Network Security on OS X

Dan O’Donnell
RAND Corporation

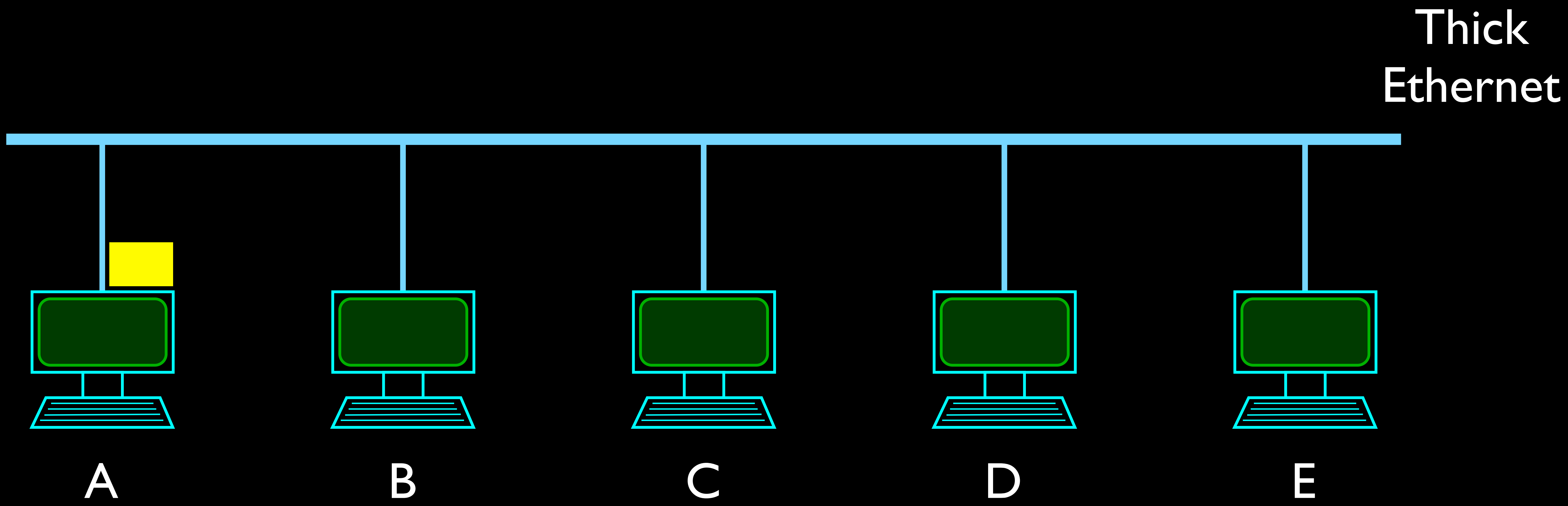
Todd Heberlein
Net Squared, Inc.

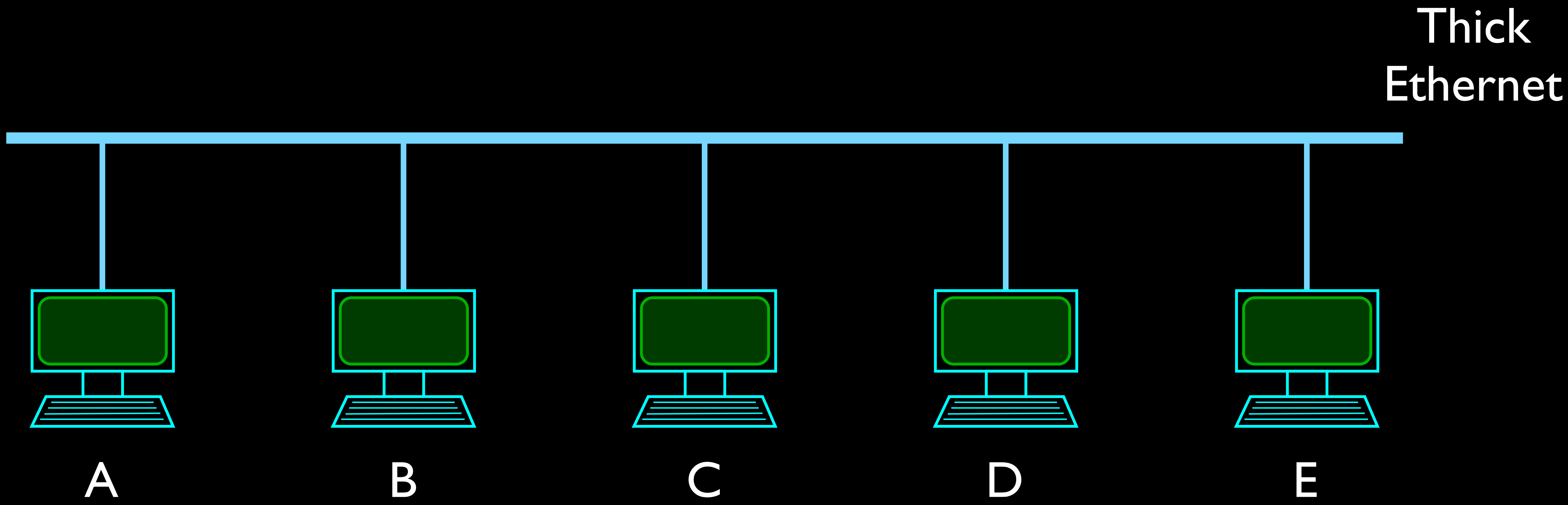
Act 1: History & Challenges of Network Analysis

Where we were

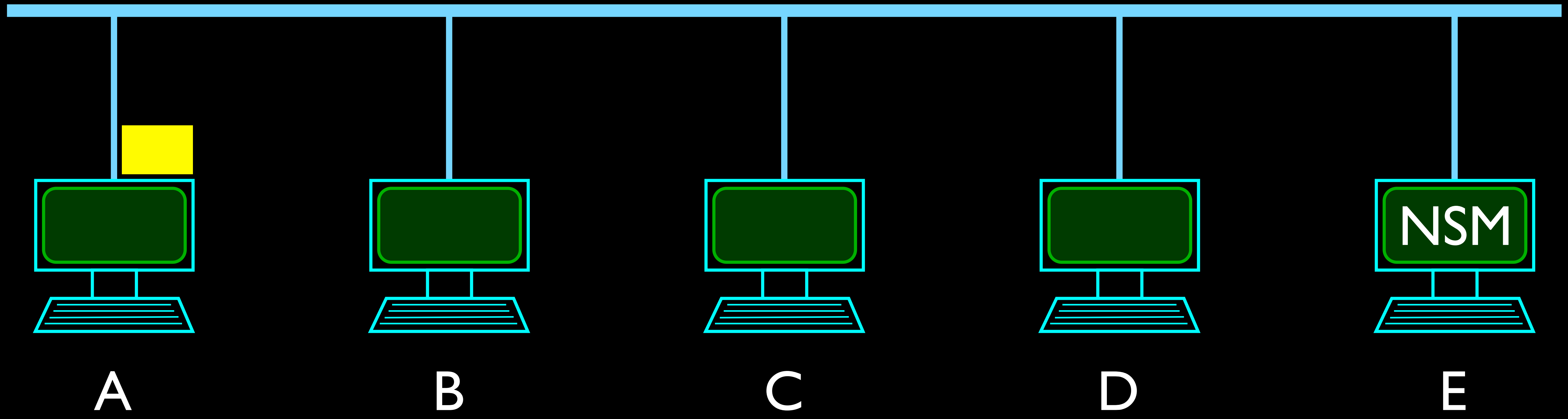
Where we are

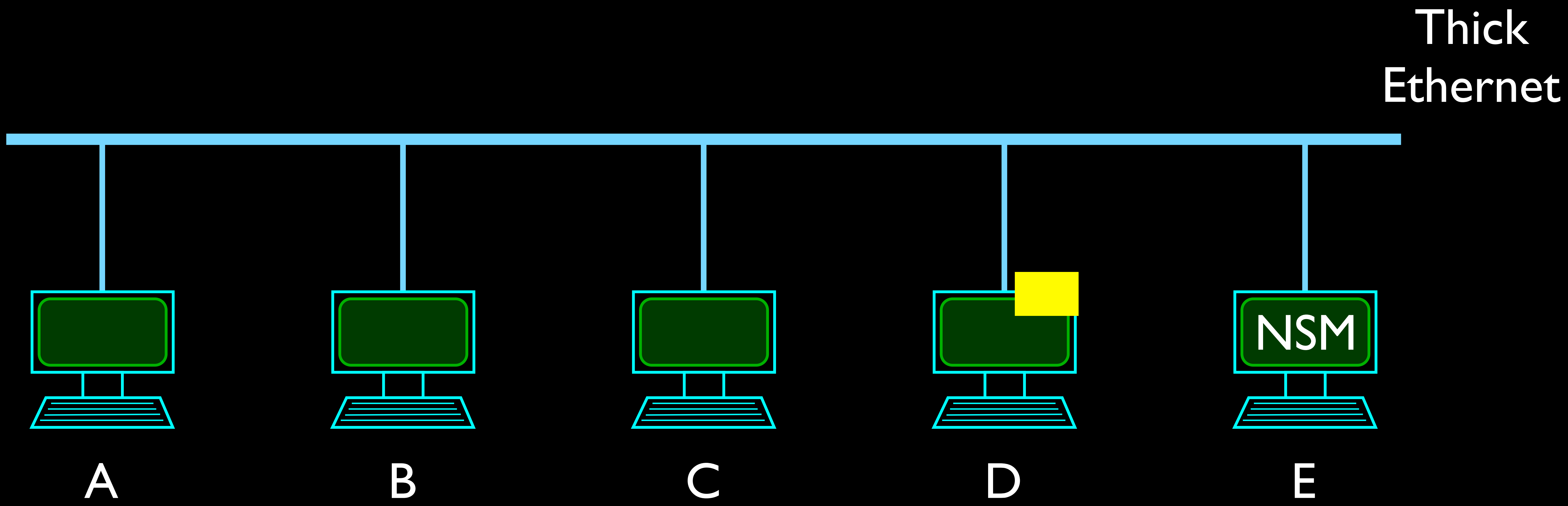
Where we are going

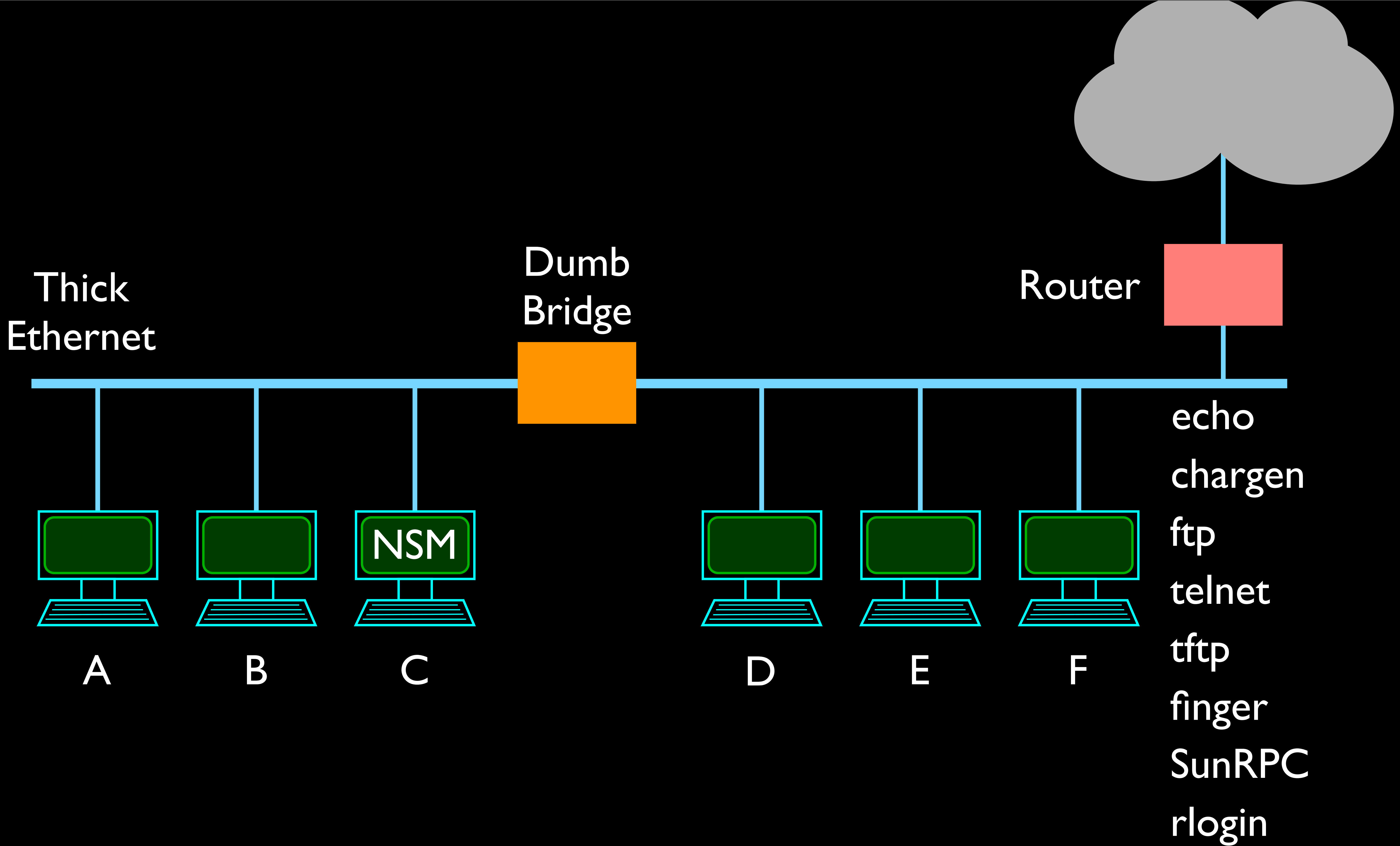

Thick Ethernet
A
B
C
D
E


Thick Ethernet
A
B
C
D
E

Thick Ethernet




Thick
Ethernet
NSM
A
B
C
D
E



Thick Ethernet

Dumb Bridge

Router

NSM

A

B

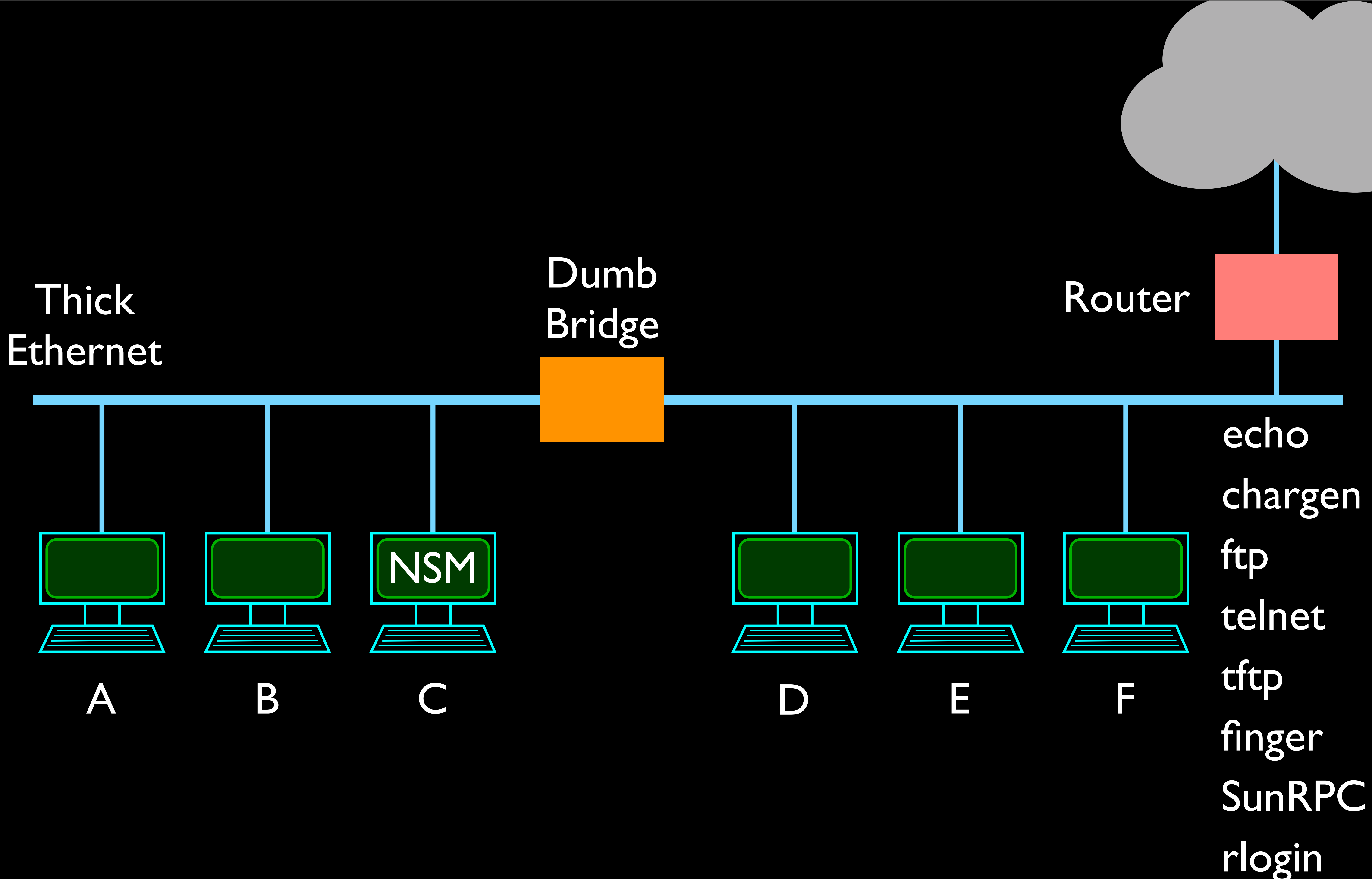
C

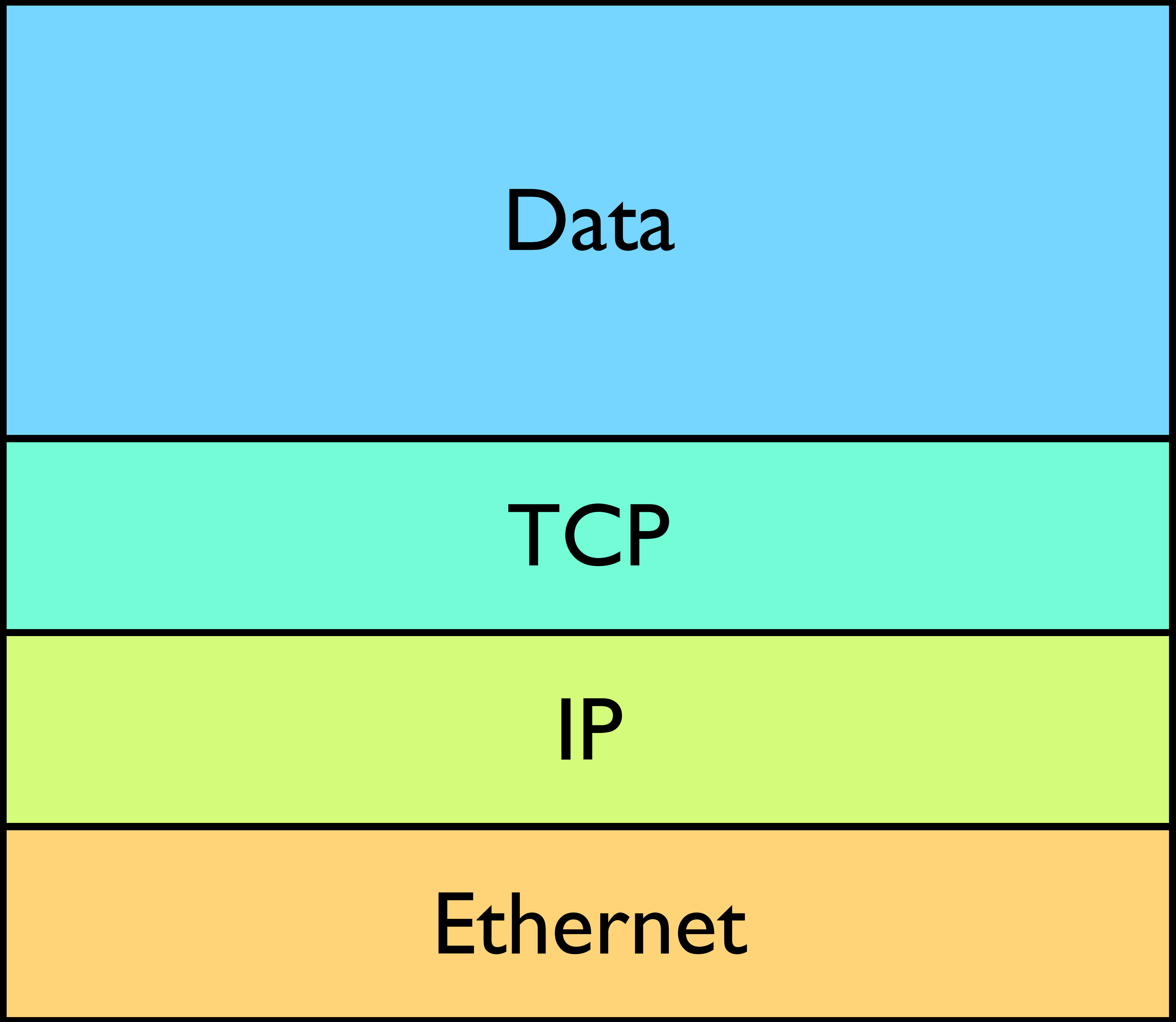
D

E

F

echo
chargen
ftp
telnet
tftp
finger
SunRPC
rlogin


Thick Ethernet
Dumb Bridge
Router
NSM
A
B
C
D
E
F
echo
chargen
ftp
telnet
tftp
finger
SunRPC
rlogin



