Application Layer
DNS/HTTP

Kevin Scrivnor

COMP 429

Spring 2023

DNS – the Domain Name System

- Important for a few reasons
  - Translates human readable domain names into machine readable IP addresses
  - Allows for geographical based answers
  - Allows for load balancing

- On the right,
  - DNS results for ipchicken.com
  - ANSWER SECTION contains mapping

```
[kscrivnor@evi ~]$ dig ipchicken.com

; <<>> DiG 9.11.36-RedHat-9.11.36-3.el8_6.1 <<>> ipchicken.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 965
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
;; QUESTION SECTION:
;ipchicken.com.                 IN      A

;; ANSWER SECTION:
ipchicken.com.          300     IN      A       104.26.8.109
ipchicken.com.          300     IN      A       104.26.9.109
ipchicken.com.          300     IN      A       172.67.73.20

;; Query time: 22 msec
;; SERVER: 192.168.254.254#53(192.168.254.254)
;; WHEN: Mon Oct 24 12:54:40 PDT 2022
;; MSG SIZE  rcvd: 90
```

History of DNS

- hosts.txt
  - Text file on the machine
  - Listed every hostname and IP address
  - Was updated nightly
- Still have something like this today

```
[kscrivnor@evi ~]$ cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.254.210 institution.home
[kscrivnor@evi ~]$ ssh institution.home
The authenticity of host 'institution.home (192.168.254.210)' can't be established.
ECDSA key fingerprint is SHA256:WCLMuEW6UFsFQWND7haAVhVDUGWAyUpOUnwF+7FiZ2Y.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'institution.home' (ECDSA) to the list of known hosts.
kscrivnor@institution.home's password:
```

DNS Lookup Process

- Obviously the idea on the previous slide does not scale
- DNS invented in 1983 to manage scale

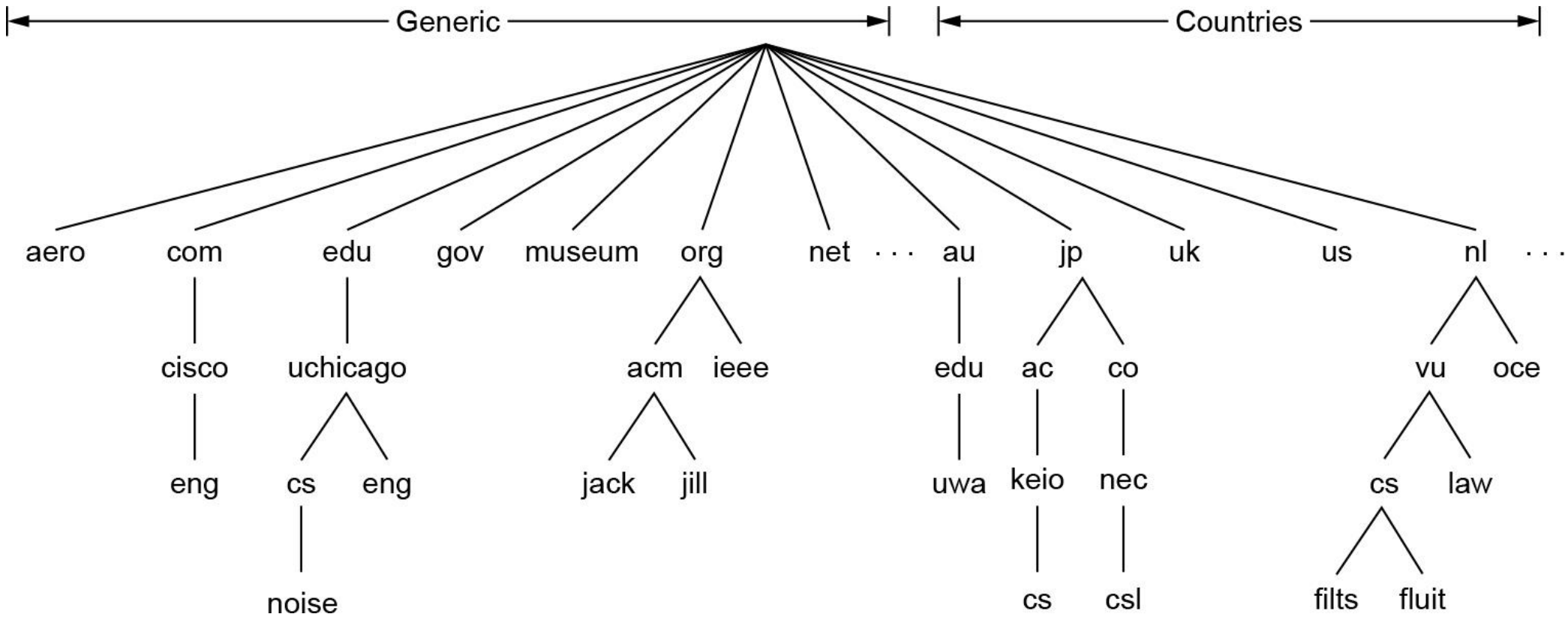
- Application calls function: gethostbyname([domain name])
  - This is called the stub resolver
- The stub resolver calls the local resolver
- The local resolver then performs a recursive lookup against a set of DNS resolvers
- Eventually returning the IP address to the Application

Recursive Lookups and Caching

- To lookup cs.csuci.edu
  - The local resolver looks up the domain backwards
  - edu find the edu information
  - edu.csuci find the csuci.edu information
  - edu.csuci.cs find where cs.csuci.edu is
- When looking up it.csuci.edu
  - edu.csuci already found in previous lookup, cached
  - edu.csuci.it find where it.csuci.edu is
- .edu for instance, is a top level domain (TLD)
- it.csuci.edu. is a FQDN (Fully Qualified Domain Name)

