# Project – Wireshark Lab – Discover who is talking on your network

# Key Concepts / Outcomes

Whether you are capturing live data, or are using a saved PCAP file, one of the first things you want to try and identify is what devices are communicating on your network.

This lab is intended to help you:

* Identify who is talking to whom on your network
* Locate the top talkers
* List applications that are seen on your network

# Tasks to complete

* Download the following pcap file : ***http-espn101.pcapng***
* Open the file using Wireshark

#### Let’s first try to identify who is talking to whom on this network capture.

* Select the “Statistics” tab and choose “Resolved Addresses”

1. List 10 different websites that were captured in this PCAP file?
2. gtm.ooyala.com.akadnes.ney
3. espn.go.com
4. google.com
5. imworldwide.com
6. symantec.com
7. overdrive1.visiblemeasures.com
8. log.wip.go.com
9. go.com.112.2o7.net
10. g1.v.fwmrm.net
11. akamaiedge.net

* Select the “Statistics” tab and choose “Protocol Hierarchy Statistics”

1. What percentage of the overall traffic was TCP traffic?

Percent packets: 96.3%, Percent Bytes 95.9%

1. What percentage of the overall traffic was UDP traffic?

Percent packets: 3.7%, Percent Bytes 0.0%

* Select the “Statistics” tab and choose “Conversations”
* Familiarize yourself with the Conversations window…
  + Select / deselect different conversation types
  + Select the different conversation type tabs along the top and see the different conversation lists
  + Click on the Name resolution box to convert IP addresses to resolved DNS names

1. How many IPv4 conversations can you identify in this PCAP?

37 conversations

1. How many conversations used TCP?

63 conversations

1. How many conversations used UDP?

82 conversations

* Return to the main Wireshark window and select Frame #5

1. What website is being visited in Frame #5? (I want the domain name, not just the IP address)

Frame #5 : www.espn.com

1. Since this appears to be a TCP connection, how many packets will be involved in the initial handshake?

It’s 3-way handshakes, so 2 packets involved in the initial handshake then it got 2 http packets after the handshakes. In total is 5 packets

1. List the frame #s that are involved in the initial TCP handshake.

the initial TCP handshake involved until frame #4891

1. Now that communication appears to have been established between the two devices, what is happening beginning with frame 8?

It started to extract the http data then established communication with domain server.

1. How many frames are involved in an HTTP handshake?

Just 1 handshake.

1. List the frames that are involved in the HTTP handshake beginning with frame #8.

Frame #9

1. There appears to be some sort of error in the response packet. What appears to have happened?

Redirect error respond code 301/302. What means the destination or doc trying to access has been moved to other destination.

* Go into the HTTP portion of frame #9 and look for the “Location” field.

1. What do you learn from the “Location field of frame #9?

That the espn server communicated with the ISP provider comcast.

1. Explain what you see happening in the following frames:
   * Frame 10 – Ipv4 request from espn to comcast the isp/domain server
   * Frame 11 – domain server is looking into the answer
   * Frame 12 – Ipv6 request from espn to comcast the isp/domain server
   * Frame 13 - domain server is looking into the answer
2. What is the difference between an A address and an AAAA address?
   * A address = IPv4
   * AAAA address = IPv6
3. Now explain what you think is happening in the following frames:
   * Frame 14 – Reestablish the communication with espn that they know the answer | TCP (1/3 handshake) \* are you there espn
   * Frame 15 – espn respond to comcast that espn received the answer | TCP (2/3 handshake) \*yes
   * Frame 16 – comcast confirmed that espn is there |TCP (3/3 handshake)
   * Frame 17 – comcast sent the http that the espn requested

* Go to the very end of frame 17 and explain what you see in the last four fields of the frame’s HTTP section.

1. How many other frames are involved in this request?

2 frames , frame 128 and frame 4612

1. What frame contains the response to this particular request?

TCP segments, plain texts of website script.

1. What frame contains the next request?

Frame #4612

* Go to the next frame in the request

1. What frame contains the response to this second request?

Request URI update addresss, cookie pair, URI query. Prev frame request, Frame respond, next request frame.

