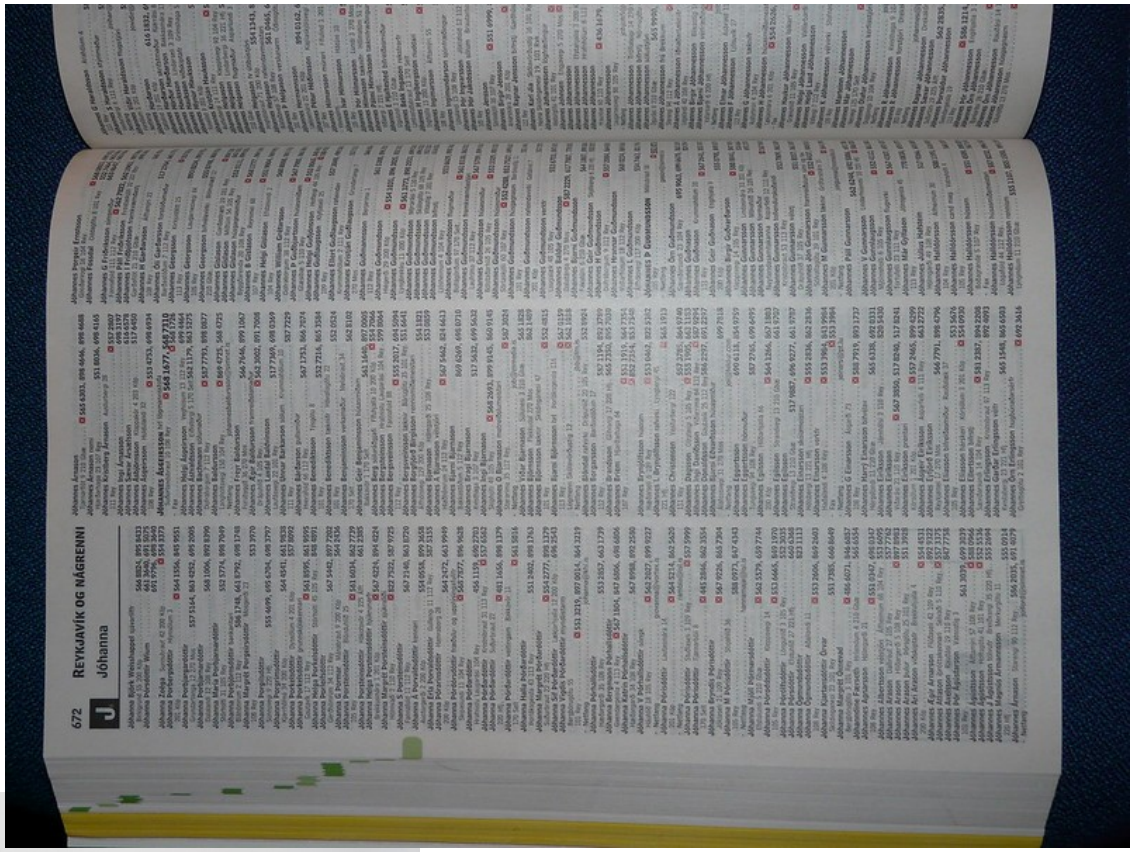
DNS

What it is, How it’s used, how it’s attacked and How it’s defended

Craig L Bowser
@reswob10
CISSP, GSEC, GCED,
GCDA

- 20 years Information Security
- Currently Practice Director Data Analytics at GuidePoint Security
- Presenter
  - Multiple SANS Summits from 2015-2019
  - BlackHat 2020, BSidesCharm 2019, BSidesDC 2019, Derbycon 2016
- Blog at www.shadowtrackers.net/blog
- Mentor for SEC555
- Christian, Father, Husband, Geek, Scout Leader who enjoys woodworking, sci-fi, fantasy, home networking

Photo by Fred Nassar on Unsplash



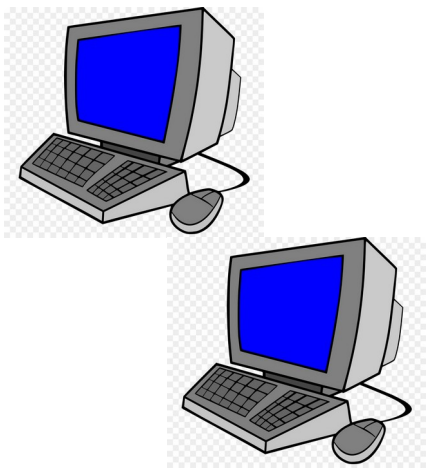
"Iceland phonebook is sorted on first names" by selmerv is licensed with CC BY 2.0.