Domain Names are Hierarchical

- We define the hierarchy as what area the DNS resolver is responsible for



DNS Query Format

- QNAME
  - the query name, the domain name you're looking for
- 16-bit transaction identifier
  - Maps a query to an answer
  - Too small and easily attacked
  - Solution: ugly hack

- Usually sent over UDP
  - Unencrypted, plaintext
- Recent changes now include sending over TCP
  - DNS-over-TLS (DoT)
  - DNS-over-HTTPS (DoH)
  - Both exist in the name of privacy, not actually true

Privacy and DNS

- Whoever your local resolver is, that who gets the data
  - ISP typically sets DNS to itself
  - Some users opt to use Google, 4.4.4.4 or 8.8.8.8
  - Others opt to use Cloudflare, 1.1.1.1
- Whether encrypted or not, the local resolver receives the name of the website you want to visit and when

- Partial Solution: QNAME minimization
  - Query root server only for edu, not gitlord.cs.csuci.edu
  - Query edu server only for csuci.edu
  - Query csuci.edu server only for cs.csuci.edu
  - Query cs.csuci.edu server only for gitlord.cs.csuci.edu

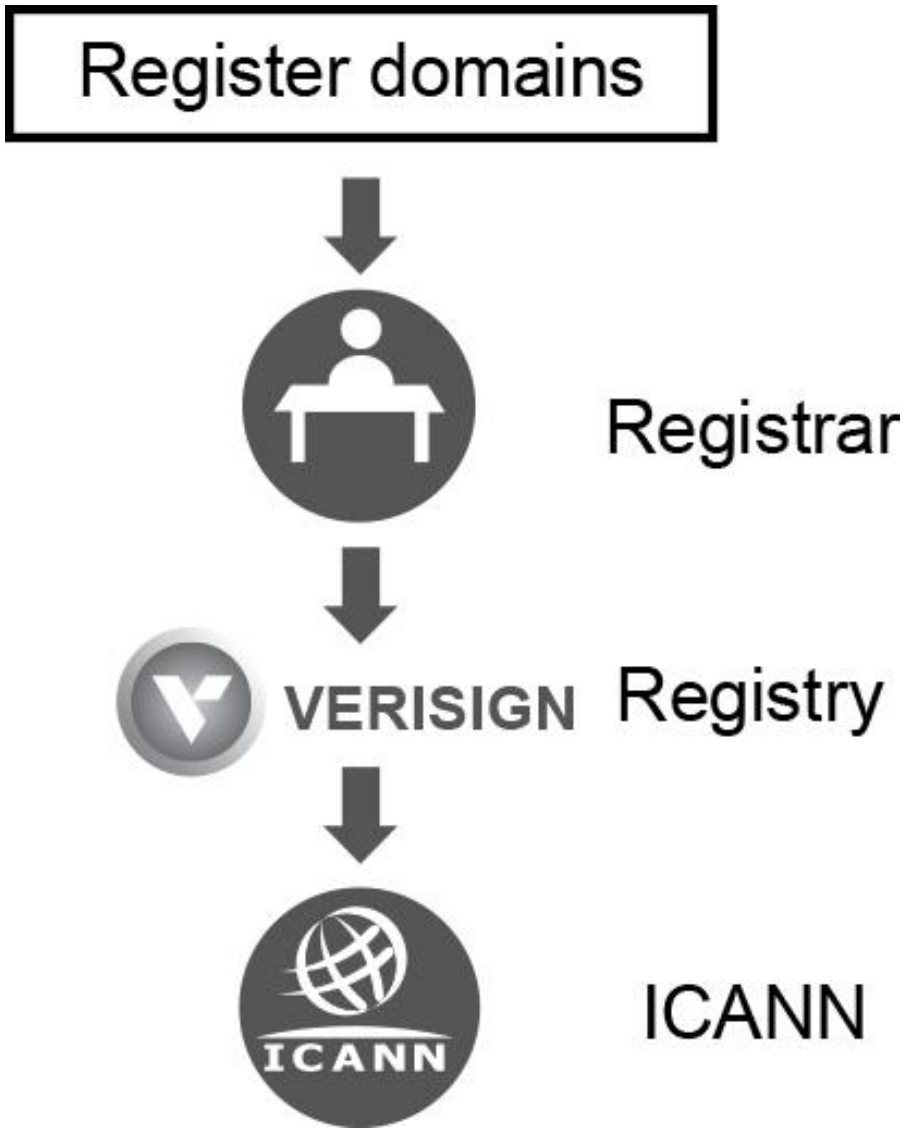
Who oversees the hierarchy?

- Same as IP addresses
- ICANN
  - Internet Corporation for Assigned Names and Numbers
  - In this case, the “assigned names” portion
- The Internet is divided into over 250 TLDs
- 2012 ICANN allowed companies to apply for TLDs
  - Google/Amazon both applied for about 100 domains each
  - At the cost of $200,000 each

Domain	Intended use	Start date	Restricted?
com	Commercial	1985	No
edu	Educational institutions	1985	Yes
gov	Government	1985	Yes
int	International organizations	1988	Yes
mil	Military	1985	Yes
net	Network providers	1985	No
org	Non-profit organizations	1985	No
aero	Air transport	2001	Yes
biz	Businesses	2001	No
coop	Cooperatives	2001	Yes
info	Informational	2002	No
museum	Museums	2002	Yes
name	People	2002	No
pro	Professionals	2002	Yes
cat	Catalan	2005	Yes
jobs	Employment	2005	Yes
mobi	Mobile devices	2005	Yes
tel	Contact details	2005	Yes
travel	Travel industry	2005	Yes
xxx	Sex industry	2010	No

How to Register a Domain

- ICANN appoints a company as a Registry
  - Verisign is the registry for *com*
- Registrars sell directly to users
  - GoDaddy, NameCheap, Domain.com, etc
- IT manages the registration of csuci.edu
  - Then manages their own subdomains under csuci.edu
  - No need to purchase sub domains as IT controls the rest



