

2550 Intro to cybersecurity

L25: Networking

Ran Cohen/abhi shelat

Get access to the lecture machine

```
ssh <github username>@l21.neucrypt.org
```

Requires you to have your ssh key uploaded to Github.

We will be flipping between slides and console experiments.


How does this work?

The image shows a Firefox browser window in Private Browsing mode. The address bar contains the text "Search with Google or enter address". The main content area features the Firefox logo and the text "Firefox". Below this is a search bar with the text "Search the Web". A section titled "You're in a Private Window" explains that Firefox clears search and browsing history when the app is quit or all Private Browsing tabs and windows are closed. It also includes a link for "Common myths about private browsing". At the bottom, there is a section titled "Need more privacy?".

The Network DevTools panel is open at the bottom, showing a list of filters: "All", "HTML", "CSS", "JS", "XHR", "Fonts", "Images", "Media", "WS", "Other". The "All" filter is selected. The panel also shows a "Filter URLs" input field and a "No requests" status.

Inspector Console Debugger Style Editor Performance Memory Network Storage Accessibility Application

Filter URLs

- Perform a request or **Reload** the page to see detailed information about network activity.
- Click on the  button to start performance analysis. [?](#)

No requests


How does this work?

The image shows a Firefox browser window in Private Browsing mode. The address bar contains the text "Search with Google or enter address". The main content area features the Firefox logo and the text "Firefox". Below this is a search bar with the text "Search the Web". A section titled "You're in a Private Window" explains that Firefox clears search and browsing history when the app is quit or all Private Browsing tabs and windows are closed. It also includes a link for "Common myths about private browsing". At the bottom, there is a section titled "Need more privacy?".

The Network DevTools panel is open at the bottom, showing a list of filters: "All", "HTML", "CSS", "JS", "XHR", "Fonts", "Images", "Media", "WS", "Other". The "All" filter is selected. The panel also shows a "Filter URLs" input field and a "No requests" status.

Inspector Console Debugger Style Editor Performance Memory Network Storage Accessibility Application

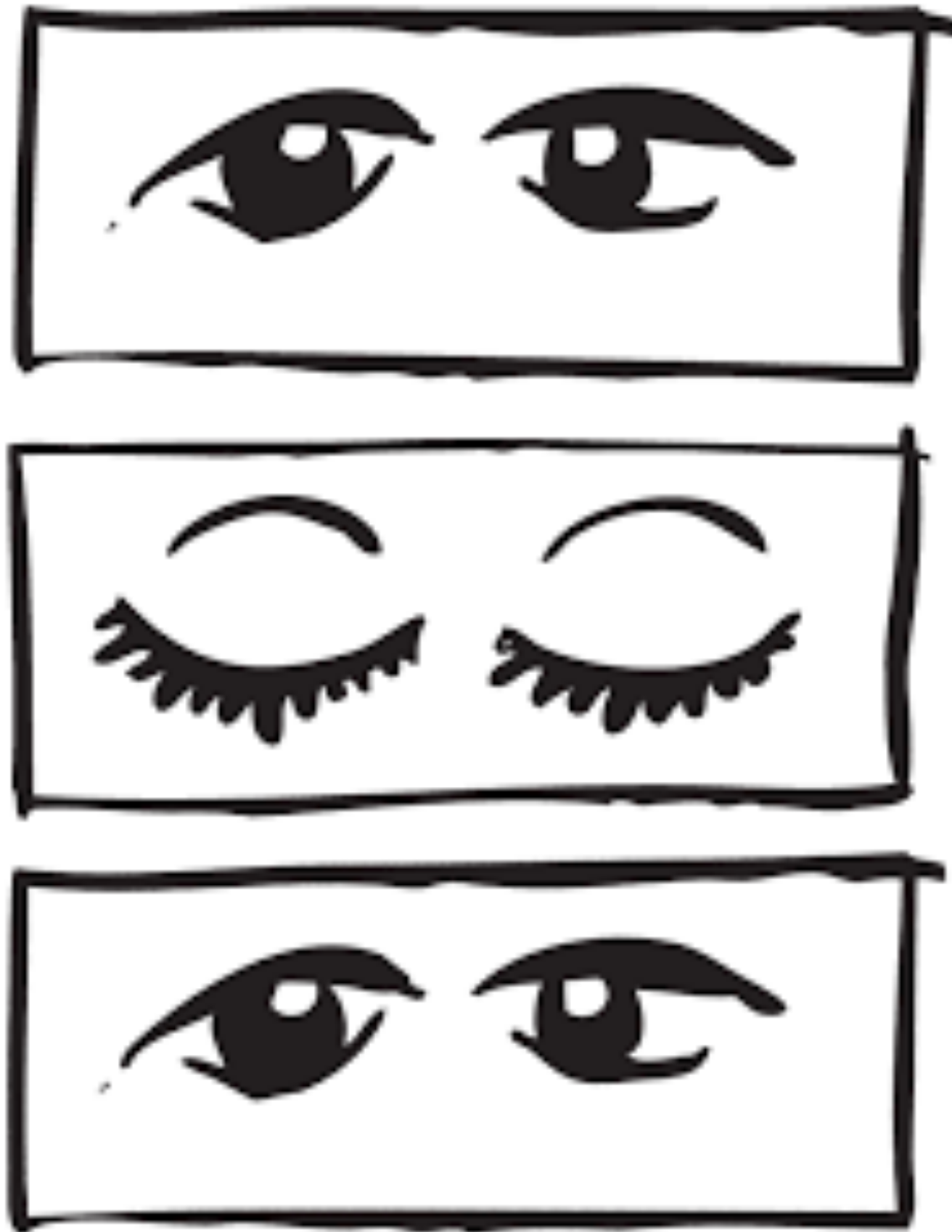
Filter URLs

- Perform a request or **Reload** the page to see detailed information about network activity.
- Click on the  button to start performance analysis. [?](#)

No requests

Networks

How long does it take to blink?



People also ask

How long is a blink of an eye? ^

The **duration** of a **blink** is on average 100–150 milliseconds according to UCL researcher and between 100–400 ms according to the Harvard Database of Useful Biological Numbers. Closures in excess of 1000 ms were defined as microsleeps.

en.wikipedia.org › wiki › Blinking ▾

[Blinking - Wikipedia](#)

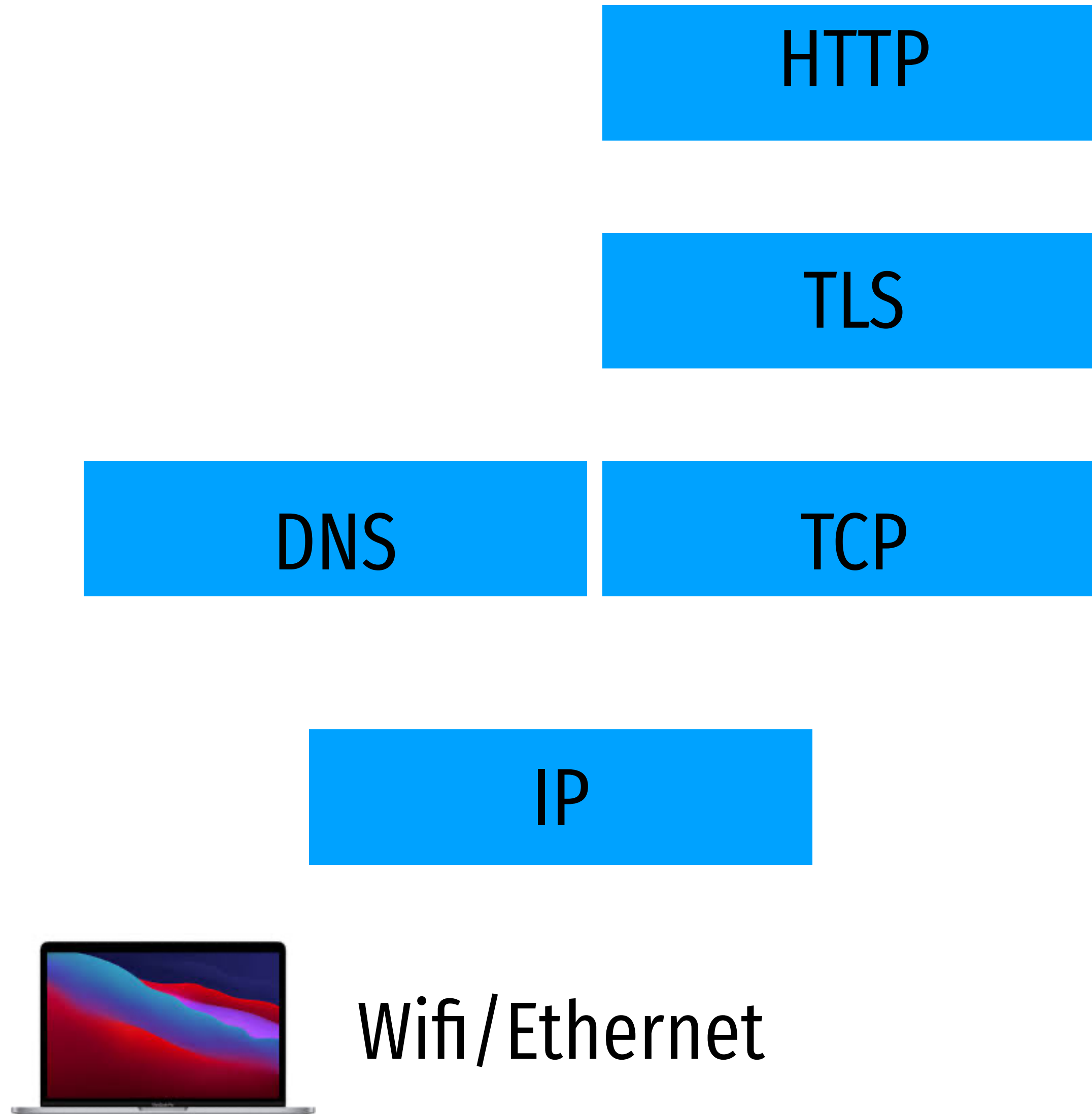
Search for: [How long is a blink of an eye?](#)

Network protocols

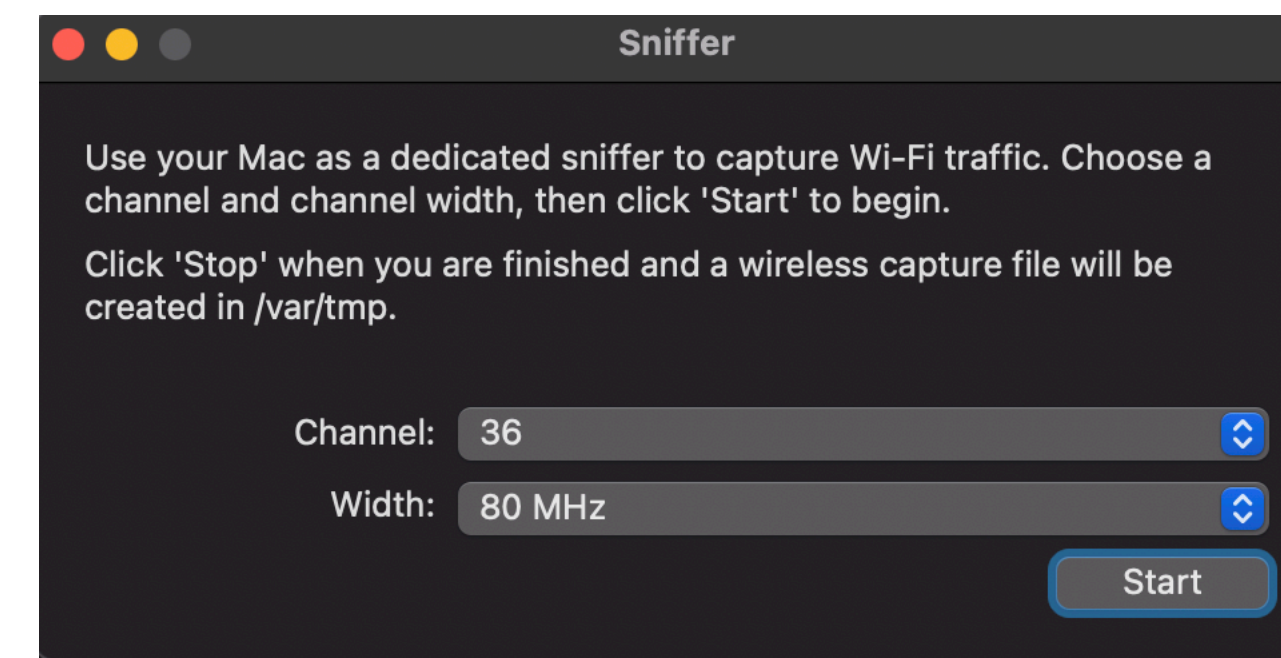
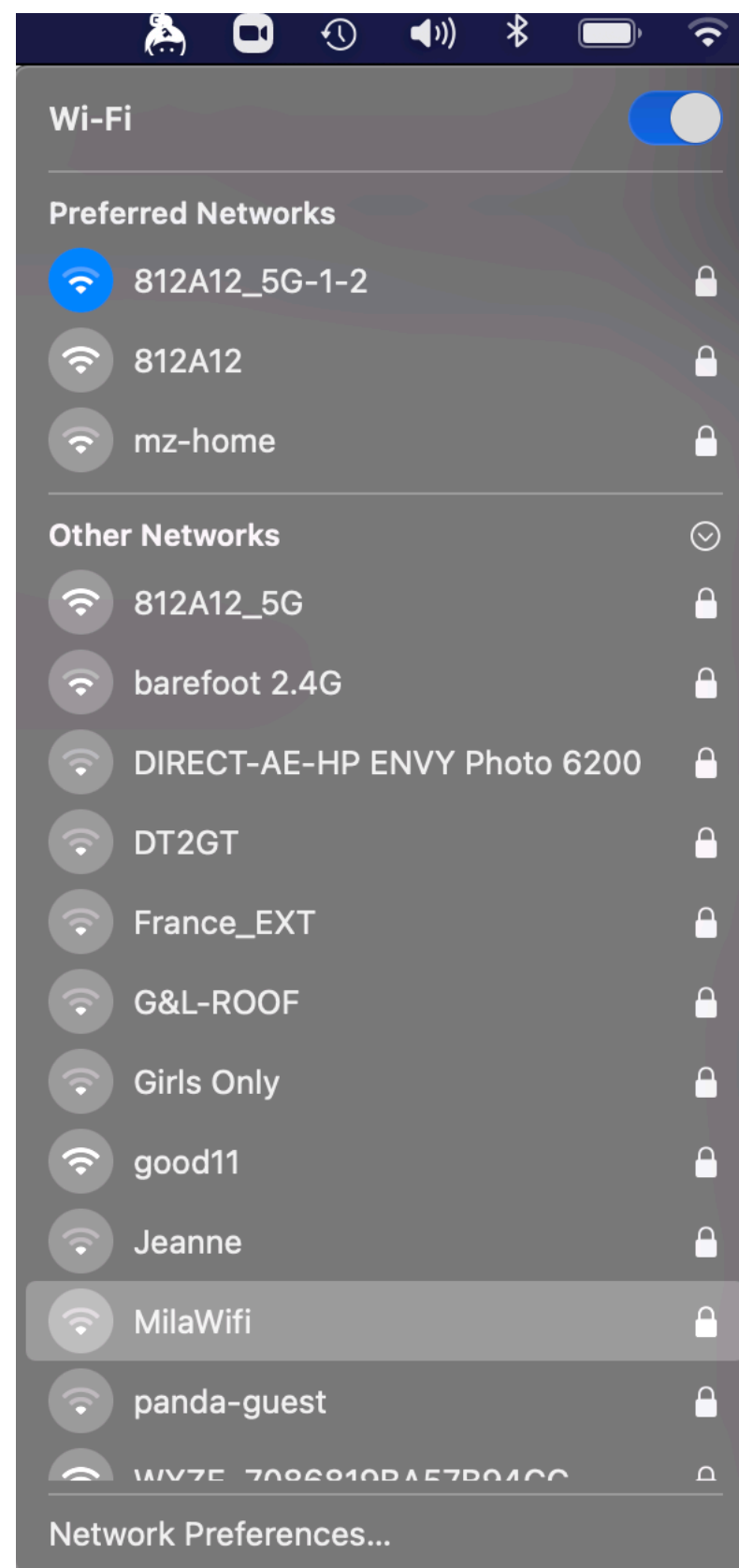