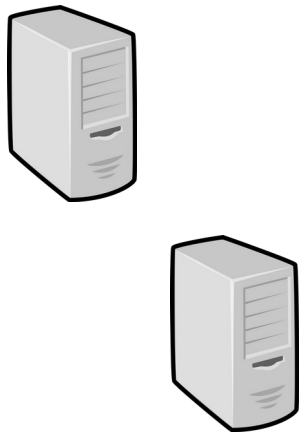
Photo by Compare Fibre on Unsplash

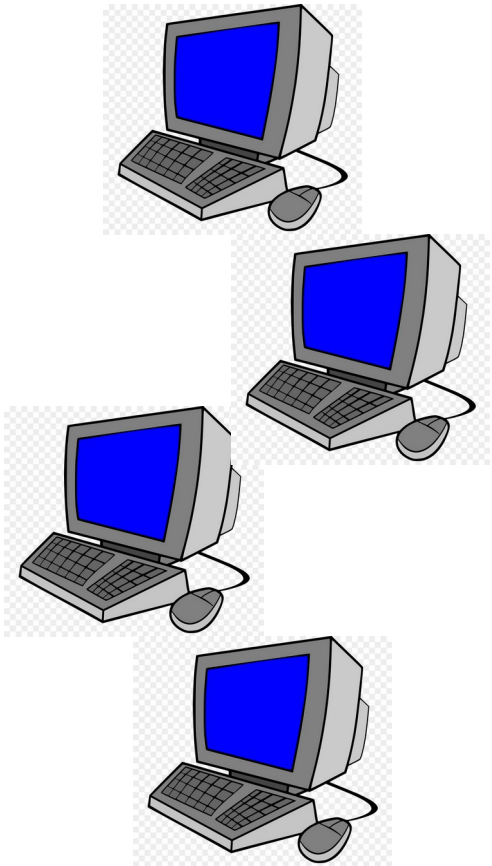
1.2.3.4

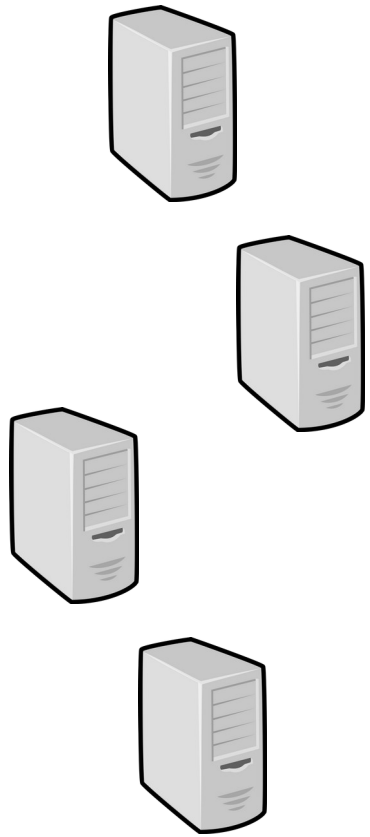
9.8.7.6

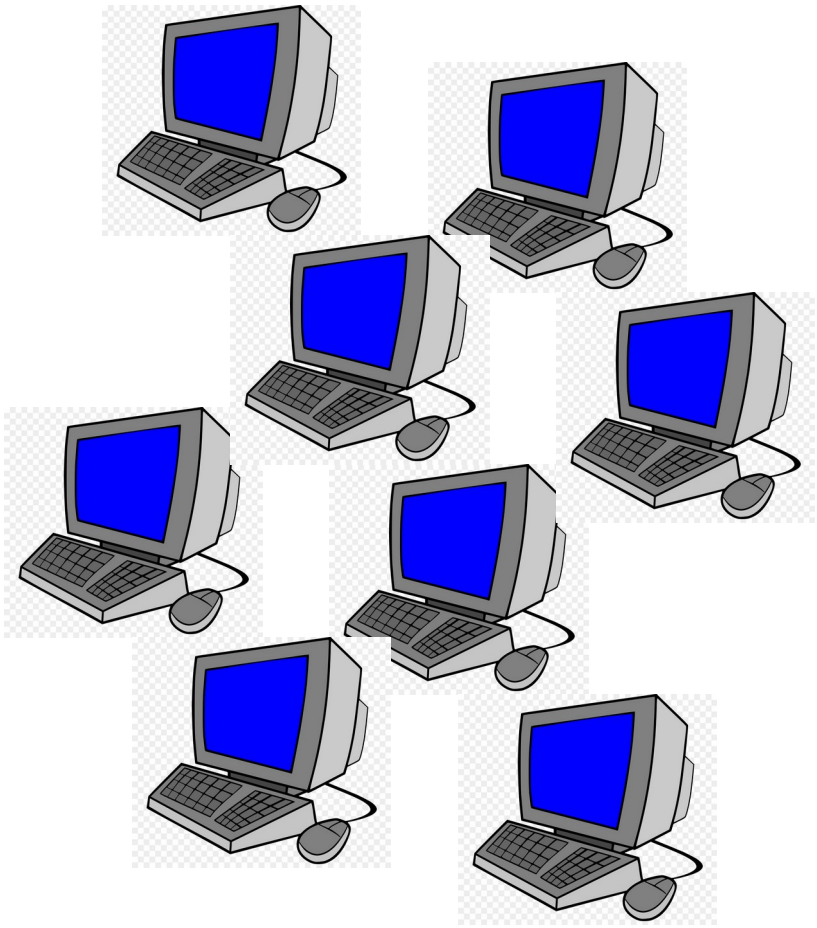
Images from War Games United Artists Stud