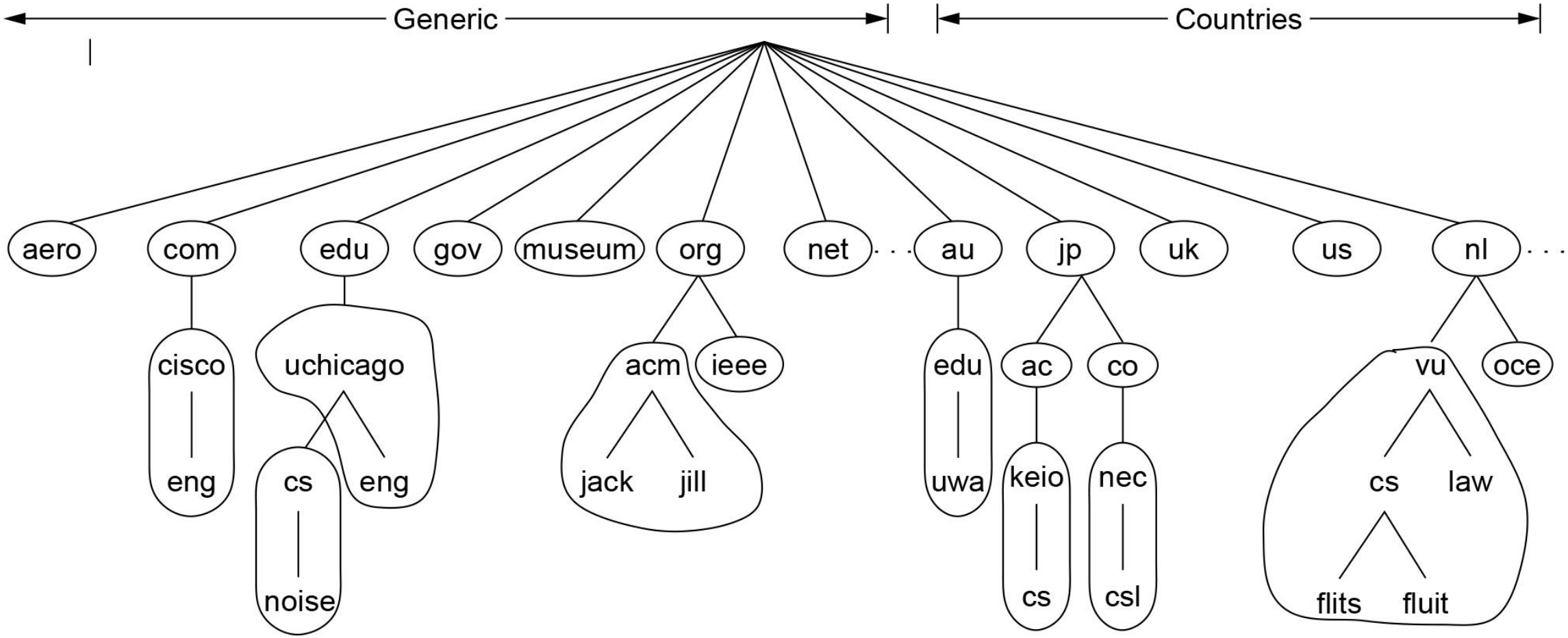
Domain Hierarchy

- In America
  - .edu for educational
  - .gov for government
  - .mil for military
  - Regulated domain hierarchies
- In Japan
  - ac.jp for educational
  - co.jp for commercial/anything
- Netherlands however,
  - .nl for all

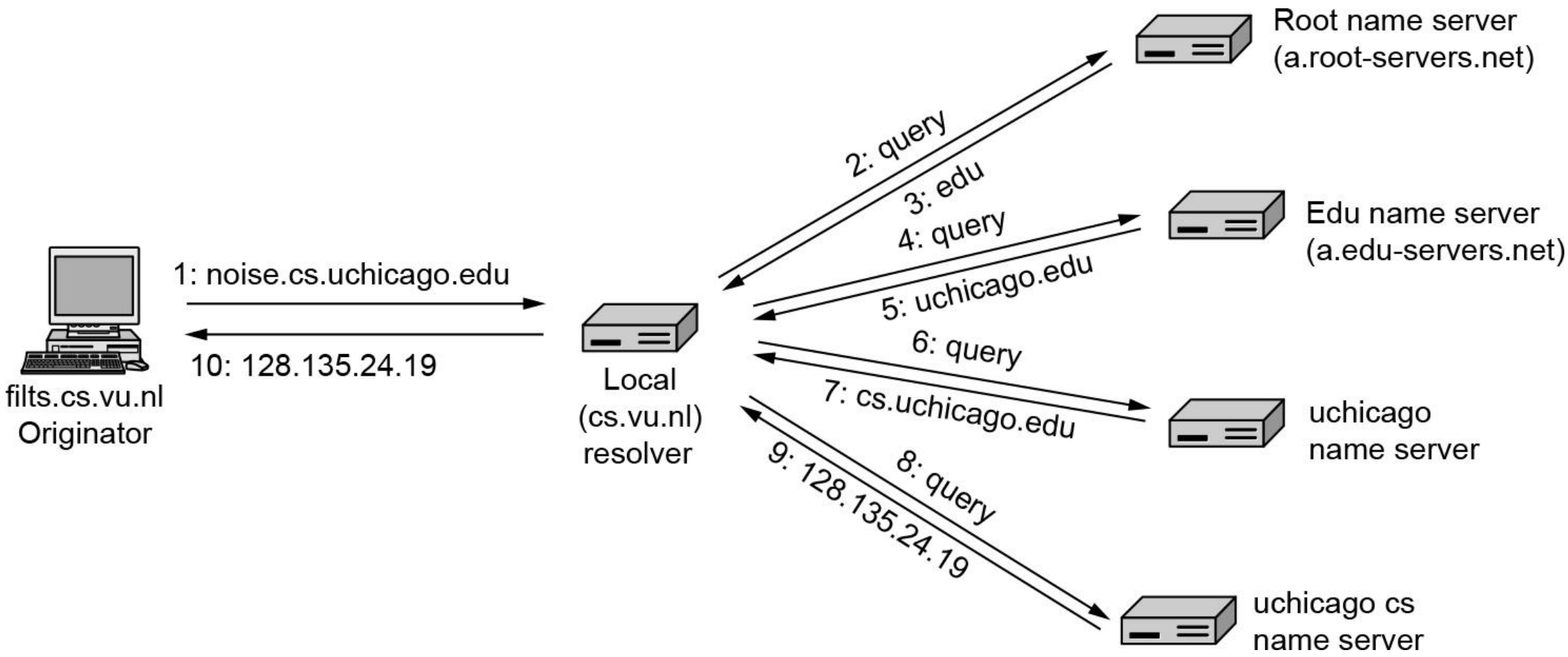
- Examples of CS department websites around the world
  - cs.chicago.edu
  - cs.vu.nl
  - cs.uwa.edu.au
  - compsci.csuci.edu
- Formerly cs.csuci.edu but were afraid people would mix it up with Chicano Studies