Wifi/Ethernet

Network protocols







Wireshark

Mac-c4910cb5378d_ch36_2020-12-08_08.30.09.659.pcap

Apply a display filter ... <⌘/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000		fc:49:2d:0d:fc:fd ...	802.11	72	Acknowledgement
2	0.013288	c2:93:5b:20:ea:e0	Broadcast	802.11	248	Beacon frame,
3	0.013297		AmazonTe_67:d6:0c ...	802.11	72	Acknowledgement
4	0.018339	Google_bb:a8:cf	Broadcast	802.11	306	Beacon frame,
5	0.026894	Netgear_56:04:44	Broadcast	802.11	318	Beacon frame,
6	0.026913	f0:72:ea:27:37:2a	Broadcast	802.11	284	Beacon frame,
7	0.026916	9e:8f:e0:93:cc:d0	Broadcast	802.11	291	Beacon frame,
8	0.033084	5e:7d:7d:53:19:01	Broadcast	802.11	383	Beacon frame,
9	0.033094	5e:7d:7d:53:19:03	Broadcast	802.11	383	Beacon frame,
10	0.033694	5c:7d:7d:52:19:06	Broadcast	802.11	407	Beacon frame,
11	0.041877		80:da:13:85:55:a6 ...	802.11	72	Clear-to-send
12	0.048110	22:86:8c:c2:ca:e2	Broadcast	802.11	248	Beacon frame,
13	0.049068	7e:8f:e0:93:cc:d0	Broadcast	802.11	291	Beacon frame,
14	0.051958	f0:72:ea:37:00:52	Broadcast	802.11	283	Beacon frame,
15	0.053011	80:da:13:1f:d5:41	Broadcast	802.11	239	Beacon frame,
16	0.053186	80:da:13:1f:d5:43	Broadcast	802.11	284	Beacon frame,
17	0.054472	Netgear_56:04:44	Broadcast	802.11	318	Beacon frame,
18	0.054788	5c:7d:7d:32:3f:81 (5c:7d:7d:32:3f:81) (TA)	fc:49:2d:0d:fc:fd ...	802.11	68	802.11 Block
19	0.055646	5c:7d:7d:32:3f:81 (5c:7d:7d:32:3f:81) (TA)	fc:49:2d:0d:fc:fd ...	802.11	68	802.11 Block
20	0.056126	5c:7d:7d:32:3f:81 (5c:7d:7d:32:3f:81) (TA)	AmazonTe_3f:d6:d6 ...	802.11	76	Request-to-se

> Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Radiotap Header v0, Length 58
> **802.11 radio information**
> IEEE 802.11 Acknowledgement, Flags:C

Mac-c4910cb5378d_ch36_2020-12-08_08.30.09.659.pcap Packets: 1989 · Displayed: 1989 (100.0%) Profile: Default

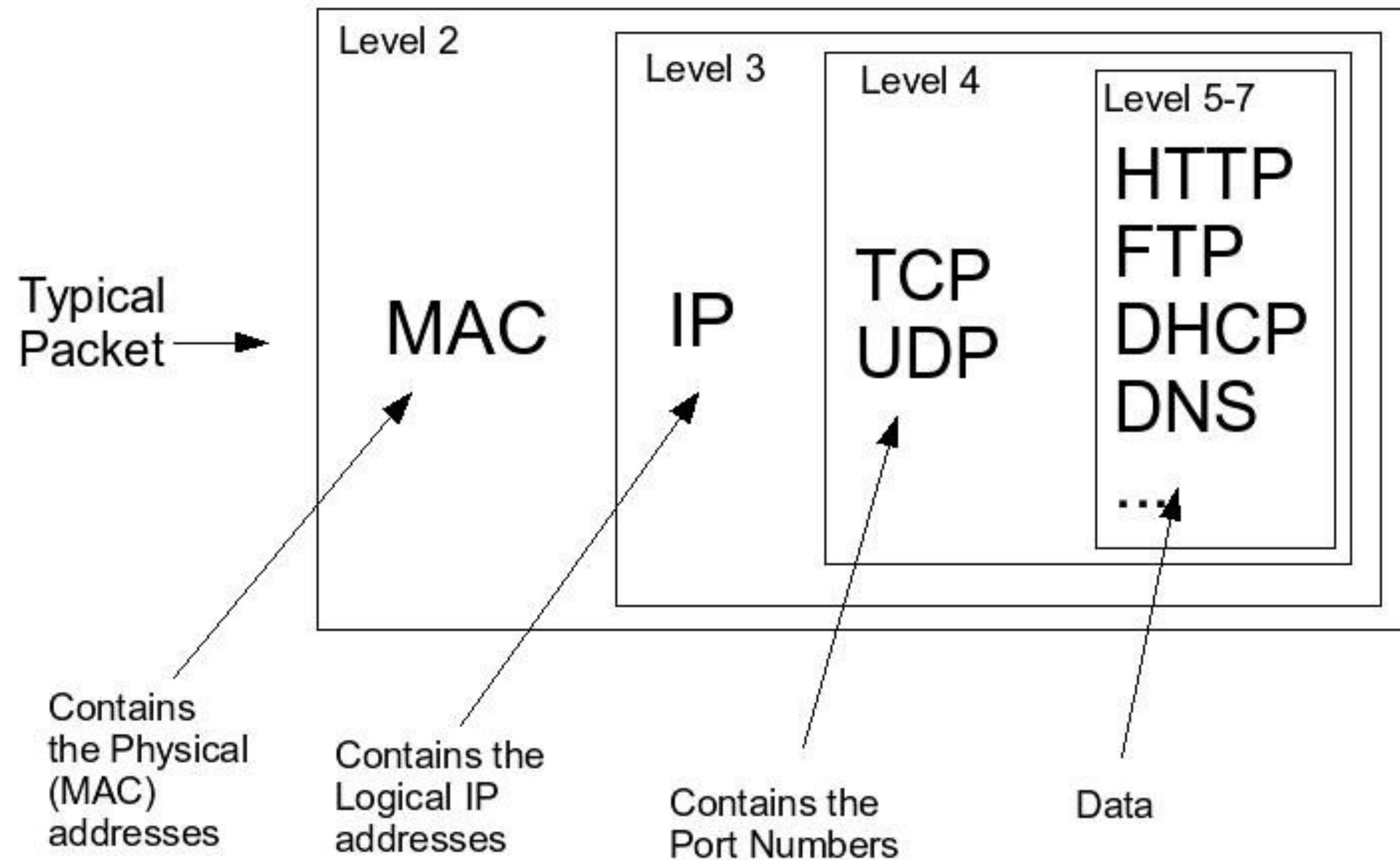


traceroute

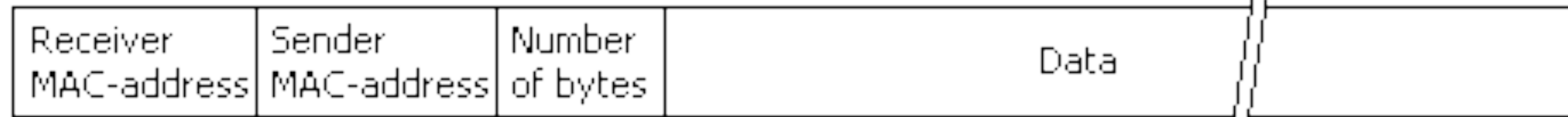
```
MacBook-Pro:Desktop abhi$ traceroute -A www.northeastern.edu
traceroute: Warning: www.northeastern.edu has multiple addresses; using 23.38.112.43
traceroute to e12215.dscb.akamaiedge.net (23.38.112.43), 64 hops max, 52 byte packets
 1 [AS0] router.asus.com (192.168.1.1)  4.343 ms  3.298 ms  3.188 ms
 2 [AS7922] 96.120.67.185 (96.120.67.185) 10.345 ms 11.228 ms 10.395 ms
 3 [AS33657] 24.124.212.73 (24.124.212.73) 10.965 ms 10.040 ms 10.032 ms
 4 [AS7922] 162.151.150.6 (162.151.150.6) 9.843 ms 9.079 ms 9.787 ms
 5 [AS7922] be-334-ar01.needham.ma.boston.comcast.net (96.108.70.141) 12.047 ms 12.082 ms 12.034 ms
 6 [AS7922] 50-222-48-18-static.hfc.comcastbusiness.net (50.222.48.18) 17.514 ms 17.504 ms 19.669 ms
 7 [AS35994] a23-38-112-43.deploy.static.akamaitechnologies.com (23.38.112.43) 12.001 ms 14.432 ms 12.884 ms
MacBook-Pro:Desktop abhi$
```



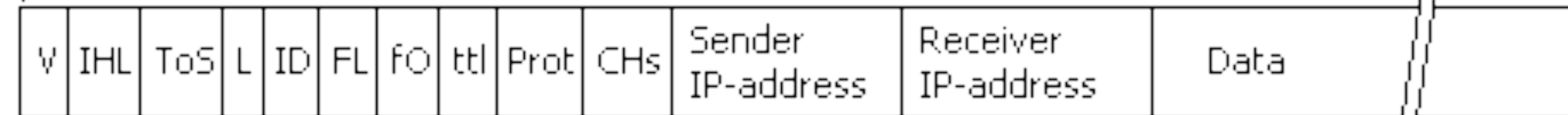
Anatomy of a packet



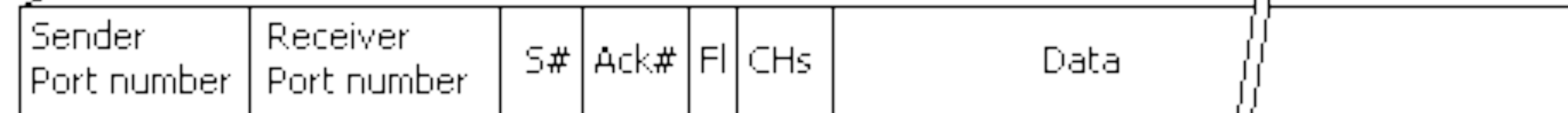
Ethernet Packet



IP Packet



TCP Packet



<http://internetsequoia.blogspot.com/>



<http://learn-networking.com/tcp-ip/how-the-internet-layer-works>

Example packet capture

2020-12-08 14:11:07.473254 42:01:0a:96:00:01 > 42:01:0a:96:00:03, IPv4, length 587: (tos 0x0, ttl 47, id 0, offset 0, flags [DF], proto TCP (6), length 573)

24.147.105.137.53946 > 10.150.0.3.8000: tcp 521

```
0x0000: 4201 0a96 0003 4201 0a96 0001 0800 4500 B.....B.....E.
0x0010: 023d 0000 4000 2f06 bd06 1893 6989 0a96 *= ..@./.....i ...
0x0020: 0003 d2ba 1f40 e734 de06 3b40 95fc 8018 .....@.4..;@....
0x0030: 0800 1a3b 0000 0101 080a 064a fe59 9a5b ...;.....J.Y.[
0x0040: 8cc8 504f 5354 202f 6c6f 6769 6e20 4854 ..POST./login.HT
0x0050: 5450 2f31 2e31 0d0a 486f 7374 3a20 6c32 TP/1.1..Host:.l2
0x0060: 342e 6e65 7563 7279 7074 2e6f 7267 3a38 4.neucrypt.org:8
0x0070: 3030 300d 0a4f 7269 6769 6e3a 2068 7474 000..Origin:.htt
0x0080: 703a 2f2f 6c32 342e 6e65 7563 7279 7074 p://l24.neucrypt
0x0090: 2e6f 7267 3a38 3030 300d 0a43 6f6e 7465 .org:8000..Conte
0x00a0: 6e74 2d54 7970 653a 2061 7070 6c69 6361 nt-Type:.applica
0x00b0: 7469 6f6e 2f78 2d77 7777 2d66 6f72 6d2d tion/x-www-form-
0x00c0: 7572 6c65 6e63 6f64 6564 0d0a 4163 6365 urlencoded..Acce
0x00d0: 7074 2d45 6e63 6f64 696e 673a 2067 7a69 pt-Encoding:.gzi
0x00e0: 702c 2064 6566 6c61 7465 0d0a 436f 6e6e p,.deflate..Conn
0x00f0: 6563 7469 6f6e 3a20 6b65 6570 2d61 6c69 ection:.keep-ali
0x0100: 7665 0d0a 5570 6772 6164 652d 496e 7365 ve..Upgrade-Inse
0x0110: 6375 7265 2d52 6571 7565 7374 733a 2031 cure-Requests:.1
0x0120: 0d0a 4163 6365 7074 3a20 7465 7874 2f68 ..Accept:.text/h
0x0130: 746d 6c2c 6170 706c 6963 6174 696f 6e2f tml,application/
0x0140: 7868 746d 6c2b 786d 6c2c 6170 706c 6963 xhtml+xml,applic
0x0150: 6174 696f 6e2f 786d 6c3b 713d 302e 392c ation/xml;q=0.9,
0x0160: 2a2f 2a3b 713d 302e 380d 0a55 7365 722d */*;q=0.8..User-
0x0170: 4167 656e 743a 204d 6f7a 696c 6c61 2f35 Agent:.Mozilla/5
0x0180: 2e30 2028 4d61 6369 6e74 6f73 683b 2049 .0.(Macintosh;.I
0x0190: 6e74 656c 204d 6163 204f 5320 5820 3130 ntel.Mac.OS.X.10
0x01a0: 5f31 355f 3629 2041 7070 6c65 5765 624b _15_6).AppleWebK
0x01b0: 6974 2f36 3035 2e31 2e31 3520 284b 4854 it/605.1.15.(KHT
0x01c0: 4d4c 2c20 6c69 6b65 2047 6563 6b6f 2920 ML,.like.Gecko).
0x01d0: 5665 7273 696f 6e2f 3134 2e30 2e31 2053 Version/14.0.1.S
0x01e0: 6166 6172 692f 3630 352e 312e 3135 0d0a afari/605.1.15..
0x01f0: 5265 6665 7265 723a 2068 7474 703a 2f2f Referer:.http://
0x0200: 6c32 342e 6e65 7563 7279 7074 2e6f 7267 l24.neucrypt.org
0x0210: 3a38 3030 302f 6c6f 6769 6e0d 0a43 6f6e :8000/login..Con
0x0220: 7465 6e74 2d4c 656e 6774 683a 2033 340d tent-Length:.34.
0x0230: 0a41 6363 6570 742d 4c61 6e67 7561 6765 .Accept-Language
0x0240: 3a20 656e 2d75 730d 0a0d 0a :.en-us....
```

Demos

Download Wireshark

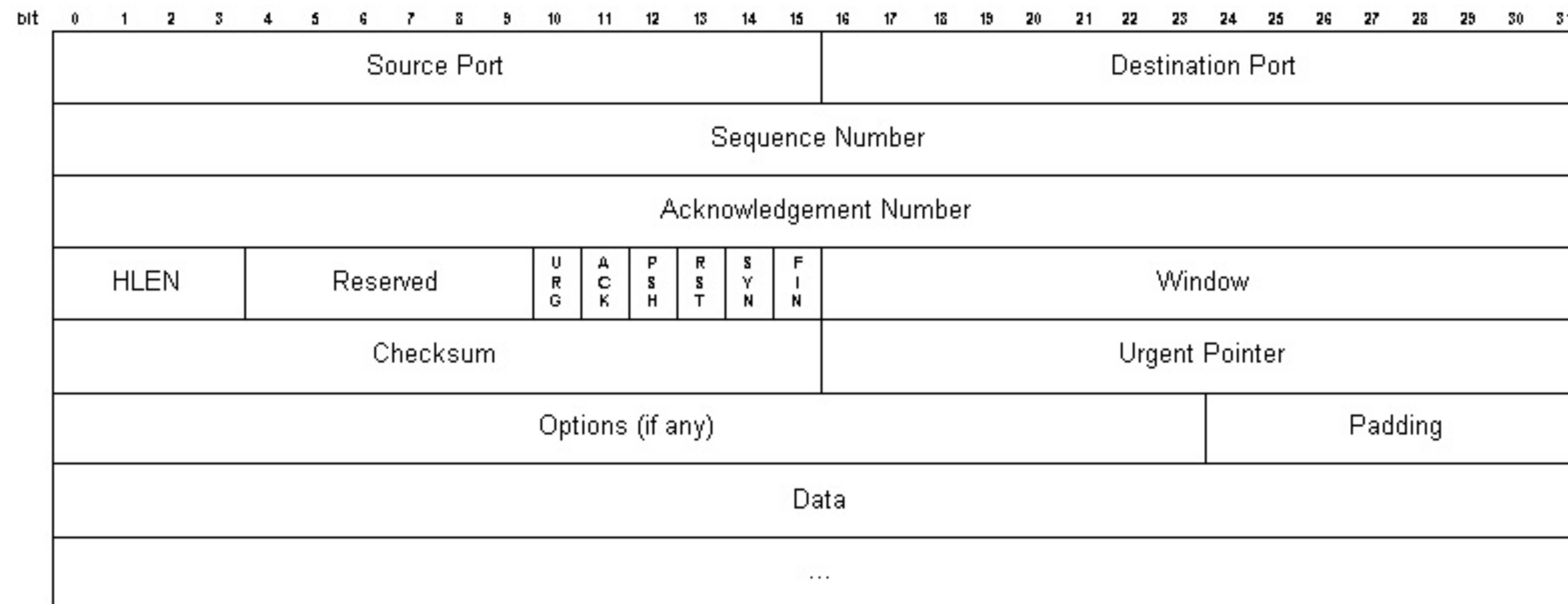
<https://www.wireshark.org/download.html>