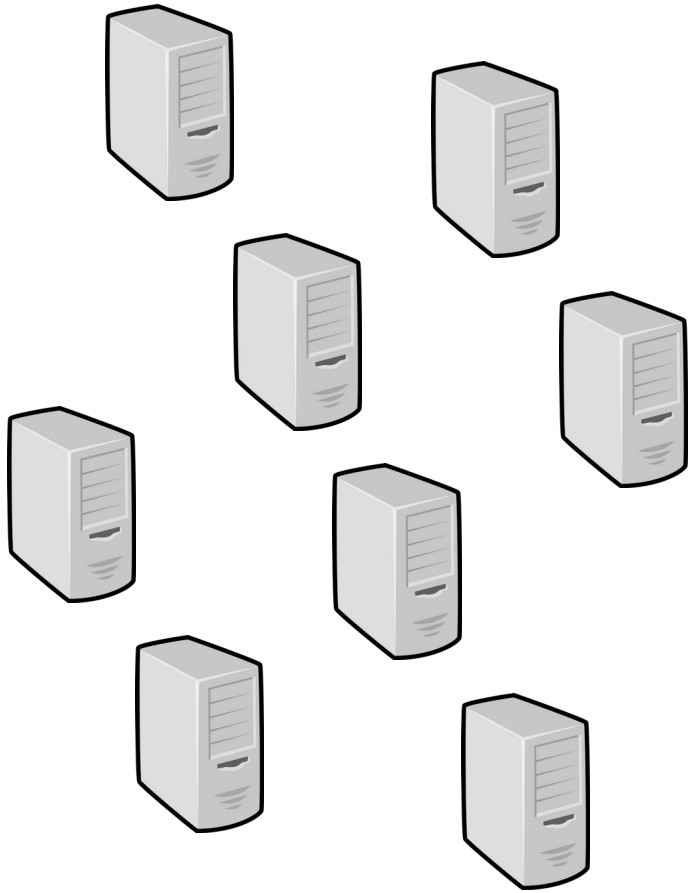


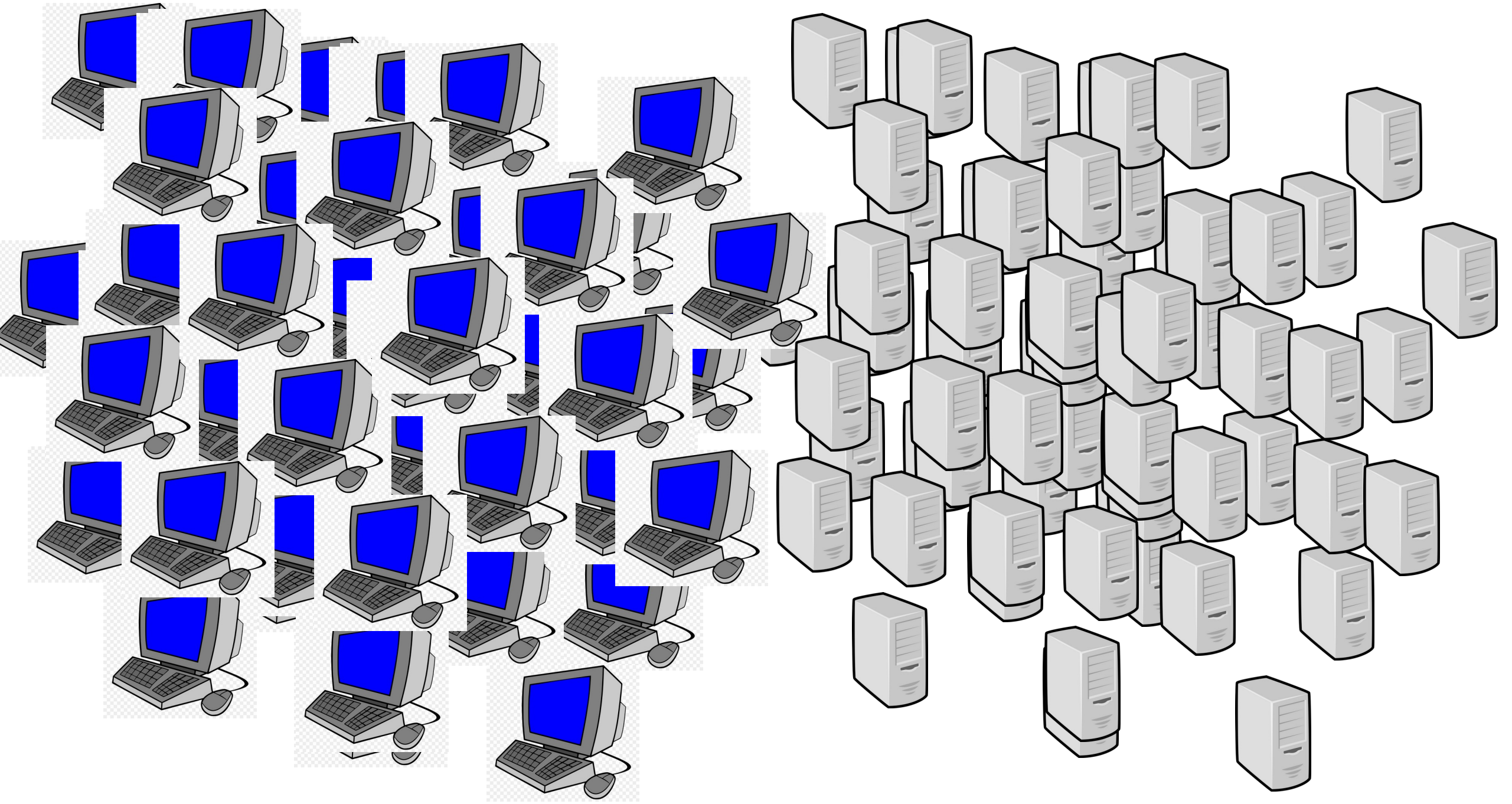












Domain Name Server - DNS

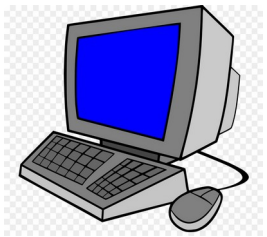
- Elizabeth Feinier and Jon Postal, two pivotal people who built and maintained early directory services.
- RFC 882 and 883 in 1983
- Superseded by RFCs 1034 and 1035 in 1987
- Berkeley Internet Name Domain, BIND, which is the application that acts as authoritative name servers for domains and as resolvers for queries released in 1985
- Uses UDP and TCP port 53
- Largely unchanged in 35 years

