INTERNETWORKING MISC

CS 130

Creative Software Architectures for Collaborative Projects

Prof. Donald J. Patterson

Content adapted from Essentials of Software Engineering 3rd edition by Tsui, Karam, Bernal
Jones and Bartlett Learning

TOOLS SHOWN TODAY

MTR

- A network diagnostic tool
  - example “sudo mtr -t www.djp3.net”

```
                                My traceroute  [v0.86]
Codex-Perductum.local (0.0.0.0)                                Wed Sep  7 10:07:19 2016
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                  Packets                Pings
 Host                                          Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.45.63.254                                0.0%     8    0.8   0.8   0.6   1.0   0.0
 2. KHCore-KHDist.westmont.edu                  0.0%     8    0.9   0.8   0.7   0.9   0.0
 3. PA-FW.westmont.edu                          0.0%     8    1.3   1.2   0.9   1.5   0.0
 4. ip176-11.outside.westmont.edu               0.0%     8    1.8   1.5   1.3   1.8   0.0
 5. wsip-174-78-247-41.sd.sd.cox.net            0.0%     8    6.7   6.1   5.5   6.7   0.0
 6. ip68-4-11-200.oc.oc.cox.net                 0.0%     8    6.5   6.8   5.5  14.1   2.9
 7. ashbbprj02-ae2.0.rd.as.cox.net              0.0%     7   78.9  79.0  78.4  79.7   0.0
 8. aggr501a-94-core9.iad3.rackspace.net        0.0%     7   79.9  79.6  79.2  80.1   0.0
 9. ???
10. corea-dcpe1.iad3.rackspace.net              0.0%     7   79.8  79.8  79.5  80.3   0.0
11. corea-core7.iad3.rackspace.net              0.0%     7   80.5  80.1  79.3  80.9   0.0
12. core7-aggr403a-8.iad3.rackspace.net         0.0%     7   79.9  79.6  79.3  80.0   0.0
13. 104.239.160.189                             0.0%     7   79.5  79.5  79.1  80.1   0.0
```

TOOLS SHOWN TODAY

MTR

- “combines the functionality of the traceroute and ping programs in a single network diagnostic tool.
- As mtr starts, it investigates the network connection between the host mtr runs on and HOSTNAME by sending packets with purposely low TTLs. It continues to send packets with low TTL, noting the response time of the intervening routers. This allows mtr to print the response percentage and response times of the internet route to HOSTNAME. A sudden increase in packet loss or response time is often an indication of a bad (or simply overloaded) link.
- The results are usually reported as round-trip-response times in milliseconds and the percentage of packetloss.”

TOOLS SHOWN TODAY

DIG

- A DNS lookup utility
  - "dig +trace www.djp3.net"

```
; <<>> DiG 9.8.3-P1 <<>> +trace www.djp3.net
;; global options: +cmd
.                       262510  IN      NS      b.root-servers.net.
.                       262510  IN      NS      g.root-servers.net.
.                       262510  IN      NS      m.root-servers.net.
.                       262510  IN      NS      i.root-servers.net.
.                       262510  IN      NS      a.root-servers.net.
.                       262510  IN      NS      j.root-servers.net.
.                       262510  IN      NS      k.root-servers.net.
.                       262510  IN      NS      d.root-servers.net.
.                       262510  IN      NS      l.root-servers.net.
.                       262510  IN      NS      h.root-servers.net.
.                       262510  IN      NS      c.root-servers.net.
.                       262510  IN      NS      f.root-servers.net.
.                       262510  IN      NS      e.root-servers.net.
;; Received 508 bytes from 10.50.10.4#53(10.50.10.4) in 61 ms

net.                    172800  IN      NS      e.gtld-servers.net.
net.                    172800  IN      NS      g.gtld-servers.net.
net.                    172800  IN      NS      k.gtld-servers.net.
net.                    172800  IN      NS      i.gtld-servers.net.
net.                    172800  IN      NS      c.gtld-servers.net.
net.                    172800  IN      NS      l.gtld-servers.net.
net.                    172800  IN      NS      a.gtld-servers.net.
net.                    172800  IN      NS      h.gtld-servers.net.
net.                    172800  IN      NS      m.gtld-servers.net.
net.                    172800  IN      NS      j.gtld-servers.net.
net.                    172800  IN      NS      f.gtld-servers.net.
net.                    172800  IN      NS      d.gtld-servers.net.
net.                    172800  IN      NS      b.gtld-servers.net.
;; Received 499 bytes from 192.5.5.241#53(192.5.5.241) in 109 ms

djp3.net.               172800  IN      NS      ns3.hover.com.
djp3.net.               172800  IN      NS      ns1.hover.com.
djp3.net.               172800  IN      NS      ns2.hover.com.
;; Received 141 bytes from 192.43.172.30#53(192.43.172.30) in 65 ms

www.djp3.net.           900     IN      A       104.239.160.189
;; Received 46 bytes from 64.98.148.13#53(64.98.148.13) in 73 ms
```