Download ch6.pcap

<https://shelat.khoury.northeastern.edu/dl/20f-2550/channel6.pcap>

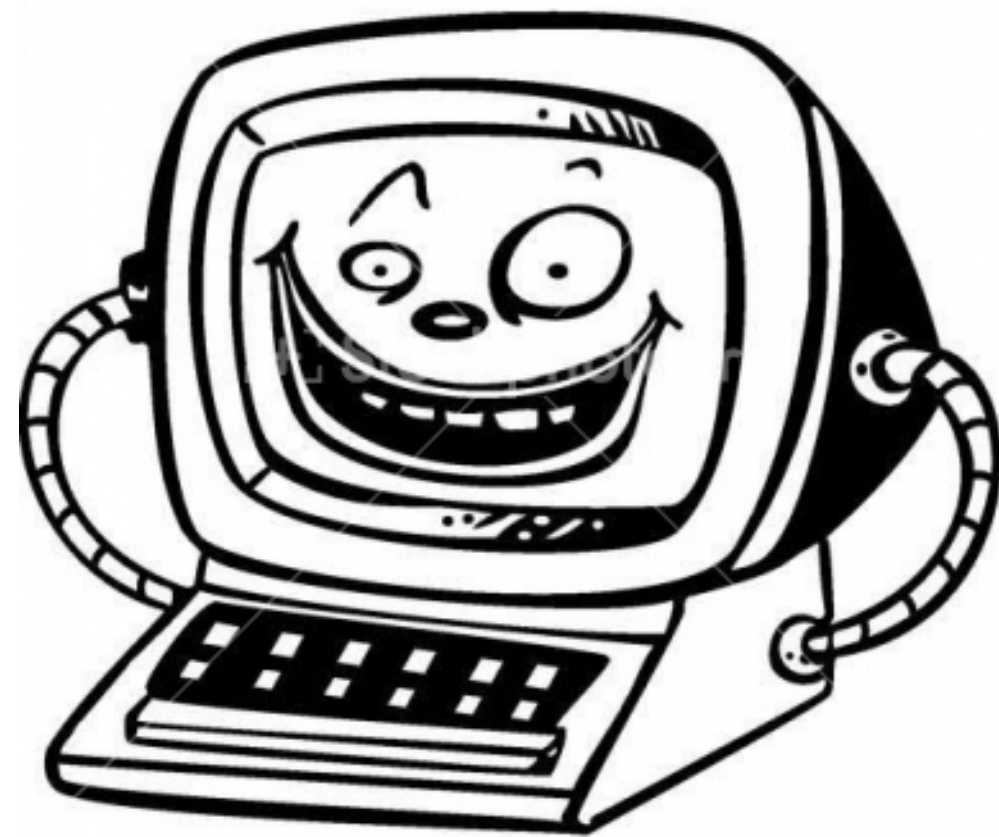
TCP

msg delivery guarantee: data arrives in order, receipt acknowledged



How a TCP begins

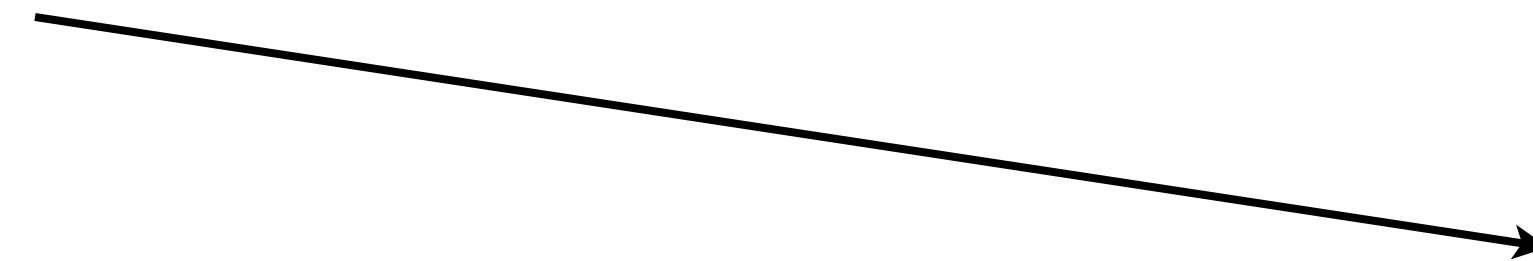
Alice



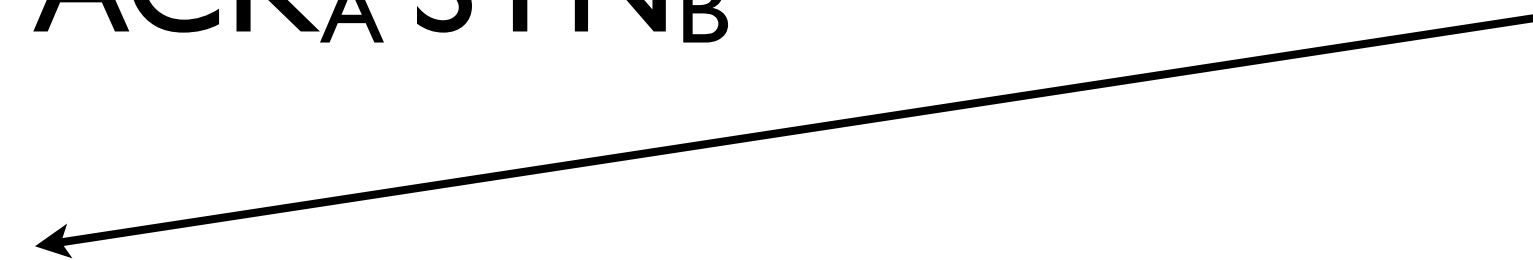
Bob



SYN_A



$ACK_A SYN_B$

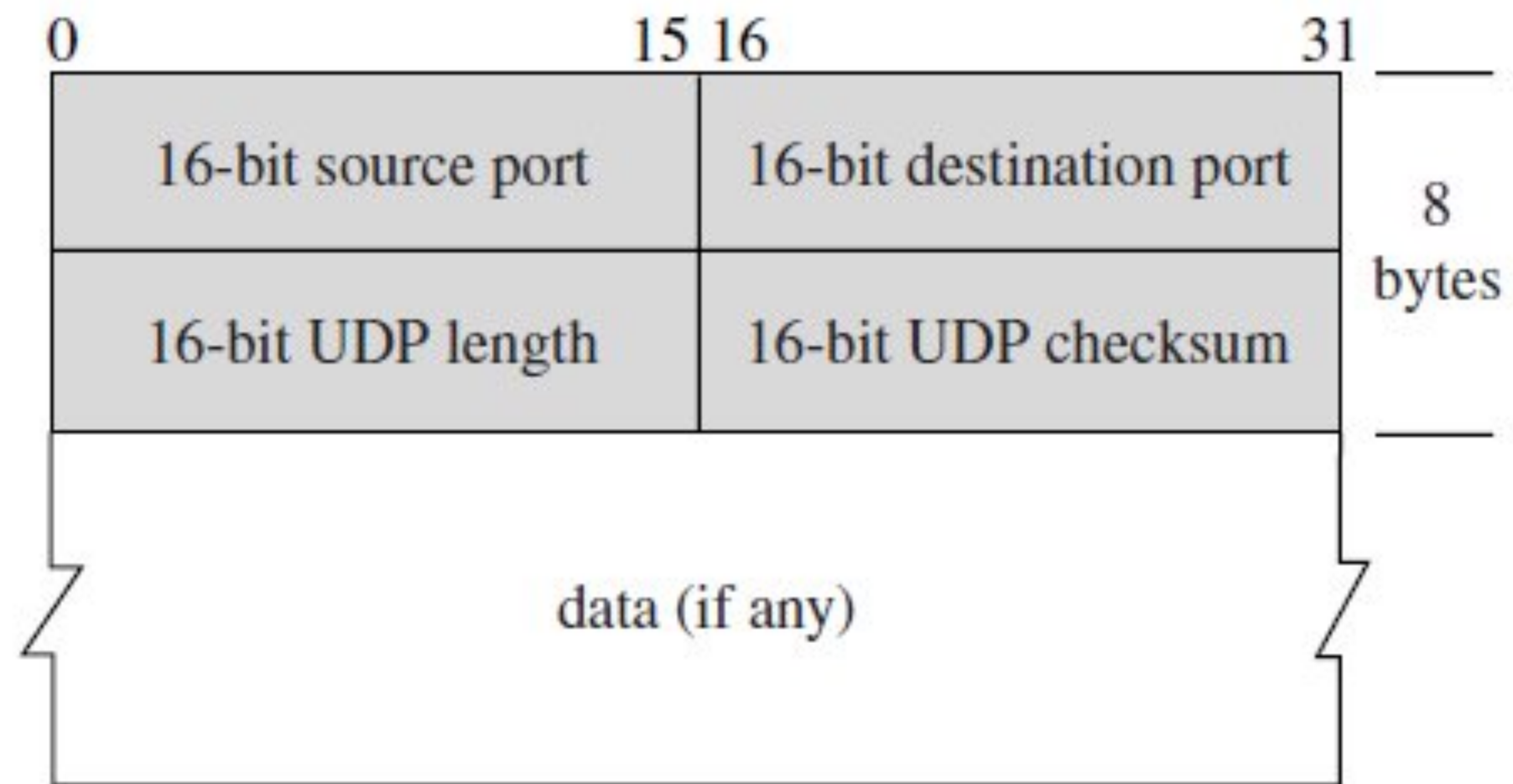


ACK_B



UDP

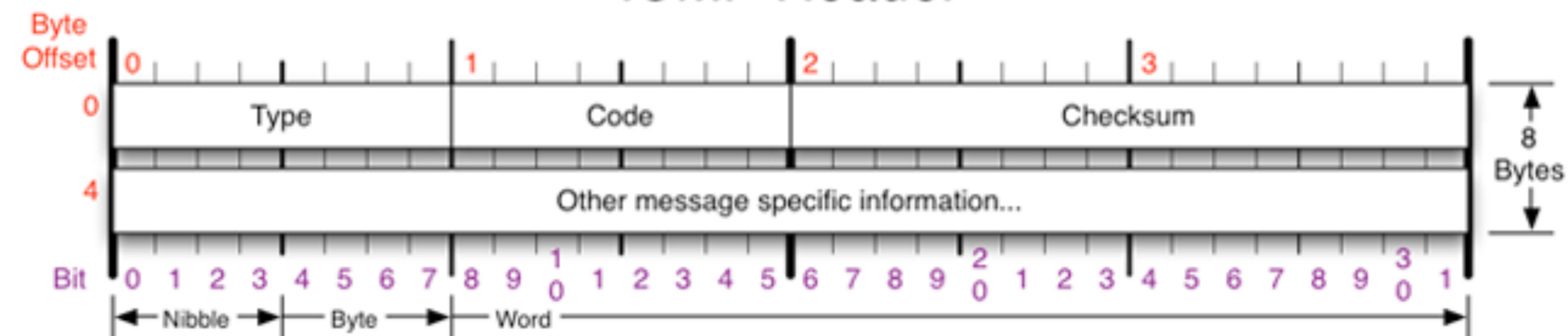
msg delivery guarantee: best effort



ICMP

IP packet out-of-band messaging

ICMP Header



Destination unreachable

- Time exceeded
- Parameter problem
- Redirect to better gateway
- Reachability test (echo / echo reply)
- Message transit delay (timestamp request / reply)



https

Safari is using an encrypted connection to www.northeastern.edu.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.northeastern.edu.

USERTrust RSA Certification Authority
InCommon RSA Server CA
www.northeastern.edu

www.northeastern.edu
Issued by: InCommon RSA Server CA
Expires: Sunday, May 29, 2022 at 7:59:59 PM Eastern Daylight Time
This certificate is valid

Trust
Details

Subject Name	
Country or Region	US
Postal Code	02115
State/Province	Massachusetts
Locality	Boston
Street Address	360 Huntington Ave.
Organization	Northeastern University
Organizational Unit	Information Technology Services
Common Name	www.northeastern.edu

Issuer Name	
Country or Region	US
State/Province	MI
Locality	Ann Arbor
Organization	Internet2
Organizational Unit	InCommon
Common Name	InCommon RSA Server CA

Hide Certificate OK

ACCEPT AND CONTINUE


```
abhi@l21:~/l25$ openssl s_client -connect www.google.com:443 -showcerts
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = GTS CA 101
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
verify return:1
---
Certificate chain
 0 s:C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
  i:C = US, O = Google Trust Services, CN = GTS CA 101
-----BEGIN CERTIFICATE-----
MIIEyTCCA7GgAwIBAgIRA0WJUBT/plbPAGAAAACAVf4wDQYJKoZIhvcNAQELBQAw
QjELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBSUENVzdCBTZXJ2aWNlczET
d3cuZ29vZ2xlLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABKLISJuNl7yH
...
4oVg67pw7d42SpfMsYF1j8EC55iuyuLBlgeZ71B37dyGo3ZvfkTdGXwEFAEhn/eC
ne2mhh7QQGKD3Dp5mHmxPXDAQlJ6phDvsHVXCpE=
-----END CERTIFICATE-----
 1 s:C = US, O = Google Trust Services, CN = GTS CA 101
  i:OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
-----BEGIN CERTIFICATE-----
MIIESjCCAzKgAwIBAgINAeO0mqGNiqmBJWlQuDANBgkqhkiG9w0BAQsFADBMMSAw
HgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMjETMBEGA1UEChMKR2xvYmFs
...
IRdAvKLWZu/axBVbzYmqmwkm5zLSDW5nIAJbELCQCZwMH56t2Dvqofxs6BBcCFIZ
USpxu6x6td0V7SvJCCosirSmIatj/9dSSVDQibet8q/7UK4v4ZUN80atnZz1yg=
-----END CERTIFICATE-----
---
Server certificate
subject=C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com

issuer=C = US, O = Google Trust Services, CN = GTS CA 101

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 2640 bytes and written 386 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
```

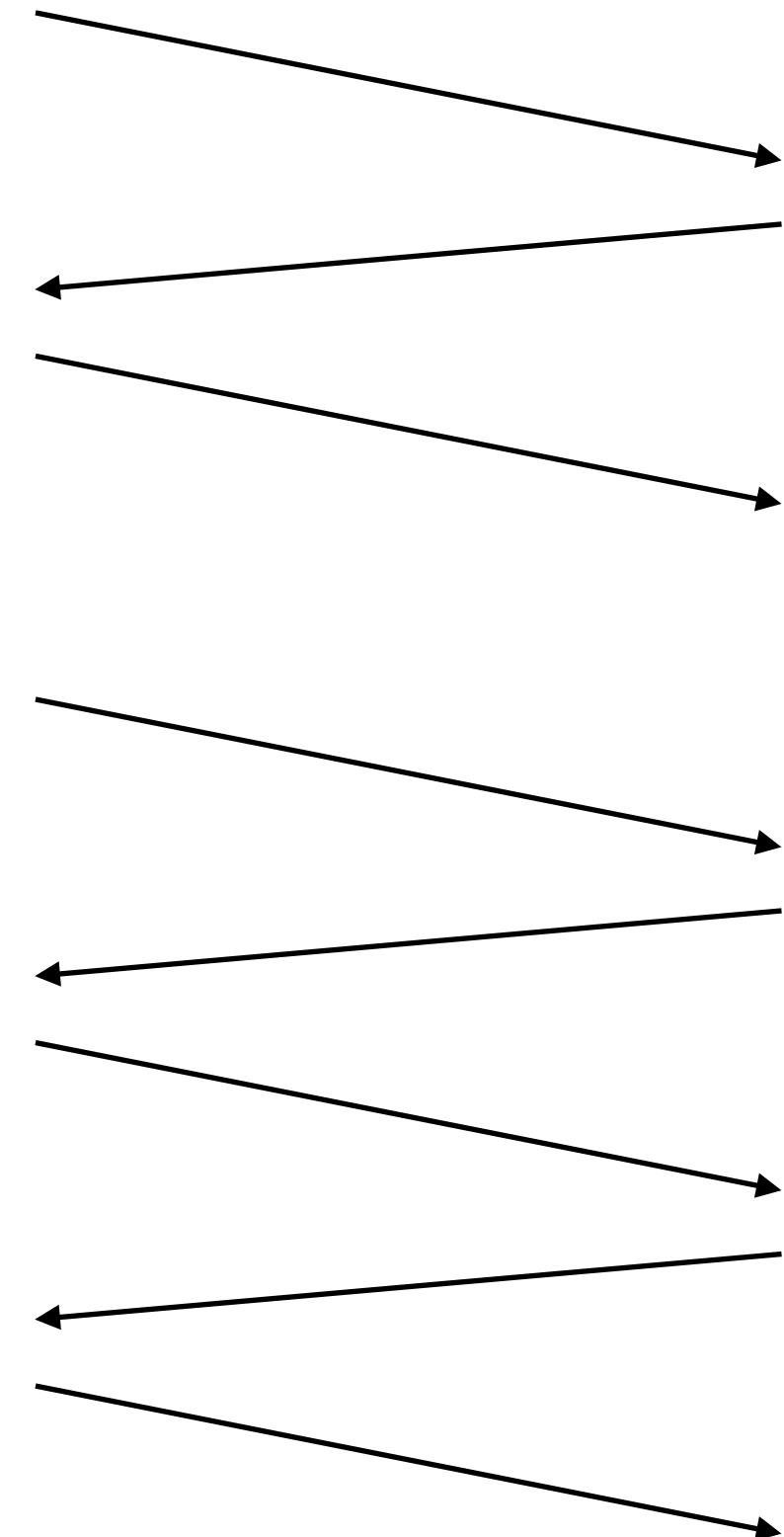
```

abhi@l21:~/l25$ openssl s_client -connect www.google.com:443 -showcerts
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = GTS CA 101
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
verify return:1
---
Certificate chain
 0 s:C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
  i:C = US, O = Google Trust Services, CN = GTS CA 101
-----BEGIN CERTIFICATE-----
MIIEyTCCA7GgAwIBAgIRA0WJUBT/plbPAgAAAACAVf4wDQYJKoZIhvcNAQELBQAw
QjELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBSUENvbnVzdCBTZXJ2aWNlczET
d3cuZ29vZ2xlLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABKLISJuNl7yH
...
4oVg67pw7d42SpfMsYF1j8EC55iuyuLBlgeZ71B37dyGo3ZvfkTdGXwEFAEhn/eC
ne2mhh7QQGKD3Dp5mHmxPXDAQlJ6phDvsHVXCpE=
-----END CERTIFICATE-----
 1 s:C = US, O = Google Trust Services, CN = GTS CA 101
  i:OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
-----BEGIN CERTIFICATE-----
MIIESjCCAzKgAwIBAgINAeO0mqGNiqmBJWlQuDANBgkqhkiG9w0BAQsFADBMMSAw
HgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMjETMBEGA1UEChMKR2xvYmFs
...
IRdAvKLWZu/axBVbzYmqmwkm5zLSDW5nIAJbELCQCZwMH56t2Dvqofxs6BBcCFIZ
USpxu6x6td0V7SvJCCosirSmIatj/9dSSVDQibet8q/7UK4v4ZUN80atnZz1yg=
-----END CERTIFICATE-----
---
Server certificate
subject=C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com

issuer=C = US, O = Google Trust Services, CN = GTS CA 101

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 2640 bytes and written 386 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)

```



Network stack

HTTP

TLS

DNS

TCP

IP

Wifi/Ethernet

How does neu.edu resolve to IP address?