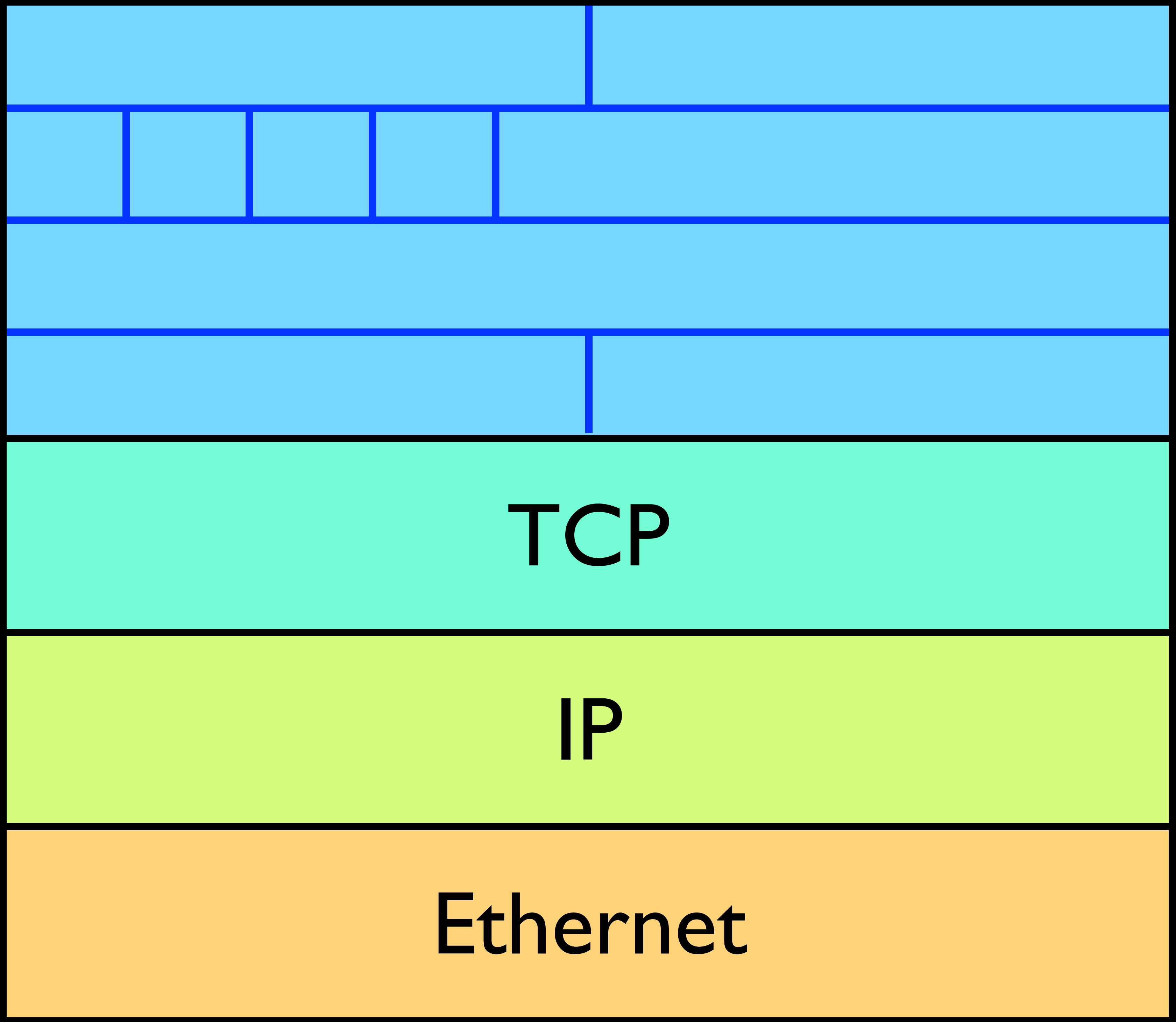
Data

TCP

IP

Ethernet

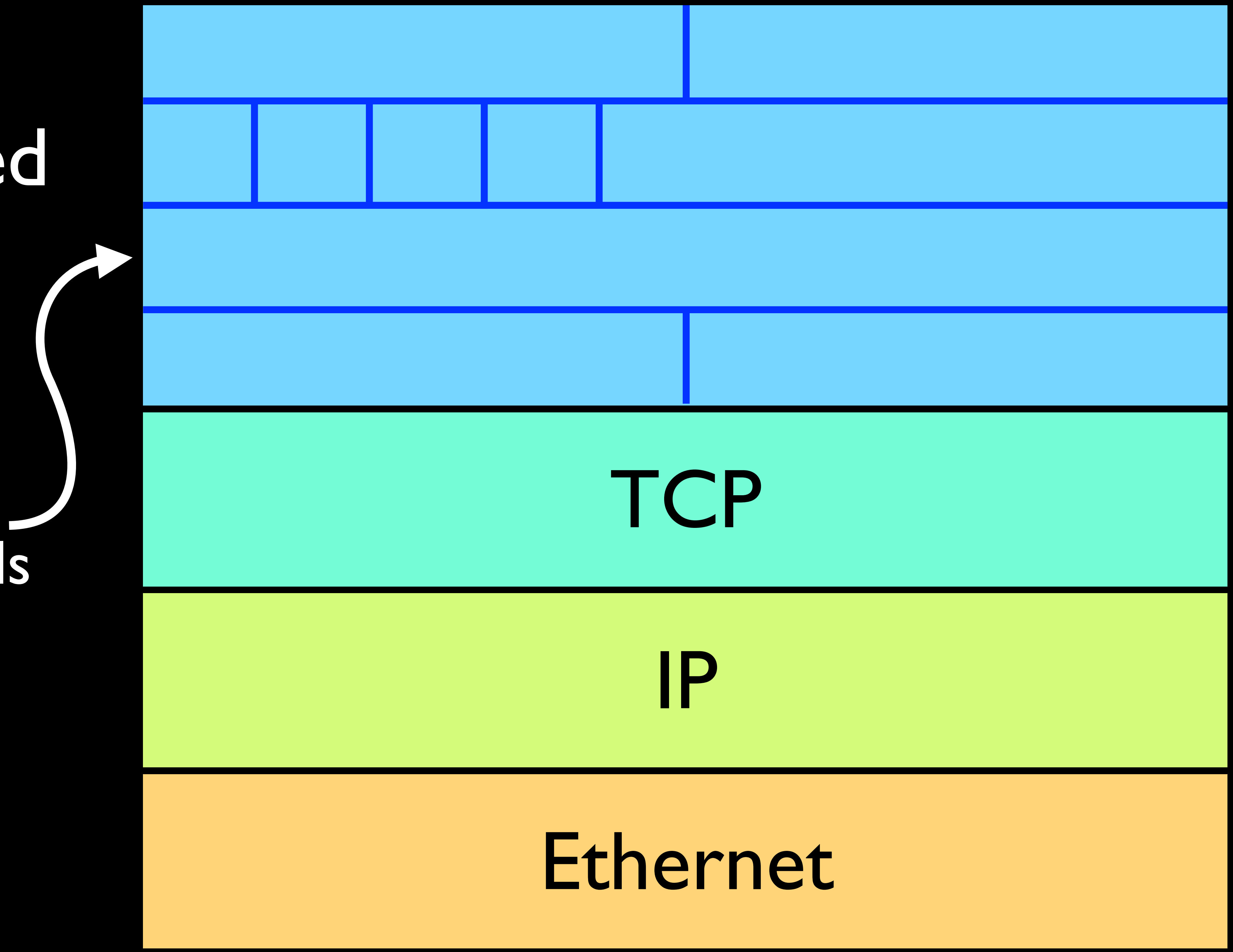
Structured
Data



Deep
Packet
Inspection

Structured Data

Many of Wireshark’s 1100+ protocols live here



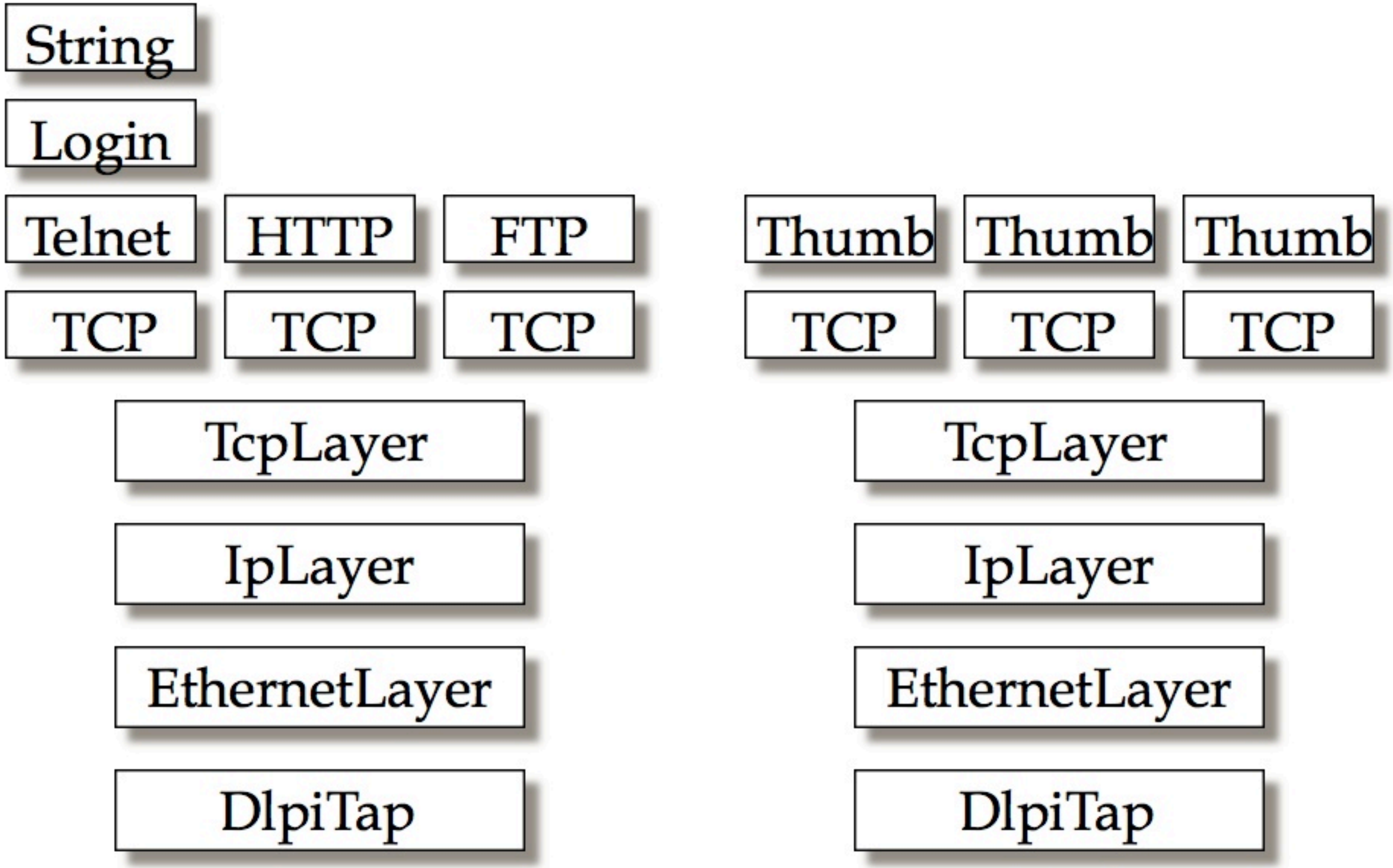
TCP

IP

Ethernet

Deep **P**acket **I**nspection

Example NMF Kernel



String

Login

Telnet HTTP FTP

TCP TCP TCP

TcpLayer

IpLayer

EthernetLayer

DlpiTap

Thumb Thumb Thumb

TCP TCP TCP

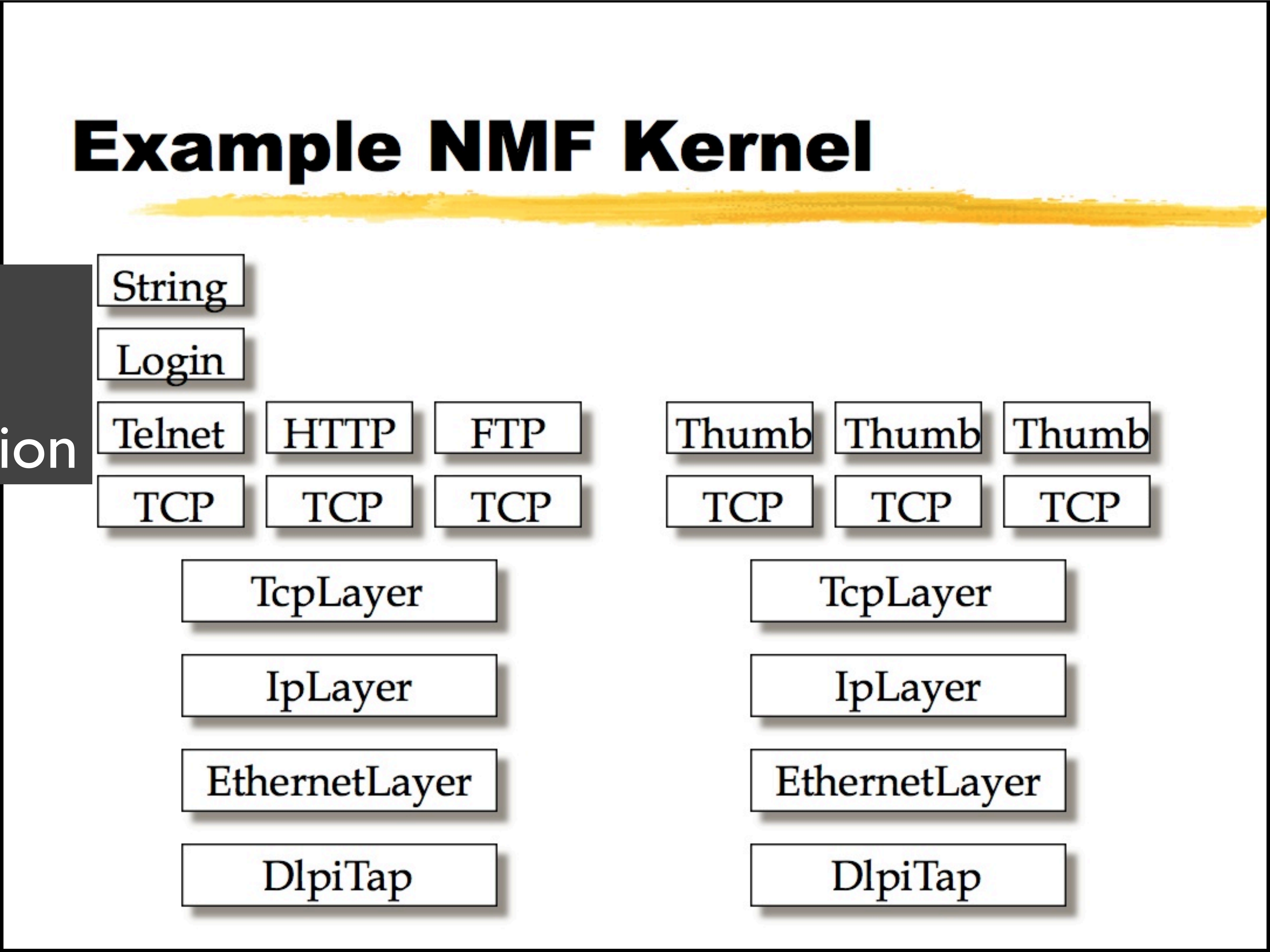
TcpLayer

IpLayer

EthernetLayer

DlpiTap

Deep
Packet
Inspection



Example NMF Kernel

String

Login

Telnet HTTP FTP

TCP TCP TCP

TcpLayer

IpLayer

EthernetLayer

DlpiTap

Thumb Thumb Thumb

TCP TCP TCP

TcpLayer

IpLayer

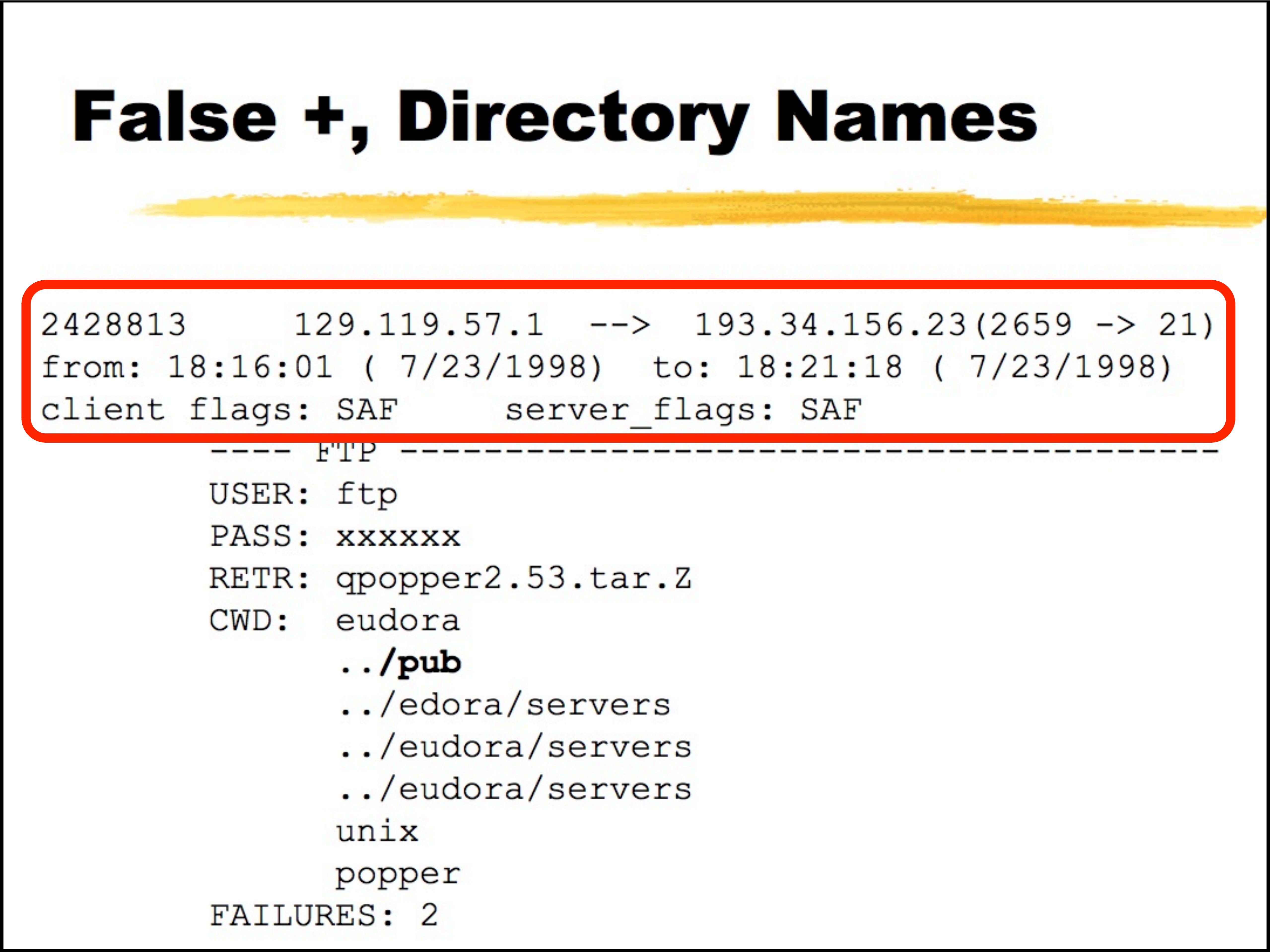
EthernetLayer

DlpiTap

False +, Directory Names

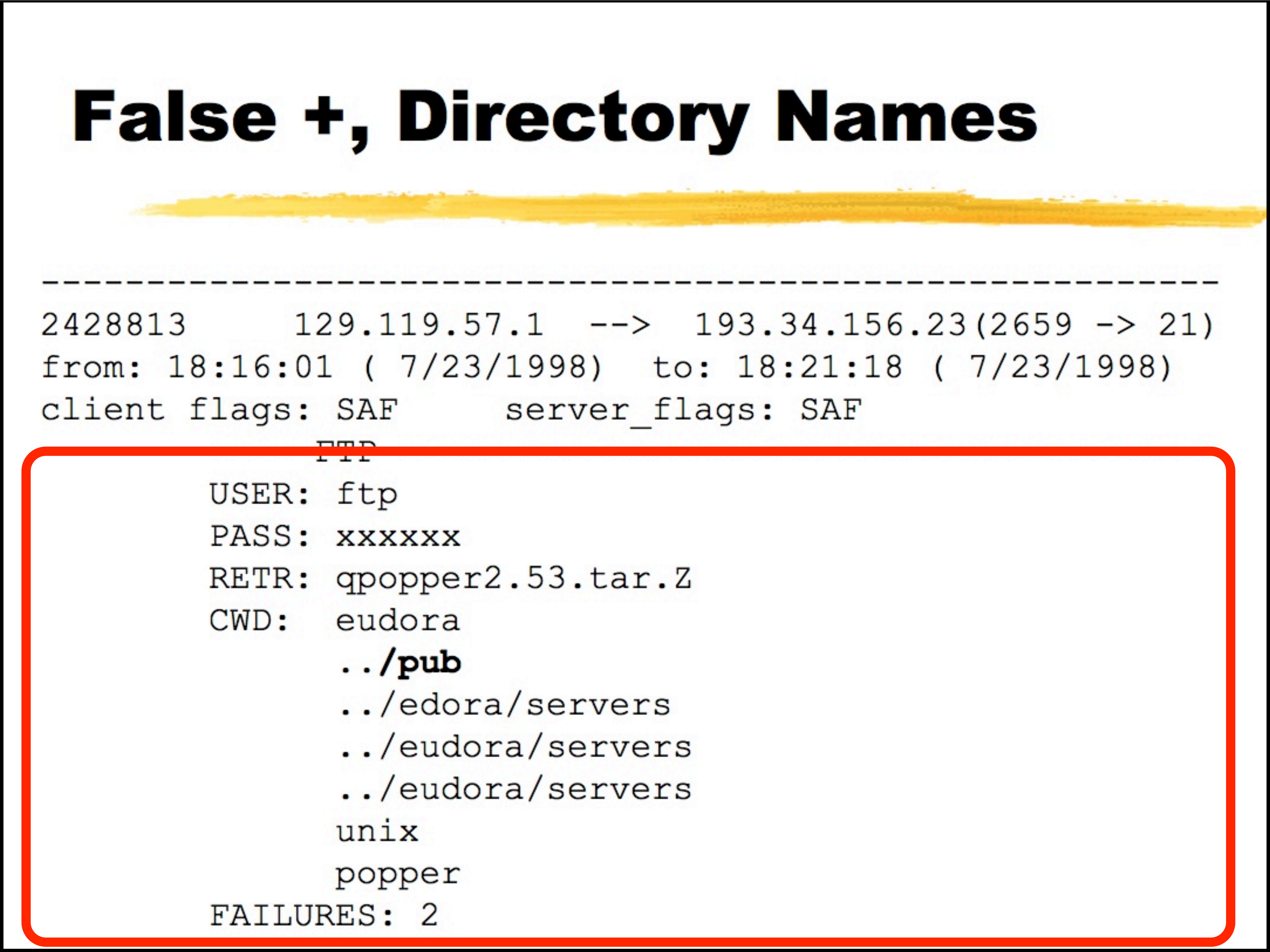
```
--------------------------------------------------------
2428813     129.119.57.1  -->  193.34.156.23(2659 -> 21)
from: 18:16:01 ( 7/23/1998)  to: 18:21:18 ( 7/23/1998)
client flags: SAF     server_flags: SAF
        ---- FTP ---------------------------------------
        USER: ftp
        PASS: xxxxxx
        RETR: qpopper2.53.tar.Z
        CWD:  eudora
              ../pub
              ../edora/servers
              ../eudora/servers
              ../eudora/servers
              unix
              popper
        FAILURES: 2
```

TCP/IP
Headers



False +, Directory Names

```
2428813     129.119.57.1   -->  193.34.156.23(2659 -> 21)
from: 18:16:01 ( 7/23/1998)  to: 18:21:18 ( 7/23/1998)
client flags: SAF      server_flags: SAF
        ---- FTP ---------------------------------------
        USER: ftp
        PASS: xxxxxx
        RETR: qpopper2.53.tar.Z
        CWD:  eudora
              ../pub
              ../edora/servers
              ../eudora/servers
              ../eudora/servers
              unix
              popper
        FAILURES: 2
```