TOOLS SHOWN TODAY

DIG

- “dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools tend to have less functionality than dig.”

TOOLS SHOWN TODAY

HOST

- A DNS lookup utility

```
[504]djp3@Codex-Perductum: ~
$ host www.westmont.edu
www.westmont.edu has address 10.50.10.130
[505]djp3@Codex-Perductum: ~
$ host 10.50.10.130
130.10.50.10.in-addr.arpa domain name pointer www.westmont.edu.
```

TOOLS SHOWN TODAY

HOST

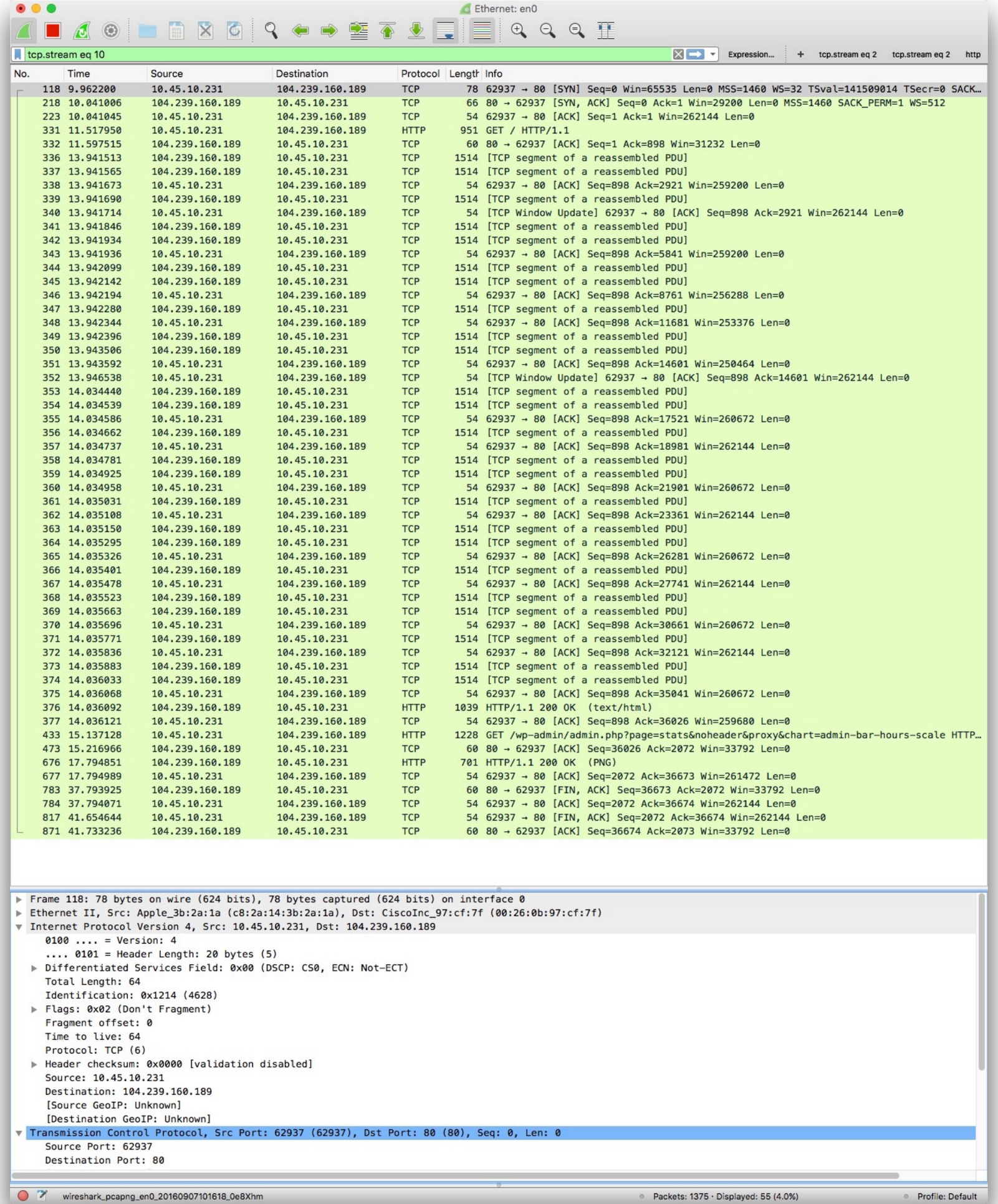
- “host is a simple utility for performing DNS lookups. It is normally used to convert names to IP addresses and vice versa. When no arguments or options are given, host prints a short summary of its command line arguments and options.”