Network exploits

Previous insight: security vulnerabilities arise when **external input** is not verified.

Network insight: security vulnerabilities arise due to failures of design and abstraction.

Networks were designed for convenience.

Security was an afterthought.

Networks increase number of possible attackers.
(Attack surface is increased.)

Networks provide some anonymity to the attacker.

Issues with

Privacy of Information

Authentication of parties

Availability of services

Infrastructure attacks

actively listen and modify traffic as it flows across your nodes

denial-of-service

attack the routers that control traffic flow

attack the domain naming system to redirect traffic

Availability attacks

ICMP

ECHO request

“Ping”

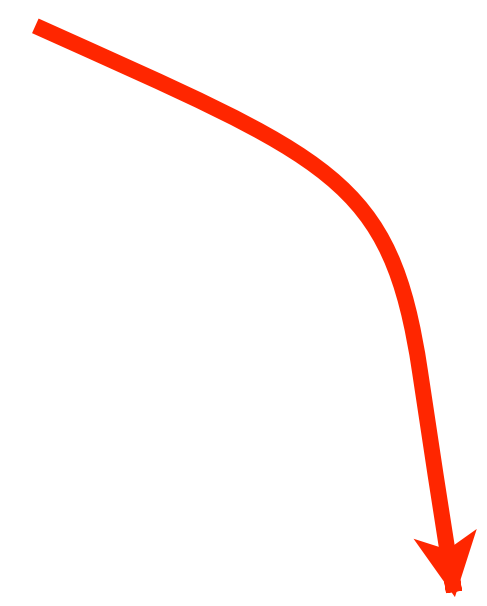
IP HDR
8
0

ECHO request

Code 0

Attacker

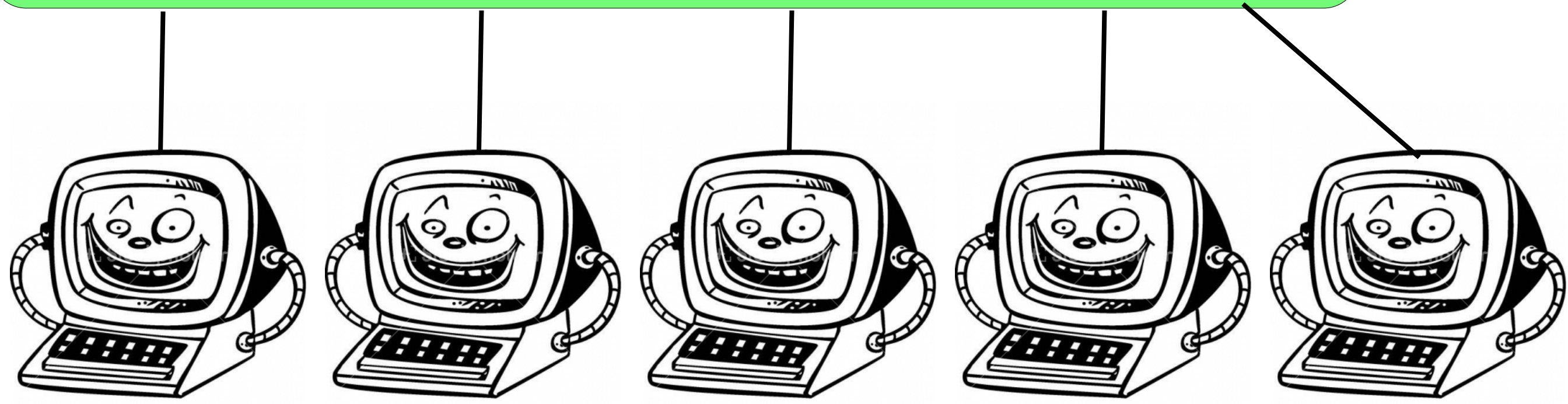
SRC:Victim
DES: Broadcast
8 ECHO
0



Network



Victim



Patsies

http://www.stockphotopro.com/photo_of/cartoon/5809266ZQA/ cartoon_computer_

https://encrypted-tbn3.google.com/images?q=tbn:ANd9GcQGg_2LSF_hjV2xtAzqWY0e_ICU8Tlc2fDbZ4n29jZATD4Vzlx8nA

Attacker

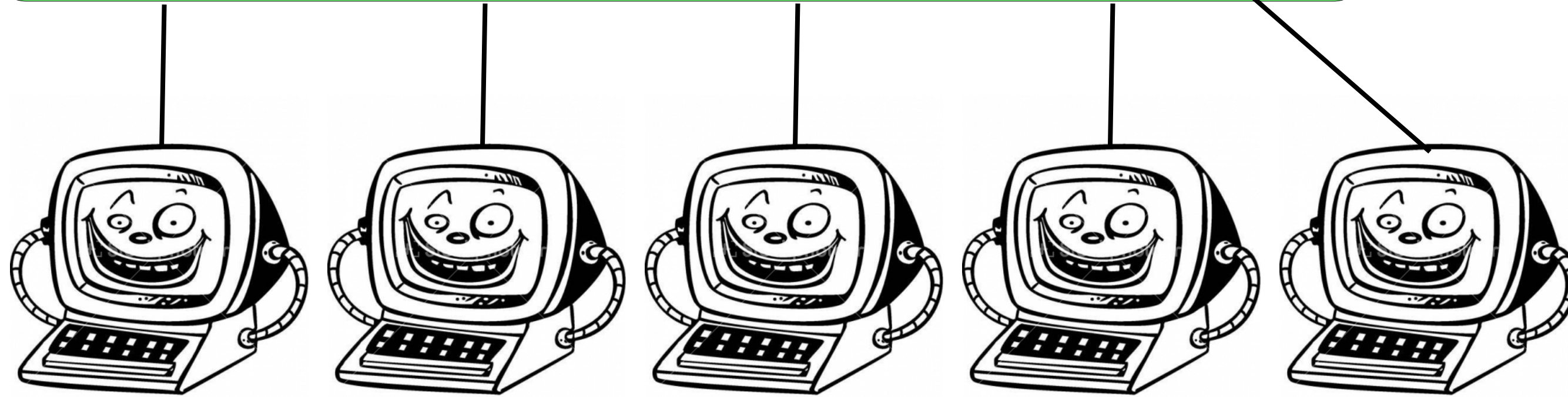
SRC:Victim
DES: Broadcast
8 ECHO
0



Network



Victim



Unaware accomplices

This computer now receives thousands of packets.

What missing security property
enables the attack?

What missing security property
enables the attack?

Authentication
of parties

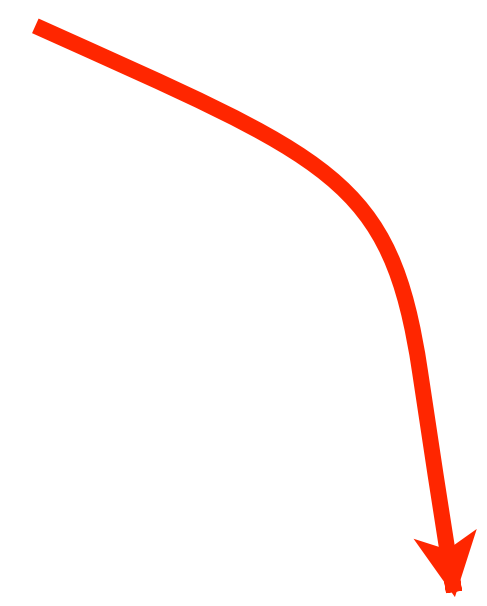
The SRC/DST fields of a packet are unauthenticated.
It is possible to mimic any node on the internet.

Proper network configuration can limit the attack.

What steps should a network **router/gateway/accesspoint** take?

Attacker

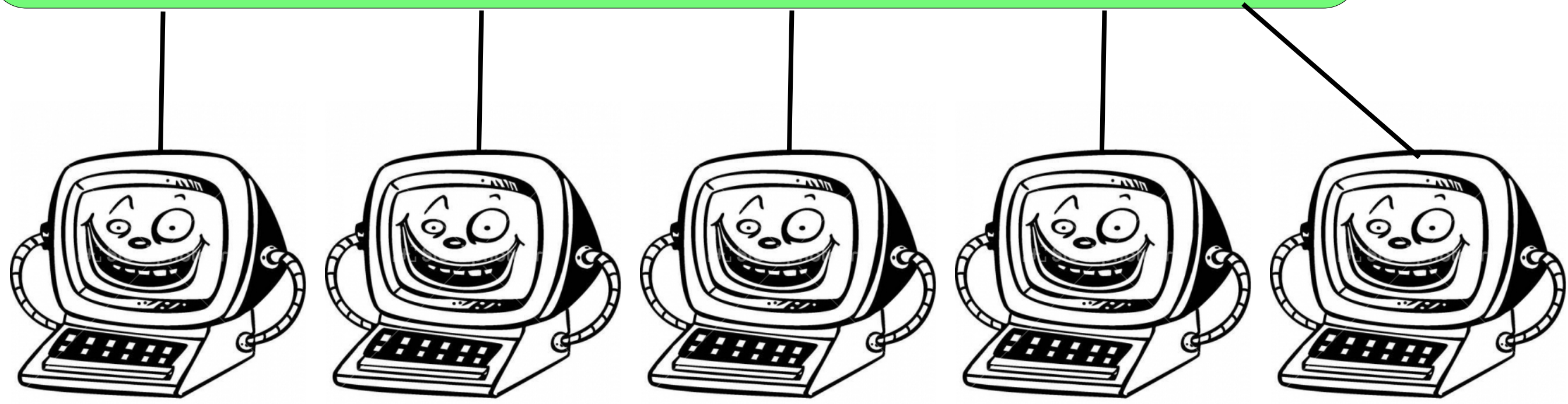
SRC:Victim
DES: Broadcast
8 ECHO
0



Network



Victim



Patsies

This computer now receives thousands of packets.

http://www.stockphotopro.com/photo_of/cartoon/5809266ZQA/ cartoon_computer_

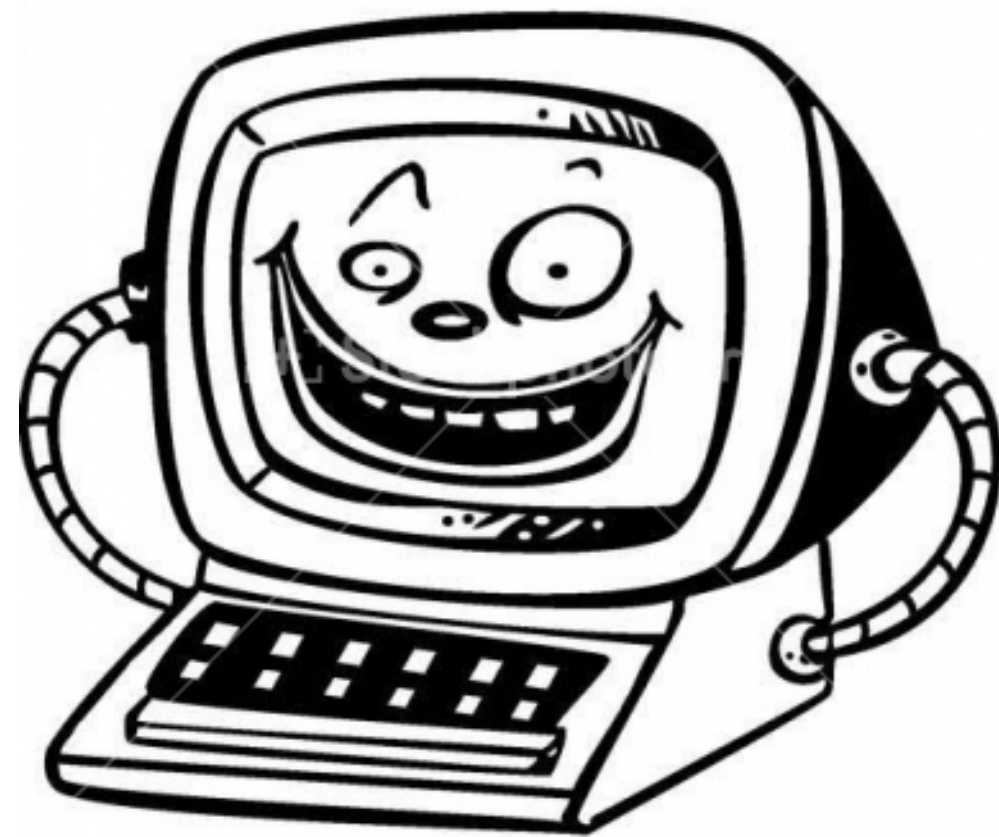
https://encrypted-tbn3.google.com/images?q=tbn:ANd9GcQGg_2LSF_hjV2xtAzqWY0e_ICU8Tlc2fDbZ4n29jZATD4Vzlx8nA

Attacker is able to **LEVERAGE** its resources.

1 attack packet becomes 1000s.