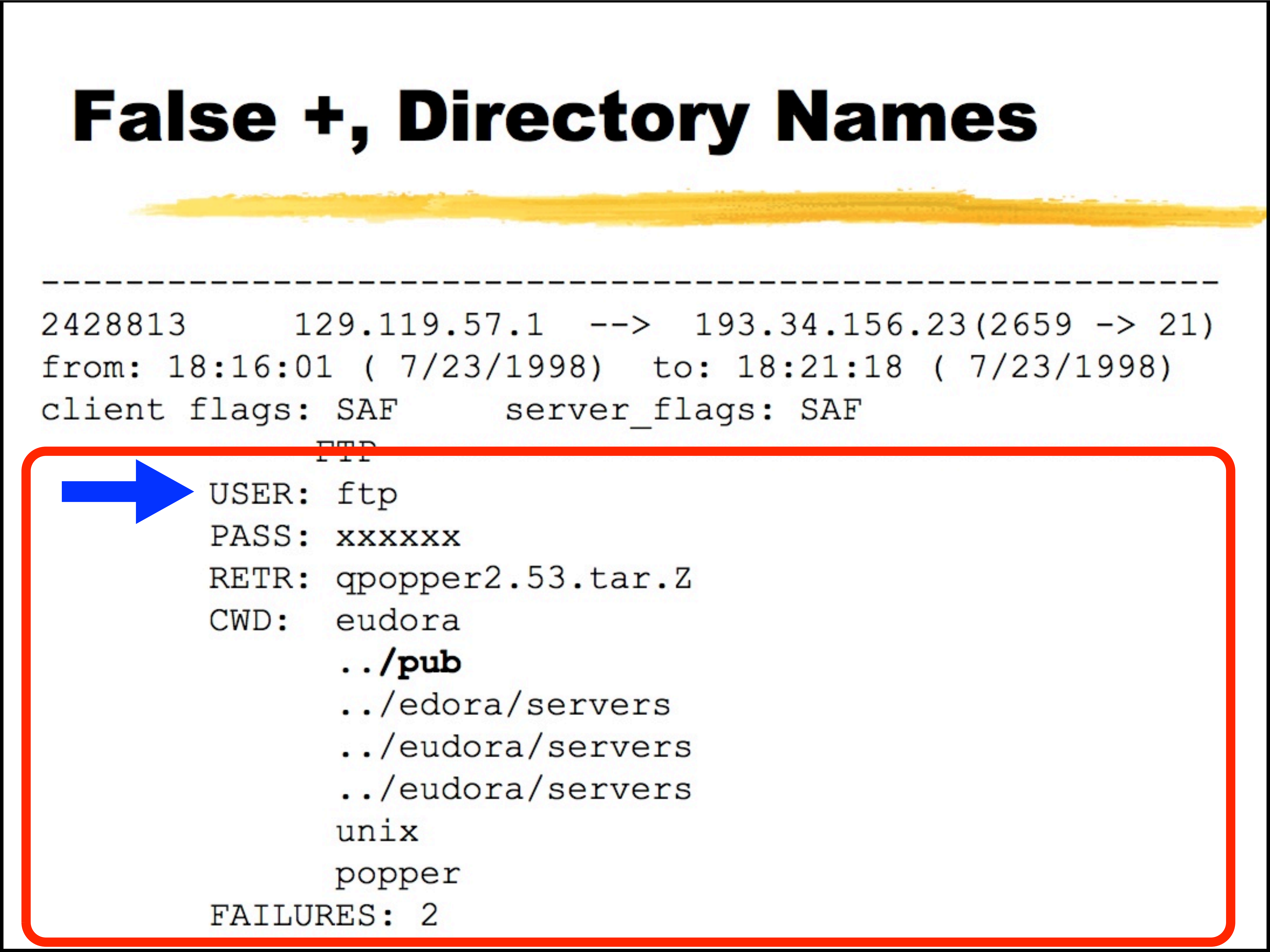


False +, Directory Names

```
------------------------------------------------------
2428813     129.119.57.1  -->  193.34.156.23(2659 -> 21)
from: 18:16:01 ( 7/23/1998)  to: 18:21:18 ( 7/23/1998)
client flags: SAF     server_flags: SAF
             FTP
        USER: ftp
        PASS: xxxxxx
        RETR: qpopper2.53.tar.Z
        CWD:  eudora
              ../pub
              ../edora/servers
              ../eudora/servers
              ../eudora/servers
              unix
              popper
        FAILURES: 2
```

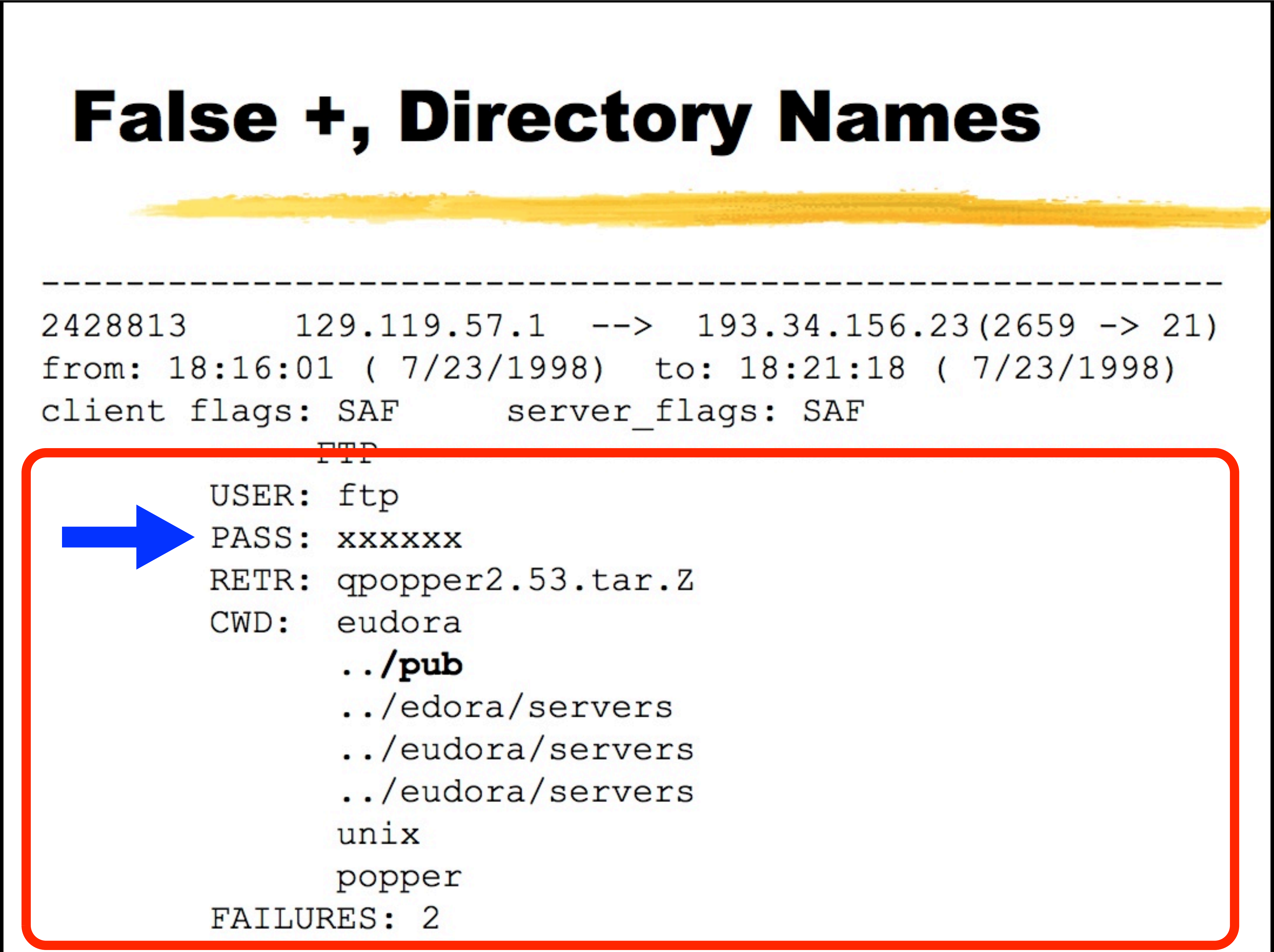
Data

Data



False +, Directory Names

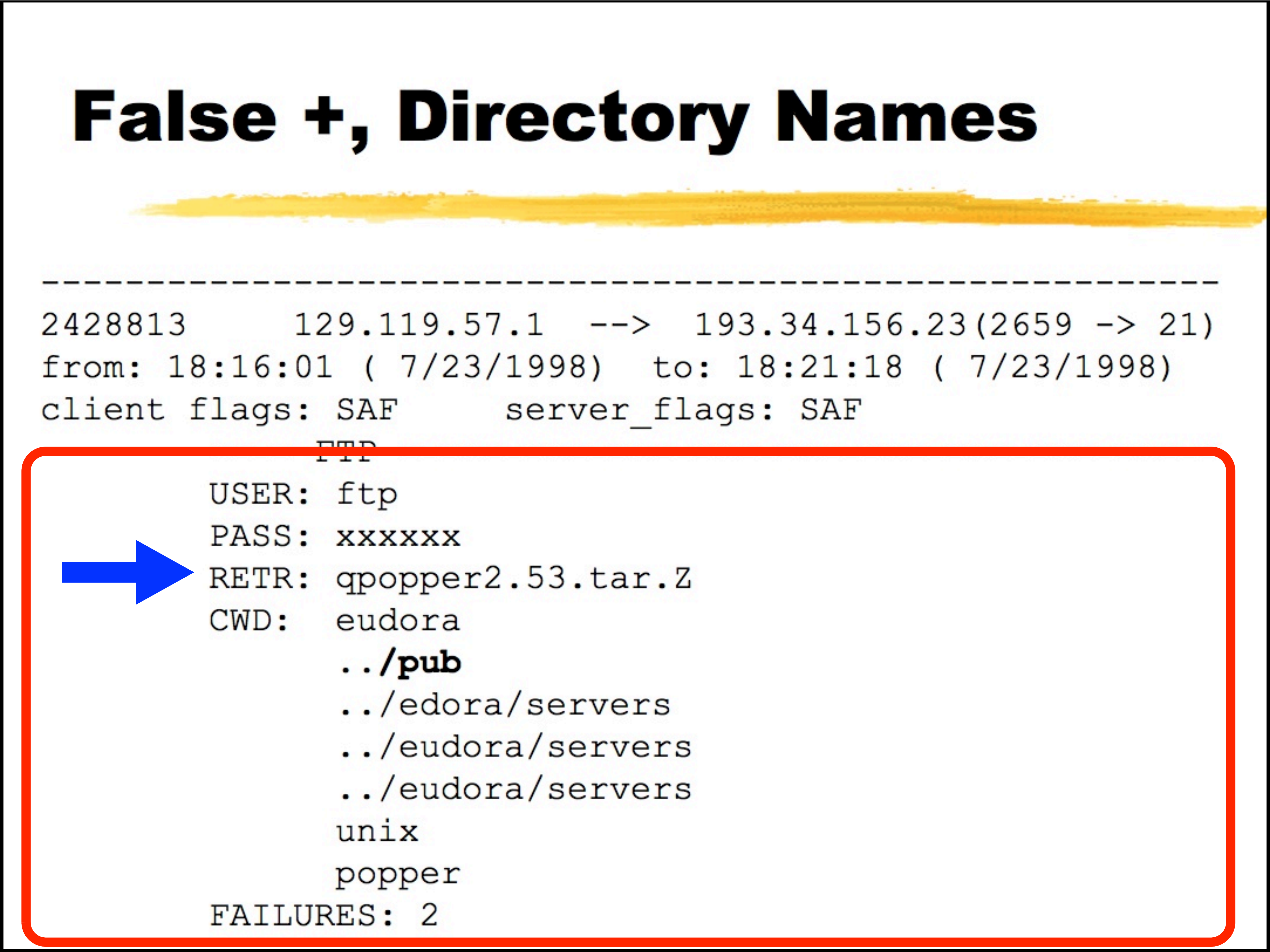
```
--------------------------------------------------------
2428813     129.119.57.1  -->  193.34.156.23(2659 -> 21)
from: 18:16:01 ( 7/23/1998)  to: 18:21:18 ( 7/23/1998)
client flags: SAF    server_flags: SAF
             FTP
        USER: ftp
        PASS: xxxxxx
        RETR: qpopper2.53.tar.Z
        CWD:  eudora
              ../pub
              ../edora/servers
              ../eudora/servers
              ../eudora/servers
              unix
              popper
        FAILURES: 2
```



False +, Directory Names

```
--------------------------------------------------------
2428813     129.119.57.1  -->  193.34.156.23(2659 -> 21)
from: 18:16:01 ( 7/23/1998)  to: 18:21:18 ( 7/23/1998)
client flags: SAF     server_flags: SAF
             FTP
        USER: ftp
        PASS: xxxxxx
        RETR: qpopper2.53.tar.Z
        CWD:  eudora
              ../pub
              ../edora/servers
              ../eudora/servers
              ../eudora/servers
              unix
              popper
        FAILURES: 2
```

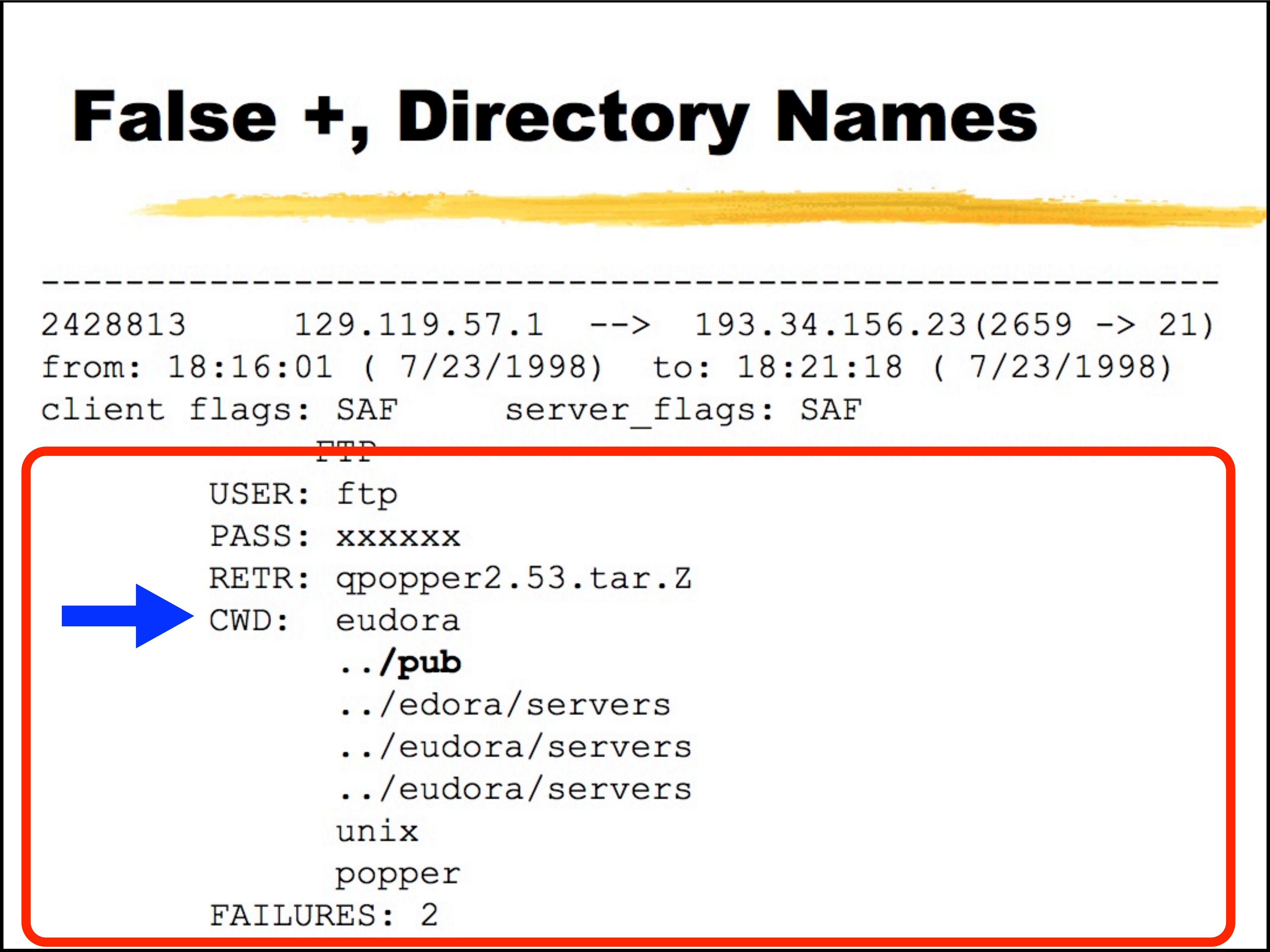
Data



False +, Directory Names

```
--------------------------------------------------------
2428813     129.119.57.1  -->  193.34.156.23(2659 -> 21)
from: 18:16:01 ( 7/23/1998)  to: 18:21:18 ( 7/23/1998)
client flags: SAF     server_flags: SAF
             FTP
        USER: ftp
        PASS: xxxxxx
        RETR: qpopper2.53.tar.Z
        CWD:  eudora
              ../pub
              ../edora/servers
              ../eudora/servers
              ../eudora/servers
              unix
              popper
        FAILURES: 2
```

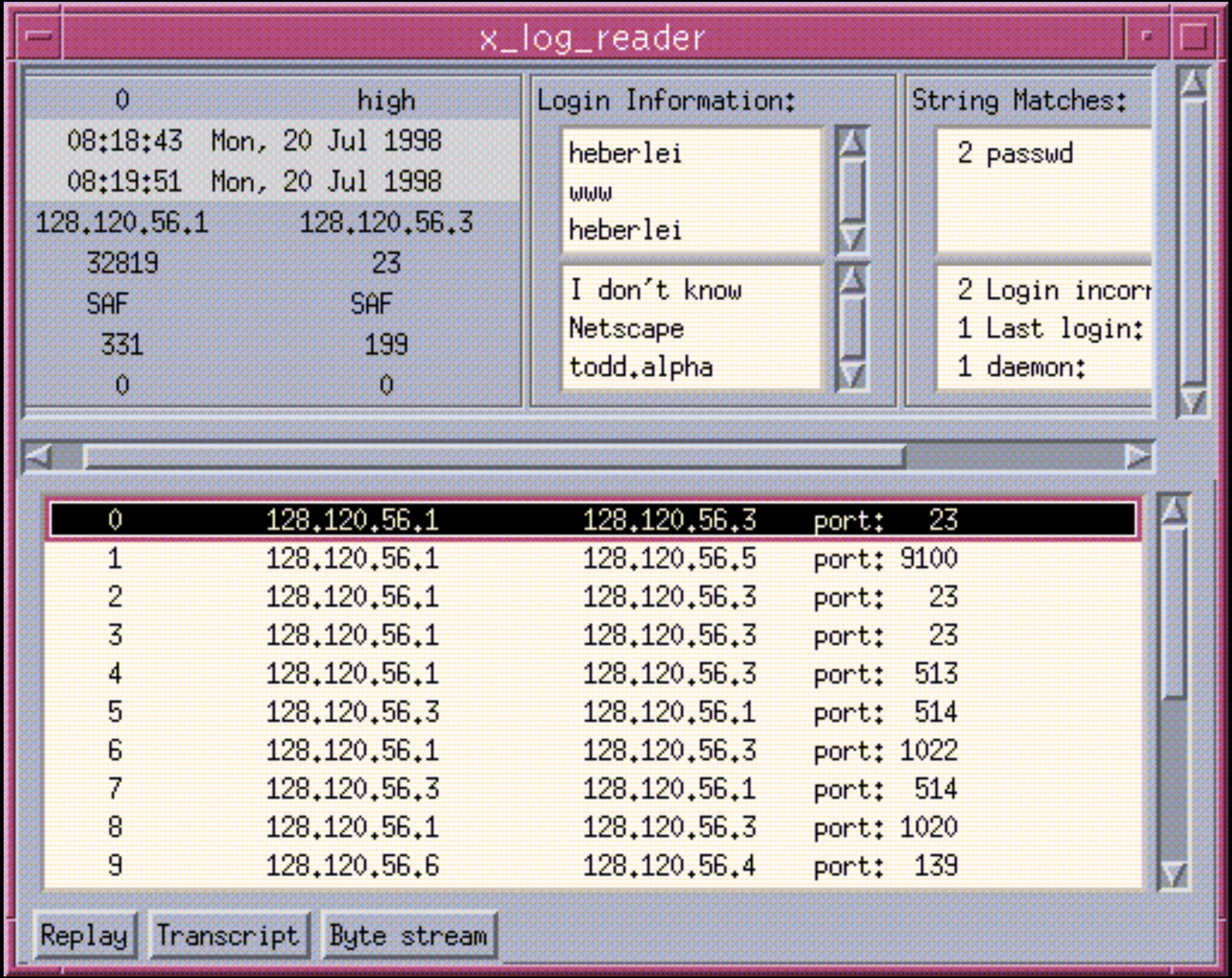
Data



False +, Directory Names

```
--------------------------------------------------------
2428813     129.119.57.1  -->  193.34.156.23(2659 -> 21)
from: 18:16:01 ( 7/23/1998)  to: 18:21:18 ( 7/23/1998)
client flags: SAF     server_flags: SAF
             FTP
        USER: ftp
        PASS: xxxxxx
        RETR: qpopper2.53.tar.Z
        CWD:  eudora
              ../pub
              ../edora/servers
              ../eudora/servers
              ../eudora/servers
              unix
              popper
        FAILURES: 2
```

Data



```
      0                 high
  08:18:43   Mon, 20 Jul 1998
  08:19:51   Mon, 20 Jul 1998
128.120.56.1        128.120.56.3
    32819                23
    SAF                 SAF
     331                 199
      0                   0
```

Login Information:

```
heberlei
www
heberlei
```

```
I don't know
Netscape
todd.alpha
```