TOOLS SHOWN TODAY

WIRESHARK

- “Interactively dump and analyze network traffic”

- “Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions.”
- https://www.wireshark.org/
  - recommend install with package manager like brew



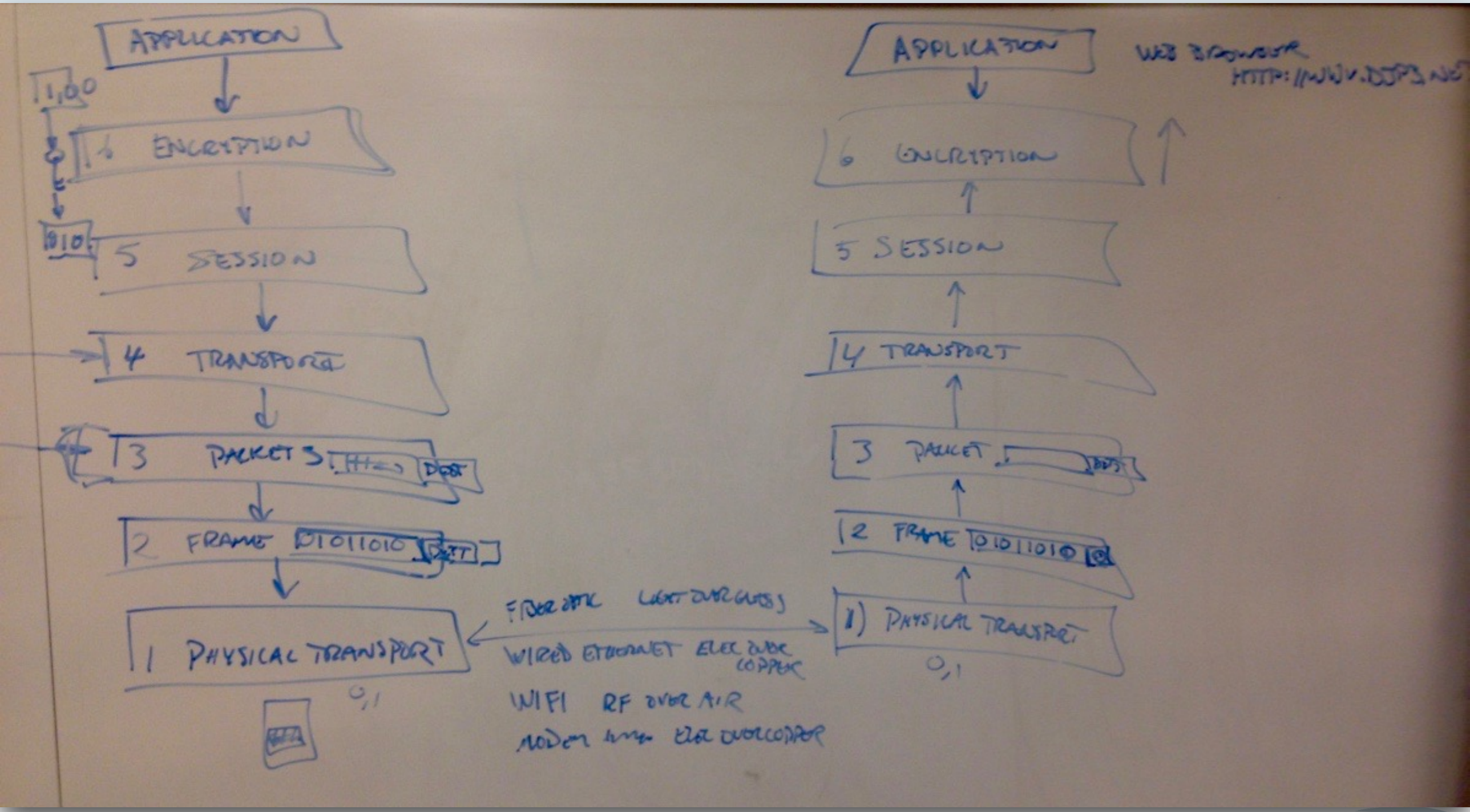
This is the complete network traffic exchange for loading www.djp3.net in Chrome, down to the individual bits that were sent across the Ethernet

