**Wireshark**

* Wireshark is a network packet capturing and analysis tool
* Wireshark can import .pcap files, which is a file of a saved packet capture session
* Wireshark has 3 panes that display different information about the current capturing session
* The display filter allows quick filtering of certain packets (The bookmark button to the left of the 'Apply a display filter...' line will give a few example filters)

**Pane 1: Packet Stream**

* The packet stream pane displays every captured packet in the current session
* Important information in this pane includes source and destination IP/MAC addresses, Protocol and Info
* The color coding can give some visual representation of the packet's purpose (ie. Black color usually means that the packet is related to an error, like packet retransmission or unreachable destination)

**Pane 2: Packet Information**

* The packet information pane lists as much information about the selected packet as one could need
* Most information can be derived without using the drop down arrow, but if more detail is desired, you may use the drop down arrow to get more detailed information

**Pane 3: Packet Data**

* The packet data pane displays the hex information of the packets data
* This is where you can see what types of files are being sent by the packet and any hidden plain text messages in the packet data

**Simple HTTP Request**

* Packets 1-3 show SYN/ACK handshake between user and server
* Packet 4 shows GET request
* Packet 6 shows requested document (HTML) being sent

**HTTP w/ jpegs**

* Use filter http.request.method == GET (case-sensitive)
* Right click packet 50 and click 'follow' then click 'HTTP stream'
* Note the filter has changed to follow a particular stream of packets associated with that particular get request
* select packet 72 and, in pane 2 right click the line that says 'JPEG File Interchange Format'
* select 'Show Packet Bytes...'

(if time show arp spoofing pcap file)