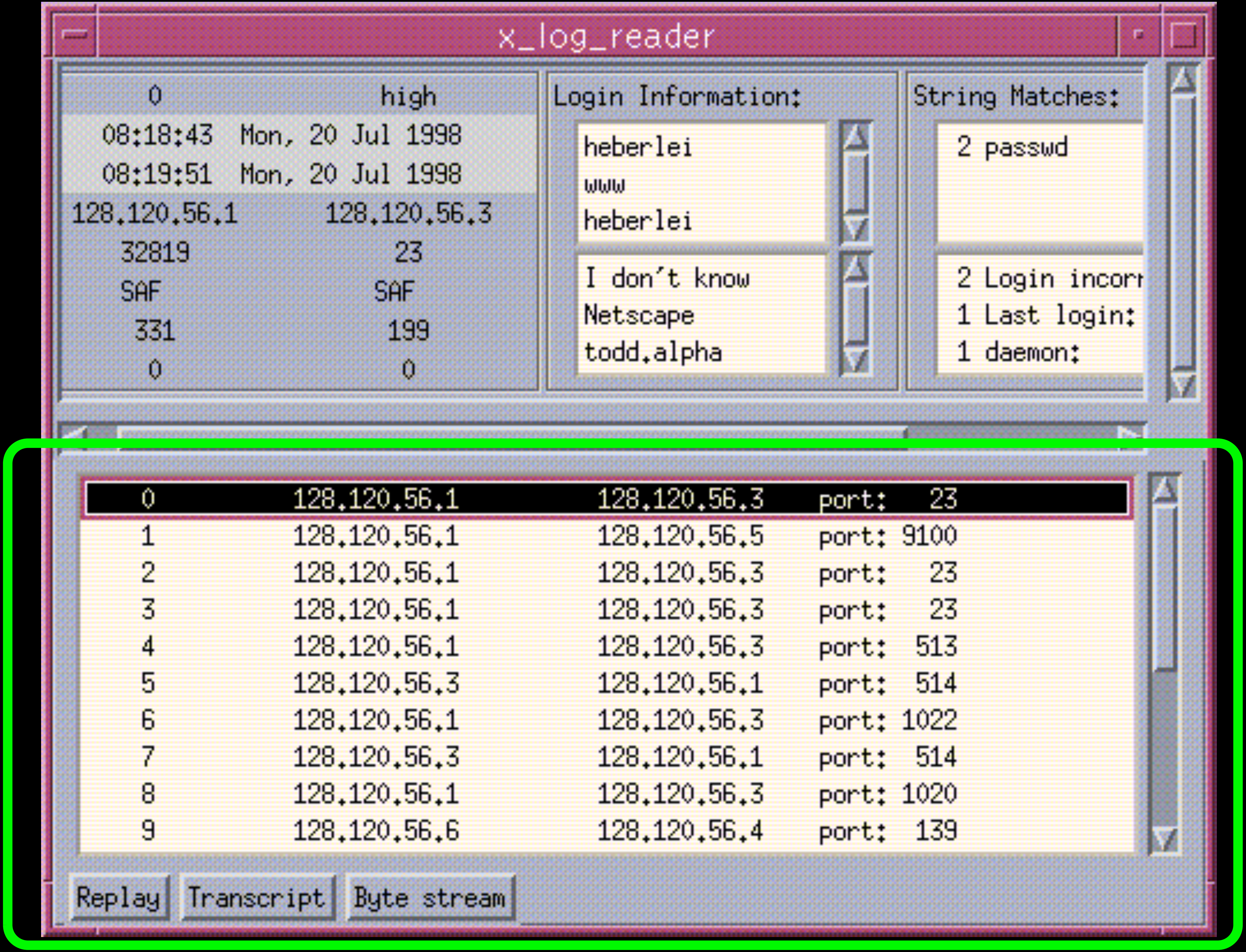
String Matches:

```
2 passwd
```

```
2 Login incorr
1 Last login:
1 daemon:
```

```
0    128.120.56.1    128.120.56.3    port:   23
1    128.120.56.1    128.120.56.5    port: 9100
2    128.120.56.1    128.120.56.3    port:   23
3    128.120.56.1    128.120.56.3    port:   23
4    128.120.56.1    128.120.56.3    port:  513
5    128.120.56.3    128.120.56.1    port:  514
6    128.120.56.1    128.120.56.3    port: 1022
7    128.120.56.3    128.120.56.1    port:  514
8    128.120.56.1    128.120.56.3    port: 1020
9    128.120.56.6    128.120.56.4    port:  139
```

Hub:
See
everything



x_log_reader

```
0                      high
08:18:43  Mon, 20 Jul 1998
08:19:51  Mon, 20 Jul 1998
128.120.56.1      128.120.56.3
32819                 23
SAF                  SAF
331                  199
0                     0
```

Login Information:

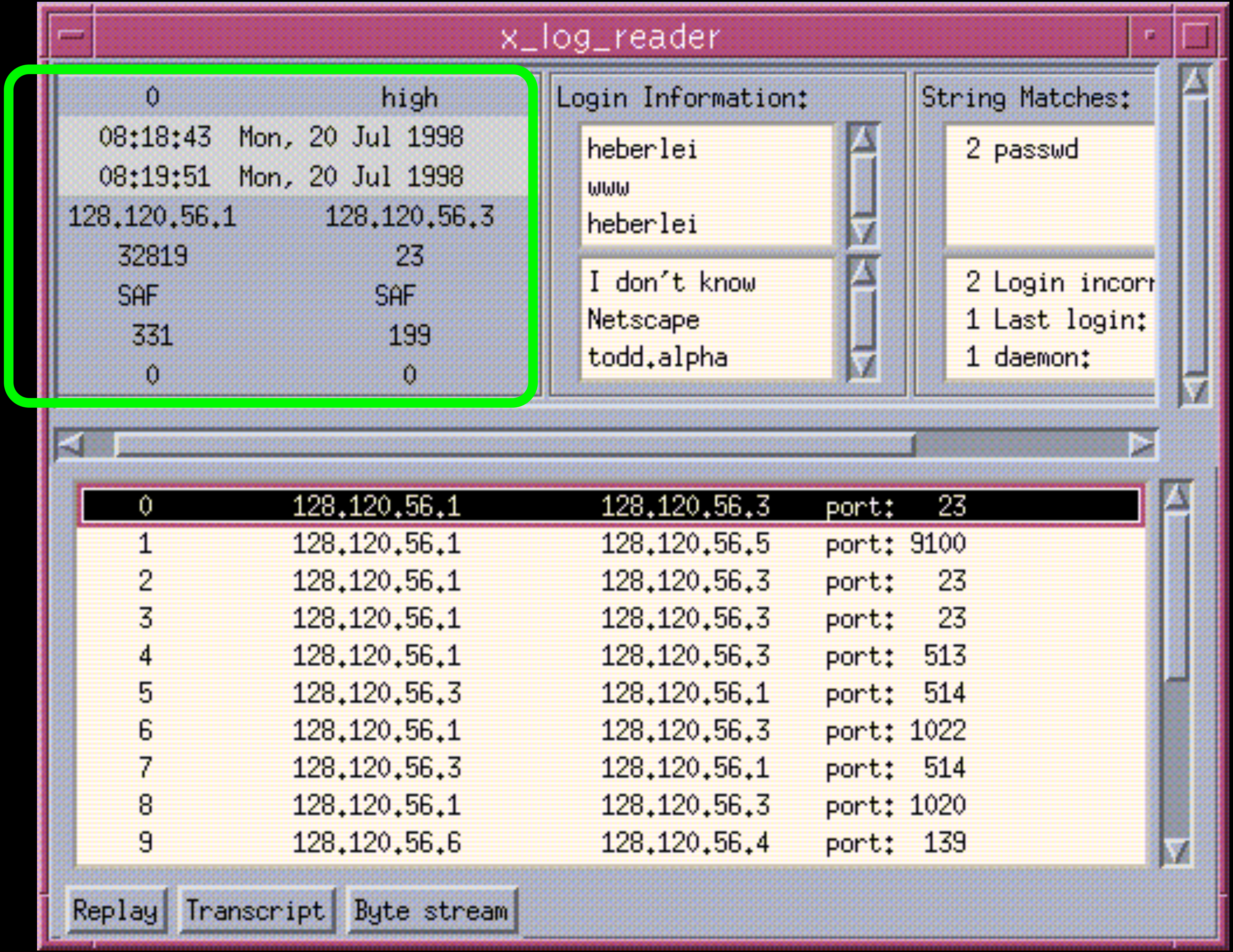
```
heberlei
www
heberlei

I don't know
Netscape
todd.alpha
```

String Matches:

```
2 passwd

2 Login incorr
1 Last login:
1 daemon:
```

```
0    128.120.56.1    128.120.56.3    port:   23
1    128.120.56.1    128.120.56.5    port: 9100
2    128.120.56.1    128.120.56.3    port:   23
3    128.120.56.1    128.120.56.3    port:   23
4    128.120.56.1    128.120.56.3    port:  513
5    128.120.56.3    128.120.56.1    port:  514
6    128.120.56.1    128.120.56.3    port: 1022
7    128.120.56.3    128.120.56.1    port:  514
8    128.120.56.1    128.120.56.3    port: 1020
9    128.120.56.6    128.120.56.4    port:  139
```

TCP/IP
Headers



```
      0                  high
   08:18:43  Mon, 20 Jul 1998
   08:19:51  Mon, 20 Jul 1998
128.120.56.1         128.120.56.3
    32819                 23
    SAF                  SAF
     331                 199
      0                    0
```

Login Information:

```
heberlei
www
heberlei
```

```
I don't know
Netscape
todd.alpha
```

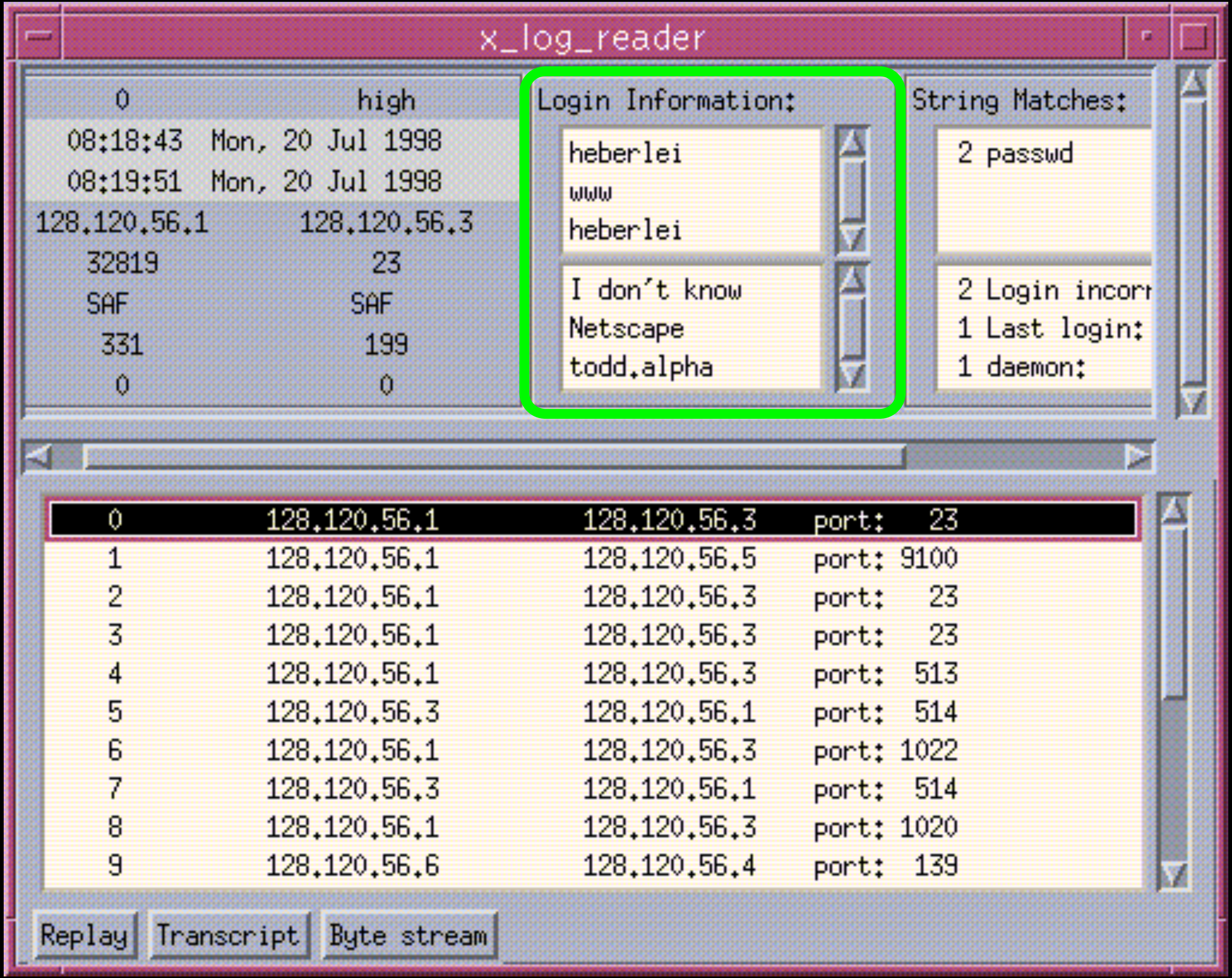
String Matches:

```
2 passwd
```

```
2 Login incorr
1 Last login:
1 daemon:
```

```
0    128.120.56.1    128.120.56.3    port:   23
1    128.120.56.1    128.120.56.5    port: 9100
2    128.120.56.1    128.120.56.3    port:   23
3    128.120.56.1    128.120.56.3    port:   23
4    128.120.56.1    128.120.56.3    port:  513
5    128.120.56.3    128.120.56.1    port:  514
6    128.120.56.1    128.120.56.3    port: 1022
7    128.120.56.3    128.120.56.1    port:  514
8    128.120.56.1    128.120.56.3    port: 1020
9    128.120.56.6    128.120.56.4    port:  139
```

Login & passwords



```
       0                        high
  08:18:43  Mon, 20 Jul 1998
  08:19:51  Mon, 20 Jul 1998
128.120.56.1          128.120.56.3
     32819                  23
     SAF                   SAF
      331                  199
       0                    0
```

Login Information:

```
heberlei
www
heberlei
```

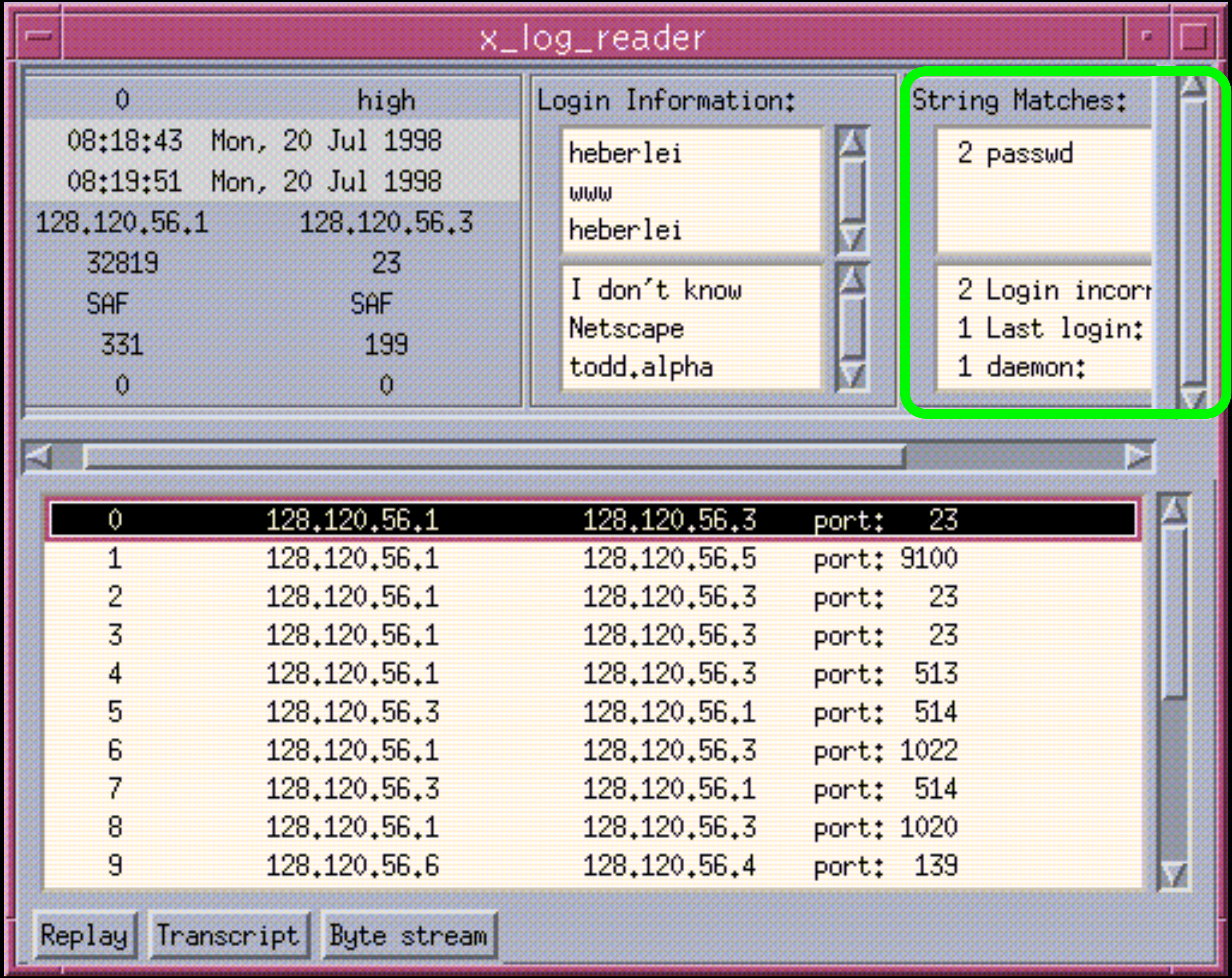
```
I don't know
Netscape
todd.alpha
```

String Matches:

```
2 passwd
```

```
2 Login incorr
1 Last login:
1 daemon:
```

```
 0        128.120.56.1        128.120.56.3     port:   23
 1        128.120.56.1        128.120.56.5     port: 9100
 2        128.120.56.1        128.120.56.3     port:   23
 3        128.120.56.1        128.120.56.3     port:   23
 4        128.120.56.1        128.120.56.3     port:  513
 5        128.120.56.3        128.120.56.1     port:  514
 6        128.120.56.1        128.120.56.3     port: 1022
 7        128.120.56.3        128.120.56.1     port:  514
 8        128.120.56.1        128.120.56.3     port: 1020
 9        128.120.56.6        128.120.56.4     port:  139
```



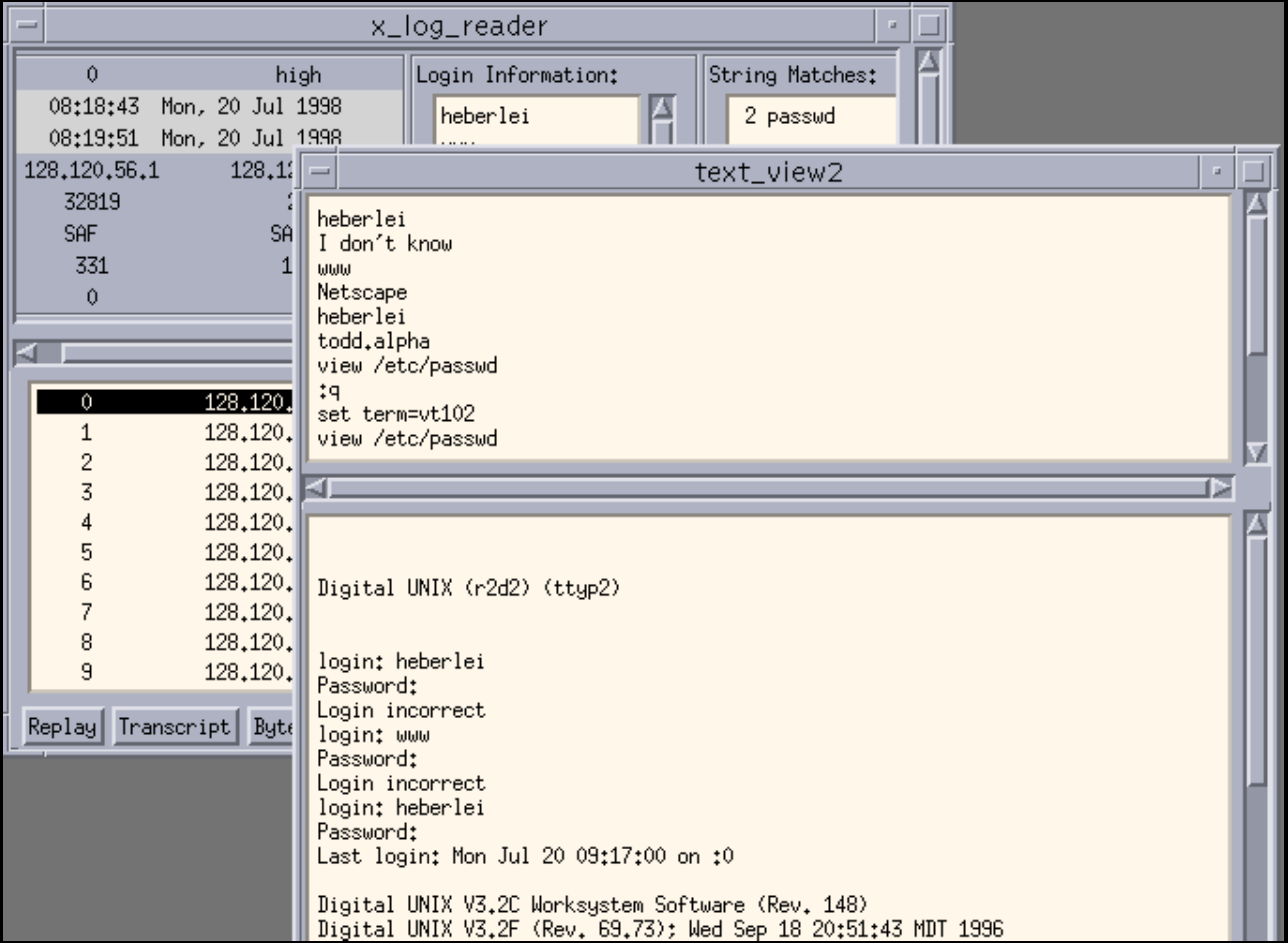
```
        0                      high
   08:18:43  Mon, 20 Jul 1998
   08:19:51  Mon, 20 Jul 1998
128.120.56.1            128.120.56.3
     32819                   23
     SAF                    SAF
      331                   199
       0                     0
```

```
Login Information:
  heberlei
  www
  heberlei

  I don't know
  Netscape
  todd.alpha
```

```
String Matches:
  2 passwd

  2 Login incorr
  1 Last login:
  1 daemon:
```

```
  0        128.120.56.1        128.120.56.3     port:   23
  1        128.120.56.1        128.120.56.5     port: 9100
  2        128.120.56.1        128.120.56.3     port:   23
  3        128.120.56.1        128.120.56.3     port:   23
  4        128.120.56.1        128.120.56.3     port:  513
  5        128.120.56.3        128.120.56.1     port:  514
  6        128.120.56.1        128.120.56.3     port: 1022
  7        128.120.56.3        128.120.56.1     port:  514
  8        128.120.56.1        128.120.56.3     port: 1020
  9        128.120.56.6        128.120.56.4     port:  139
```

String matches



```
0            high
08:18:43  Mon, 20 Jul 1998
08:19:51  Mon, 20 Jul 1998
128.120.56.1    128.12
32819           2
SAF             SA
331             1
0
```