TOOLS SHOWN TODAY

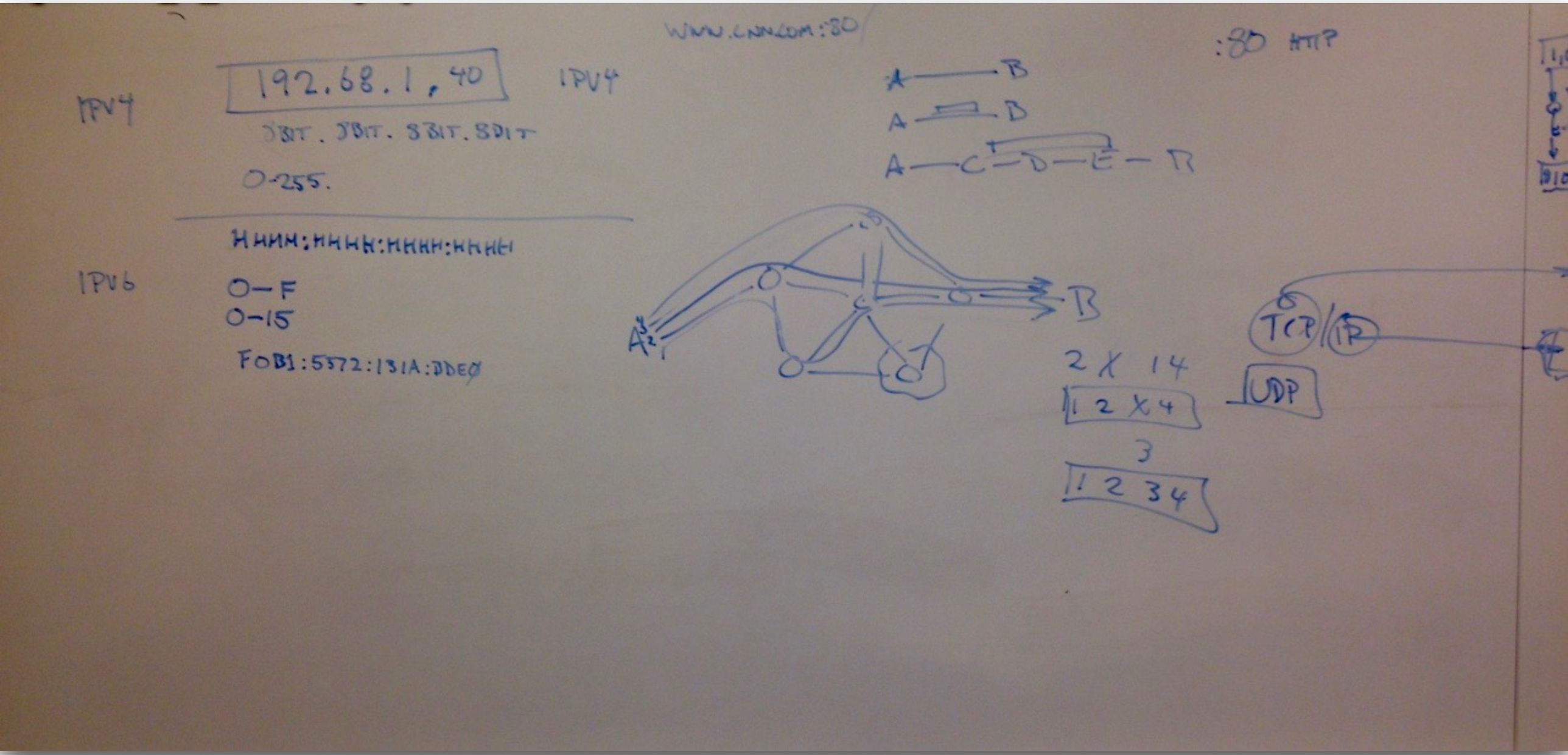
WIRESHARK

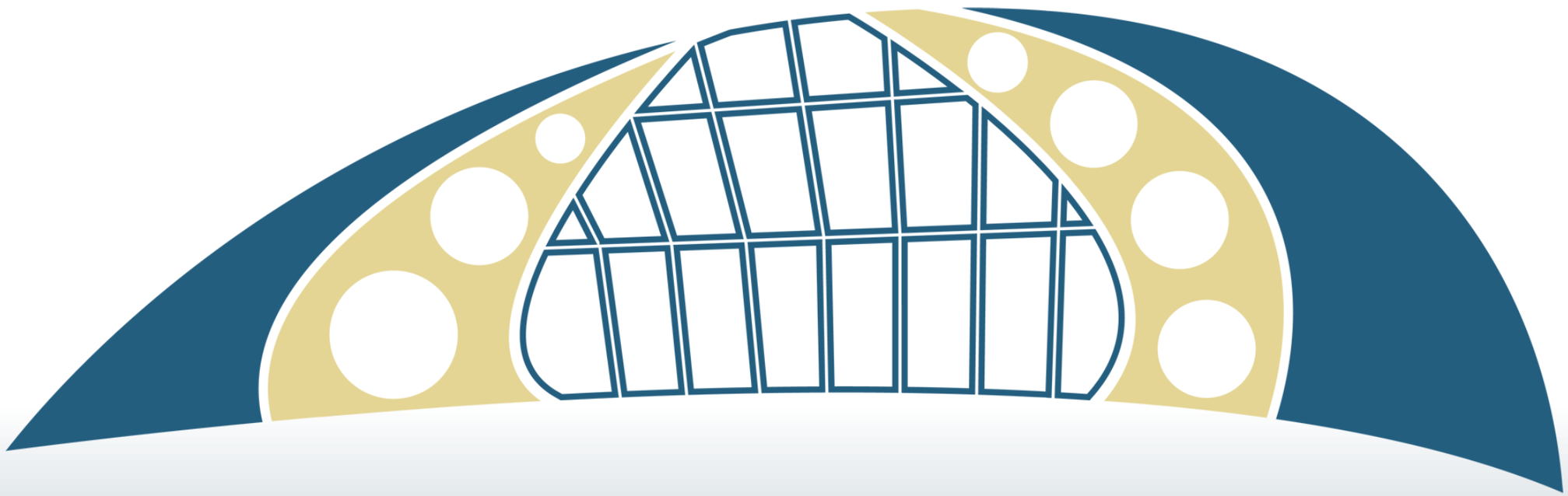
- “Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions.”

OSI MODEL OF THE NETWORK



NETWORKING DETAILS





WESTMONT INSPIRED

COMPUTING LAB