Domain Hierarchy

- In this case, CS wanted to be in control of their own DNS, whereas the English department did not care



DNS Resolution in Action (in 10 easy steps!)



Extensions and Enhancements

- The local resolver used to be your ISPs resolver by default
- This made it easy for companies to geographically provide you the best IP answer
- Many people now like to give their data away to google for free, so they use 8.8.8.8 or 4.4.4.4 as their DNS
  - This makes it difficult to locate the client…

- EDNS Client Subnet includes the local IP subnet and sends it to the DNS resolver
  - Solves the problem described above when the “local” resolver is not actually local

DNS Responses/Resource Records (Answers)

- 5 tuple
  - Domain name
  - Time to live
  - Class
  - Type
  - Value
- Example
  - `;; ANSWER SECTION:`
  - `compsci.csuci.edu.  86400  IN  A  13.86.237.209`

5 tuple

- Domain Name
  - Which record this answer applies to
- Time to Live
  - How stable the record is
  - 86400 is 24 hours in seconds, considered very stable
- Class
  - IN
  - Always “IN”, meaning “Internet Information”
  - Nothing else is seen in practice
- Type
  - A records are IPv4 (32 bits), AAAA are IPv6 (32*4 = 128 bits)
- Value
  - The IP address

The Many Types of DNS Records

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

Configuring a DNS Server

- Zone example file:

```
$TTL 3D
@       IN      SOA     land-5.com. root.land-5.com. (
                        199609206       ; serial, todays date + todays serial
#
                        8H              ; refresh, seconds
                        2H              ; retry, seconds
                        4W              ; expire, seconds
                        1D )            ; minimum, seconds
                NS      land-5.com.
                NS      ns2.psi.net.
                MX      10 land-5.com.  ; Primary Mail Exchanger
                TXT     "LAND-5 Corporation"

localhost       A       127.0.0.1

router          A       206.6.177.1

land-5.com.     A       206.6.177.2
ns              A       206.6.177.3
```

Contention over DNS Names

- gov is restricted to US government websites
- ca.gov is restricted to California government websites
- edu is restricted to education institutions
- These are obvious and make sense
- pro
  - What does it mean to be a professional?
- tv
  - Country domain for Tuvalu
  - Small nation of about 10,000 people
  - Government income largely come from leasing the .tv domain out
- Domain Squatting?

Onto HTTP

The World Wide Web

- Began at CERN in 1989
- Idea: help large teams work globally to share information on particle physics
- CERN Physicist Tim Bernes-Lee created a text-based prototype and presented it at the 1991 Hypertext Conference

- Inspired Marc Anderson to develop the first GUI browser: Mosaic
  - Which after success, he then left the company and founded another one called…

Netscape

- Very successful IPO, kicked off the dot-com bubble
- Code named “Mozilla” for Mosaic Killer
  - Marketing did not appreciate this logo everywhere
- 1998 Netscape Navigator 5.0 source code released

HTTP/0.9 - one line protocol

- Client request is a single ASCII character string.
- Client request is terminated by a carriage return (CRLF).
- Server response is an ASCII character stream.
- Server response is a hypertext markup language (HTML).
- Connection is terminated after the document transfer is complete.

