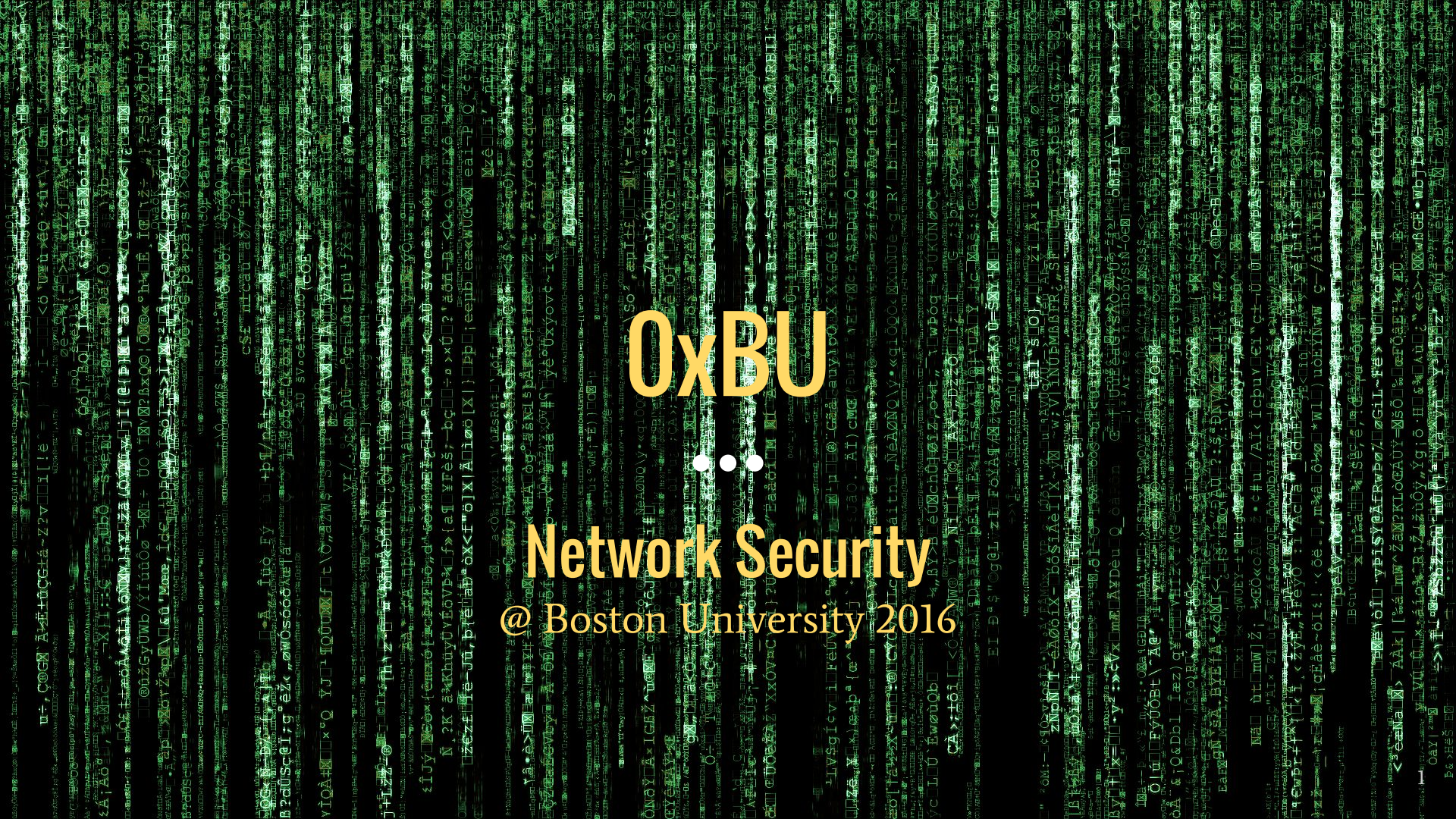
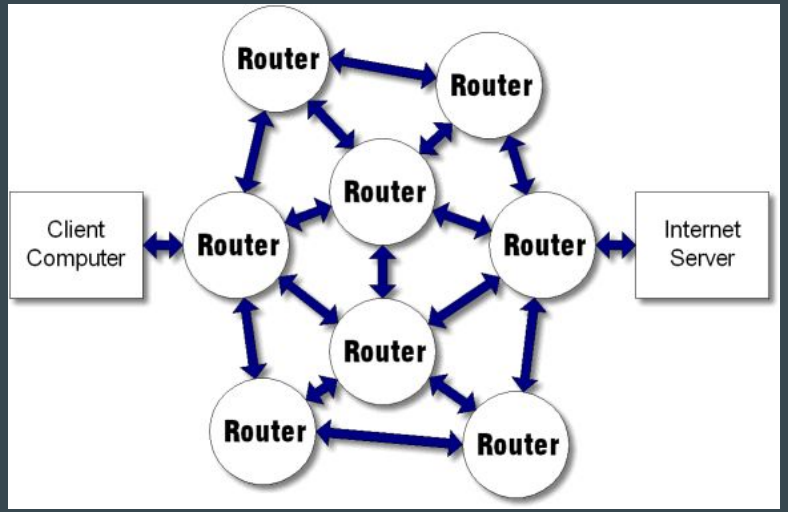

