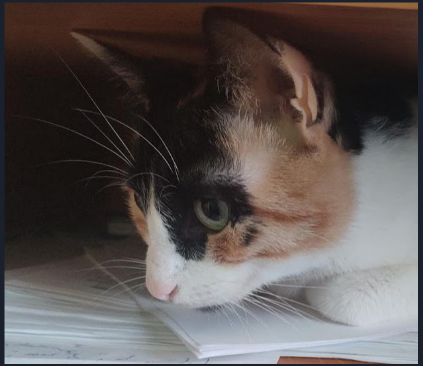
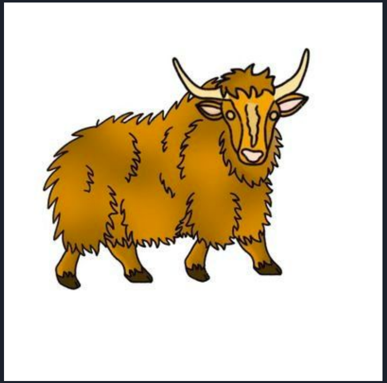
Intro to Forensics

UNbreakable 2021 - Bootcamp

yakuhito@presentation:~# whoami

- High School Student (11th grade @ CNMV)
- CEH, OSCP, OSCE, OSWE
- #TeamRomania (ECSC 2019)
- CTF Player @ HTsP + CodWer
- X-MAS CTF/GTF org
- blog.kuhi.to
- PCO (proud cat owner)





Talk Outline

- Part 1 - Network Forensics
  - The boring stuff (theory)
  - zanger (UNR1), not-clear(UNR2), The Cat(X-MAS 2020)
- Q&A
- Part 2 - Memory Forensics
  - Volatility (+ challs)

The boring stuff (theory)

TCP

- Transmission Control Protocol
- Follow TCP Stream
- Flags?
- Ports!

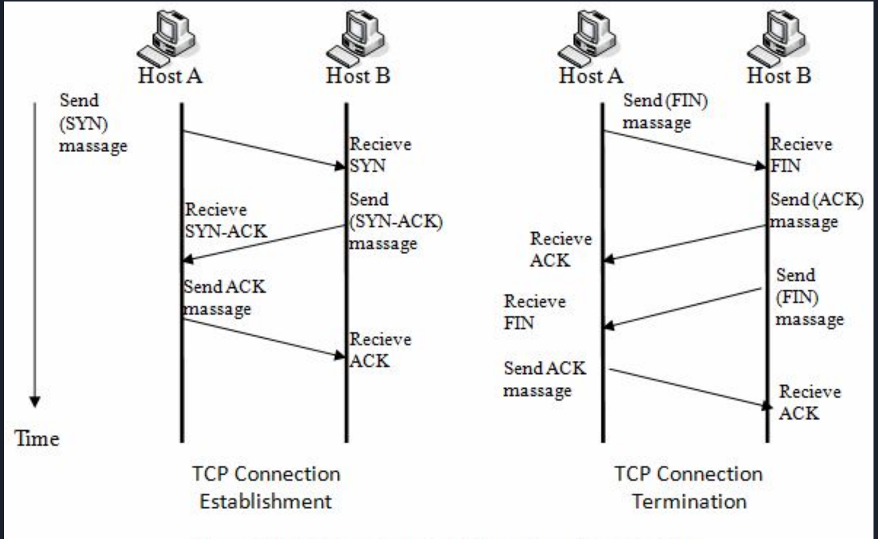
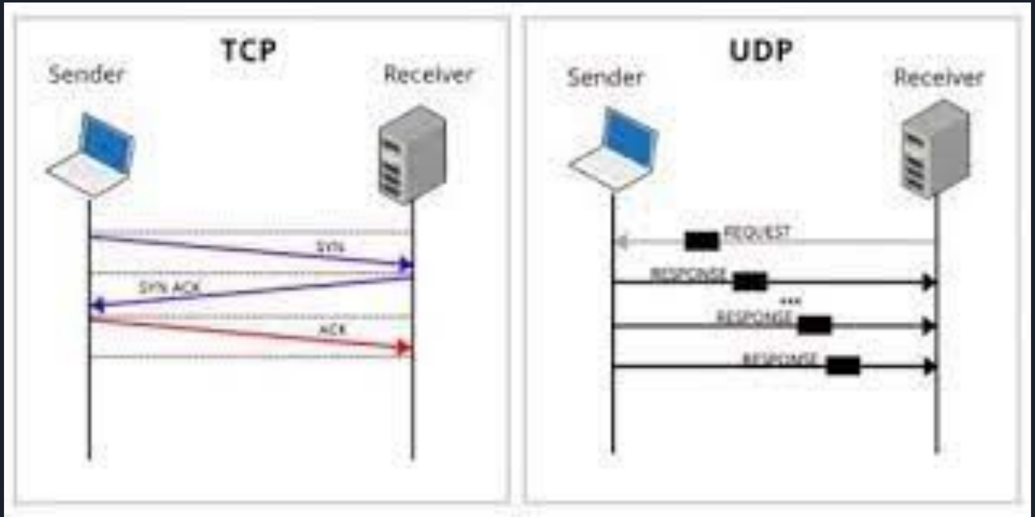