How a TCP begins

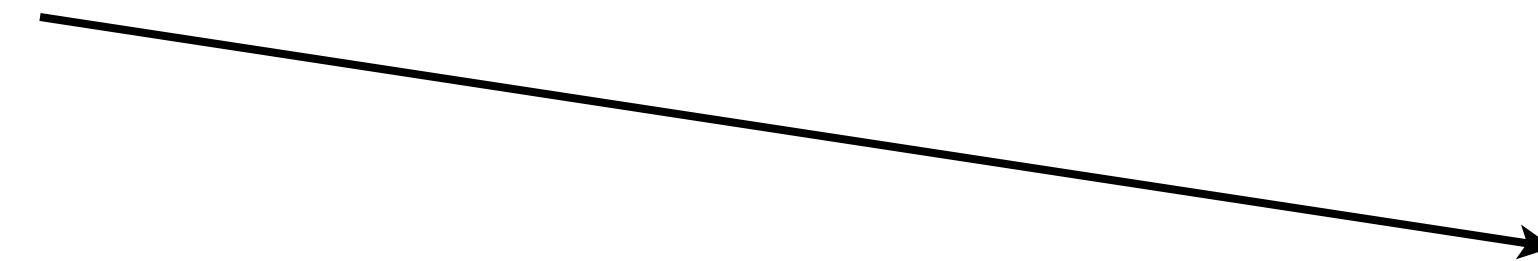
Alice



Bob



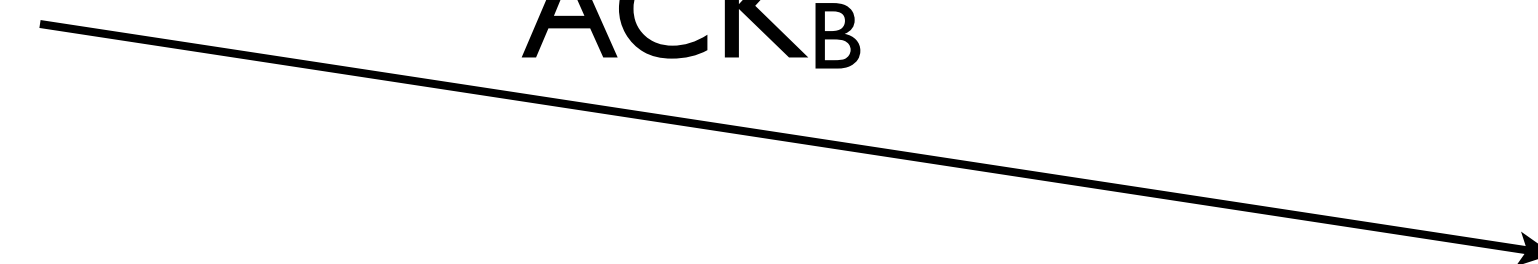
SYN_A



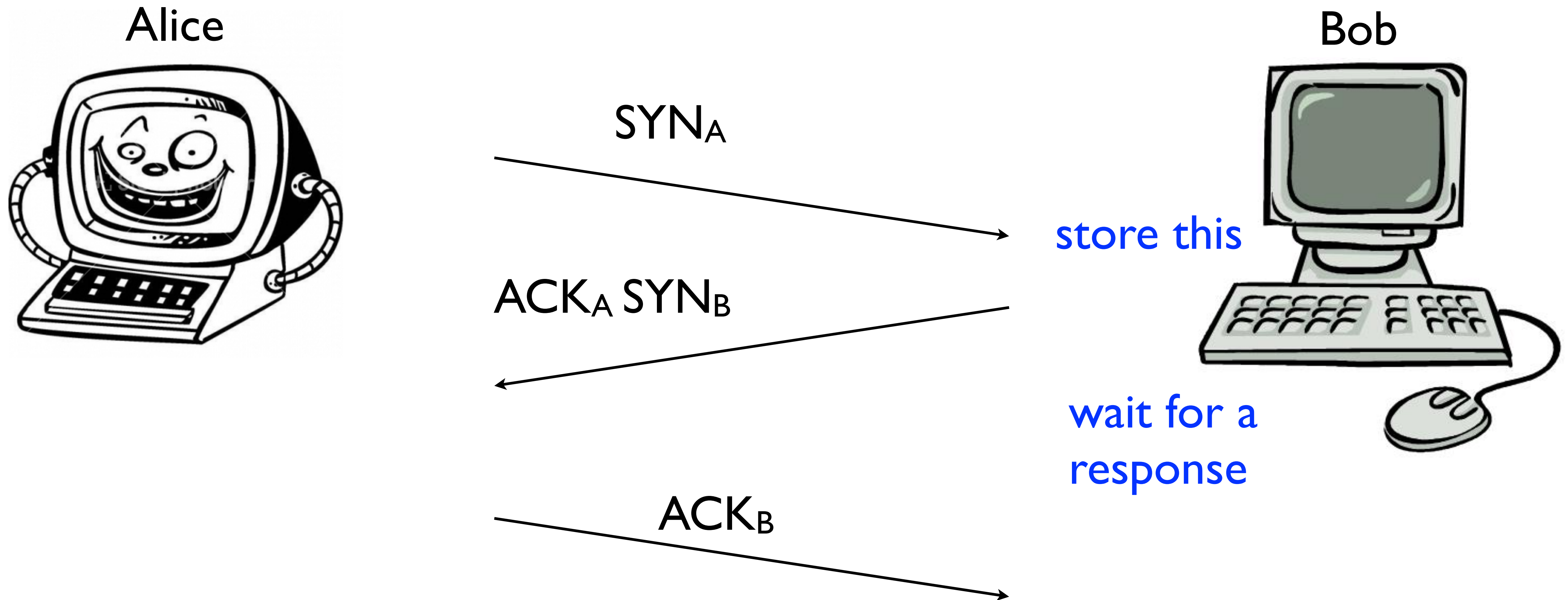
$ACK_A SYN_B$



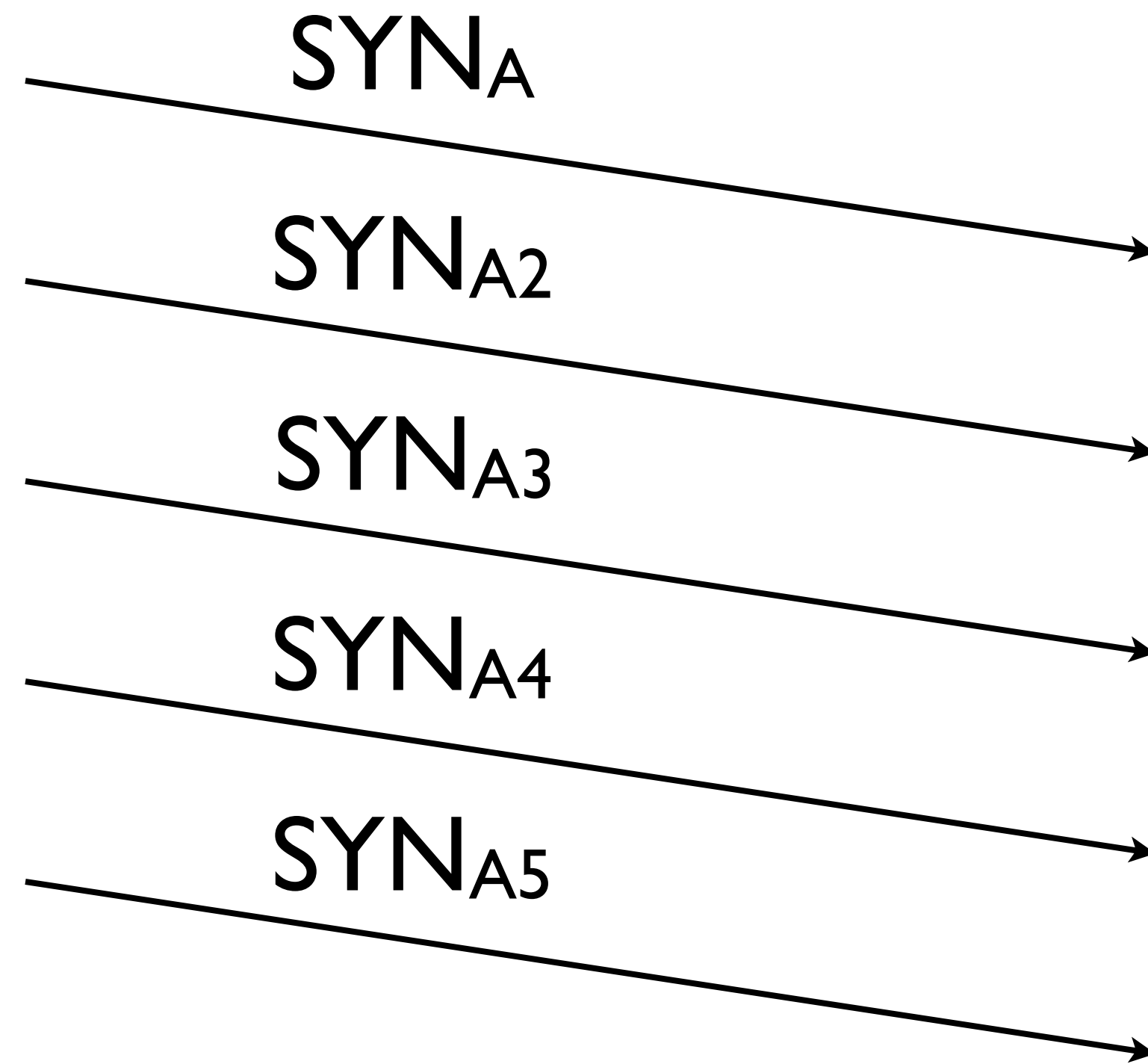
ACK_B



How a TCP begins



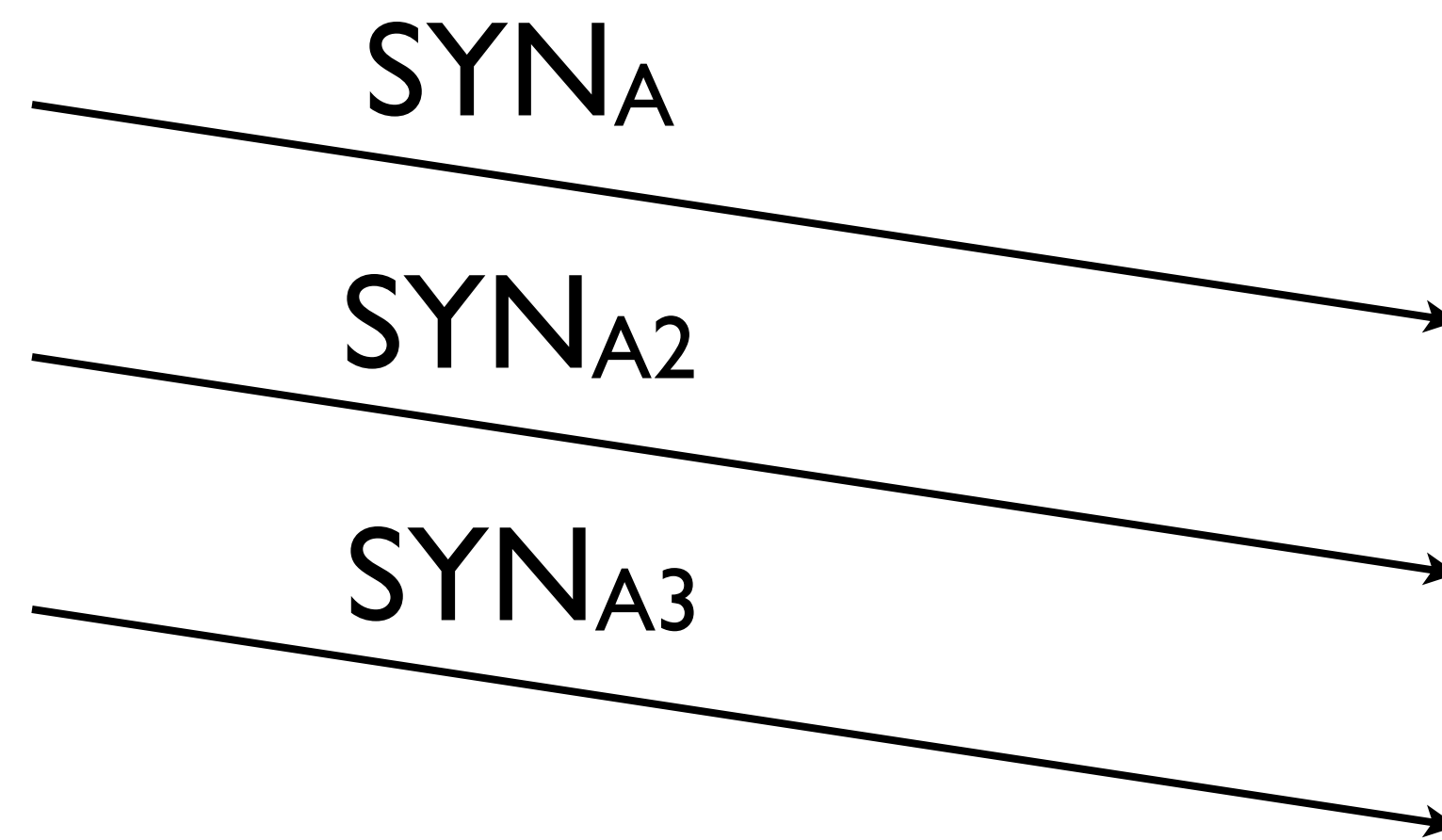
How a TCP flood begins



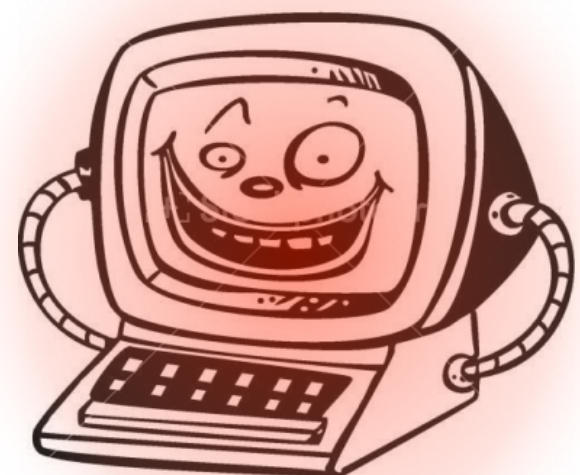
victim stores
each of these
for timeout
(1-2 min)

soon, entire
memory is
consumed

Amplification



victim stores
each of these
for timeout
(1-2 min)



1 32b packet causes **1024b** alloc.



Ping of DEATH

Normal PING requests require 32 bytes.

Attack: send a 65k PING request.

DNS traffic amplification

```
dig yahoo.com any
```

```
:: Query time: 6 msec
```

```
:: SERVER: 128.143.2.7#53(128.143.2.7)
```

```
:: WHEN: Thu Sep 13 13:44:04 2012
```

```
:: MSG SIZE rcvd: 506
```

~50byte UDP packet leads to a 506b response

10x

d-172-27-45-104: abhi\$ dig +bufsize=4096 +dnssec any se @a.ns.se

```
; <<>> DiG 9.8.1-P1 <<>> +bufsize=4096 +dnssec any se @a.ns.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29242
;; flags: qr aa rd; QUERY: 1, ANSWER: 20, AUTHORITY: 0, ADDITIONAL: 26
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;se.                                IN          ANY

;; ANSWER SECTION:
se.                                172800     IN         SOA        catcher-in-the-rye.nic.se. registry-default.nic.se. 2012091304 1800 1800 864000 7200
se.                                172800     IN         RRSIG     SOA 5 1 172800 20120925190422 20120913081101 58656 se. DtVv7a9TE2PorcAHozltJ8x8lkrSJYbUf9zsAUzkZHmadMMcRvm1u1N snzCnURQHILqB7+v0mXySrpl4bW15wVZn6UjcpEEQjq7uqeahK8nOlXj
XqLvxdz5Ro7WR1+V3dAPm3RH5X7962mZrKdVXF/E01upt96+zxwimOTN lf4=
se.                                172800     IN         NS         e.ns.se.
se.                                172800     IN         NS         b.ns.se.
se.                                172800     IN         NS         c.ns.se.
se.                                172800     IN         NS         a.ns.se.
se.                                172800     IN         NS         i.ns.se.
se.                                172800     IN         NS         g.ns.se.
se.                                172800     IN         NS         d.ns.se.
se.                                172800     IN         NS         f.ns.se.
se.                                172800     IN         NS         j.ns.se.
se.                                172800     IN         RRSIG     NS 5 1 172800 20120924194433 20120911201101 58656 se. M3jZ0lhDkvBfizaxzFgsFWbAEJKN6aj4fn5ZPBIHlwgVTL7jhhsiTd2u HB9Kp0bDSwIBDxnwvGtr8g+Hem9RitYZXxHkbfP9SXhuKsZvtM7Y5WUB
CF7lwRywwnSikjb8su7Ewki7bO5aLTHCWu+1/jPDRNUofHflSqSIJxKm gvl=
se.                                172800     IN         TXT        "SE zone update: 2012-09-13 09:07:13 +0000 (EPOCH 1347527233) (auto)"
se.                                172800     IN         RRSIG     TXT 5 1 172800 20120927095501 20120913081101 58656 se. CKXLjyfqXBYQqYdkUTKPbAwhzQi24DebVrDqrhOo0vMLqCum4AwjrzaV snDHgv1KSMM9ifPYEz5jSrVUsOOyxNgmRKjmIXgjRiaylurvZjlpu2kE
Nd3ppJ5LkP7LuZnbrtVWYmFIYNzIkJDj62TZFdYrFrkGXf6JedU8ldlr zpg=
se.                                7200      IN         NSEC      0-0.se. NS SOA TXT RRSIG NSEC DNSKEY
se.                                7200      IN         RRSIG     NSEC 5 1 7200 20120924215357 20120910221101 58656 se. ZwvY5T0fW84iqsdrQkglfFhJ6aXYWmLkm+HCiv9/wisTmTj8UJC1dShm ysZnr0zZ1PS/D+ymVGc/cMiKb3d8Nq2w+/piAHpEqiOtkh38e1ngGX+C
McIBkYV5FiuEC1QSiM+D7H7GSSPrqUBx2M3heWz8MucQvO3MCL81ESsJ WaE=
se.                                3600     IN         DNSKEY    257 3 5 AwEAAZYyG1hpk8XKHNHpdO/EEg+r4YmIEC4Fn3x2DEsygxDuoT9d/QCi X1pz0omFGCaVfCWHvaScVvWd4xP4kNDnSDQxBzPwLEXE3l0cLseMJ2YM QeBPf3hGhLs6VSDnGFKAzNG4fhri9EBTLv9ubL8Kx8cWQKuu3A5HRVD3
li7IZB+0kmUKqGilQdERKt/Ec36BkK93lyGags5RrR2VDdrXCj9Yay90 KCKITk52AbwVoMPm0OYIPbD4ViBPMk5nmh/dPeCoZoVJxgANZ/doVQxR 5vDkMBYxuhrXuQk3CvZBB011NsXxk9yHtHvp/5gjUVJjvhdRvjRB6/xY R03c9owi/aM=
se.                                3600     IN         DNSKEY    256 3 5 AwEAAbTmWA2HUXP60ITEiYuK2E08t4LEcz3acvQbzRWScFNI9FWqwcDY mWjZgXYmHWsAqM/Ni3xWR+eQ7/VglTXMbVlxWMLFIPLGHce1vl69kNNN N4V/iYt0bjWwvkhys5cYYRocjfYhusGumpqJ2G9OUkjJdk5m6EH/+Llp PjJmPlg
se.                                3600     IN         DNSKEY    256 3 5 AwEAAe7gh8/AVUjbsQq9PKtoBHOfl/WHtopJCOsEoB7tOaCBov6eN7yO VZT4TOI4idc0R1HGc9bFzQ0U+/4wWBPbVItV8bm1EQm+SNtlONtd6T2d 3wDXhouf1nHCdDKt1mYXuSCaQbfgf55xYaPNLEvu5VDtwOIL9C2Gu+XdH aONnbY
se.                                3600     IN         RRSIG     DNSKEY 5 1 3600 20120924020128 20120910101101 59747 se. GEHtQQL8VOc8FiVCB7SfQ6/WYrzWhA1ftT8v2JEIRXF0e6e1TurXepZW QZ1F1jky0IQ31Qt7pbsBA/sOvfWaB4GLMKkgYG2dZgQUwifMi515cXyF
EvZzH+jg63Hh1fsorCEcRLNlxRZ4sTkUx/cH7IGp1dpZYpGIRkbQI4Tp zALzkjBulHfMM05hrt6Bh5d/3AfUhlwtN8iu5JX3qPRY+5BVufvTKVpB Dw8zR38sHeqBDL3nPLLje6PhlyyMoM0NuzZh0WfwqFmbJCs+WZiyq1QZ Nm2K3uBMQx7NLalqFptHb3XB0lhXTWE3PLNij17qg+RHHBPgzwiJY+ja pbNHCg==
```