0xBU
Network Security
@ Boston University 2016

What is the Internet (⅓)

- The Internet is a set of protocols
- Request for Comments (RFCs) organized by the Internet Engineering Task Force (IETF)
  - rfc791: "Internet Protocol"
  - rfc2616: "Hypertext Transfer Protocol -- HTTP/1.1"
  - rfc1149: "A Standard for the Transmission of IP Datagrams on Avian Carriers"

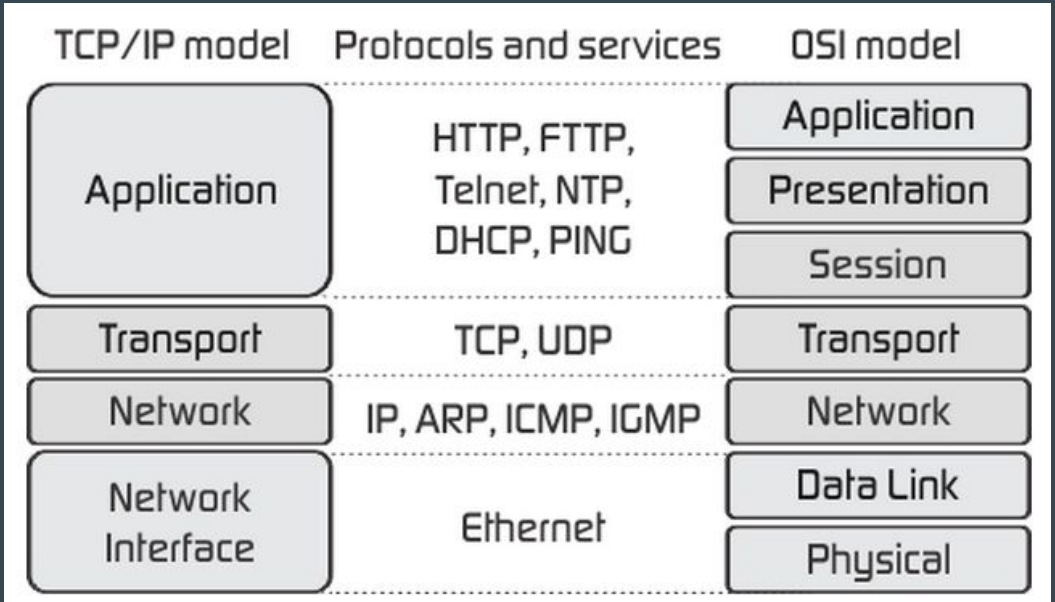
What is the Internet (⅔)

- The Internet works through a bunch of routers/hops.
  - Packets, move from one router to the other, without preserving any state.
  - The router has no clue Mary's 10 packets relate to each other.
  - Intelligence is done by the end-hosts, e.g. your browser/operating system.
  - Robust simplicity by being "dumb".



What is the Internet (3/3)

- The Internet has a layered design.
  - Each layer relies on layers below it.
  - Each layer provides a service to the layer above it.

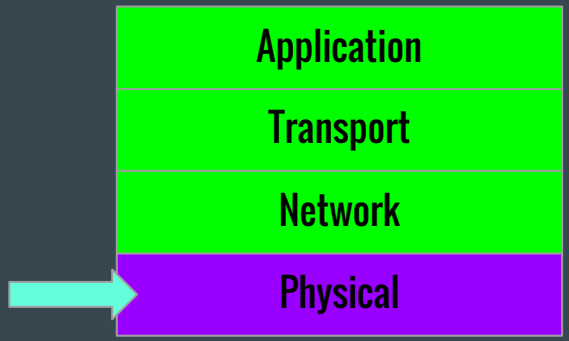


What do we want secure about the Internet?