http://clipart-library.com/

ROOT
“.”

.com, .net, .horse

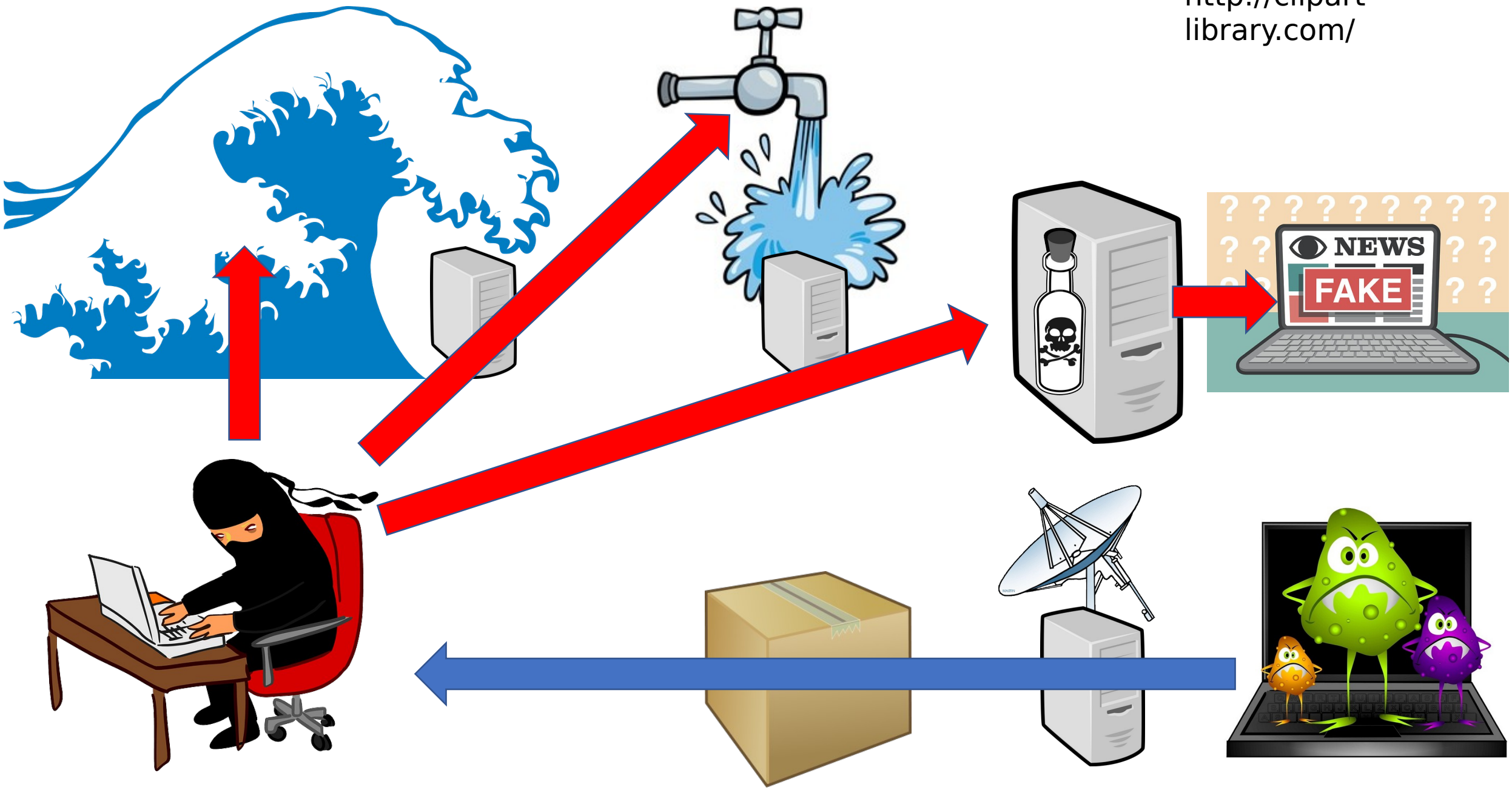
Google.com,
amazon.com
,
irs.gov,
company.net