- Example:

```
GET /about<CRLF>
(hypertext response)
```

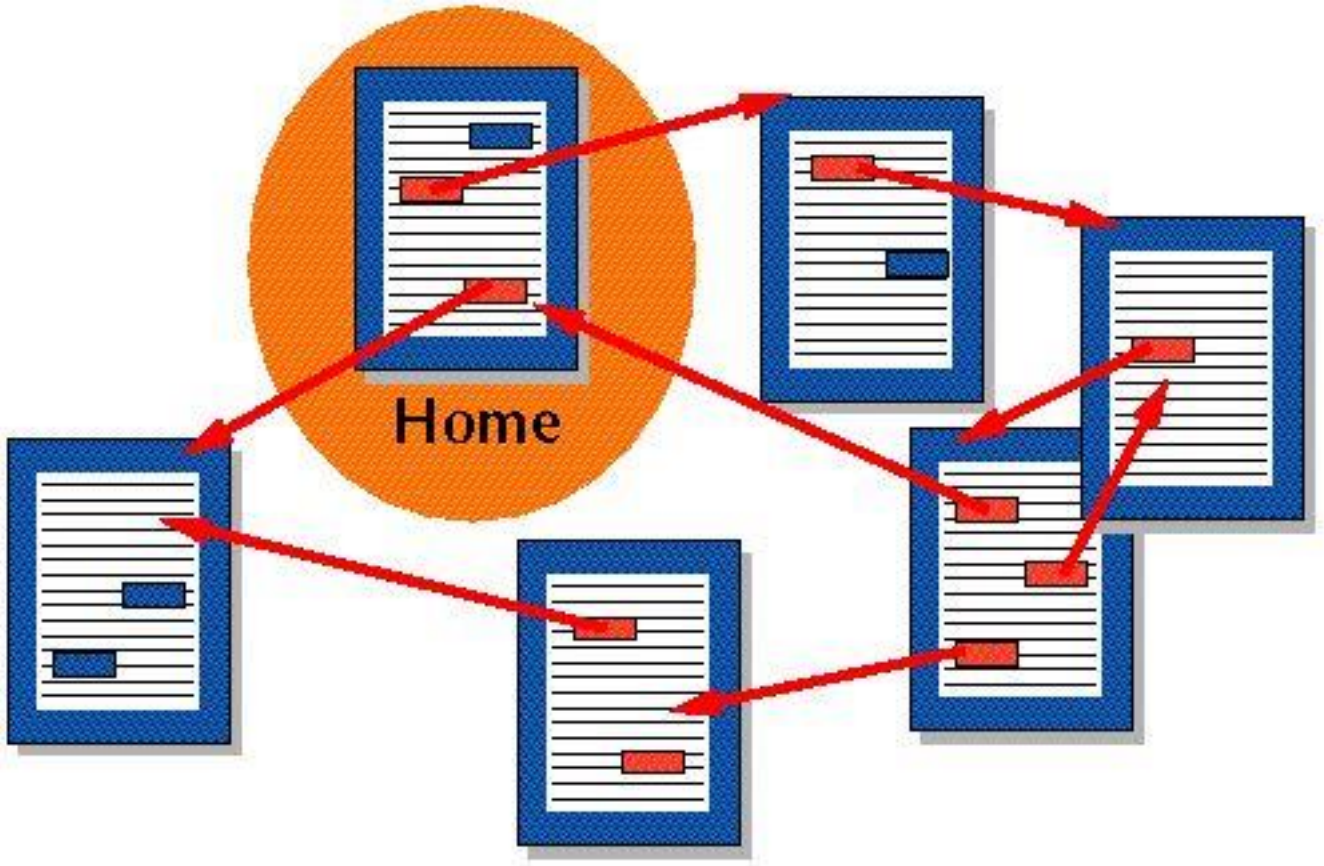
HTTP/1.0 Changes

- Request may consist of multiple newline separated header fields.
- Response object is prefixed with a response status line.
- Response object has its own set of newline separated header fields.
- Response object is not limited to hypertext.
- *The connection between server and client is closed after every request.*

```
GET /rfc/rfc1945.txt HTTP/1.0
User-Agent: CERN-LineMode/2.15 libwww/2.17b3
Accept: */*
```

Evolution of the Web: Hypertext

- **Hypertext**
  - A plain text document with the ability to have hyper links to other plain text documents.

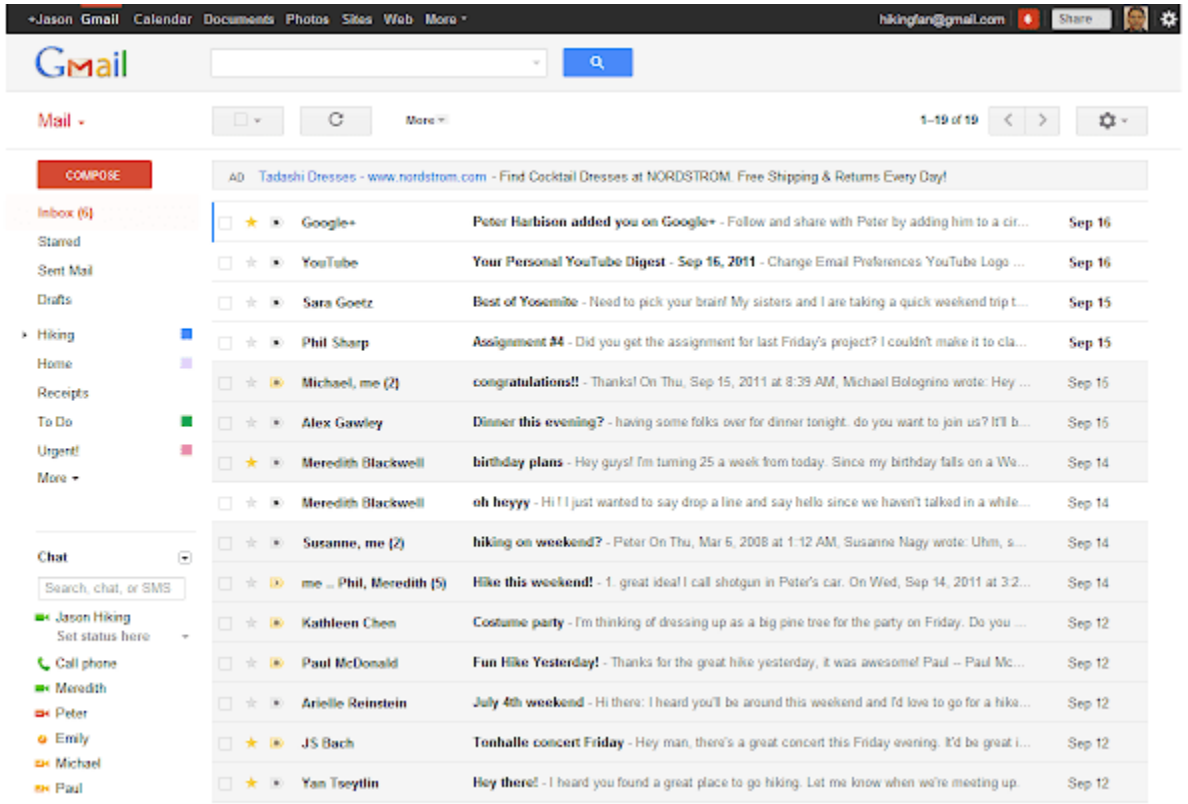


Evolution of the Web: Web Page

- Web page
  - HTML changed the definition of hypertext to include **hypermedia** resources (images and audio), and many other resources for layouts.
  - Visually appealing, still not as interactive.