- Confidentiality
  - No one can read our data unless we want them to.
  - Eve reading your emails =(
- Integrity
  - No one can manipulate our data unless we want them to.
  - Eve editing our emails =(
- Availability
  - We can access our data when want to
  - Eve ruining your Xbox experience =(

Physical Layer

The actual wire + transforming electricity into digital data



Physical Layer Security

- One of the hardest to secure
  - Attacker can eavesdrop =(
  - Attacker can spoof messages =(
  - The closest to the origin you can get

In an effort to alter the balance of Cold War, these men scoured the ocean floor for a five-inch diameter cable carry secret Soviet communications between military bases.

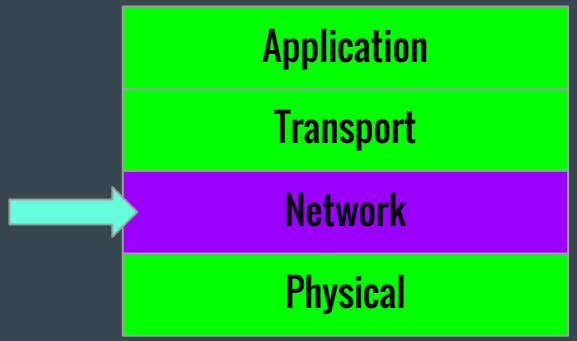
The divers found the cable and installed a 20-foot long listening device on the cable. designed to attach to the cable without piercing the casing, the device recorded all communications that occurred.

Upon their return to the United States, intelligence agents from the NSA analyzed the recordings and tried to decipher any encrypted information. The Soviets apparently were confident in the security of their communications lines, as a surprising amount of sensitive information traveled through the lines without encryption.

Upon their return to the United States, intelligence agents from the NSA analyzed the recordings and tried to decipher any encrypted information. The Soviets apparently were confident in the security of their communications lines, as a surprising amount of sensitive information traveled through the lines without encryption.

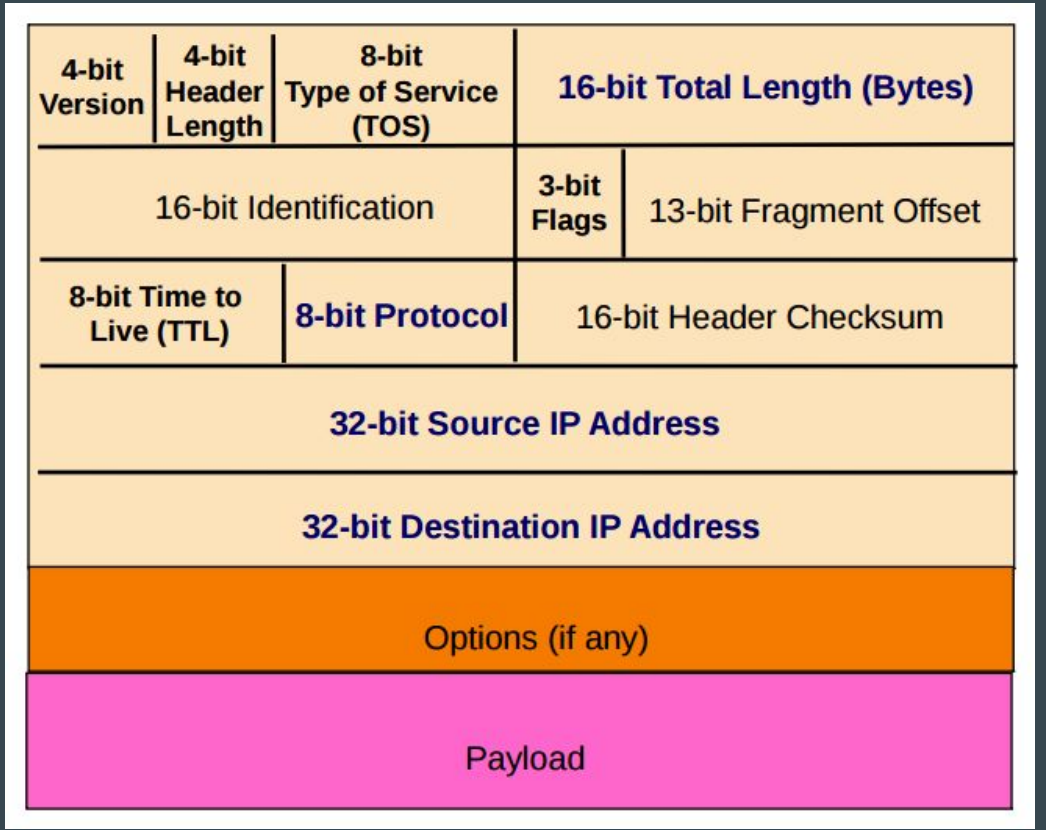
Network Layer

Transmitting digital packets, to communicate with other computers



IP Packet

- Maximum size: 65,535 bytes
- May fragment (split) into multiple pieces if a router decides
- "Best effort" protocol
  - Packets may be lost
  - Packets may be corrupted
  - Packets may be out of order
  - ???
- Payload can be anything!