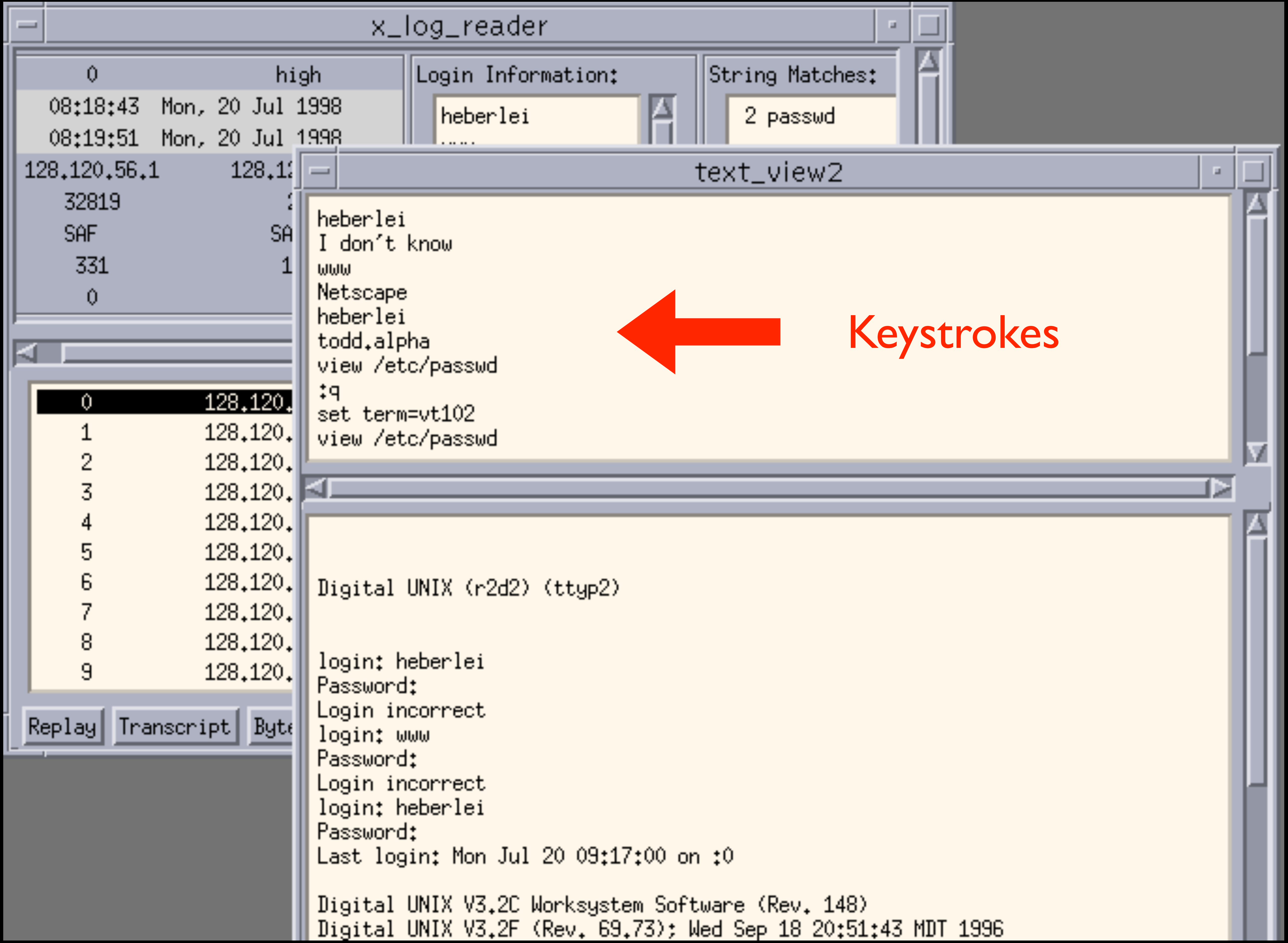
```
heberlei
```

```
2 passwd
```

```
0    128.120.
1    128.120.
2    128.120.
3    128.120.
4    128.120.
5    128.120.
6    128.120.
7    128.120.
8    128.120.
9    128.120.
```

```
heberlei
I don't know
www
Netscape
heberlei
todd.alpha
view /etc/passwd
:q
set term=vt102
view /etc/passwd
```

```



Digital UNIX (r2d2) (ttyp2)


login: heberlei
Password:
Login incorrect
login: www
Password:
Login incorrect
login: heberlei
Password:
Last login: Mon Jul 20 09:17:00 on :0

Digital UNIX V3.2C Worksystem Software (Rev. 148)
Digital UNIX V3.2F (Rev. 69.73); Wed Sep 18 20:51:43 MDT 1996
```



```
0                    high
08:18:43  Mon, 20 Jul 1998
08:19:51  Mon, 20 Jul 1998
128.120.56.1        128.12
32819                    2
SAF                     SA
331                      1
0
```

Login Information:

```
heberlei
```

String Matches:

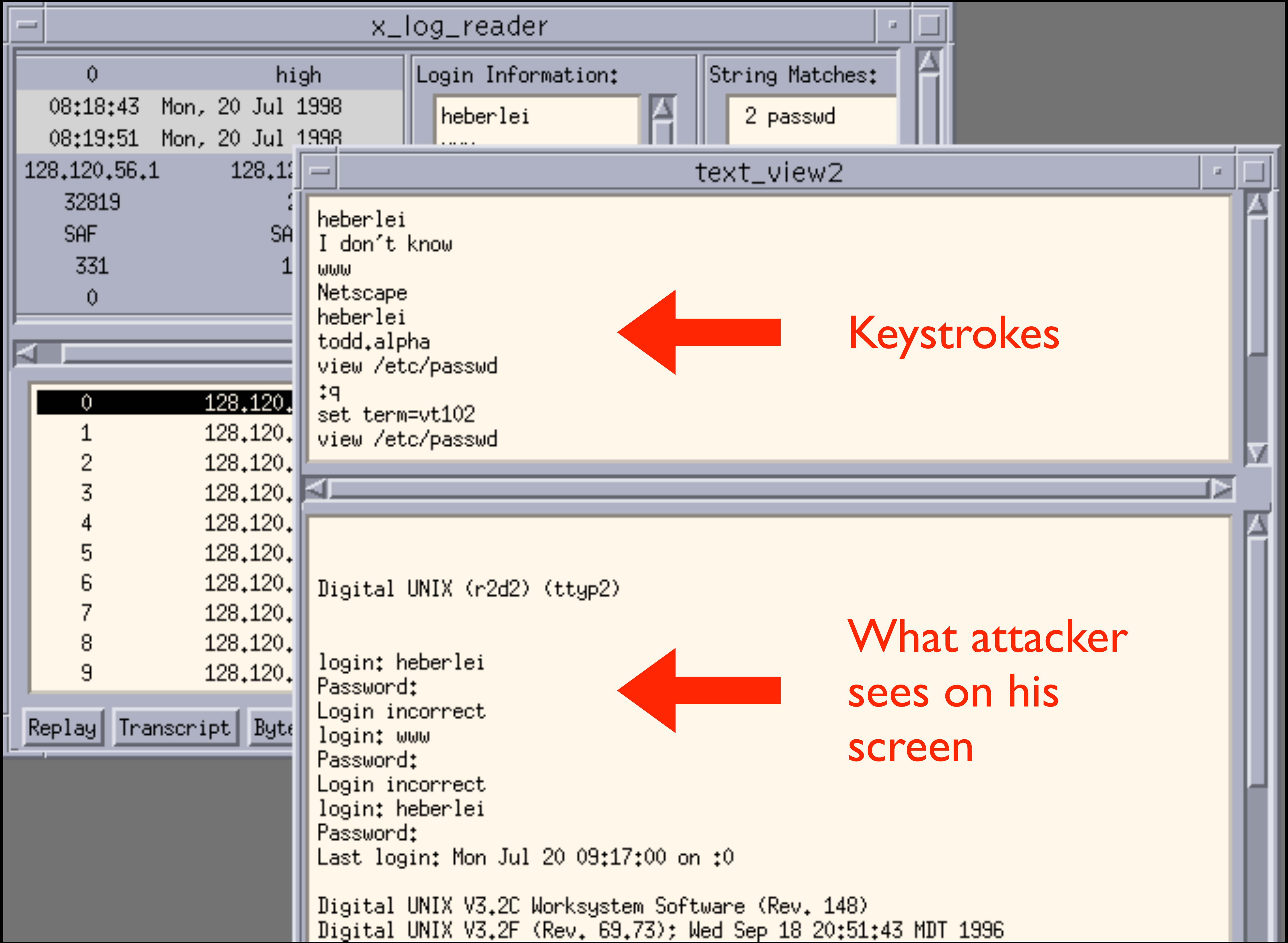
```
2 passwd
```

```
0      128.120.
1      128.120.
2      128.120.
3      128.120.
4      128.120.
5      128.120.
6      128.120.
7      128.120.
8      128.120.
9      128.120.
```

```
heberlei
I don't know
www
Netscape
heberlei
todd.alpha
view /etc/passwd
:q
set term=vt102
view /etc/passwd
```

Keystrokes

```



Digital UNIX (r2d2) (ttyp2)


login: heberlei
Password:
Login incorrect
login: www
Password:
Login incorrect
login: heberlei
Password:
Last login: Mon Jul 20 09:17:00 on :0

Digital UNIX V3.2C Worksystem Software (Rev. 148)
Digital UNIX V3.2F (Rev. 69.73); Wed Sep 18 20:51:43 MDT 1996
```



```
        0                    high
   08:18:43  Mon, 20 Jul 1998
   08:19:51  Mon, 20 Jul 1998
128.120.56.1         128.12
     32819                2
      SAF                SA
       331                1
        0
```

```
heberlei
www
```

```
2 passwd
```

```
  0          128.120.
  1          128.120.
  2          128.120.
  3          128.120.
  4          128.120.
  5          128.120.
  6          128.120.
  7          128.120.
  8          128.120.
  9          128.120.
```

```
heberlei
I don't know
www
Netscape
heberlei
todd.alpha
view /etc/passwd
:q
set term=vt102
view /etc/passwd
```

Keystrokes

```



Digital UNIX (r2d2) (ttyp2)


login: heberlei
Password:
Login incorrect
login: www
Password:
Login incorrect
login: heberlei
Password:
Last login: Mon Jul 20 09:17:00 on :0

Digital UNIX V3.2C Worksystem Software (Rev. 148)
Digital UNIX V3.2F (Rev. 69.73); Wed Sep 18 20:51:43 MDT 1996
```

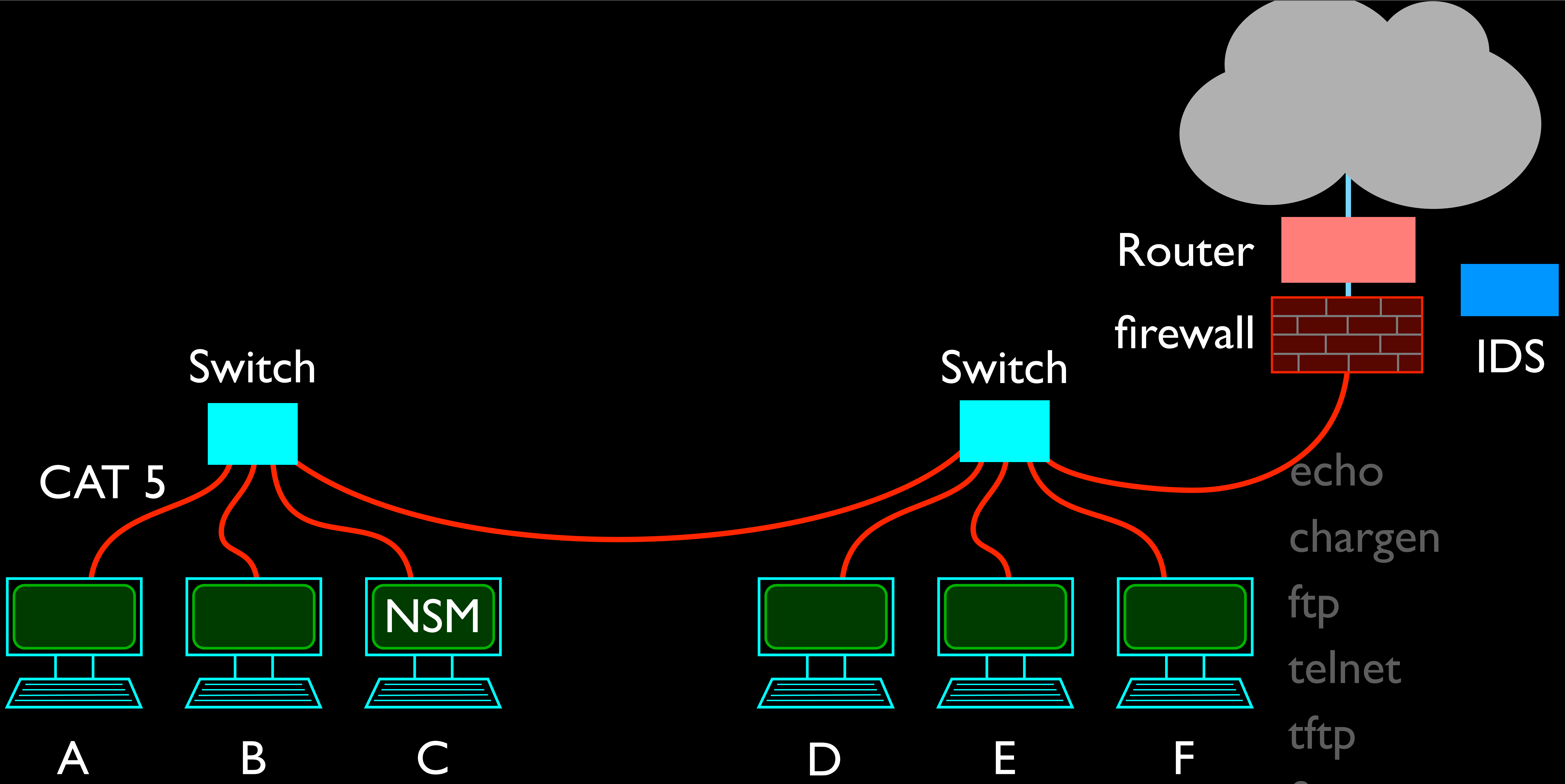
What attacker sees on his screen

Golden Age of Network Analysis

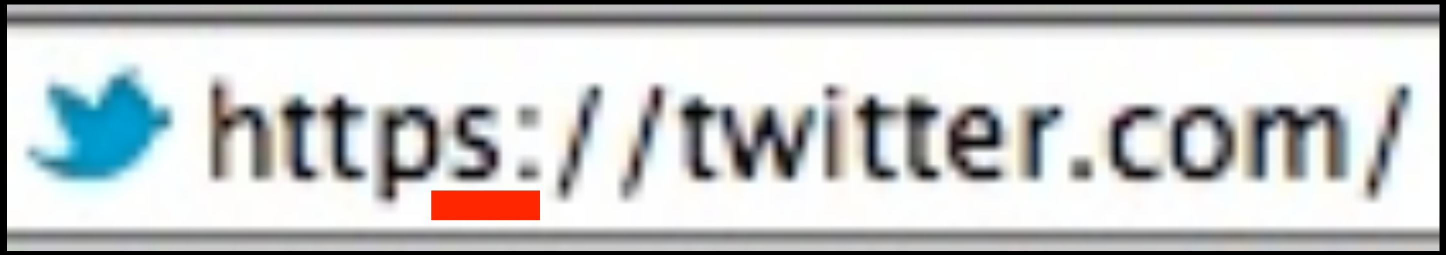
- One host could see everything
- Tons of (vulnerable) services turned on by default
- No automatic software updates (vulnerabilities lived for months/years)
- Nothing encrypted
- Weak passwords
- No firewalls – vertical & horizontal sweeps
- One IP address = one fixed host

This is the time when most network-centric tools were started

But times change...