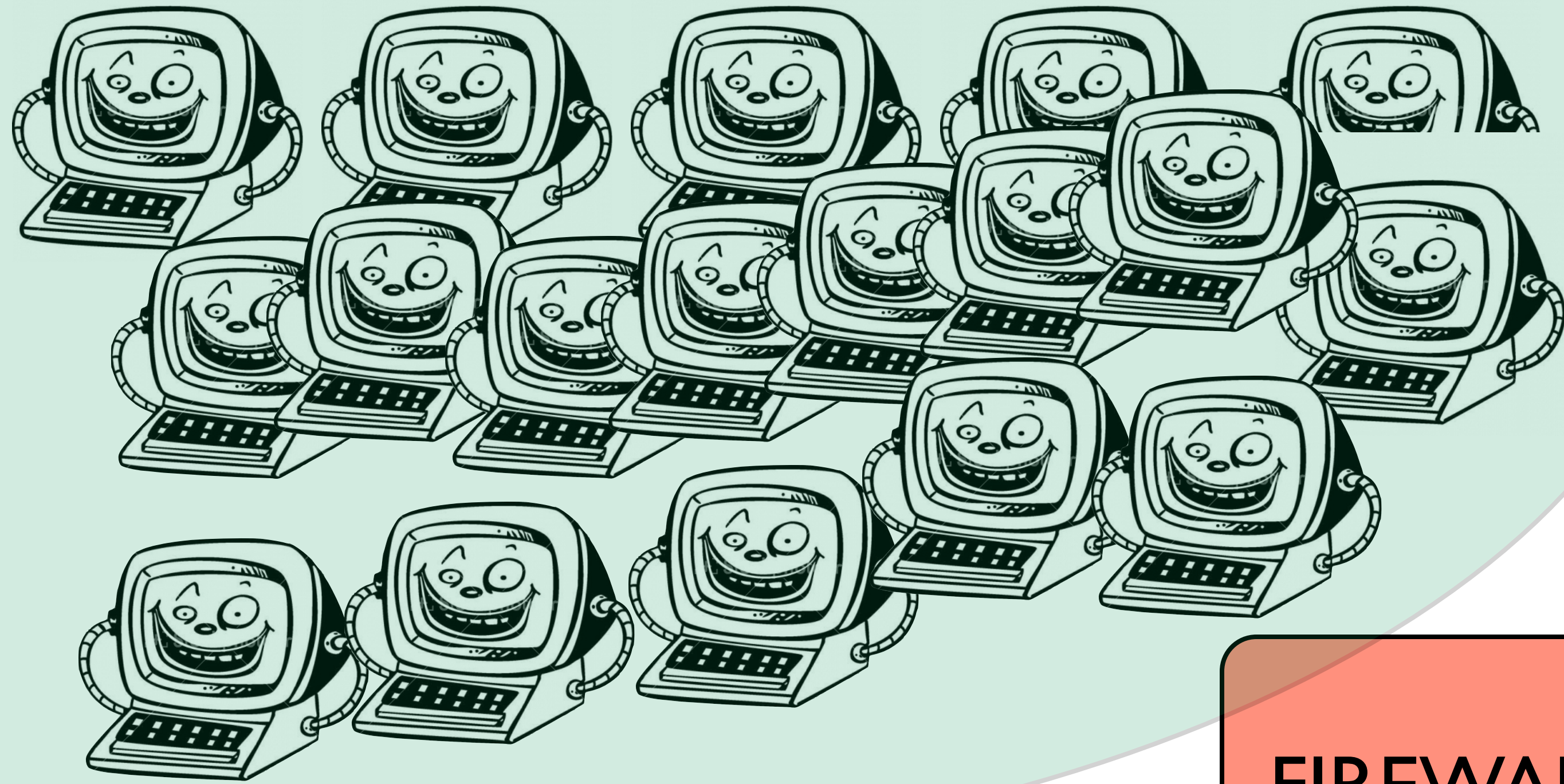
```
;; ADDITIONAL SECTION:
a.ns.se. 172800 IN A 192.36.144.107
a.ns.se. 172800 IN AAAA 2a01:3f0:0:301::53
b.ns.se. 172800 IN A 192.36.133.107
c.ns.se. 172800 IN A 192.36.135.107
d.ns.se. 172800 IN A 81.228.8.16
e.ns.se. 172800 IN A 81.228.10.57
f.ns.se. 172800 IN A 192.71.53.53
g.ns.se. 172800 IN A 130.239.5.114
g.ns.se. 172800 IN AAAA 2001:6b0:e:3::1
i.ns.se. 172800 IN A 194.146.106.22
i.ns.se. 172800 IN AAAA 2001:67c:1010:5::53
j.ns.se. 172800 IN A 199.254.63.1
j.ns.se. 172800 IN AAAA 2001:500:2c::1
```

j.ns.se. 172800 IN AAAA 2001:500:2c::1
a.ns.se. 172800 IN RRSIG A 5 3 172800 20120926094152 20120912121101 58656 se. cB0VnZRRRe7GmP+lId4rNmQJefMQKx+HOq26gCs+k3q7ZttetdFtqZQa7 hGEkWnALljwqIFgxQucnMRrSVso0uZl21zCe7katSYyK9wJSG1dpsk/G QYcMJc/
EA0deKIVkmA77TWeAi9Atl3cfgDUisibmmCJ08qp34zdoe8wBM fG0=
a.ns.se. 172800 IN RRSIG AAAA 5 3 172800 20120926005130 20120913041101 58656 se. pat/9jqrPpm/AP2czFcNct477zy9wGgnngeuul+mJsN5l46py+4x0dVS 1dp25ul7BS4nwl/I1yBcvxhPf2bavfLKOqV16p+/yfcBE9Inw8p0O13B
J9Ad87Lb+4rD2NeiFxAoj210pyR4OzsbLwjs1vclqEAzPHh+r66IFuV0 Udg=
b.ns.se. 172800 IN RRSIG A 5 3 172800 20120927063649 20120913021101 58656 se. U8gZpgfj2wCWMrSgnKLyR9VPRyiojP4IGHWISpeyvu3KTZBSzU7Xw/tu QWORTwixBkdgTSXNcKJdKQPe8PkMKzPjj/aB6w5dU/QXx7fdyGBYHqIC 2nbc5IliG6+/
aV2Eg5T5LiRj2+RWJnQWxyh6TtxtccKa5SdZ8aVz+bMGw IIE=
c.ns.se. 172800 IN RRSIG A 5 3 172800 20120925203628 20120913081101 58656 se. oqrUBu72ccG3moTYF8mENrp0d3D/n0Z9GX3tHLpu3+kckgAZEMahYeB3 VhESvysenqXHy9K++STBH/c/BpZJnOnV109mctZX691/NC7A0cUWk8cE
v2PYkSkRATryT2V4soJWbX1kGrc40UMLatqh6gY7tJPLvnkgeXOu1Fy8 Rjo=
d.ns.se. 172800 IN RRSIG A 5 3 172800 20120925050254 20120912181102 58656 se. CqEp4MhqEMzW+Tvg5wTSly/zqMoFBKNvlwr1590yShYfhtLQpXxKquLe IIHtXbY+kSaA8nKw7rhPGI06QRbW8FYYIWYP/3KSoBsVTr+ZZ19A+1wd
dK20GMC6SjAKRU4HE4vVFSZJm5lvtm5RPSzQxlT19tCwNc1Ggj5ZYaAV uj4=
e.ns.se. 172800 IN RRSIG A 5 3 172800 20120926152155 20120913021101 58656 se. qoZASSLoC2MN0bxYc8eTNWjNAlbhSzTyKgBbj4akMDyRQxTeA+YtdURZ If/5gvDjOOE7yNojuuAzHD8g+dyn5Z7cgmjLlyilo59huDUkSO0bQZsz
PBLouj9+7NmT2Q5tILJG2a9+BRFpsIE+nAxXMQRpldqJ2I+Zde+DNLU/ XTl=
f.ns.se. 172800 IN RRSIG A 5 3 172800 20120926062907 20120913041101 58656 se. kzQMEZB1F5KX06l0TrKgcqKC8Nip3J5/FyTR0O86TdfnIKjQ4Eg83/u yP1kr1LNxCKp8BFHbQKwb50WbxCW0V/BBfWU6L2jeJxz5N1r+zvCzC0v
4AnfNQhJtE3jR6d6RG4DCurkAheFcaPZtmEbYu+jaZi3xLTcw+jEQIE+ d+A=
g.ns.se. 172800 IN RRSIG A 5 3 172800 20120923205729 20120910221101 58656 se. h/pT8oAz0YJI7kN7u1Ez6EGFyco56yFNEOJn0IUuJlAIXoiCWxpa4GoV sWMUQOkffPpfZbOqZf8srgQjKmjhkJwGCn+detbGu9znmKVD1oaYbwG XT3Dn27XEBPVr0dwS5seddbKWCZm1O2v
MTI4cGp1wfuQrkmU9NfJs h0k=
g.ns.se. 172800 IN RRSIG AAAA 5 3 172800 20120924031728 20120910161101 58656 se. EIU7iR+eAlmNWeCGpLxE3998OWAyKOGsDnEgcGF9fyhcxFgw3sDB5kGR /iMGM12RhuK33S3u8te/KQ5DIByeR7Mfj+L7TJR4q1p4rwrxyI6WC45O 9wZRUtBZu/
Zv7UlvVOJDKzGdCaphqj5ey1Ll14pyg8QsBPqH2KzbJ8WE VYU=
i.ns.se. 172800 IN RRSIG A 5 3 172800 20120926182411 20120912221101 58656 se. YrdQpeZ1iZKYAos1jw6tRrE6uO/jH/EqkgdW8k8BVJPITQq66bweIEdn LDYTn7i8QoOJPPINbiNjAJxXa15pLqIE2PLZdwq9Qzf3ytg04Tctn6FV 3P+fX7aI6aZuzAjZnm6/
cBigP2s+Pq96xQbAaqTEqXid5MuKdk2k6NMd QCg=
i.ns.se. 172800 IN RRSIG AAAA 5 3 172800 20120924081359 20120911001101 58656 se. OBy/eN25dUM/kZMsY2oJb6R/VYrQmhPXt3Px401lr1HBv4YJ3HddW5tX ZHgO95CLHDMQX3VQf0zTvHeyKb5rqk/EtZwF6hk/1h6HL7FGytXlzGEB ABr/rU74yk6LU2aDJ5The0793dz8ijfj2F/
gu+WDpWP7zp3s+l9naiTM vE0=
j.ns.se. 172800 IN RRSIG A 5 3 172800 20120923152202 20120910141102 58656 se. hFM3pC0tgLGzik7ppcGQrtMDFXTxSKUGqTtbpRtTmEnRHzm3btptdOg1 IG2YHyFaD/dIKA0wa9qQqjGaifQCc8xY+MkvqFU2MEO83F/tlgmSC+un bWrbytxCXhaKjaU2ZI5/Mk5GsfvB/
fNIBBPIZ5RbrohAbXUQIK6Uz44v yQA=

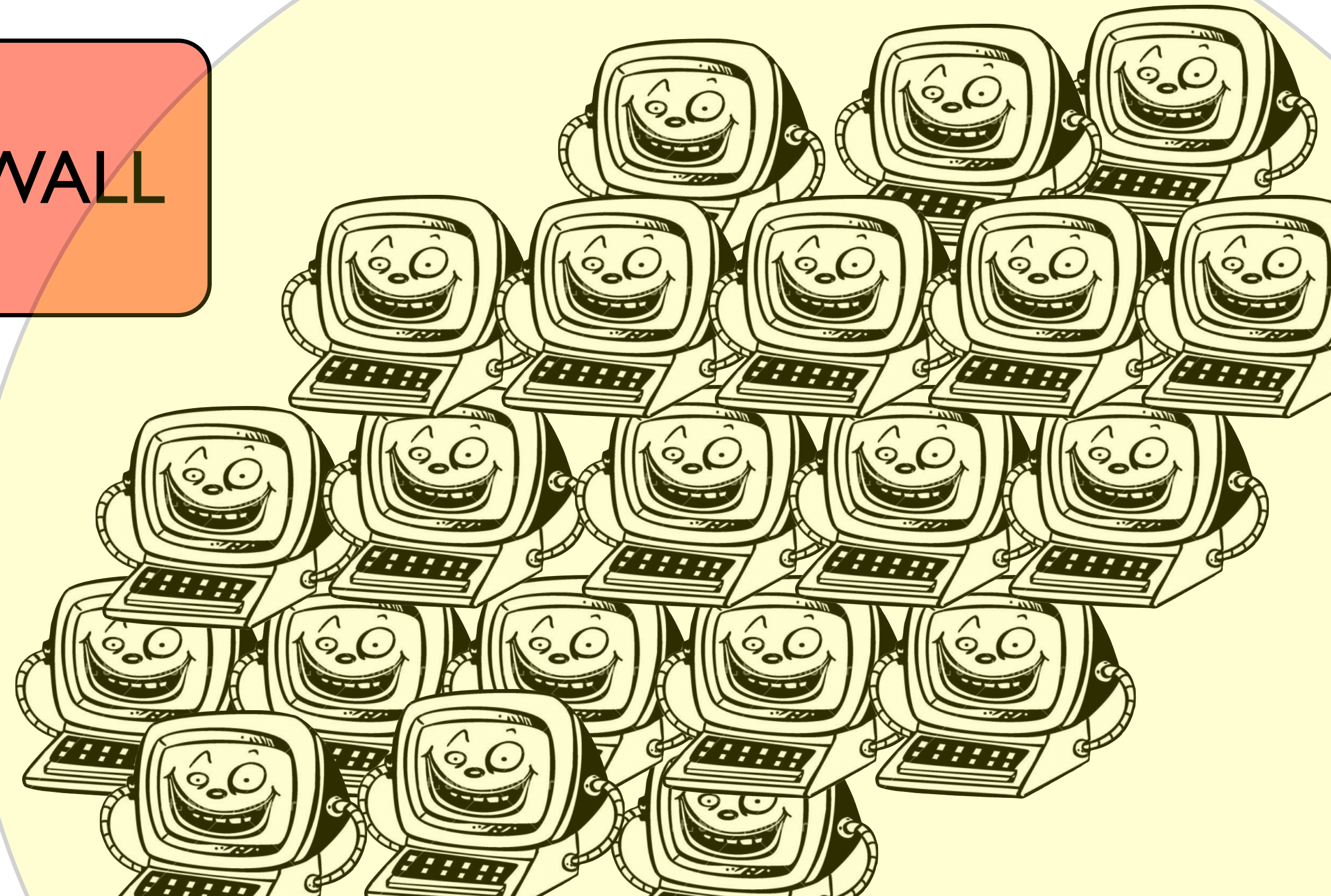
:: Query time: 126 msec
:: SERVER: 192.36.144.107#53(192.36.144.107)
:: WHEN: Thu Sep 13 06:20:08 2012

:: MSG SIZE rcvd: 4073

How to mitigate network attacks?