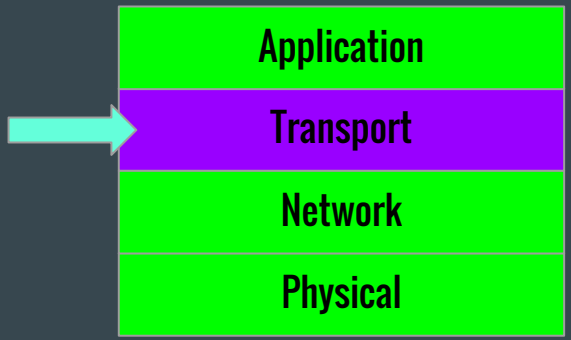


IP Packet Security

- Can set arbitrary source address
  - “Spoofing” - receiver has no idea who you are
  - Can send unwelcome return traffic to the spoof source address
- Can set arbitrary destination address
  - Enables “scanning” - brute force searching for hosts

Transport Layer

Transmitting digital packets, to communicate with other computer



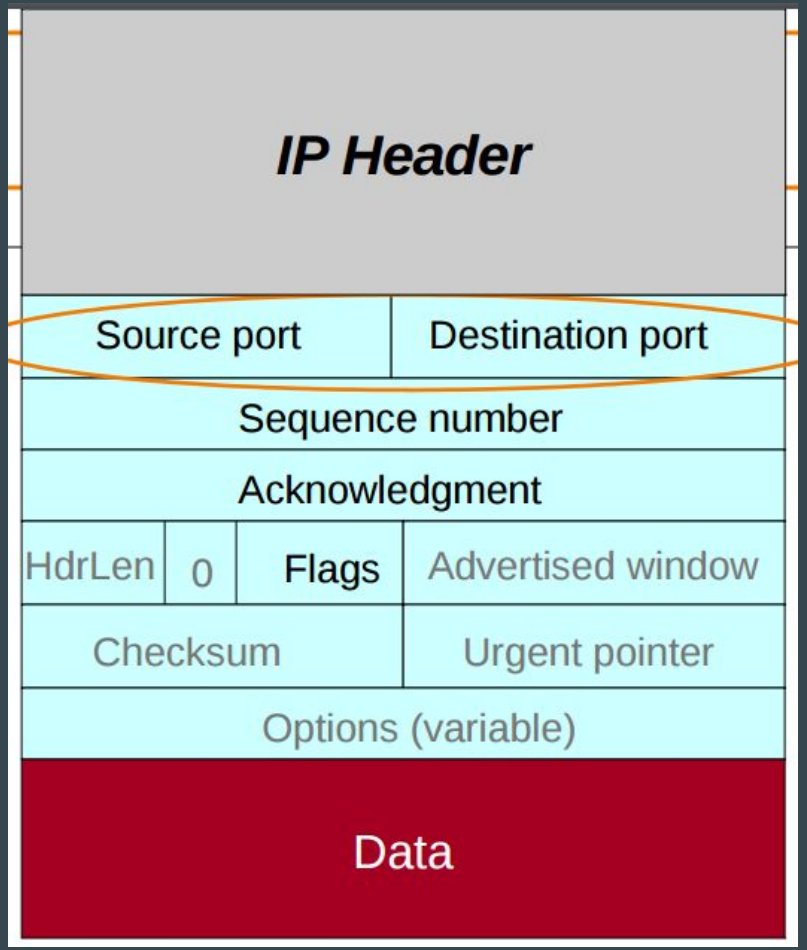
Transport Protocols

UDP - Fast. Unreliable. Simple.

TCP - Slow. Reliable. Complex.

TCP Packet

- Reliable
  - In-order packets!
  - Packet-loss detection!
- Connections
- Contained in payload of an IP packet
- Payload can be anything!