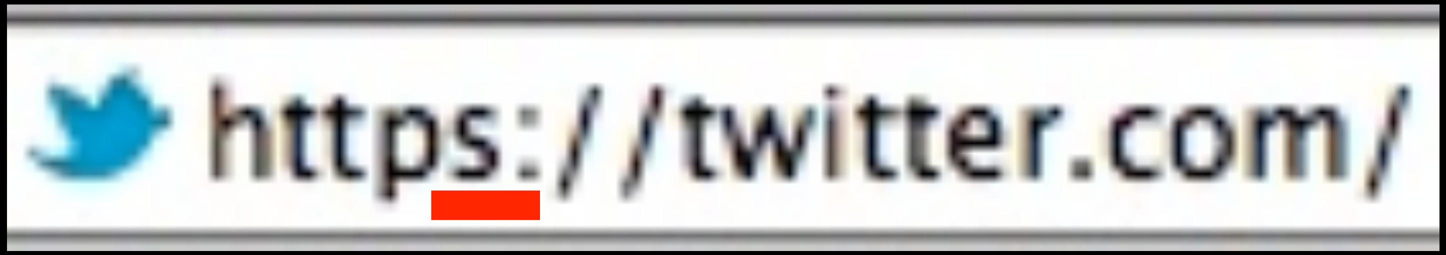


echo
chargen
ftp
telnet
tftp
finger
SunRPC
rlogin



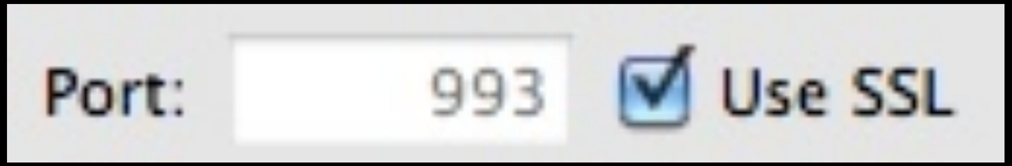
https://twitter.com/

Secure web traffic



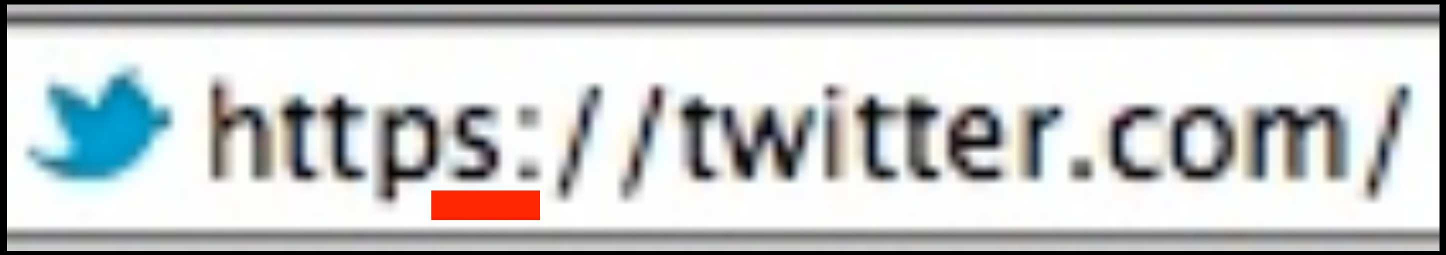
https://twitter.com/

Secure web traffic



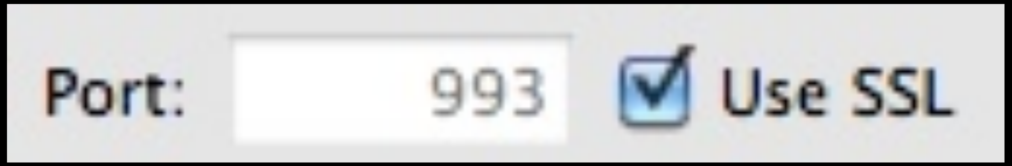
Port: 993 ☑ Use SSL

Email over IMAP



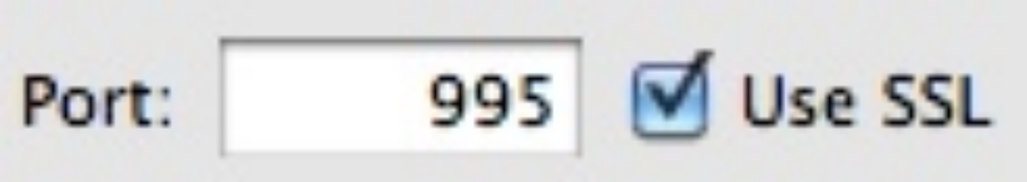
https://twitter.com/

Secure web traffic



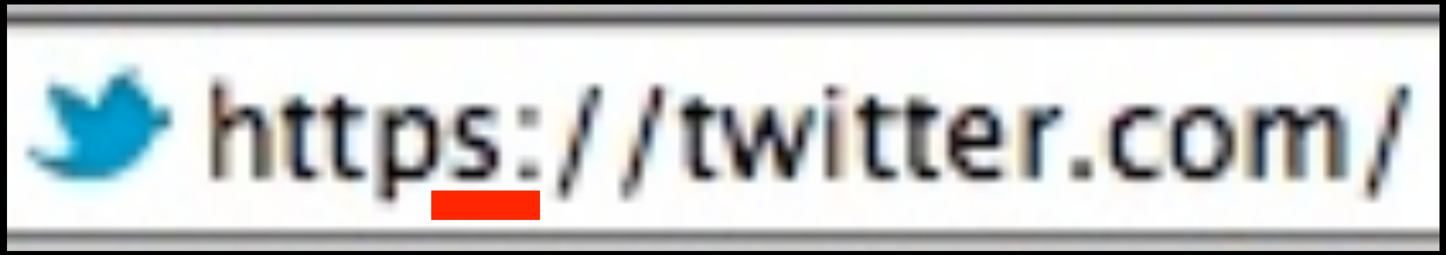
Port: 993 ☑ Use SSL

Email over IMAP



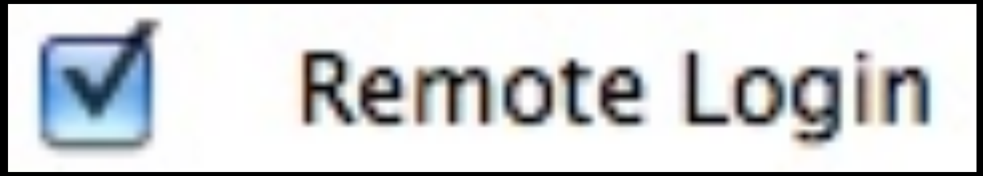
Port: 995 ☑ Use SSL

Email over POP



https://twitter.com/

Secure web traffic

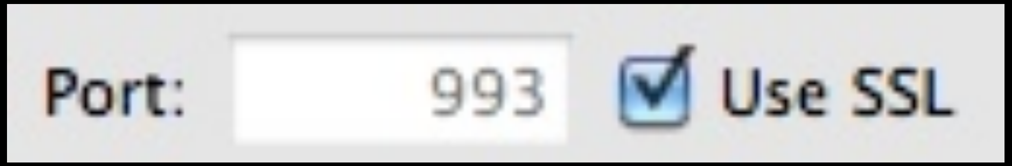


☑ Remote Login

ssh

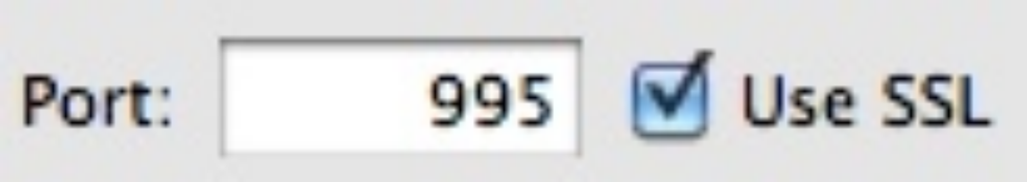
sftp

scp



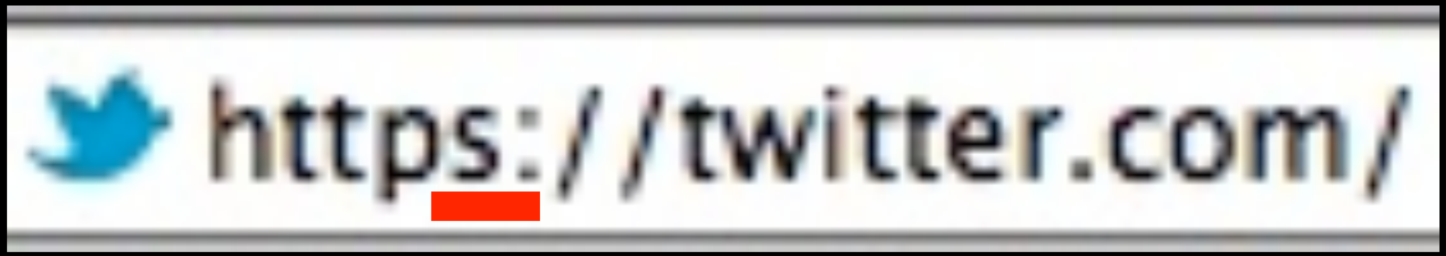
Port: 993 ☑ Use SSL

Email over IMAP



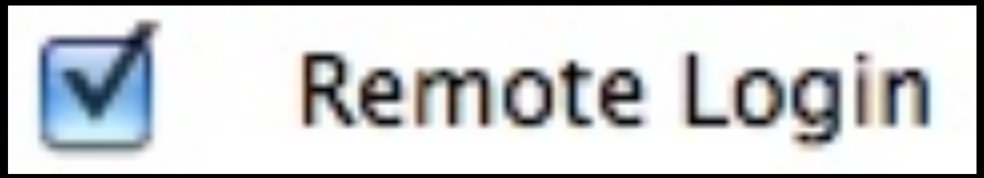
Port: 995 ☑ Use SSL

Email over POP



https://twitter.com/

Secure web traffic

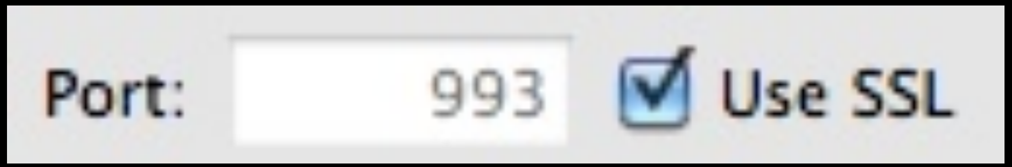


☑ Remote Login

ssh

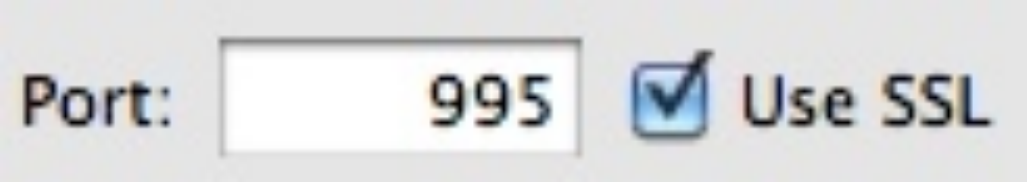
sftp

scp



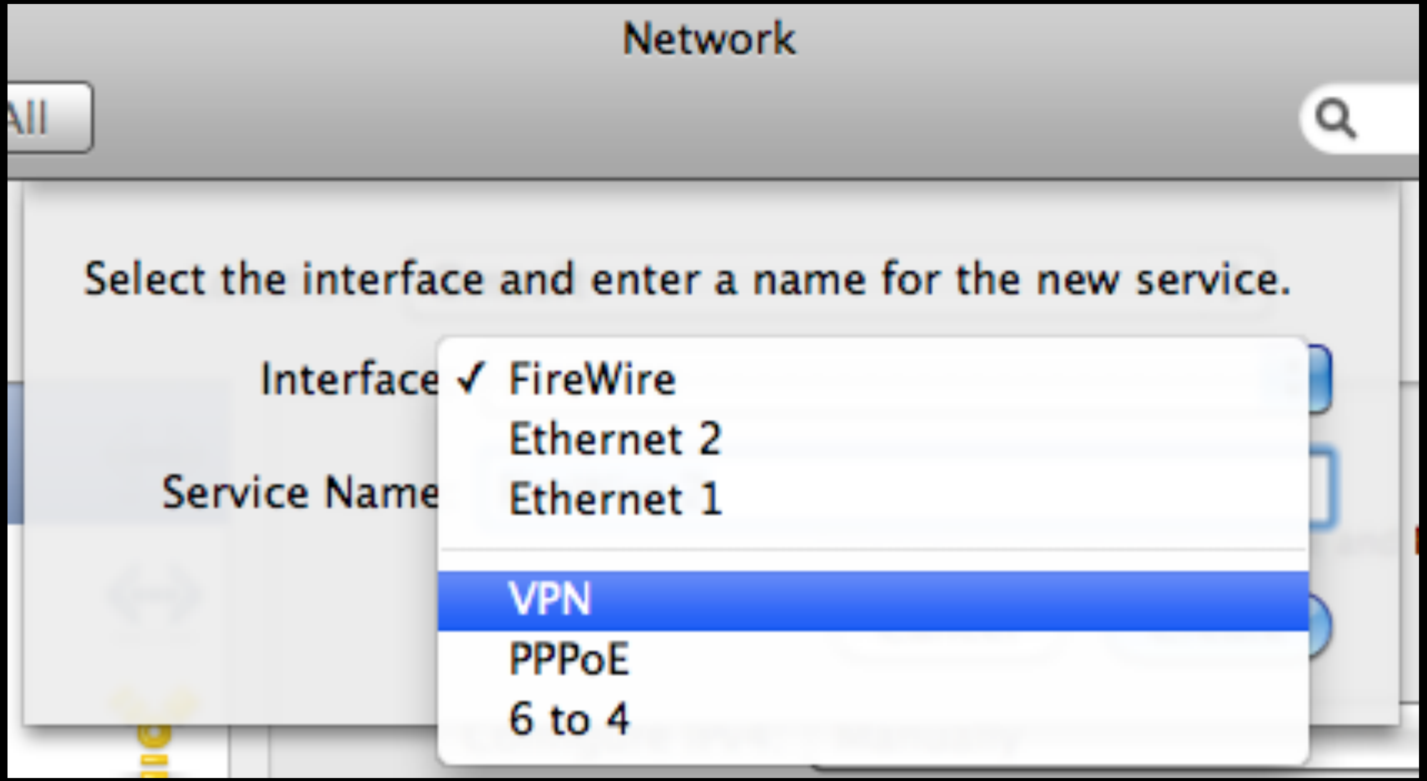
Port: 993 ☑ Use SSL

Email over IMAP



Port: 995 ☑ Use SSL

Email over POP



Network

Select the interface and enter a name for the new service.

Interface ✓ FireWire

Ethernet 2

Ethernet 1

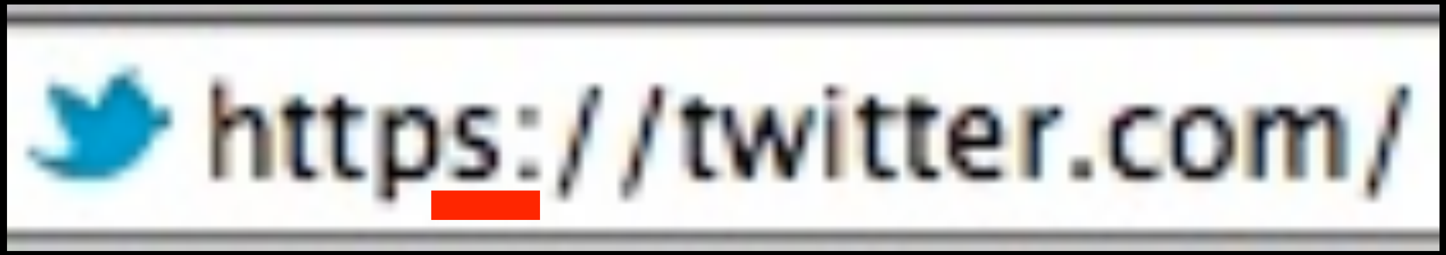
VPN

PPPoE

6 to 4

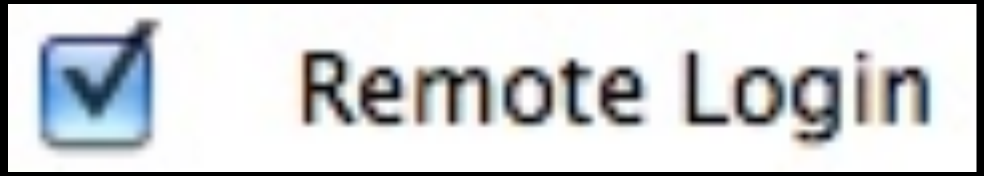
Service Name

ssh tunneling



https://twitter.com/

Secure web traffic

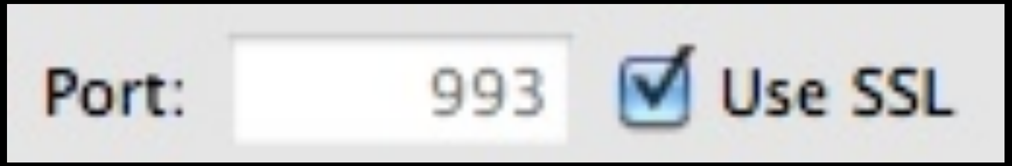


☑ Remote Login

ssh

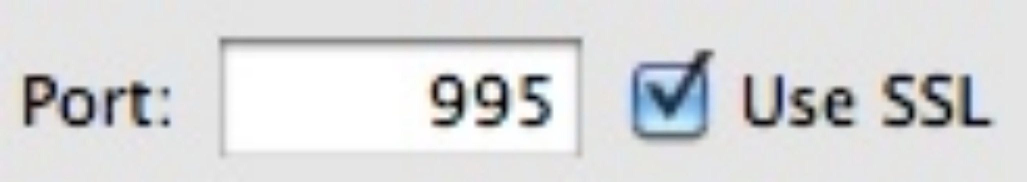
sftp

scp



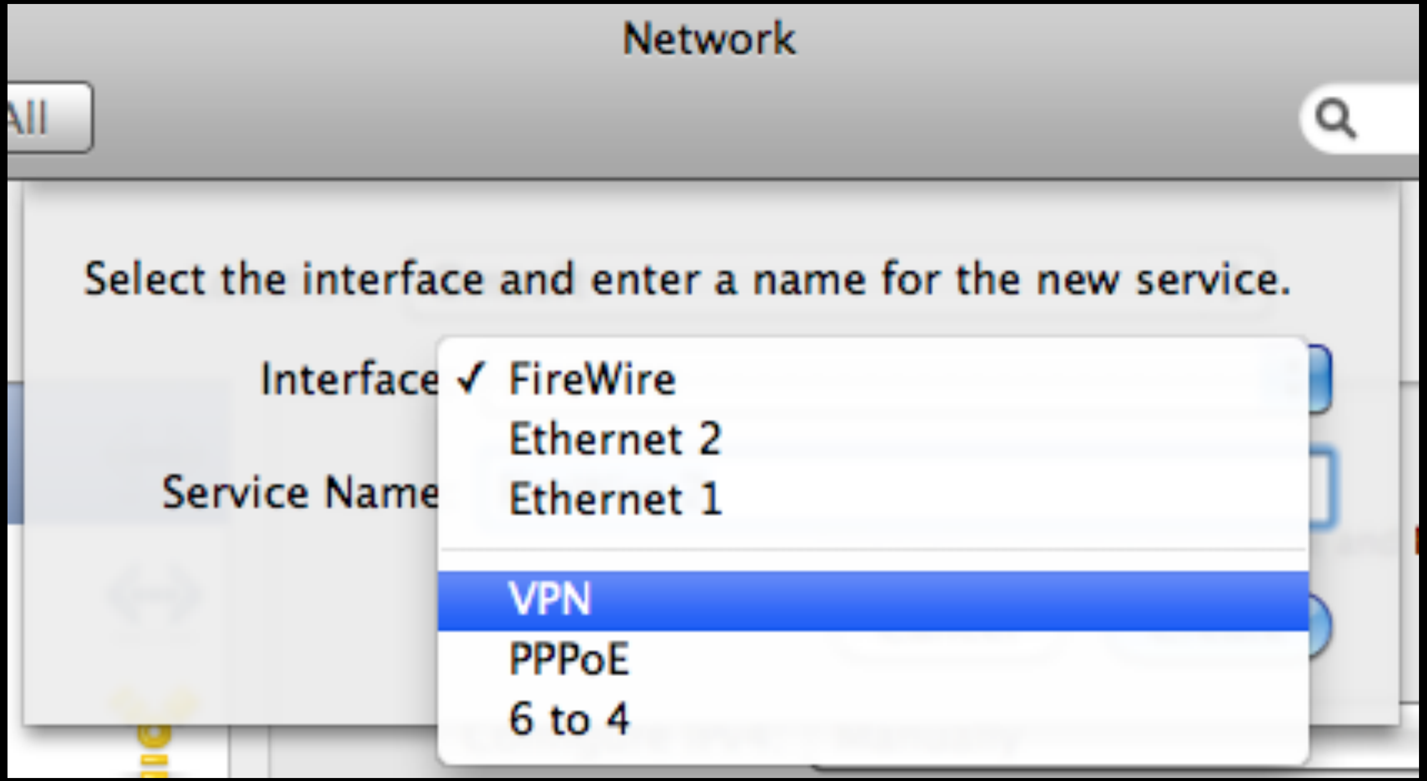
Port: 993 ☑ Use SSL

Email over IMAP



Port: 995 ☑ Use SSL

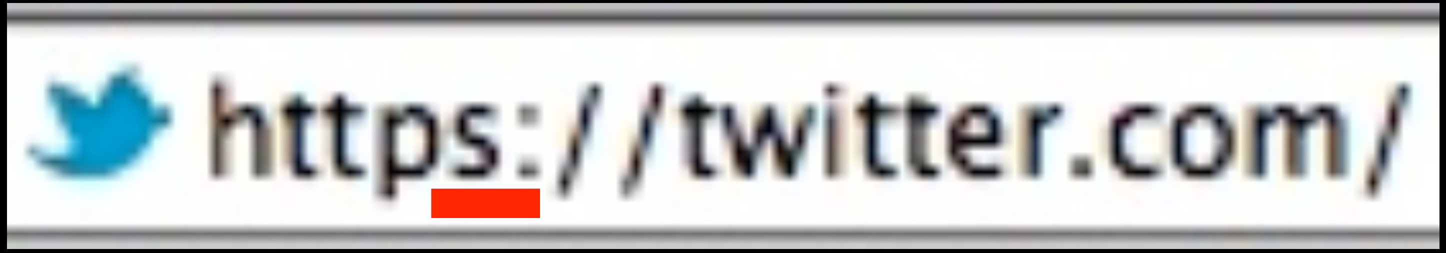
Email over POP



Select the interface and enter a name for the new service.

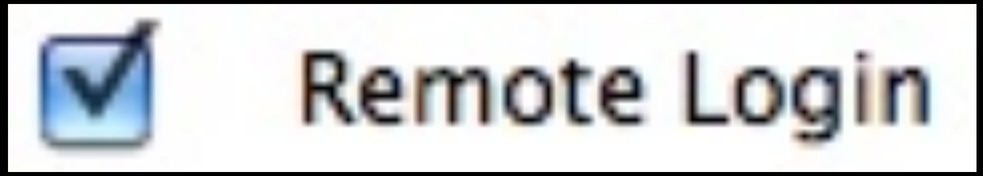
Interface ✓ FireWire

Service Name



https://twitter.com/

Secure web traffic



☑ Remote Login

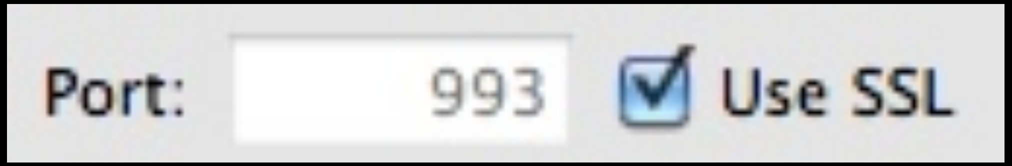
ssh

sftp

scp

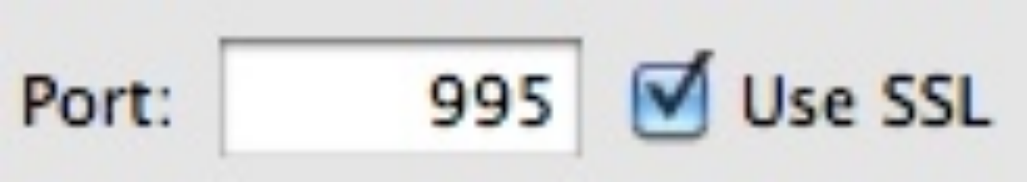
ssh tunneling

IPv6



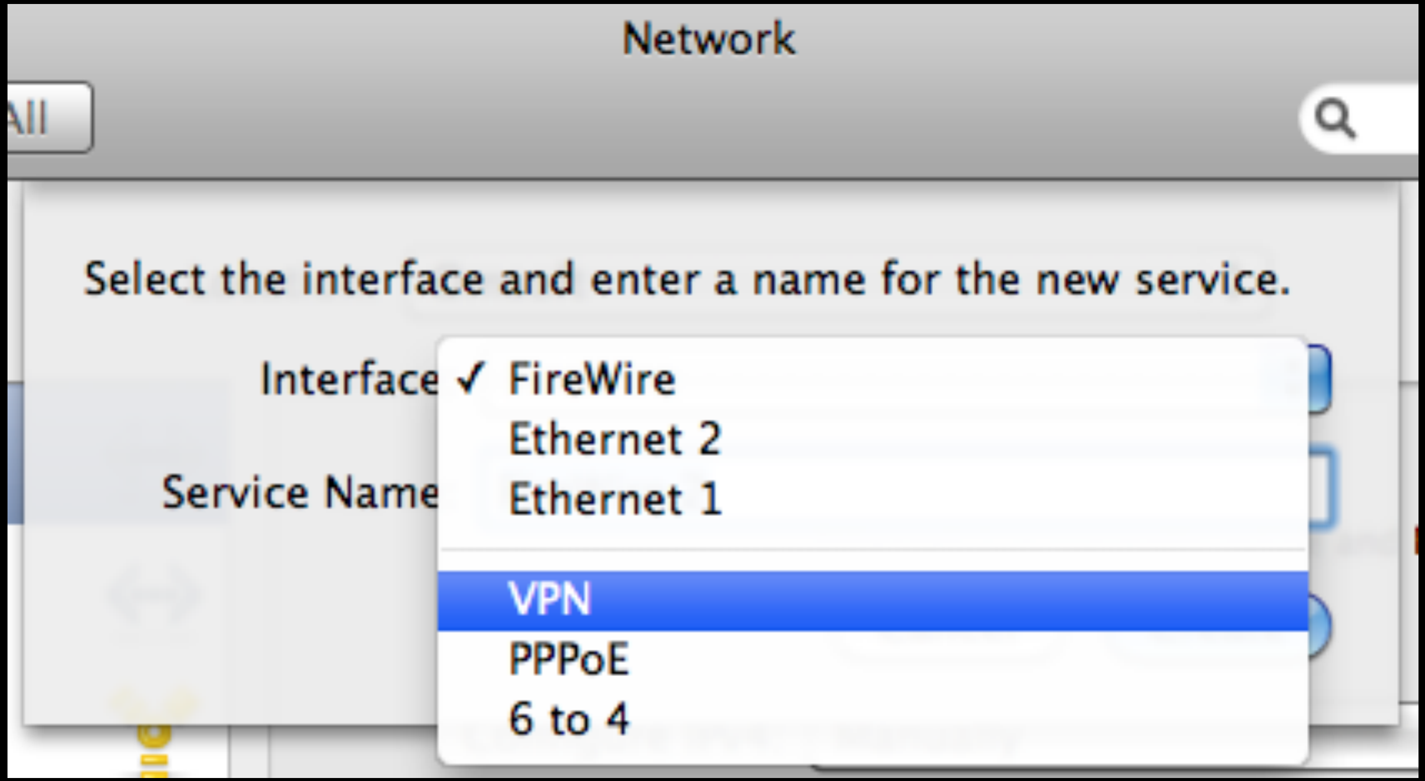
Port: 993 ☑ Use SSL

Email over IMAP



Port: 995 ☑ Use SSL

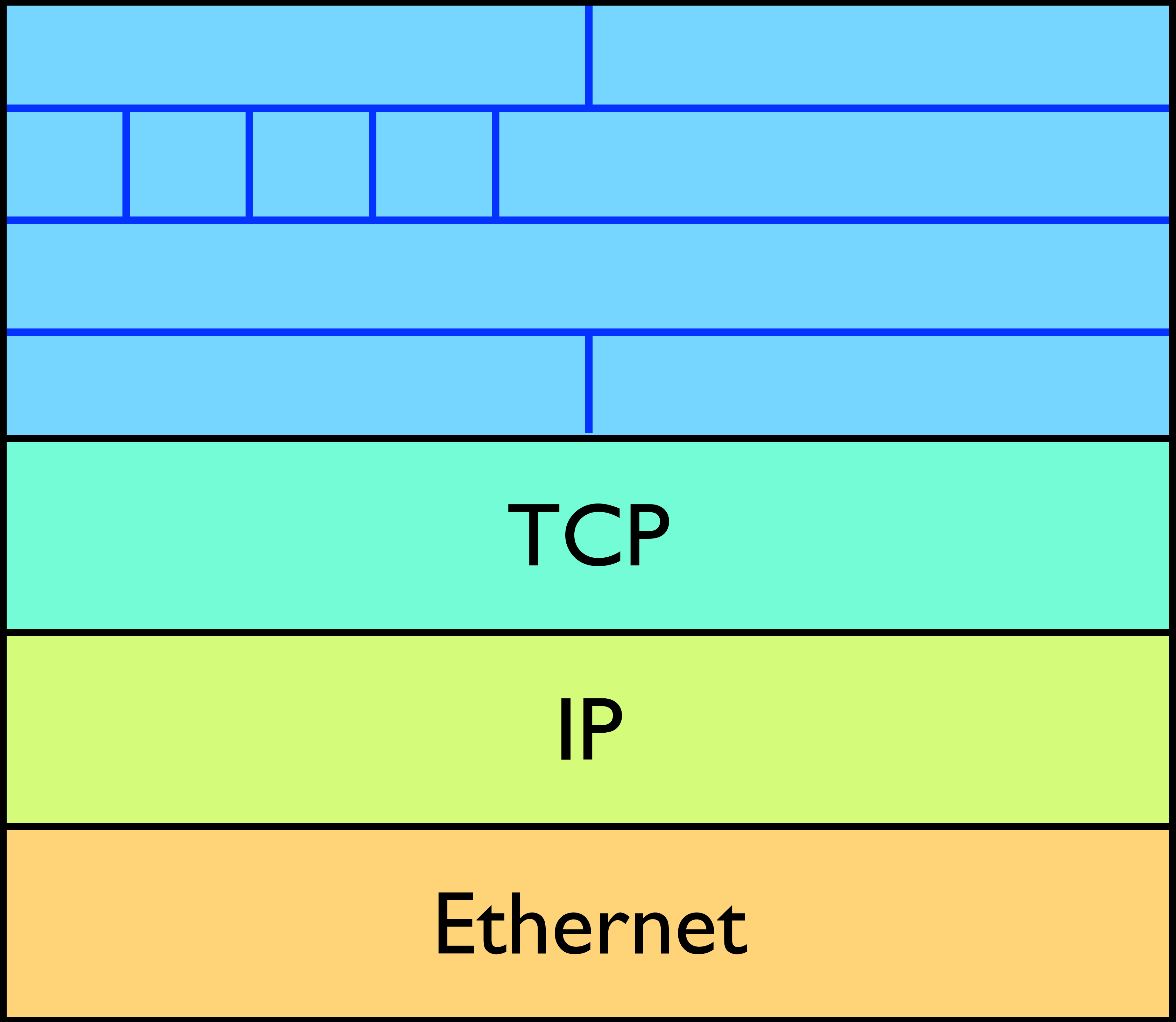
Email over POP



Select the interface and enter a name for the new service.