Evolution of the Web: Web Applications

- Web Application
  - Addition of JavaScript, DHTML, and AJAX among other things. Allows for the existence of Chromebooks basically. A computer that is just a web browser.

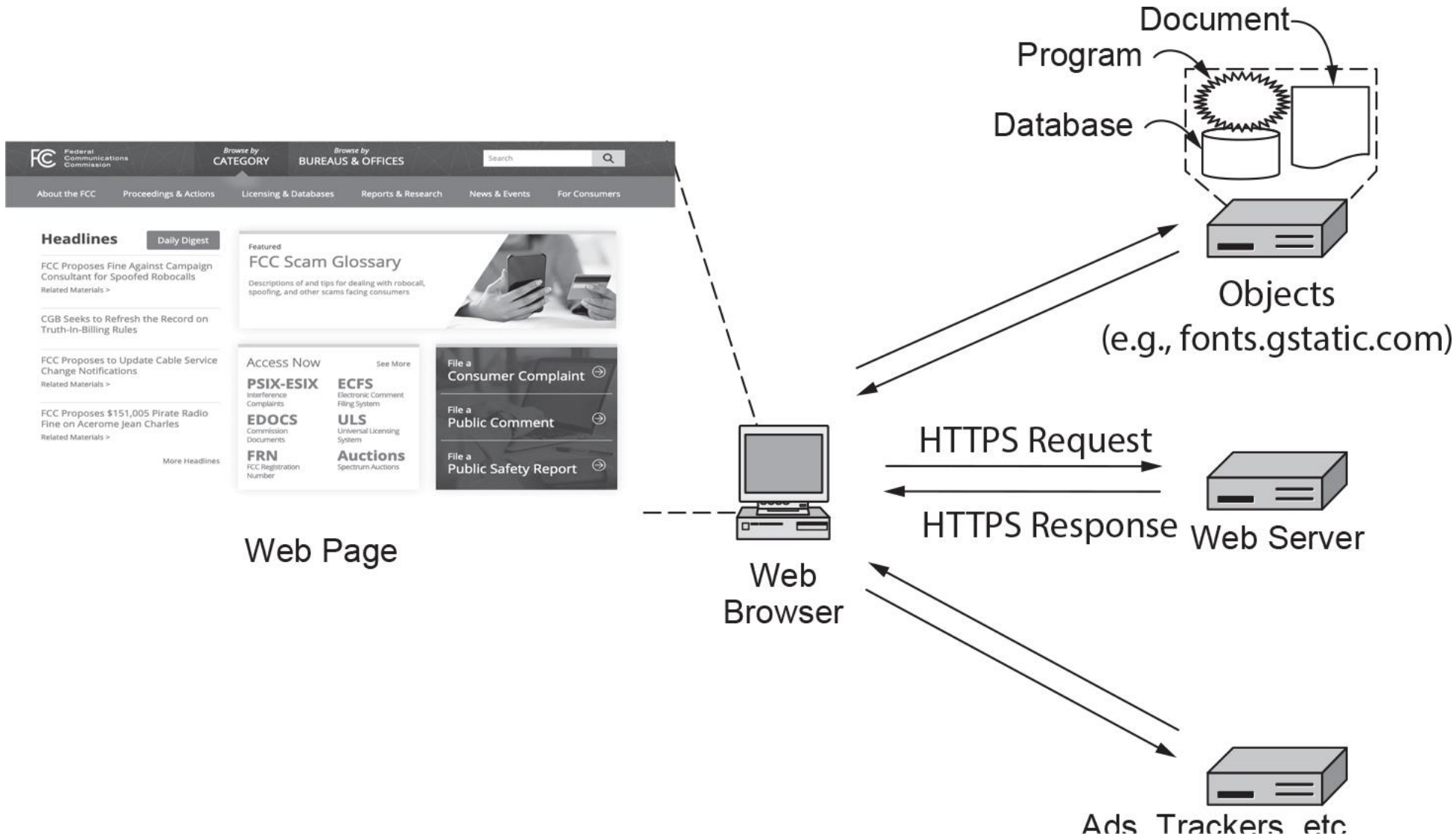


A Modern Web Page

- Contains hundreds of links to other objects
  - Which can be hosted anywhere on the Internet
  - Advertisements
    - Which track you

- Definitions
  - Index — main page, default page browser looks for
  - Stylesheets — code to control the appearance
  - Hyperlinks — clickable object that brings you to another resource