TCP (Transportation Layer)

"Hi, I'd like to hear a TCP joke."
"Hello, would you like to hear a TCP joke?"
"Yes, I'd like to hear a TCP joke."
"OK, I'll tell you a TCP joke."
"Ok, I will hear a TCP joke."
"Are you ready to hear a TCP joke?"
"Yes, I am ready to hear a TCP joke."
... (it goes on)

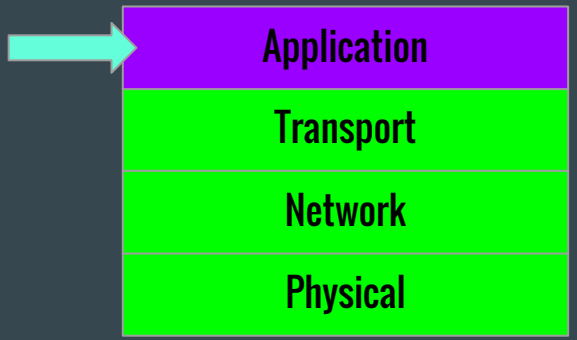
TCP Security

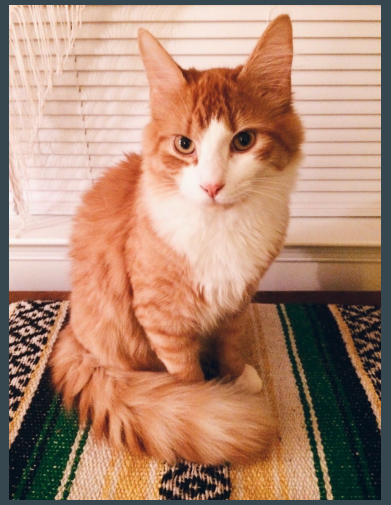
- The world is full of cheaters
  - Receiver can get data to come to them faster
- An attack simply needs to know the source and destination ports, and sequence numbers to disrupt your connection
- The same is true for injecting data, “session hijacking”

If an attacker sees (or guesses) your TCP data, then you’re gonna have a bad time

Application Layer

Everything else we need, including cat pics





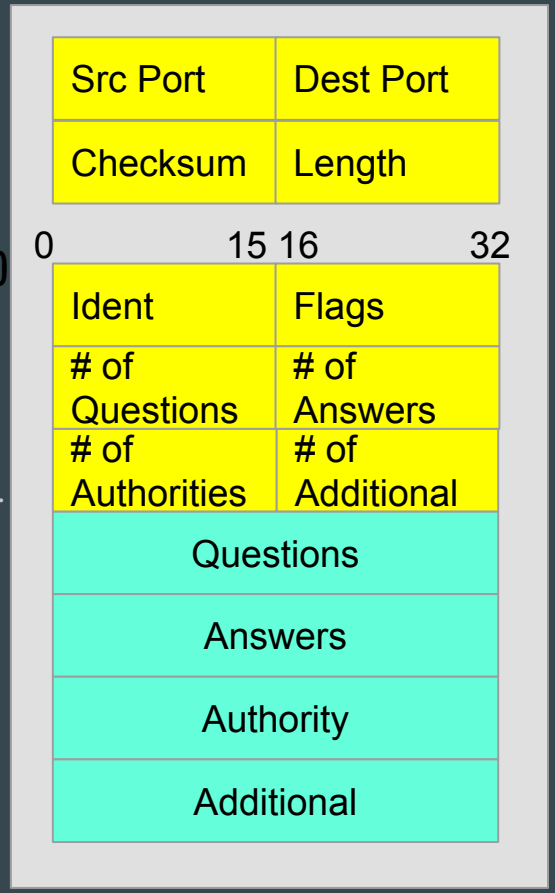
DNS (Application Layer)

People like to remember names, not IP addresses.
DNS (Domain Name System) is a distributed system to map names to IP addresses.
DNS is at the application layer of the Internet stack.

- A single root server, and a set of top-level domain (TLD) servers
  - Websites are actually "google.com." <-- Note the `.' Try it for yourself!
  - The `.' is the root server.
  - The '.com' is the TLD.
- More local (i.e. faster) DNS servers get information from the TLDs.
  - And pass that information on to you.