Interface ✓ FireWire

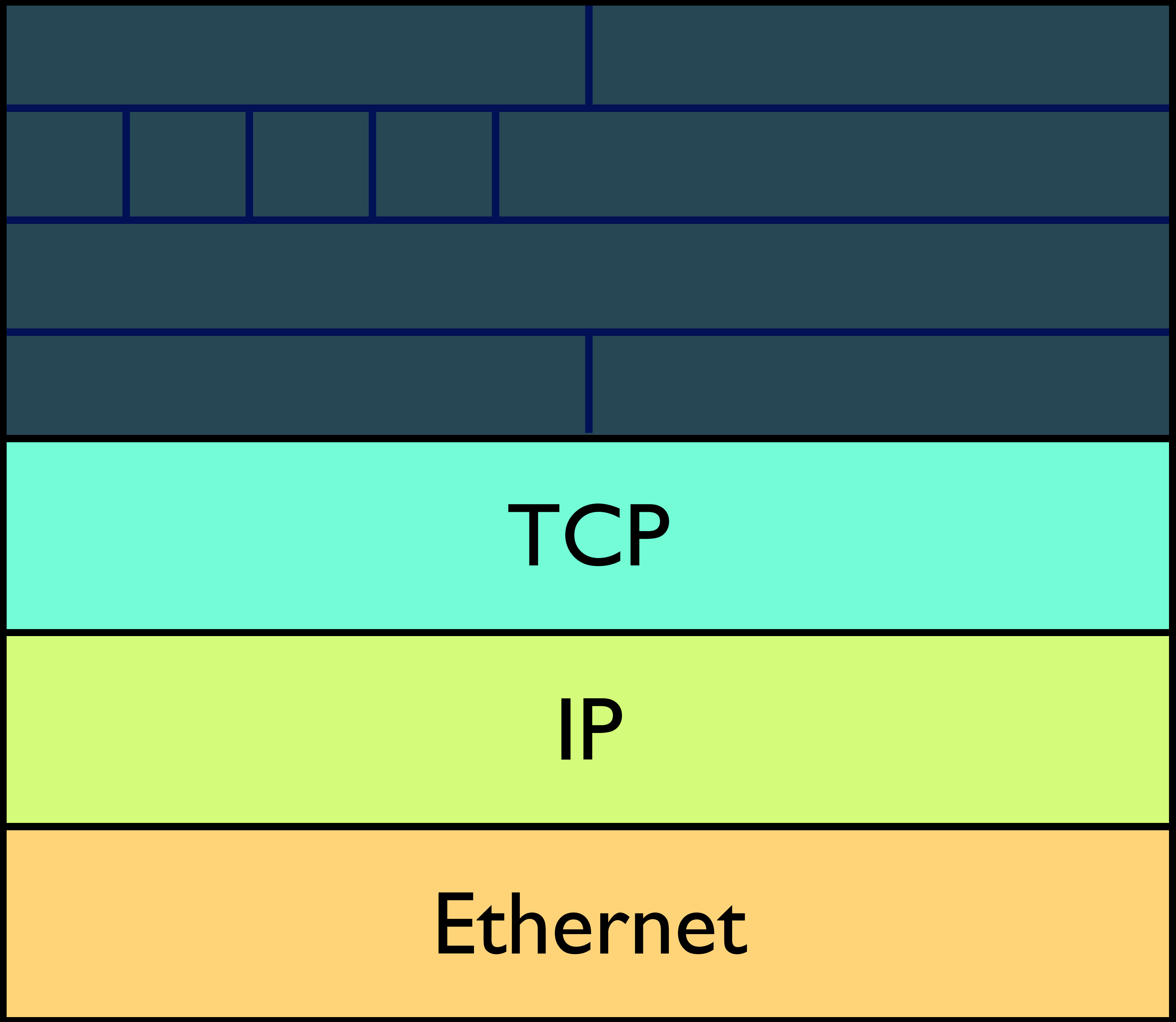
Service Name



TCP

IP

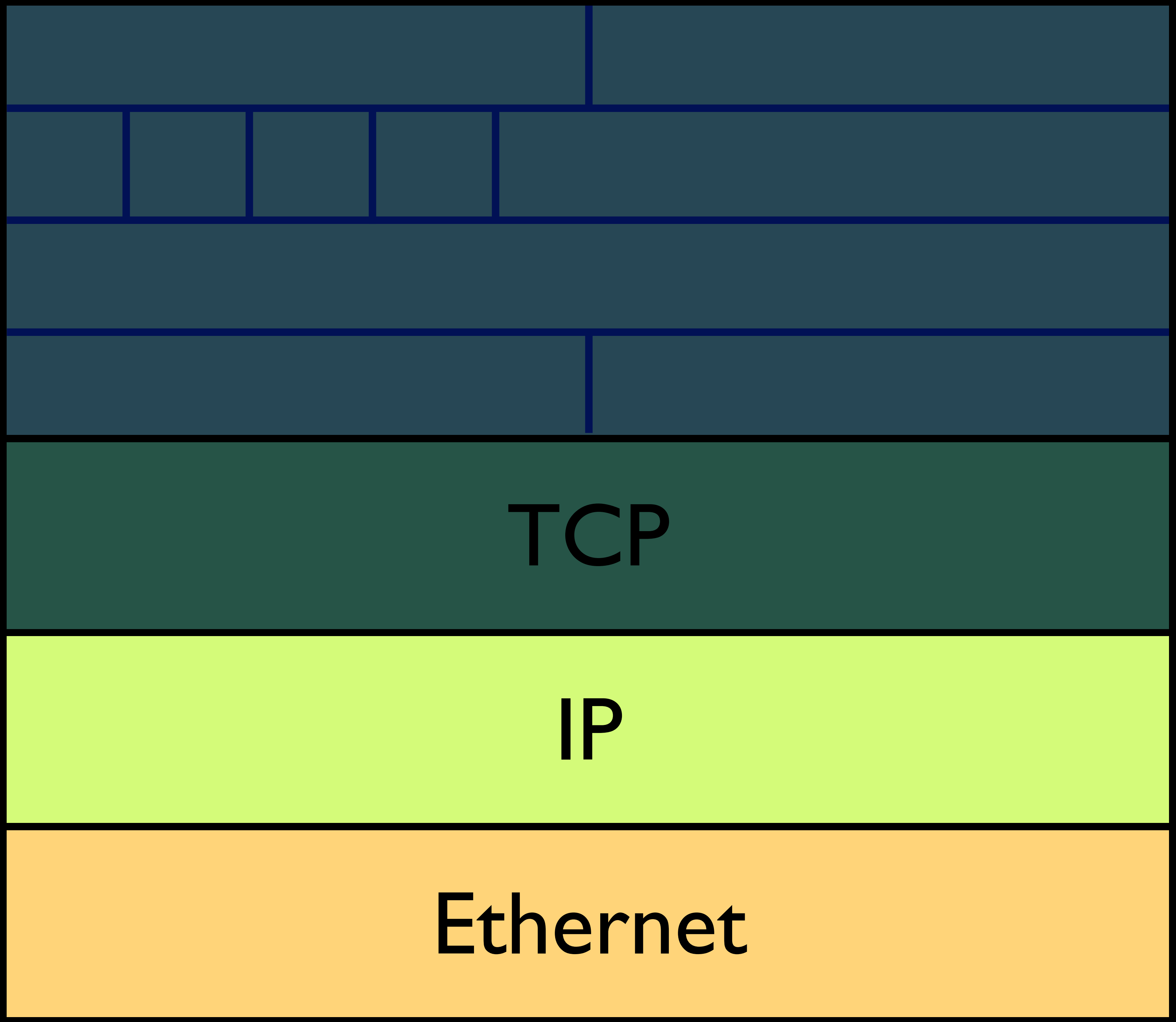
Ethernet



TCP

IP

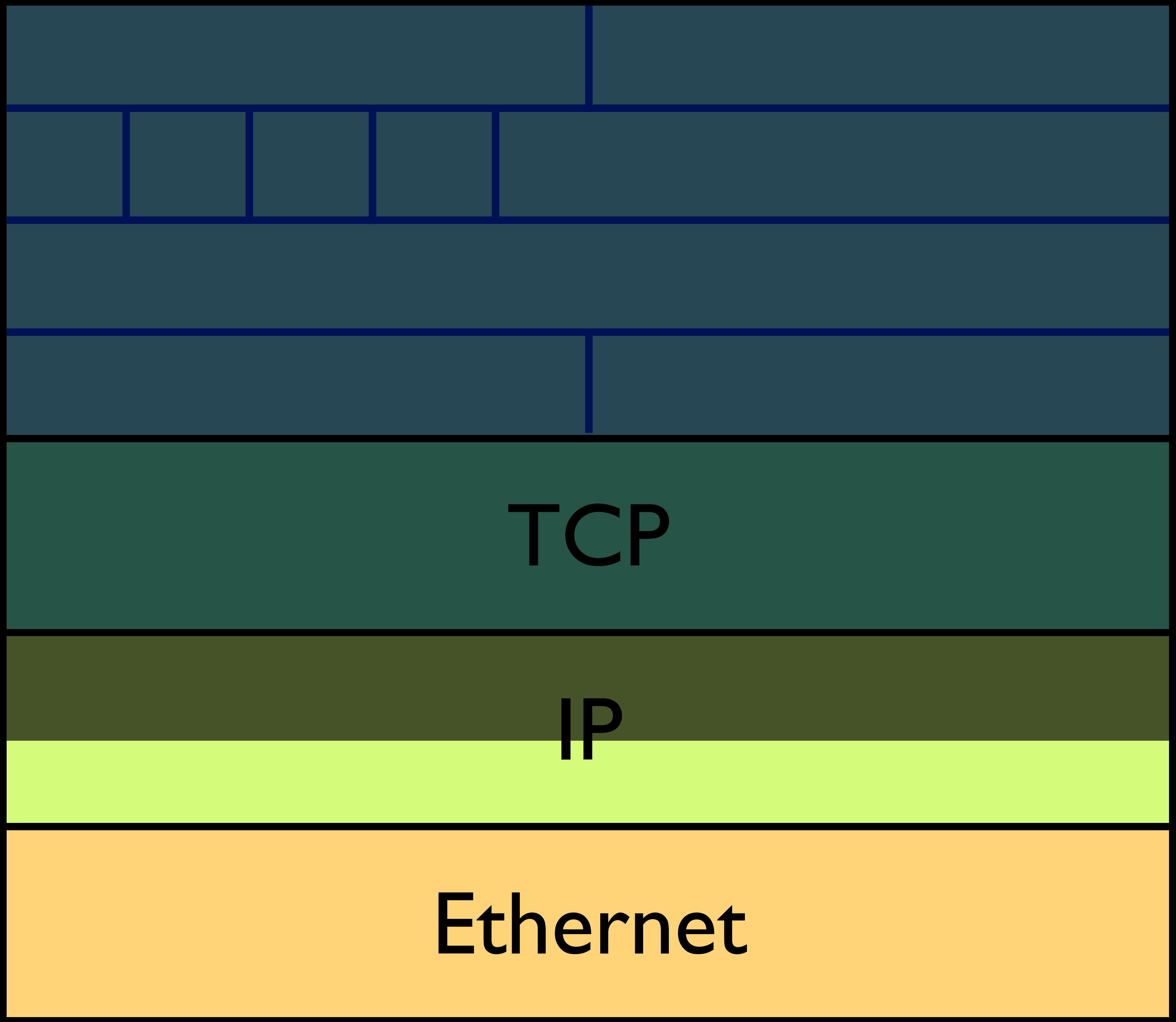
Ethernet



TCP

IP

Ethernet



TCP

IP

Ethernet

Current Age of Network Analysis

Current Age of Network Analysis

- Much harder to monitor other hosts (CALEA equip. excluded)

Current Age of Network Analysis

- Much harder to monitor other hosts (CALEA equip. excluded)
- Machines tightened down to external threats out of the box

Current Age of Network Analysis

- Much harder to monitor other hosts (CALEA equip. excluded)

- Machines tightened down to external threats out of the box

- Automatic software updates; vulnerabilities short-lived

Current Age of Network Analysis

- Much harder to monitor other hosts (CALEA equip. excluded)
- Machines tightened down to external threats out of the box
- Automatic software updates; vulnerabilities short-lived
- Ever increasing use of encryption

Current Age of Network Analysis

- Much harder to monitor other hosts (CALEA equip. excluded)
- Machines tightened down to external threats out of the box
- Automatic software updates; vulnerabilities short-lived
- Ever increasing use of encryption

- Weak passwords

Current Age of Network Analysis

- Much harder to monitor other hosts (CALEA equip. excluded)
- Machines tightened down to external threats out of the box
- Automatic software updates; vulnerabilities short-lived
- Ever increasing use of encryption
- Weak passwords
- Firewalls everywhere (on hosts too)

Current Age of Network Analysis

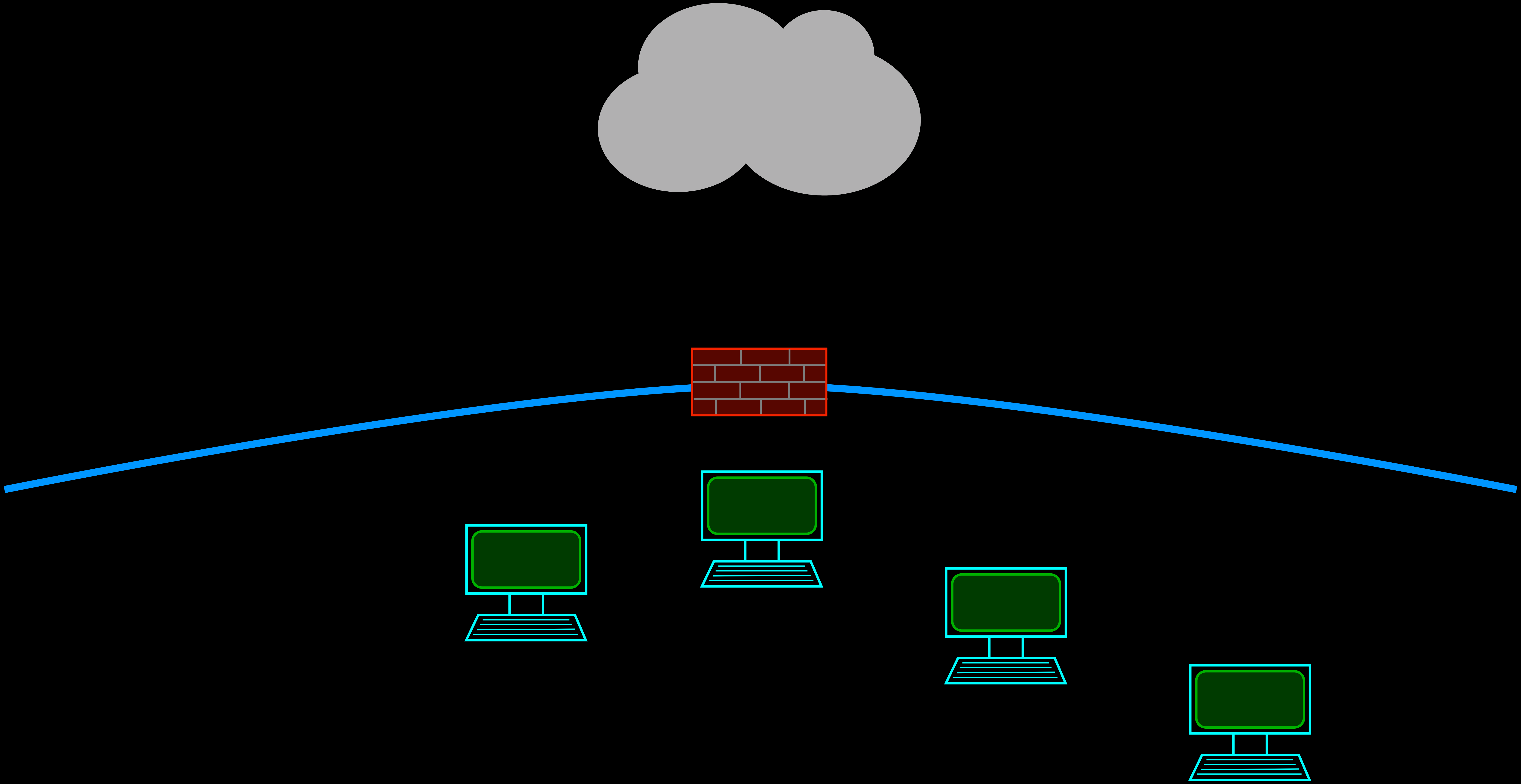
- Much harder to monitor other hosts (CALEA equip. excluded)
- Machines tightened down to external threats out of the box
- Automatic software updates; vulnerabilities short-lived
- Ever increasing use of encryption
- Weak passwords
- Firewalls everywhere (on hosts too)
- network mapping harder

Current Age of Network Analysis

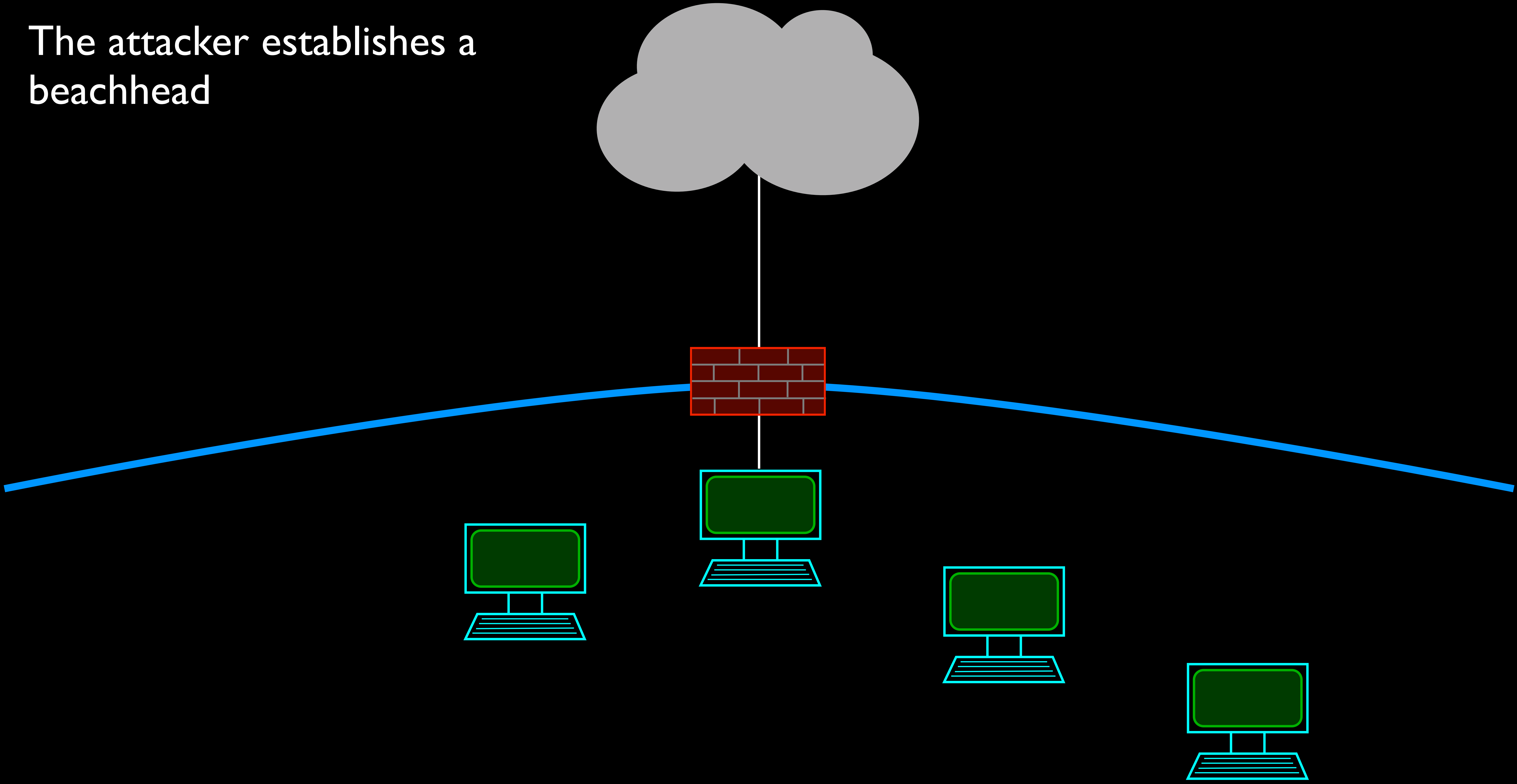
- Much harder to monitor other hosts (CALEA equip. excluded)
- Machines tightened down to external threats out of the box
- Automatic software updates; vulnerabilities short-lived
- Ever increasing use of encryption
- Weak passwords
- Firewalls everywhere (on hosts too)
- network mapping harder
- One IP address = many different hosts across time & space

