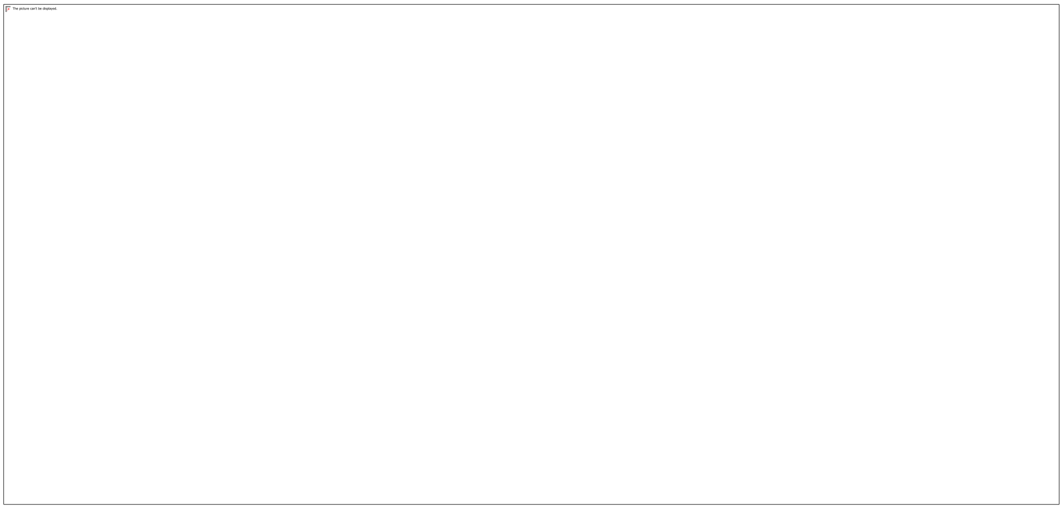
After getting a couple of traffic I streamline the filter by focusing on HTTP traffic alone, and I got a couple of details, seen the communication between my system and the http website I loaded previously.

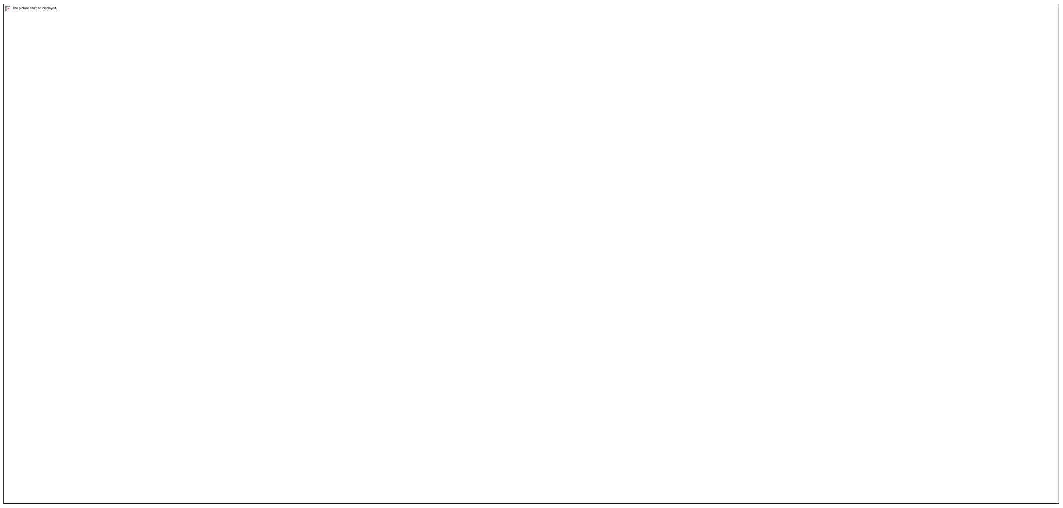
Step 5 HTTP Request / Response



To see more details about the http packet I click on one of the packet and click on the hypertext transfer protocol to find some details about the http connection, there I found a couple of details include the host website, the user agent that was used in connecting the http website, the OS that was used in connecting, the language of the web page and other detail.