www.company.net


zoom
YouTube
Music
Tik Tok

http://clipart-library.com/



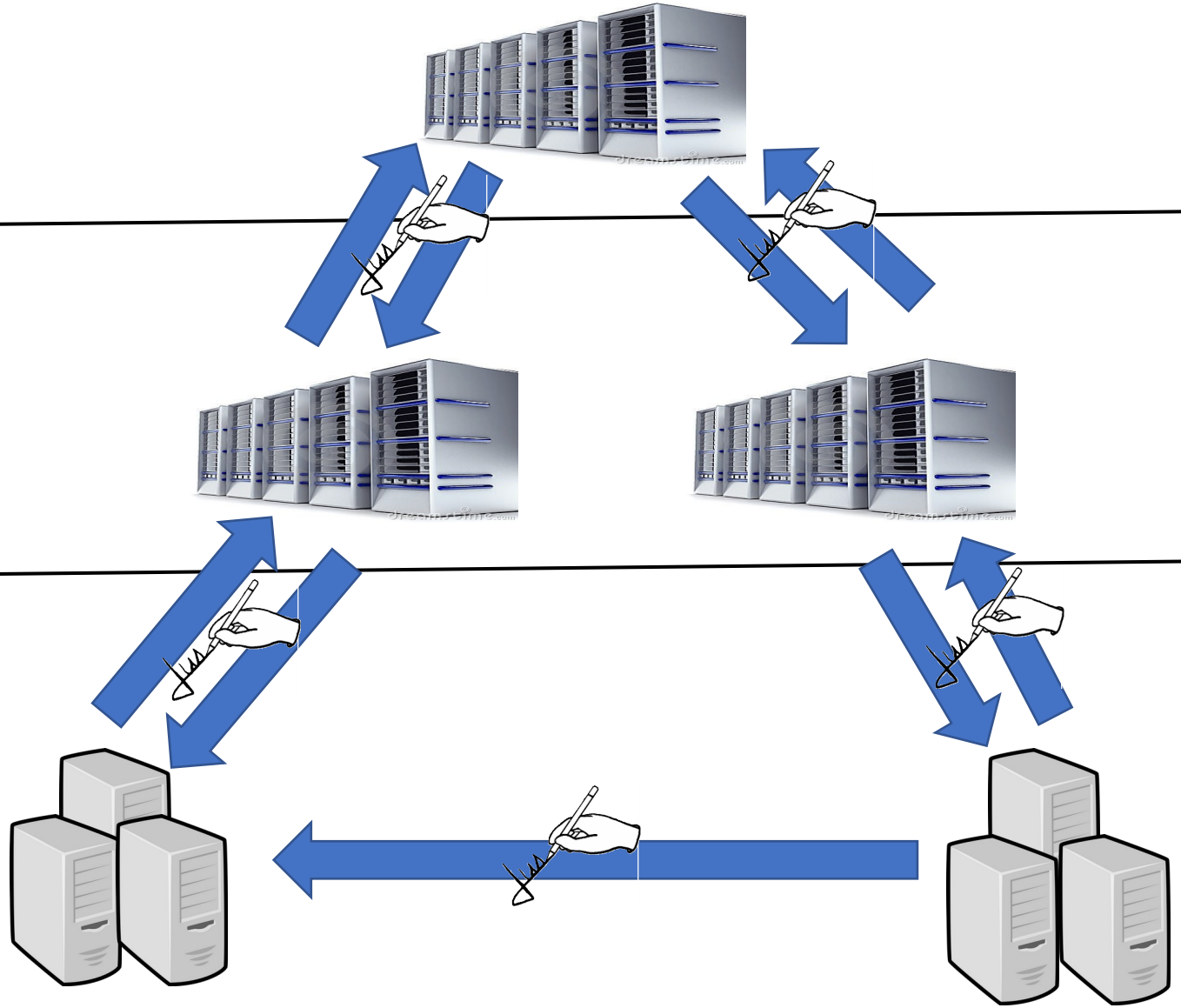
How to Protect?