FIREWALL



Firewalls

Stateless Packet Filter

Rules based on addr/port + header info

Statefull Packet Filter

above + state between each packet

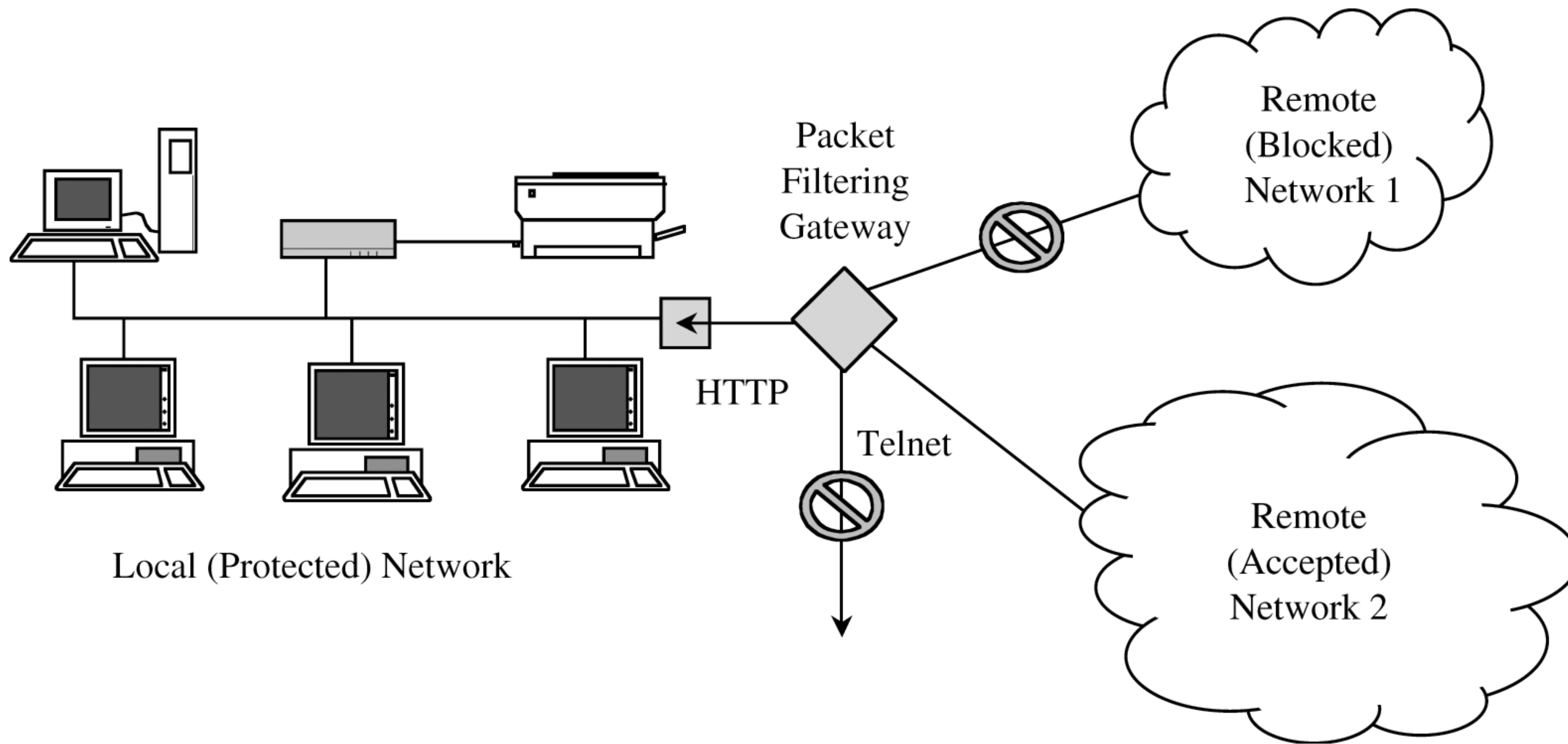
Statefull Packet Inspection

above + can inspect the data of the package

StateLESS Packet Filter

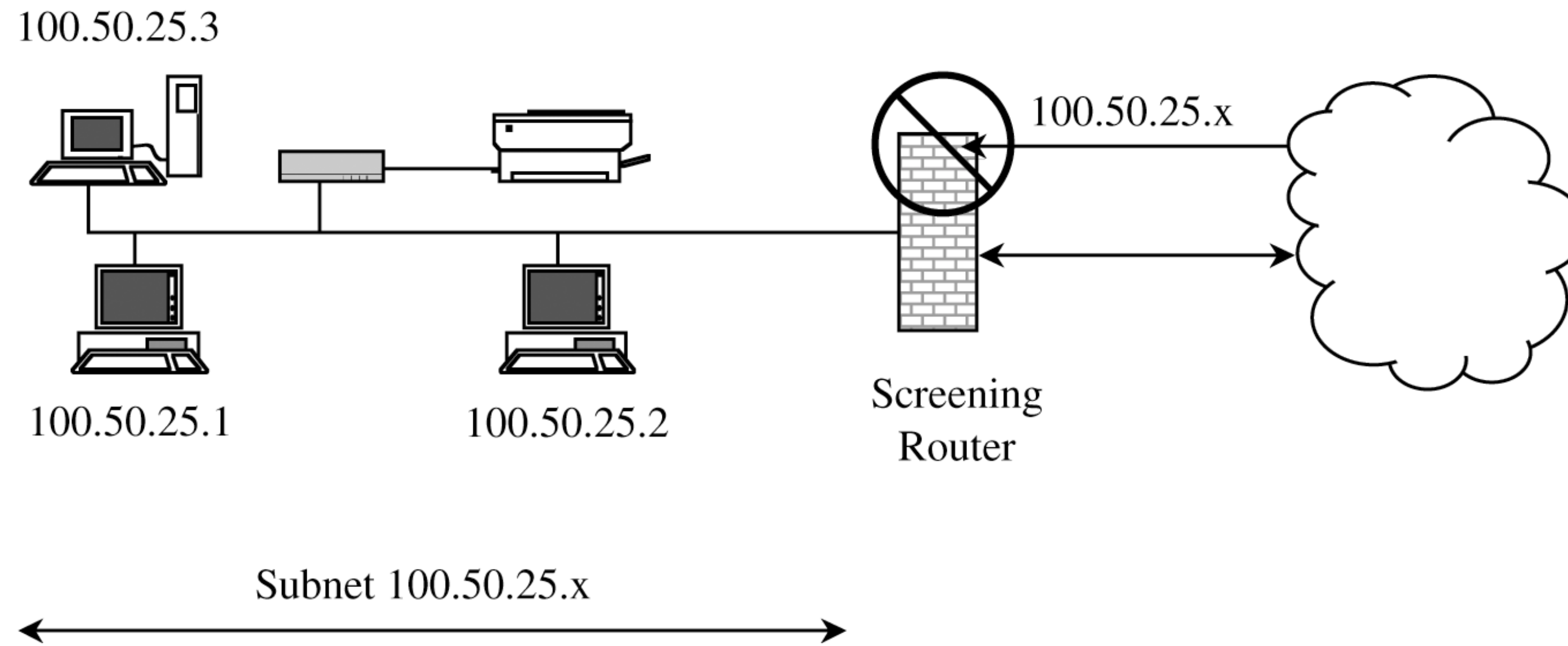
Rules based on addr/port + header info

Look at the packet and decide immediately whether to drop or forward.



- Local subnet has all traffic from remote network 1 blocks (say, network with IP address 253.128.x.x)

- Allow some traffic from Remote Network 2 (say, 253.127.x.x), but only if it is destined for port 80 (web-traffic), Drop all other ports



prevent external traffic from “spoofing” internal addresses.

StateFULL Packet Filter

Rules based on addr/port + header info

networks scans can be detected and stopped

detect invalid tcp packets

Statefull Packet Inspection

can filter for known attacks/shellcode

Review

Our main topics

Cryptography

Authentication, passwords

Authorization

Ethics and cyberlaw

Social engineering

Systems security

Exploits: System, Web, Network

Cryptography

Privacy:

Authenticity:

Hashing:

Passwords and Authentication

What is authentication?

Classes of secrets?

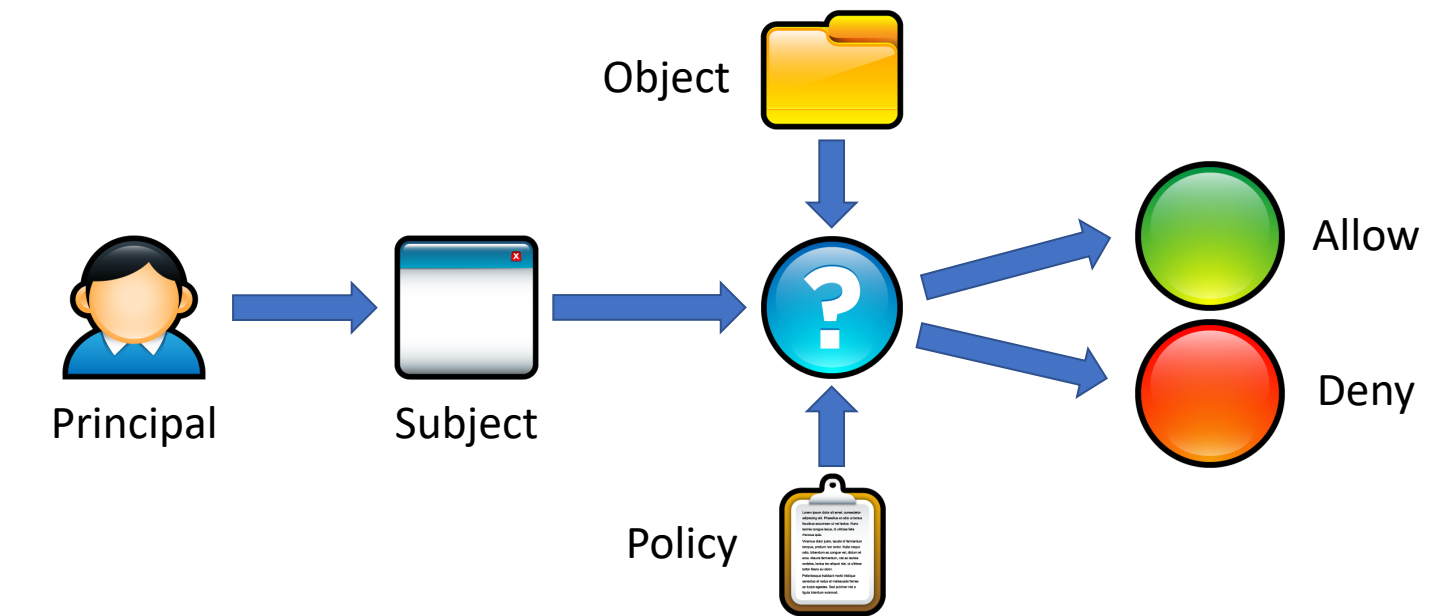
Methods and attacks against passwords?

Authorization

Basics of an access control check

Access Control Check

- Given an access request from a **subject**, on behalf of a **principal**, for an **object**, return an access control decision based on the **policy**

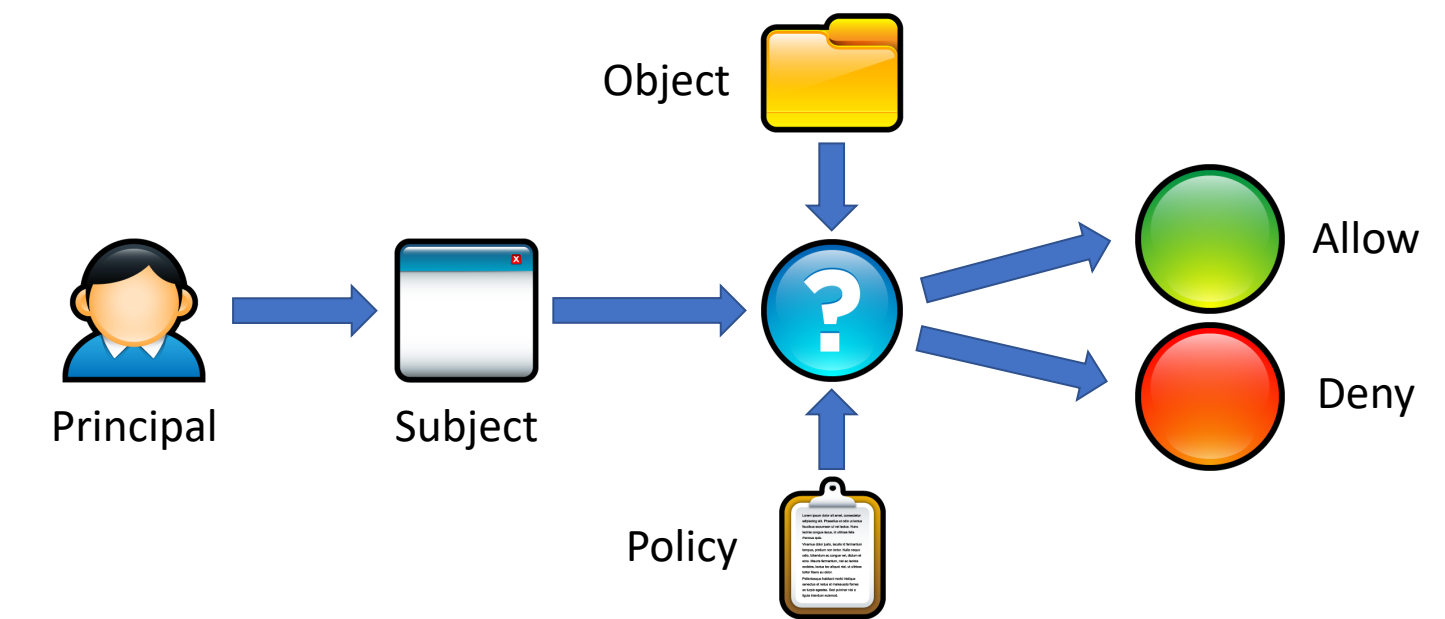


Authorization

Basics of an access control check

Access Control Check

- Given an access request from a **subject**, on behalf of a **principal**, for an **object**, return an access control decision based on the **policy**



Two types

Access Control Models

- Discretionary Access Control (DAC)**
 - The kind of access control you are familiar with
 - Access rights propagate and may be changed at subject's discretion
 - Implemented in Windows and Linux
 - Main issues:
 - Ambient authority (subjects inherit all permissions of principals)
 - Confused deputies (subject doesn't know which principal it serves); setuid
- Mandatory Access Control (MAC)**
 - Access of subjects to objects is based on a system-wide policy managed by admin δ
 - Denies users full control over resources they create
 - Bell-LaPadula: MAC for confidentiality (uses Multi Level Security)
 - Biba: MAC for integrity
 - Main issues:
 - Inflexible and complicated to manage
 - Do not prevent side channel attacks

Cybersecurity and Ethics

- Many **laws** govern cybersecurity
 - Designed to help prosecute criminals
 - Discourage destructive or fraudulent activities
- However, these laws are broad and often vague
 - Easy to violate these laws accidentally
 - Security professionals must be cautious and protect themselves
- Cybersecurity raises complex **ethical** questions
 - When and how to disclose vulnerabilities
 - How to handle leaked data
 - Line between observing and enabling crime
 - Balancing security vs. autonomy
- Ethical norms must be respected
 - Rights and expectations of individuals and companies
 - Community best-practices

Social Engineering

1. Cognitive vulnerabilities

- Subconscious decisions may be made before you are consciously aware
- Behavioral, social, memory biases

2. Social engineering tactics

- Weaponizing cognitive vulnerabilities
- Pretexting and framing
- Elicitation and persuasion

3. Social engineering attacks

- Baiting, Tailgating
- Phishing, spear phishing
- CEO fraud
- Scareware

System Security: Attack Surfaces

- Steal the device and use it
- **Social Engineering**
 - Trick the user into installing malicious software
 - Spear phishing
- **OS-level attacks**
 - Backdoor the OS
 - Direct connection via USB
 - Exploit vulnerabilities in the OS or apps (e.g. email clients, web browsers)
- **Network-level attacks**
 - Passive eavesdropping on the network
 - Active network attacks (e.g. man-in-the-middle)

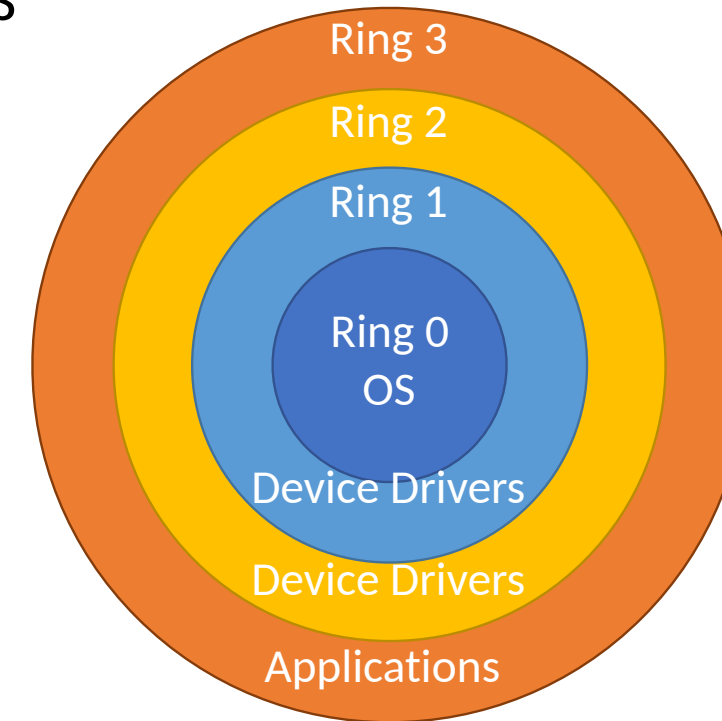
Modern defense: Isolation

Rings:

Most modern CPUs support [protected mode](#)

x86 CPUs support three rings with different privileges

- Ring 0: Operating System
 - Code in this ring may directly access any device
- Ring 1, 2: device drivers
 - Code in these rings may directly access some devices
 - May not change the protection level of the CPU
- Ring 3: userland
 - Code in this ring may not directly access devices
 - All device access must be via OS APIs
 - May not change the protection level of the CPU