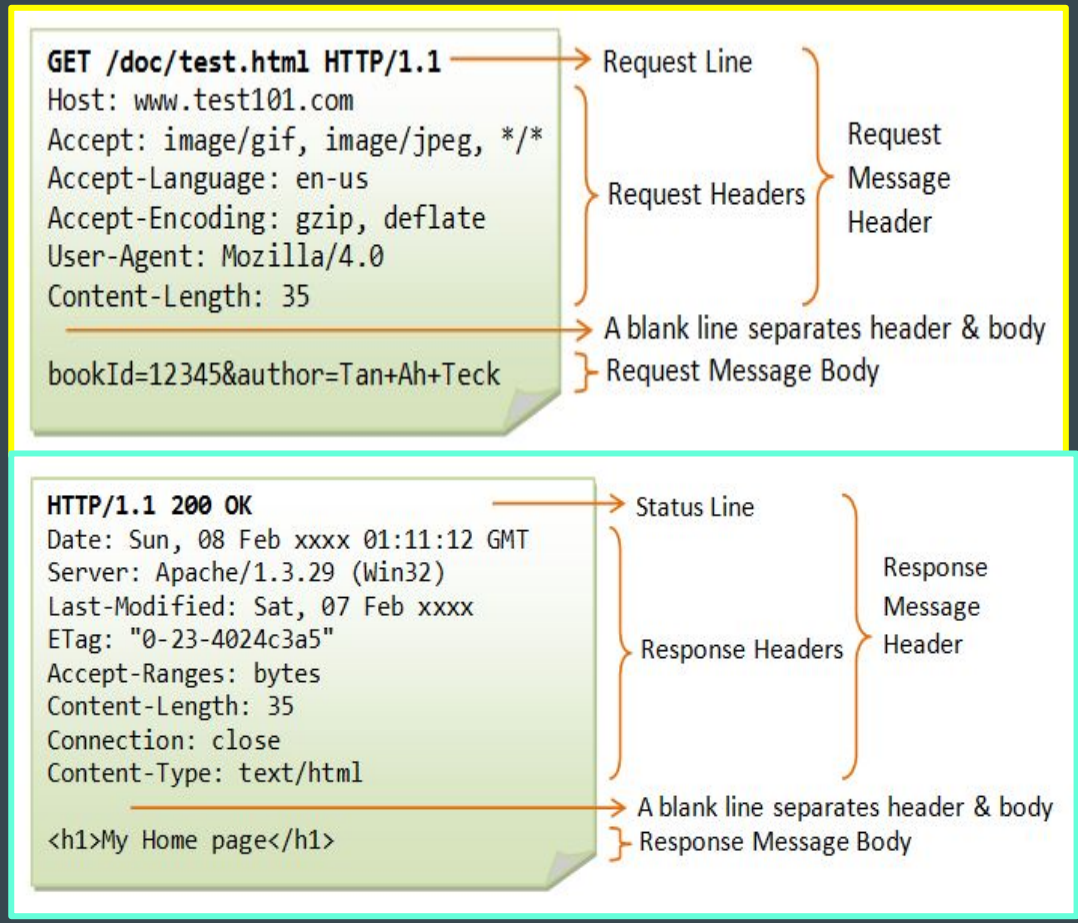
DNS Packet/Protocol

- rfc 882, 883, 1034, 1035, 1035....
- DNS Spoofing:
  - All that tells a client they should accept a response is that the response has the same original ident field.
    - 16 bits of entropy, only 64K combinations, easily bruted.
  - Where can we get more entropy?
    - DNS uses UDP for transportation (recall layers)
    - UDP consists of a source port, destination port, a checksum, length, and the data
    - Randomize the source port that a client is using!
  - Still guessable. Easily manipulated with by a man-in-the-middle attack. But, best we got.



HTTP

- Human readable
- Requests receive Responses
- Requests do “verbs”, GET, POST, DELETE, ...
- Responses send a status and response message
- Body data can be anything