Figure 2.1. TCP session establishment and termination

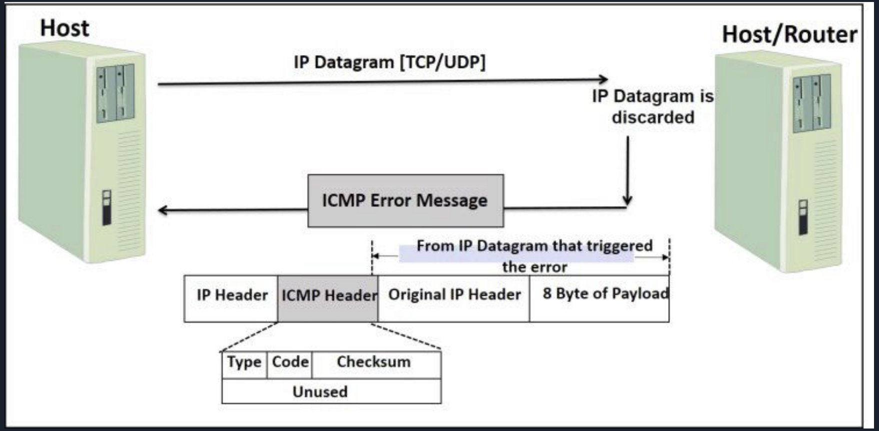
UDP

- User Datagram Protocol
- Follow UDP Stream
- Ports!



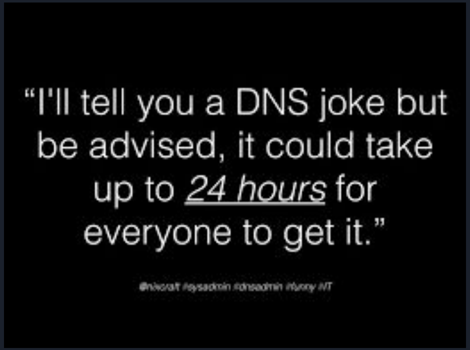
ICMP

- Internet Control Message Protocol
- “ICMP messages are typically used for diagnostic or control purposes or generated in response to errors in IP operations” - Wikipedia
- TTL
- Data field!



DNS

- Domain Name System
- It’s always DNS!
- Subdomains
- TXT records

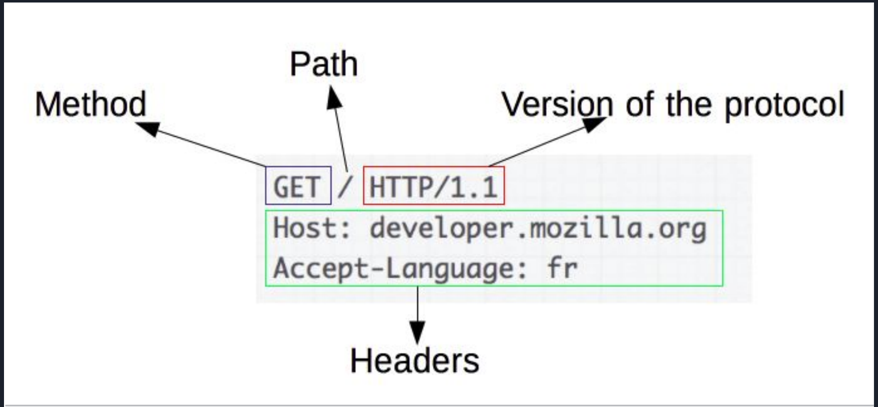


“I'll tell you a DNS joke but be advised, it could take up to *24 hours* for everyone to get it.”

@nixcraft #sysadmin #dnsadmin #funny #IT

HTTP/HTTPS

- Hypertext Transfer Protocol
- http.cat
- Powers the web
- HTTPS can be decrypted given a debug secrets file (session keys)
- Headers
- Data



```
GET / HTTP/1.1
Host: developer.mozilla.org
Accept-Language: fr
```

zanger

not-clear

The Cat

Q&A

Volatility

*

* Q&A