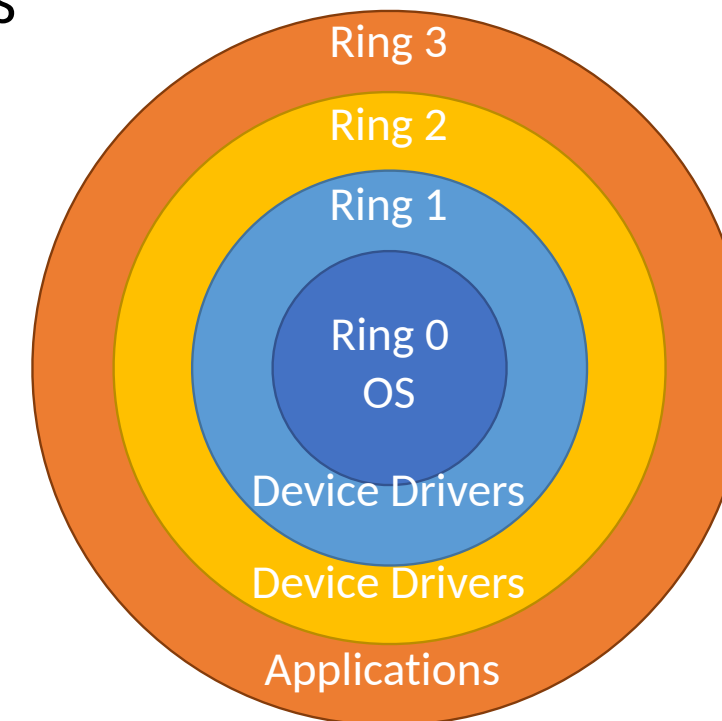


Modern defense: Isolation

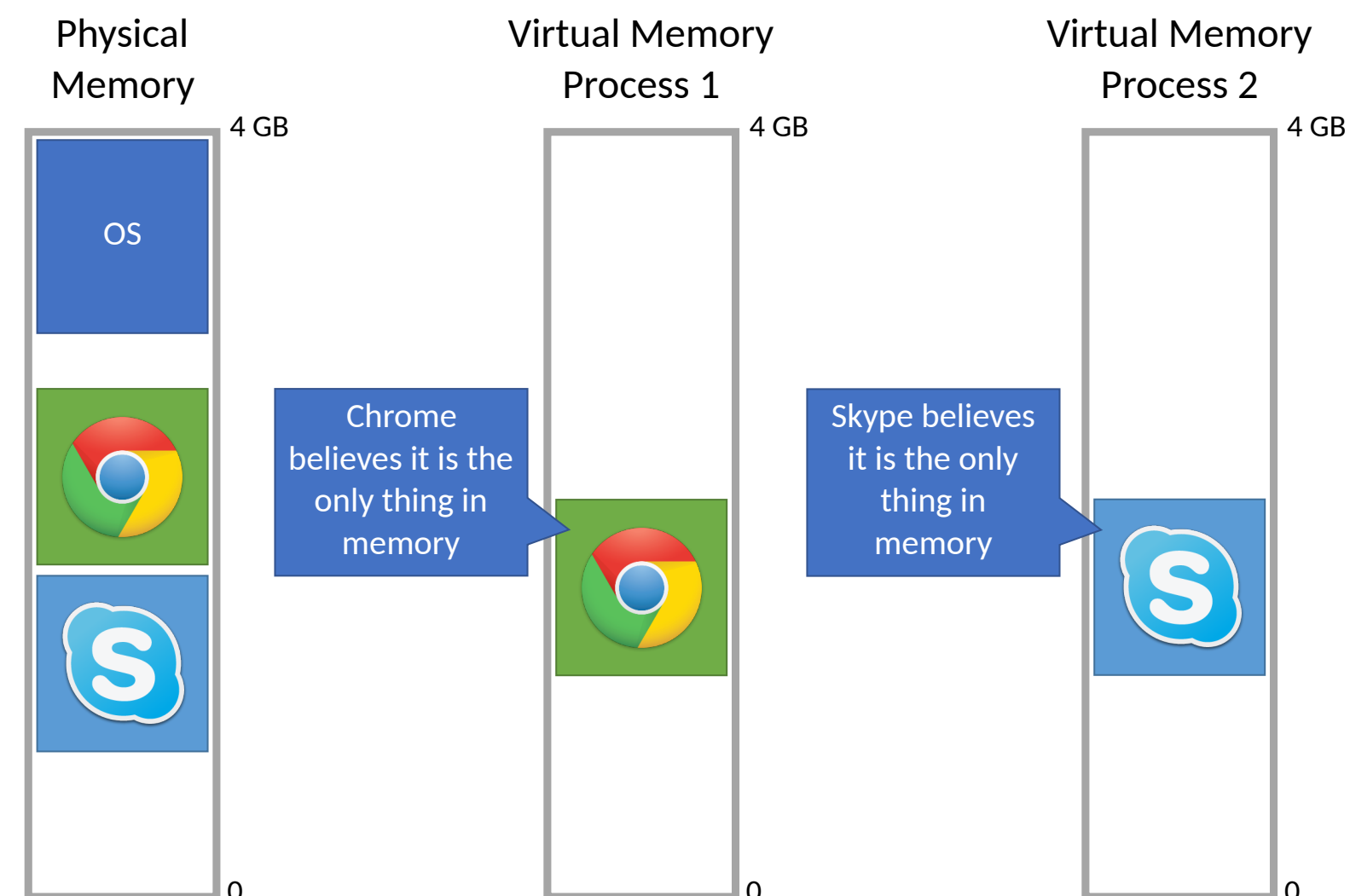
Rings:

Most modern CPUs support [protected mode](#)
x86 CPUs support three rings with different privileges

- Ring 0: Operating System
 - Code in this ring may directly access any device
- Ring 1, 2: device drivers
 - Code in these rings may directly access some devices
 - May not change the protection level of the CPU
- Ring 3: userland
 - Code in this ring may not directly access devices
 - All device access must be via OS APIs
 - May not change the protection level of the CPU



Virtual Memory:



Basis for tools

Security Technologies



Authentication

- Physical and remote access is restricted



Access control

- Processes cannot read/write any file
- Users may not read/write each other's files arbitrarily
- Modifying the OS and installing software requires elevated privileges



Firewall

- Unsolicited communications from the internet are blocked
- Only authorized processes may send/receive messages from the internet



Anti-virus

- All files are scanned to identify and quarantine known malicious code



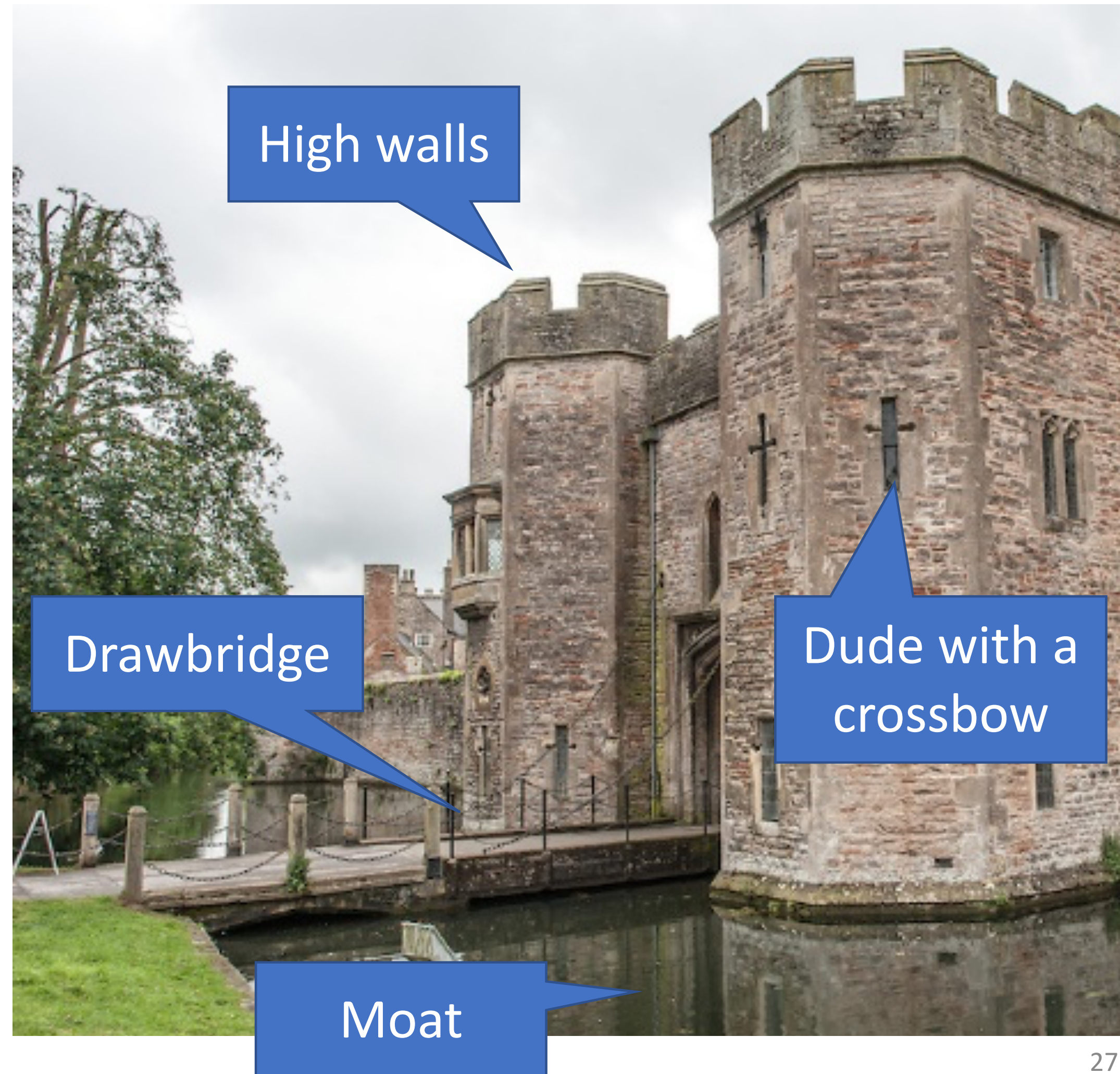
Logging

- All changes to the system are recorded
- Sensitive applications may also log their activity in the secure system log

Systems Security Principles

Defense in Depth

1. Fail-safe Defaults
2. Separation of Privilege
3. Least Privilege
4. Open Design
5. Economy of Mechanism
6. Complete Mediation
7. Compromise Recording
8. Work Factor

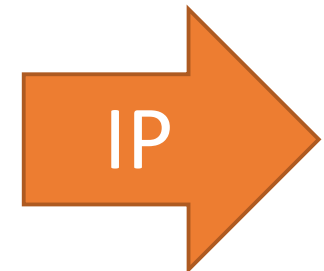


Exploits

Anatomy of an exploit

Program Crash

```
0: void func_print(char s[]) {  
    // only holds 32 characters, max  
    char buffer[32];  
1: strcpy(buffer, s);  
2: printf("%s\n",buffer);  
3: }  
4: void main(int argc, char **argv) {  
5:     for (int i=1; i < argc; i++) {  
6:         func_print(argv[i]);  
7:     }  
8: }
```

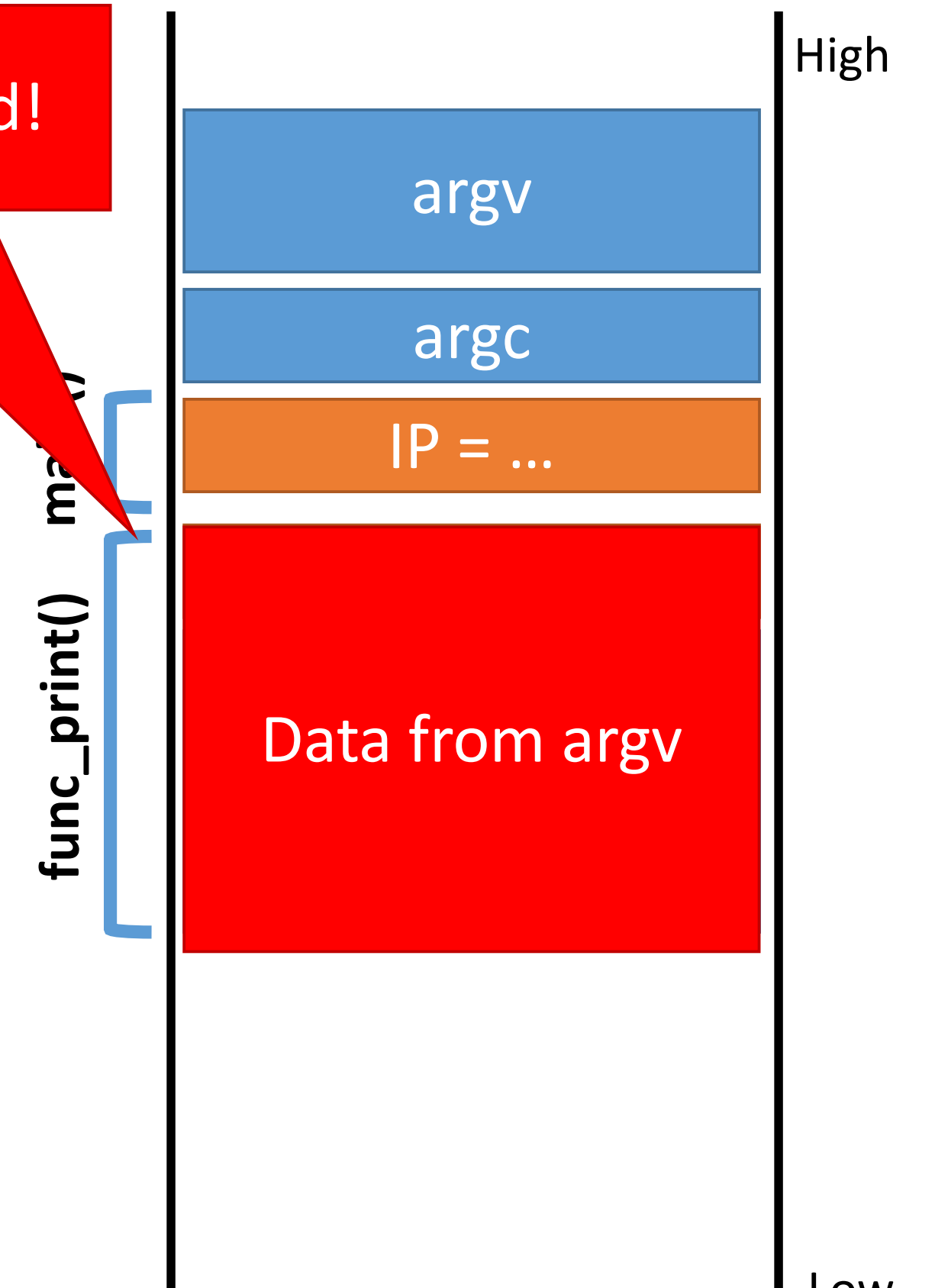


IP

Program crashes :(

Saved IP is destroyed!

Memory



Mitigations

- **Stack canaries**

- Compiler adds special sentinel values onto the stack before each saved IP
- Canary is set to a random value in each frame
- At function exit, canary is checked
- If expected number isn't found, program closes with an error

- **Non-executable stacks**

- Modern CPUs set stack memory as read/write, but no eXecute
- Prevents shellcode from being placed on the stack

- **Address space layout randomization**

- Operating system feature
- Randomizes the location of program and data memory each time a program executes

SQL Injection

```
'SELECT * FROM user_tbl WHERE user="%s" AND pw="%s";'
```

form['username']	form['password']	Resulting query
alice	123456	'... WHERE user="alice" AND pw="123456";'
bob	qwerty1#	'... WHERE user="bob" AND pw="qwerty1#";'
goofy	a"bc	'... WHERE user="goofy" AND pw="a"bc";'
weird	abc" or pw="123	'... WHERE user="weird" AND pw="abc" or pw="123";'
eve	" or 1=1; --	'... WHERE user="eve" AND pw="" or 1=1; --";'
mallory"; --		'... WHERE user="mallory"; --" AND pw="";'

5 Lessons

verify assumption about input, reject bad/unfamiliar inputs

Lesson 1:

Never trust input
from the user

Lesson 2:

^ x0r
Never mix code
and data
W^X - "write a page or execute a page"

X P44

Lesson 3:

Use the best tools
at your disposal

Lesson 4:

(get this in 2550)
Awareness and
Vigilance

Lesson 5:

Patch!

Topics we did not cover

- Crimeware Botnets
- Post-quantum cryptography
- Crypto currencies and smart contracts
- Protocol Security (TLS, wireless, SDN)
- Side channel attacks
- Secure Hardware Technologies (TPM, TXT)
- Distributed System Security and Resilience
- Privacy and regulations
- Fuzzing and software testing
- Formal verification
- Mobile and IoT security
- Machine Learning for Security
- Adversarial Machine Learning

Failures

TAs deserve thanks!

Carter, Jack, Nathan, Yash

Please submit a TRACE course review