* Go to the frame that contains the response to this second request. Wireshark has organized the last section of the frame under the title “JavaScript Object Notation.” JSON is a common format for storing and transporting data across the internet. Let’s see if we can determine what the user was reading, shall we?
* Open the JSON section and you will see a section called Object. Inside this object you will find 2 member keys.

1. What are the names of the 2 member keys?

snapshotId and snapshots

* Open the second member key and you should see a list of several objects (don’t count them, there are a lot….)
* Open the first object under the Array list and you should see 4 different member keys that are associated with this object.

1. Describe what you think this frame contains

It has a linked to twitter talking about Brandon Jenkins, probably the website cited news from twitter.

1. What do we know from Member key #1?

The entity: snapshotsID, The entity number is the number value. Probably is something from snapshot

1. What do we know from Member key #2?

The info contains in snapshot. Like where the source comes from Twitter, and the plain text contain in it.

#### Now let’s try and determine who are the most active talkers on the network in this capture file

* Sometimes if a network seems to be acting sluggish, you may be interested in seeing if there are any conversations that are taking up lots of bandwidth. This could be symptomatic of someone streaming a video, or sporting event.
* Go back to the main capture page and let’s open a different statistics page.
* Select “Statistics” and then “Conversations” and then choose the IPv4 tab of the Conversations window.
* Let’s sort by the number of bytes in each conversation from most to fewest, so click on the Bytes tab twice.

1. What two IP addresses are communicating in this conversation?

24.6.173.220 and 184.84.222.88

1. How many bytes have been transferred between the 2 of them?

2020k

* Go back to the main window and select “Statistics” and then “Endpoints.”
* Select IPv4 and then sort by the number of Bytes to determine the most chatty node on the network.

1. What device is the most active on the network?

Cadant\_31:bb:c1

1. If you resolve the domain name, who do you think this device is?

ISP provider comcast

#### Can we figure out what he “googled”?

* Go to the main Wireshark window and select “Statistics” and then “Endpoints”.
* Select the “Name Resolution” box at the bottom-left of the screen.

1. List four websites that were visited during this capture file
   * Website 1: espn.go.com
   * Website 2: google.com
   * Website 3: imrworldwide.com
   * Website 4: omtrdc.net

* Find the endpoint that includes “google.com” and highlight that entry in the table.
* Right-click on the highlighted entry and select “Apply as a filter” – “Selected”
* Make sure the list is sorted sequentially by frame number (column 1)

1. Describe what is happening in the first 3 packets of this filtered list.

They are tcp protocol handshakes that requested to google.com

* Find the first HTTP packet that shows a “Get” request and highlight that frame.
* Right click on that frame and select “Colorize conversation” and then choose a unique color for this filter.

1. Insert a screen shot of the colored frames

A picture containing table

Description automatically generated

* Find frame number 693.

1. Is this one of your newly colored frames?

yes

1. What appears to be happening in this frame? (hint: look in the Info field)

It has a picture file in it. File type: jpg

1. What is the name of the file that was downloaded?

Serve\_ESPN\_Sweepstakes\_300x250.jpg

* Fine frame number 724.

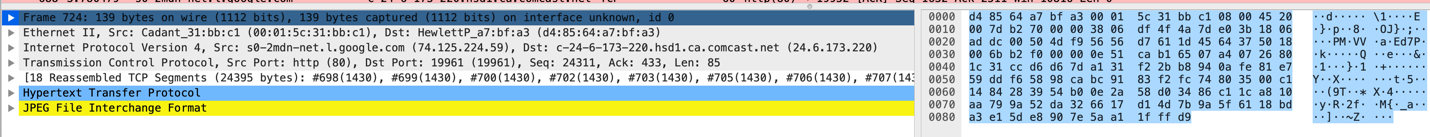
1. What appears to be happening here?

* TCP is able to break a large file down into smaller segments and can send each segment as a separate frame, then reassemble all the segments back together once all the segments arrive.

1. How many segments was this .jpg file broken into?

8 segments

1. Show a screenshot of all the frames that contain part of this file.



# What to submit to LMS

Download this file, answer all the questions and upload the completed document to the LMS.