Architectural Overview



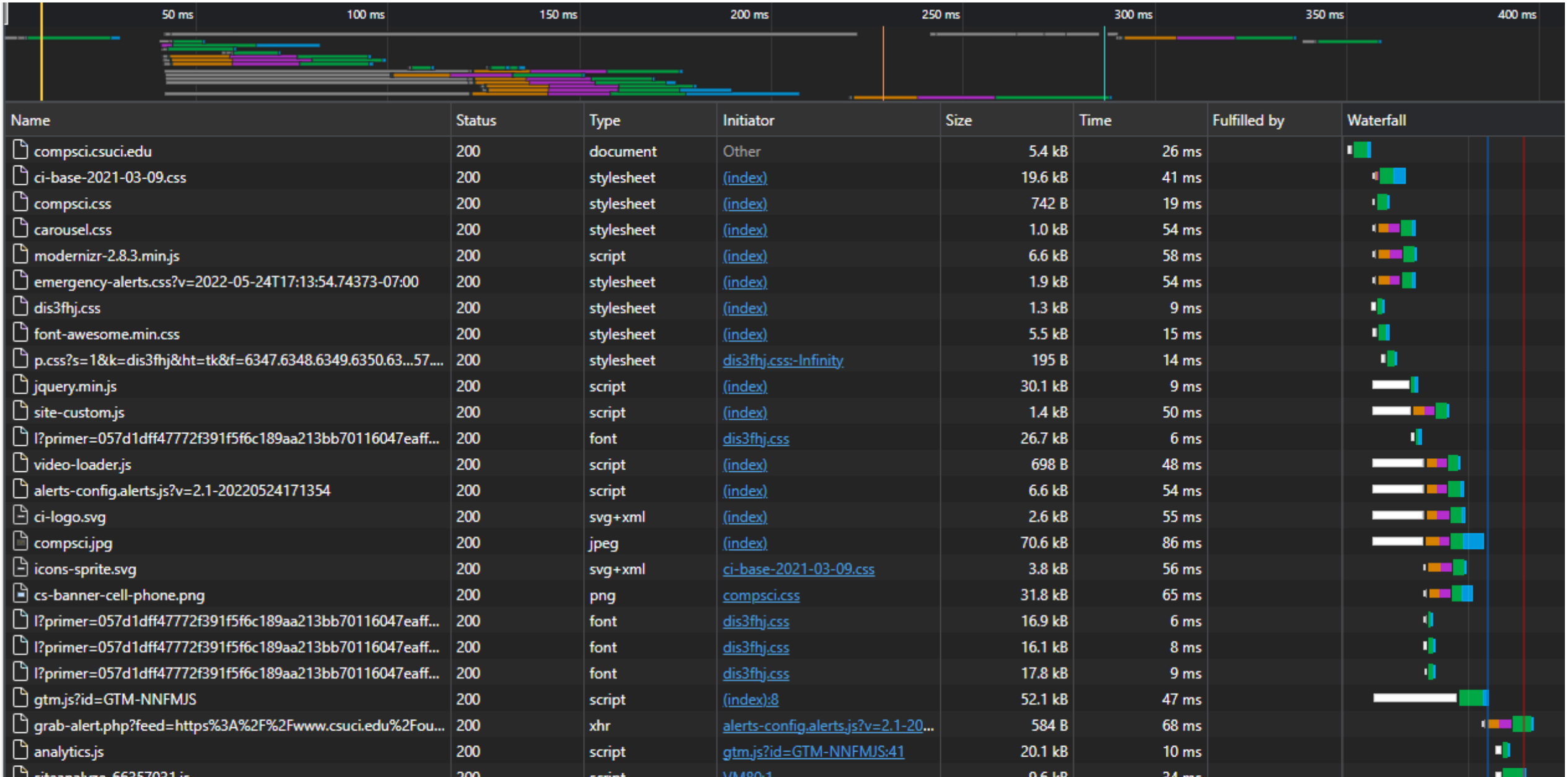
Meta Information is Needed

- Consider a social security number
  - Unique identifier for a person
  - Provides no other information
  - Name?
  - Address?
  - Language spoken?
- Networking solution: URL
  - Protocol (language spoken)
  - DNS Name (name, not IP)
  - Path (indicates specific page, address)
  - https://compsci.csuci.edu/schedule

What does the browser do?

- Reads the URL from the user
- DNS request for compsci.csuci.edu
- DNS replies with IP address
- TCP connect on port 443 based on https
- Send HTTP request for schedule page
- Server sends HTTP response with contents of schedule page
- If the page contains more links, browser fetches those URLs as well
- Browser displays the page the user
- TCP connection is closed

We can view the action in a waterfall diagram



Name	Status	Type	Initiator	Size	Time	Fulfilled by	Waterfall
compsci.csuci.edu	200	document	Other	5.4 kB	26 ms		
ci-base-2021-03-09.css	200	stylesheet	(index)	19.6 kB	41 ms		
compsci.css	200	stylesheet	(index)	742 B	19 ms		
carousel.css	200	stylesheet	(index)	1.0 kB	54 ms		
modernizr-2.8.3.min.js	200	script	(index)	6.6 kB	58 ms		
emergency-alerts.css?v=2022-05-24T17:13:54.74373-07:00	200	stylesheet	(index)	1.9 kB	54 ms		
dis3fhj.css	200	stylesheet	(index)	1.3 kB	9 ms		
font-awesome.min.css	200	stylesheet	(index)	5.5 kB	15 ms		
p.css?s=1&k=dis3fhj&ht=tk&f=6347.6348.6349.6350.63...57....	200	stylesheet	dis3fhj.css:-Infinity	195 B	14 ms		
jquery.min.js	200	script	(index)	30.1 kB	9 ms		
site-custom.js	200	script	(index)	1.4 kB	50 ms		
l?primer=057d1dff47772f391f5f6c189aa213bb70116047eaff...	200	font	dis3fhj.css	26.7 kB	6 ms		
video-loader.js	200	script	(index)	698 B	48 ms		
alerts-config.alerts.js?v=2.1-20220524171354	200	script	(index)	6.6 kB	54 ms		
ci-logo.svg	200	svg+xml	(index)	2.6 kB	55 ms		
compsci.jpg	200	jpeg	(index)	70.6 kB	86 ms		
icons-sprite.svg	200	svg+xml	ci-base-2021-03-09.css	3.8 kB	56 ms		
cs-banner-cell-phone.png	200	png	compsci.css	31.8 kB	65 ms		
l?primer=057d1dff47772f391f5f6c189aa213bb70116047eaff...	200	font	dis3fhj.css	16.9 kB	6 ms		
l?primer=057d1dff47772f391f5f6c189aa213bb70116047eaff...	200	font	dis3fhj.css	16.1 kB	8 ms		
l?primer=057d1dff47772f391f5f6c189aa213bb70116047eaff...	200	font	dis3fhj.css	17.8 kB	9 ms		
gtm.js?id=GTM-NNFMJS	200	script	(index):8	52.1 kB	47 ms		
grab-alert.php?feed=https%3A%2F%2Fwww.csuci.edu%2Fou...	200	xhr	alerts-config.alerts.js?v=2.1-20...	584 B	68 ms		
analytics.js	200	script	gtm.js?id=GTM-NNFMJS:41	20.1 kB	10 ms		