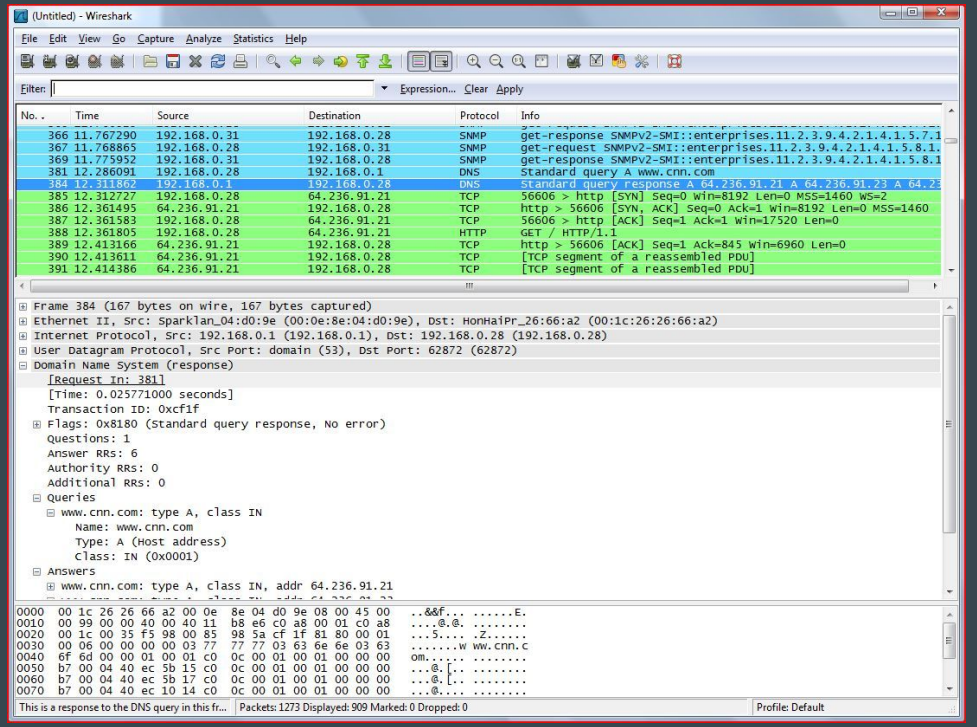
In Summary

- The Internet is a set of protocols, distributed networks, and layers
  - Physical (Ethernet)
  - Network (IP - “No guarantee.. I try my best”)
  - Transport (TCP, UDP)
  - Application (HTTP, FTP, Halo, BitTorrent, everything else)
- Network security is primarily focused on:
  - Confidentiality
  - Integrity
  - Availability
- A lot of the web is insecure if an attacker can view your data packets

H4CK3R T00LZ

Capture and Hack Data

- Wireshark
  - Record and modify all sorts of data
    - Not just web!
  - Industry standard, one of the best tools
    - Ton of fun, easy to use, modifiable
  - Give it a try yourself, and see what data your computer is sending and receiving
- aircrack-ng
  - Hack weak WiFi networks
    - Really does work



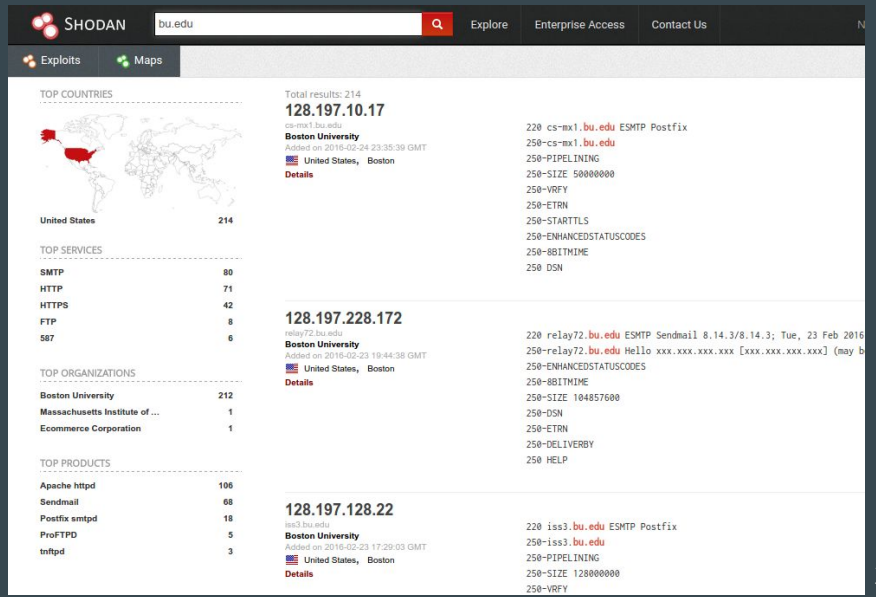
Scan the Internet/network

- nmap
  - Scan a network or machine for “info”
    - What’s running on it?
    - What version of things is it using?
    - Is it easily hackable?
- shodan
  - Global nmaping
  - Easily searchable

nmap cheatsheet:
https://www.eugenekolo.com/blog/i-can-n/

```
$ nmap eugenekolo.com

Nmap scan report for eugenekolo.com
(104.28.8.239)
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt
```