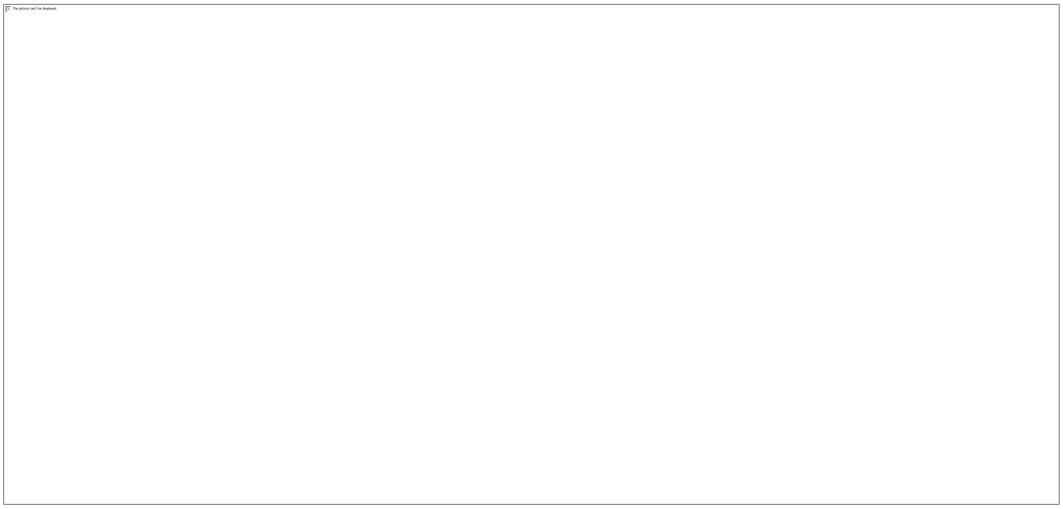
Step 6 Analyzing the packet to get more details about the website my system connected to via unsecure port 80





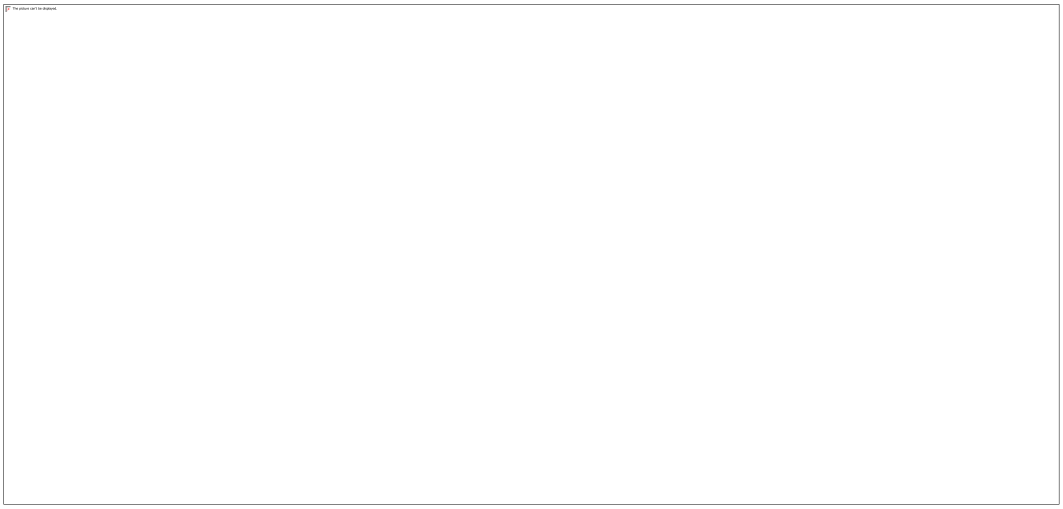
By right clicking on one of the packets and scrolling down on the drop bar to “Follow” I was able to view the TCP stream and got more details about the website including the HTML web page code.

Step 8 TCP port 80



Filtering for TCP port 80 I was able to see how my system connected and established communication with the website via TCP three way handshake (SYN, SYN ARK, ARK)

Step 9 — Final Notes / Wrap-up



Other details can be gotten from each and every packet that was scanned from your network it all depends on what you are looking to discover or troubleshoot.