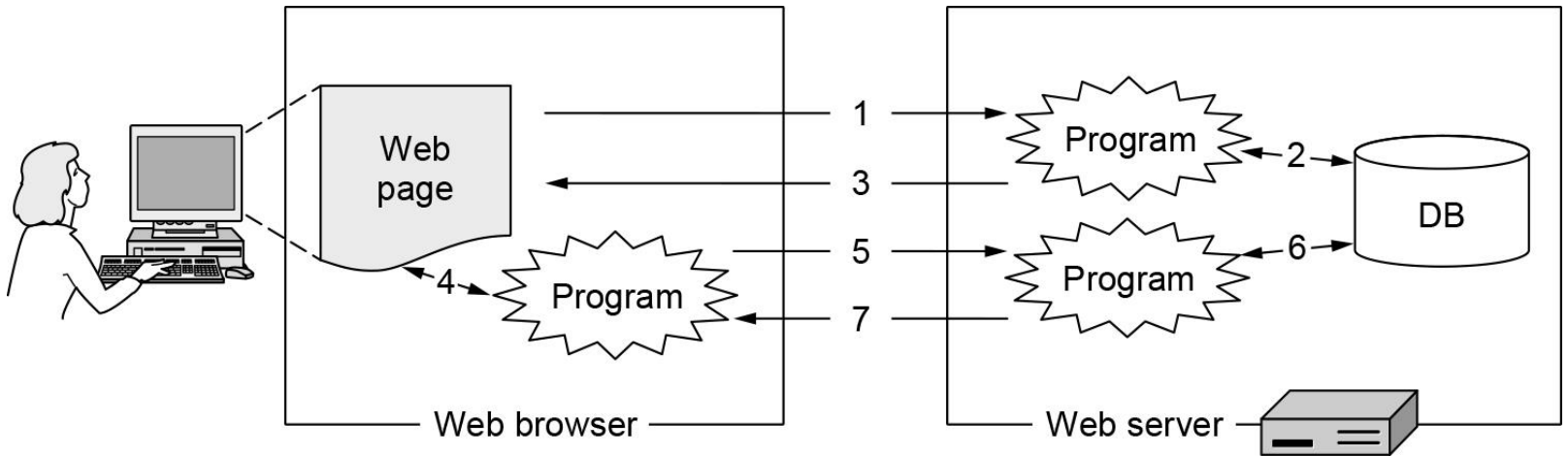
What does the server do?

- Accept a TCP connection from the browser
- Get the path to the page/resource
- Get the file from the disk
- Send the contents of the file to the client
- Release the TCP connection

- Modern servers are much more advanced than this
- In essence, this is basically what they do

Static Content vs. Dynamic Content

- Static content
  - Content that never changes, the same on the disk as it appears in the browser
  - Images
  - Videos
  - Stylesheets
  - Scripts
- Dynamic content
  - Must be generated every time the page is accessed
  - URL identifies what part of the program to execute



HTTP Protocol: methods

Method	Description
GET	Read a Web page
HEAD	Read a Web page's header
POST	Append to a Web page
PUT	Store a Web page
DELETE	Remove the Web page
TRACE	Echo the incoming request
CONNECT	Connect through a proxy
OPTIONS	Query options for a page

HTTP Protocol: responses

Code	Meaning	Examples
1xx	Information	100 = server agrees to handle client's request
2xx	Success	200 = request succeeded; 204 = no content present
3xx	Redirection	301 = page moved; 304 = cached page still valid
4xx	Client error	403 = forbidden page; 404 = page not found
5xx	Server error	500 = internal server error; 503 = try again later

HTTP Protocol: Headers

Header	Type	Contents
User-Agent	Request	Information about the browser and its platform
Accept	Request	The type of pages the client can handle
Accept-Charset	Request	The character sets that are acceptable to the client
Accept-Encoding	Request	The page encodings the client can handle
Accept-Language	Request	The natural languages the client can handle
If-Modified-Since	Request	Time and date to check freshness
If-None-Match	Request	Previously sent tags to check freshness
Host	Request	The server's DNS name
Authorization	Request	A list of the client's credentials
Referrer	Request	The previous URL from which the request came
Cookie	Request	Previously set cookie sent back to the server
Set-Cookie	Response	Cookie for the client to store

HTTP Protocols: Headers

Content-Encoding	Response	How the content is encoded (e.g., *gzip*)
Content-Language	Response	The natural language used in the page
Content-Length	Response	The page's length in bytes
Content-Type	Response	The page's MIME type
Content-Range	Response	Identifies a portion of the page's content
Last-Modified	Response	Time and date the page was last changed
Expires	Response	Time and date when the page stops being valid
Location	Response	Tells the client where to send its request
Accept-Ranges	Response	Indicates the server will accept byte range requests
Date	Both	Date and time the message was sent
Range	Both	Identifies a portion of a page
Cache-Control	Both	Directives for how to treat caches
ETag	Both	Tag for the contents of the page
Upgrade	Both	The protocol the sender wants to switch to