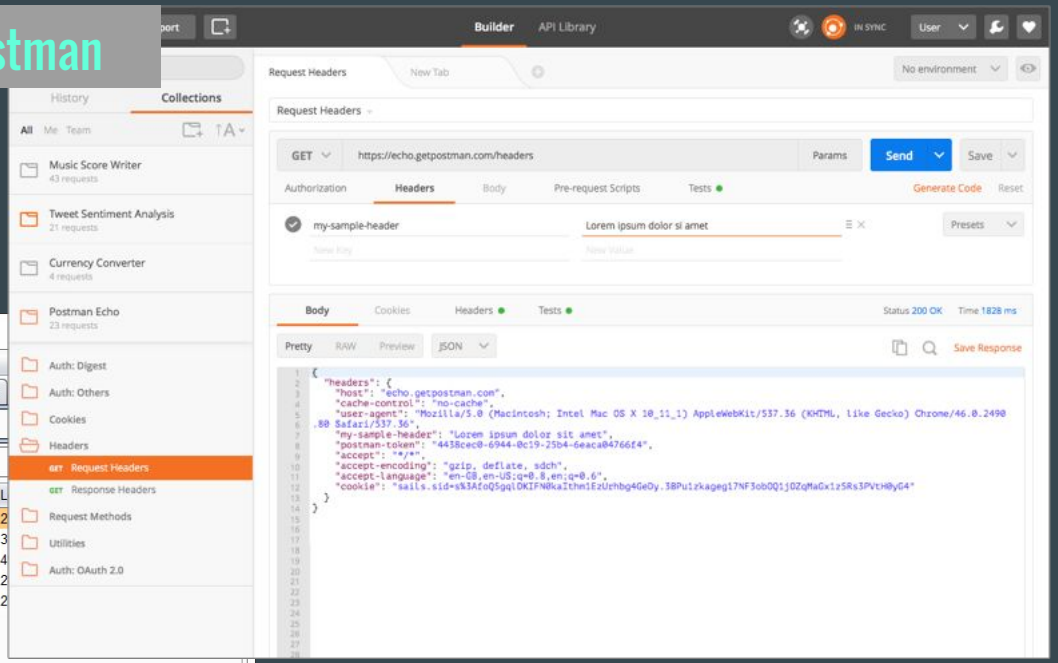


Play with HTTP

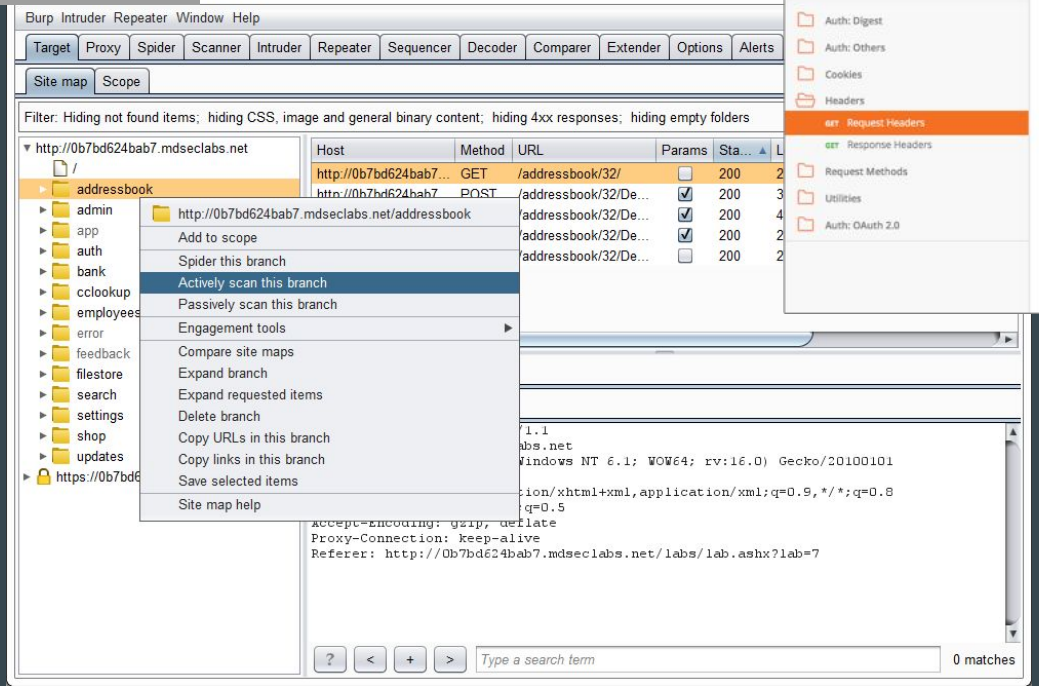
- Burpsuite
  - Intercept, modify, create, send, receive and more HTTP packets
- Postman
  - Create, send, and receive HTTP packets
    - More so for web development
- Firefox/Browser plugins
  - Modify packets
  - Chrome doesn't let you I believe?

Play with HTTP

Postman



Burp



Demos

Live @ 0xBU

Next week

Challenge1: ssh tiny@pwnable.kr -p2222 (pw:guest)

Challenge2: http://web2014.picoctf.com/injection4/

__libc_fini