- Split resolver and authoritative DNS servers
- Block all DNS traffic not going to your own DNS
- Patch DNS server, OS and DNS application
- Limit access to DNS server
- Strong authentication to DNS server
- Monitor DNS traffic
- DNSSEC

ROOT
“.”

.com, .net, .horse

Google.com,
amazon.com
,
irs.gov,
company.net



http://clipart-library.com/

Privacy?

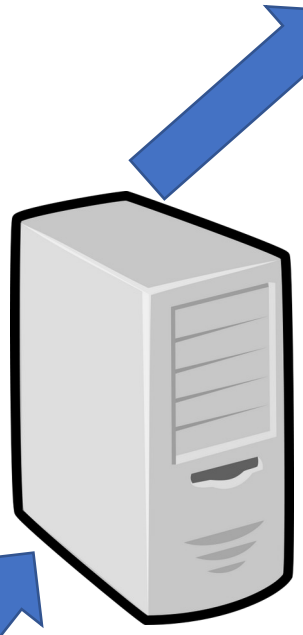
Not So Much....

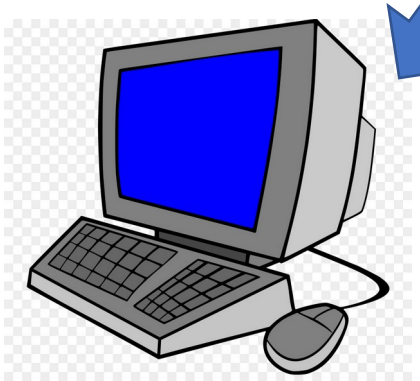
Everything is in clear text.....

1609110276.455161 CCckl52NHXPl0D1IW1 192.168.1.5 60354 8.8.8.8 53 udp 13271 0.019134 youtube-ui.l.google.com 1 C_INTERNET 1 A 0 NOERROR F F T T 0 172.217.7.174,172.217.13.238,172.217.15.78,172.217.7.206,172.217.9.206,172.217.5.238,172.217.164.174,172.217.15.110,172.217.2.110,172.217.164.142,172.217.7.238,142.250.73.206 299.000000,299.000000,299.000000,299.000000,299.000000,299.000000,299.000000,299.000000,299.000000,299.000000 F

1609110276.455161 CCckl52NHXPl0D1IW1
192.168.1.5 60354 8.8.8.8 53 udp 13271 0.019134
youtube-ui.l.google.com 1 C_INTERNET 1 A 0
NOERROR F F T T 0
172.217.7.174,172.217.13.238,172.217.15.78,172.2
17.7.206,172.217.9.206,172.217.5.238,172.217.164
.174,172.217.15.110,172.217.2.110,172.217.164.14
2,172.217.7.238,142.250.73.206
299.000000,299.000000,299.000000,299.000000,2
99.000000,299.000000,299.000000,299.000000,29
9.000000,299.000000,299.000000,299.000000 F

http://clipart-library.com/





DOT & DOH to the rescue

DOT (DNS over TLS)

- RFC7858 and RFC8310
- Uses port 853,
- Available in Win10,
- Used in Android 9+, IOS has support but not enabled

DOH (DNS over HTTPS)

- RFC8484
- Uses port 443 with TLS
- FF enabled by default
- Available in Chrome, Edge, Opera

Considerations

- DOH is not a panacea
  - Multiple ways information leaks about your session, to say nothing of the actual session
- Using a US based DNS?
  - Subject to national security inquiries

Craig L Bowser
cbowser@shadowtrackers.net
@reswob10 - twitter