Act 2: Why Network Analysis

Typical Attack Scenario

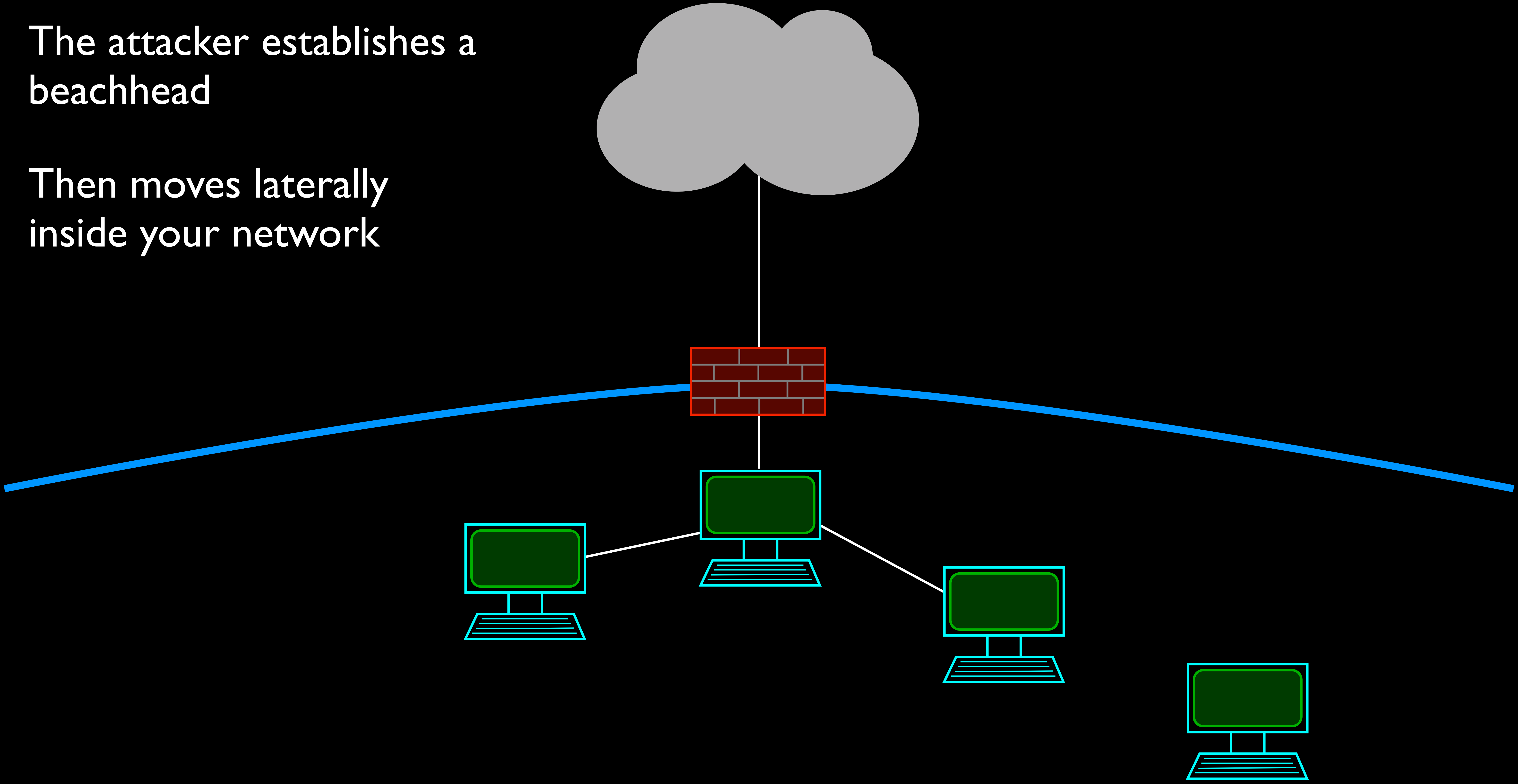


The attacker establishes a beachhead



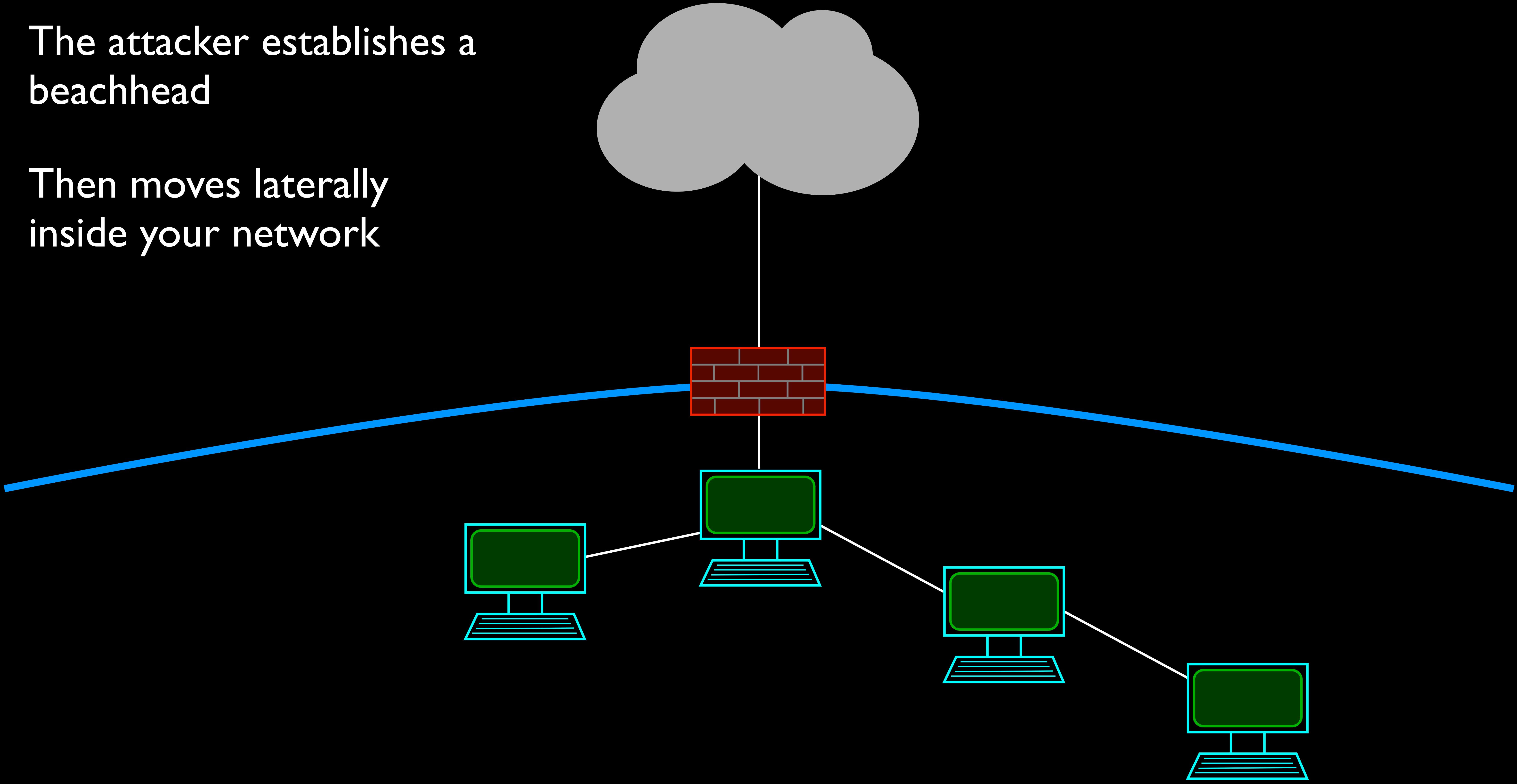
The attacker establishes a beachhead

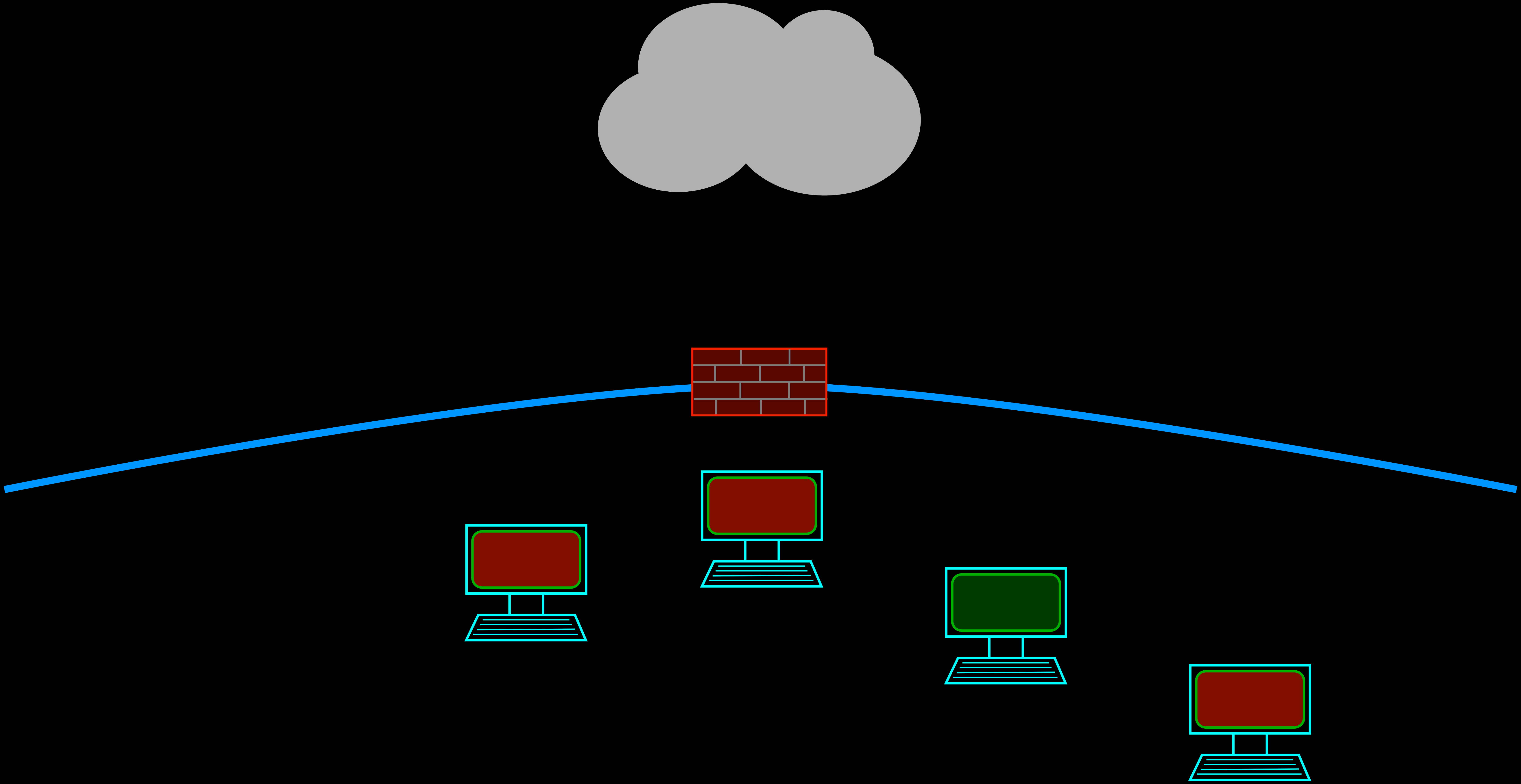
Then moves laterally inside your network



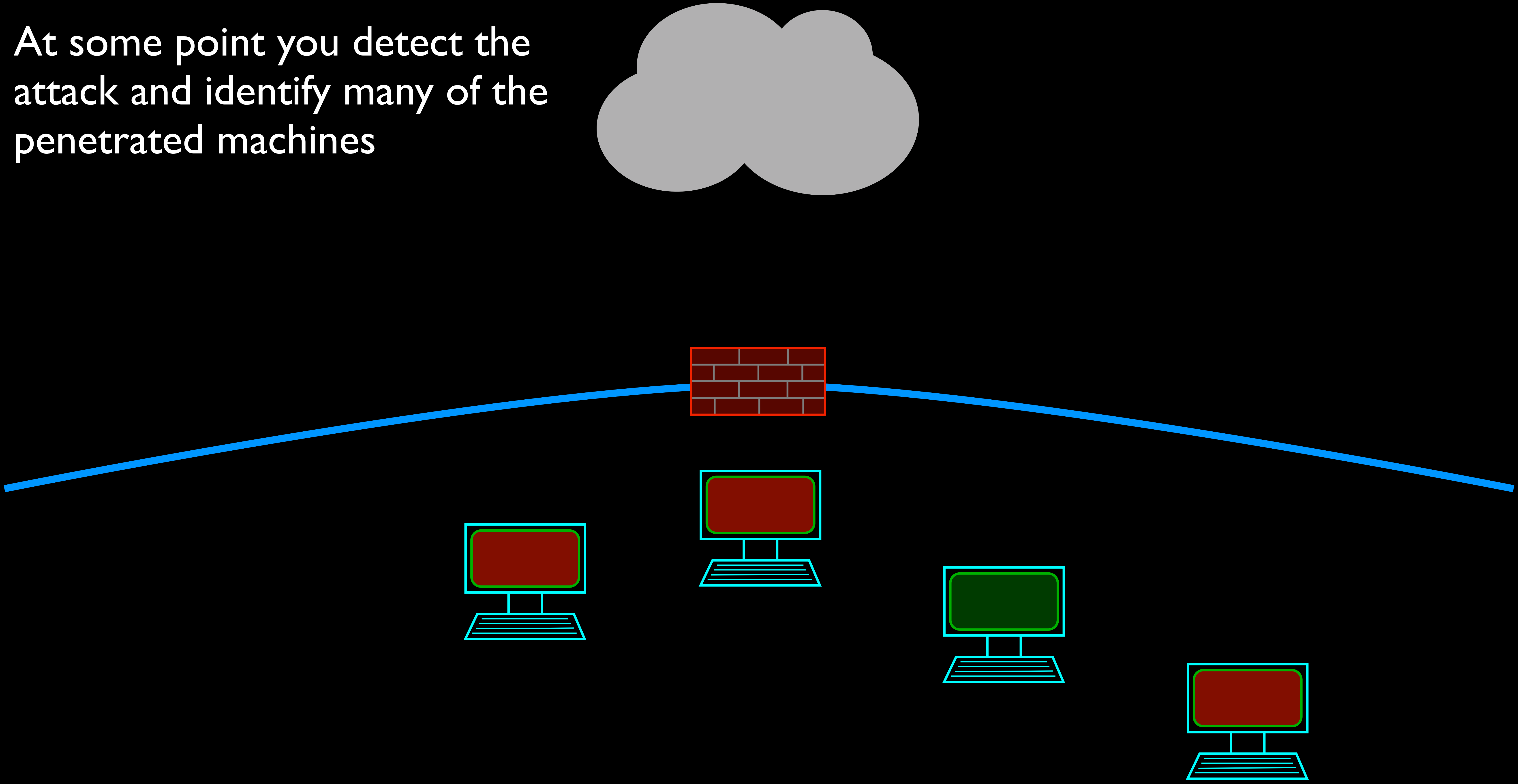
The attacker establishes a beachhead

Then moves laterally inside your network



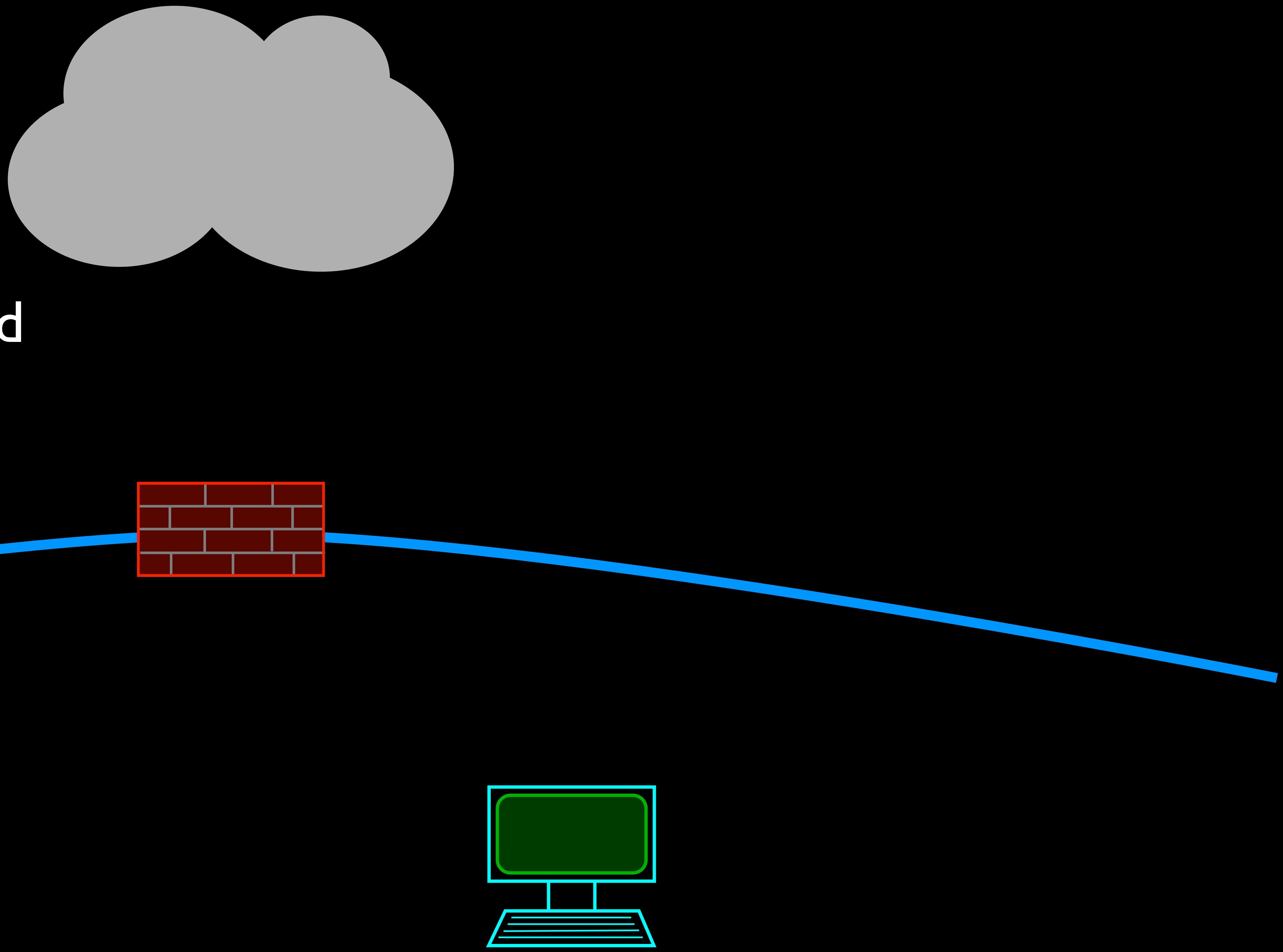


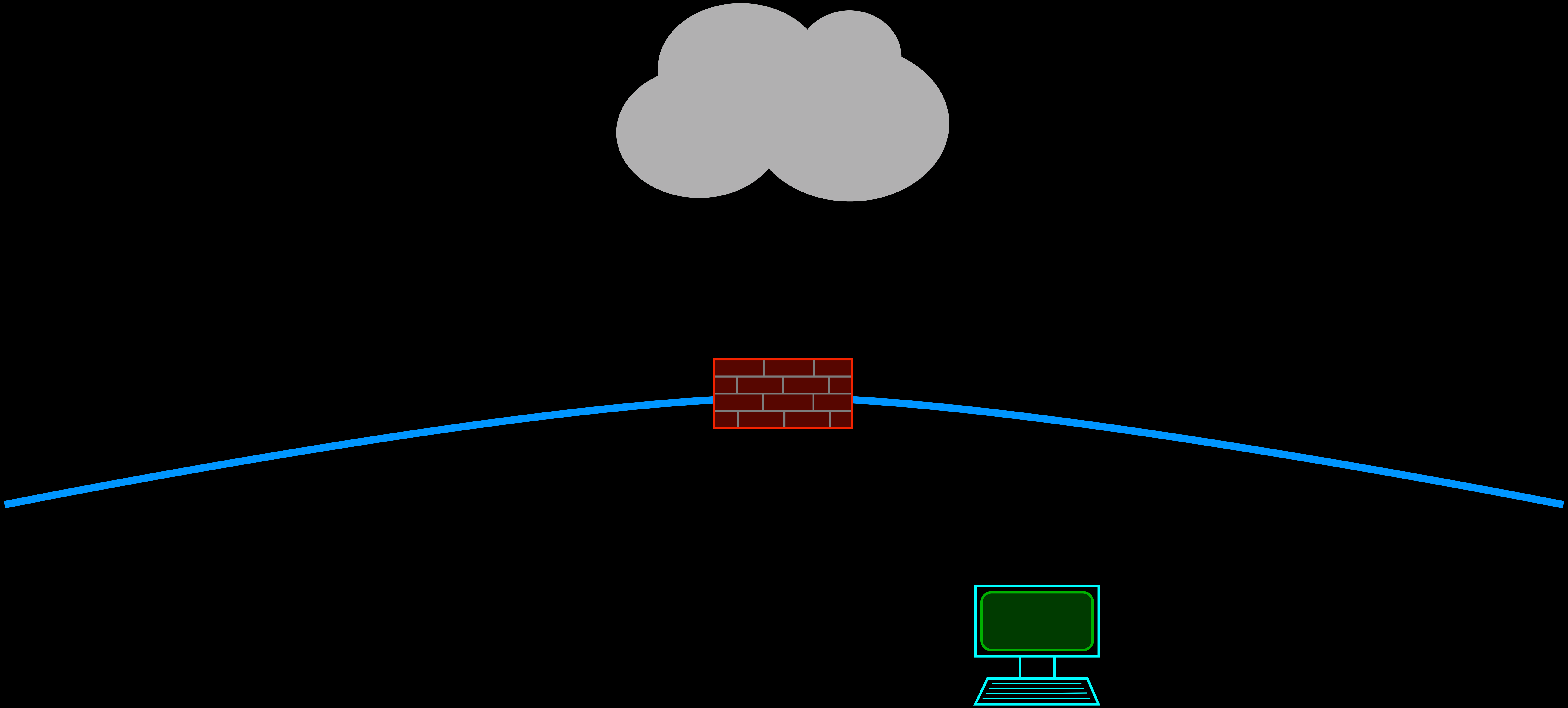
At some point you detect the attack and identify many of the penetrated machines



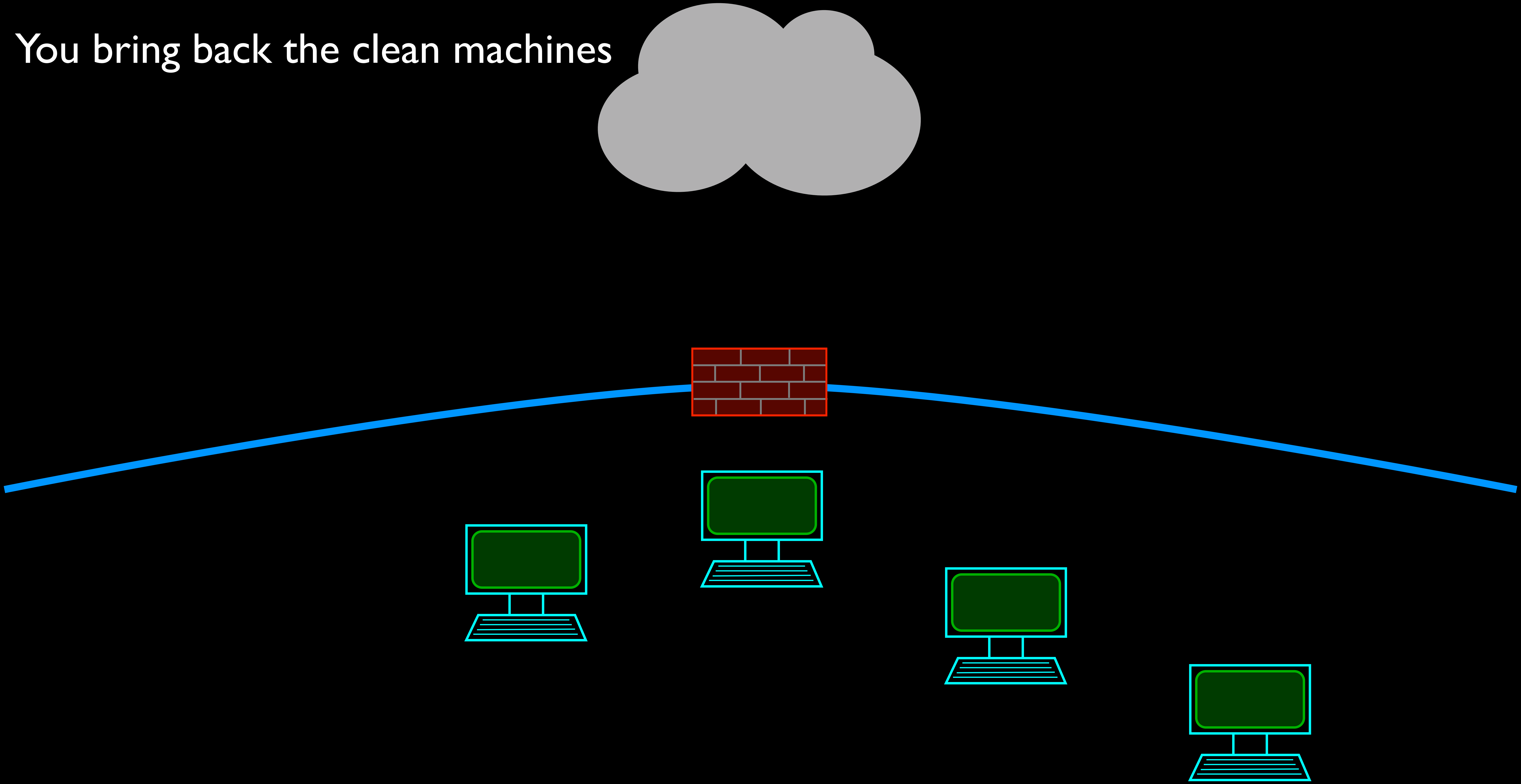
At some point you detect the attack and identify many of the penetrated machines

Your take them out of service and scrub them



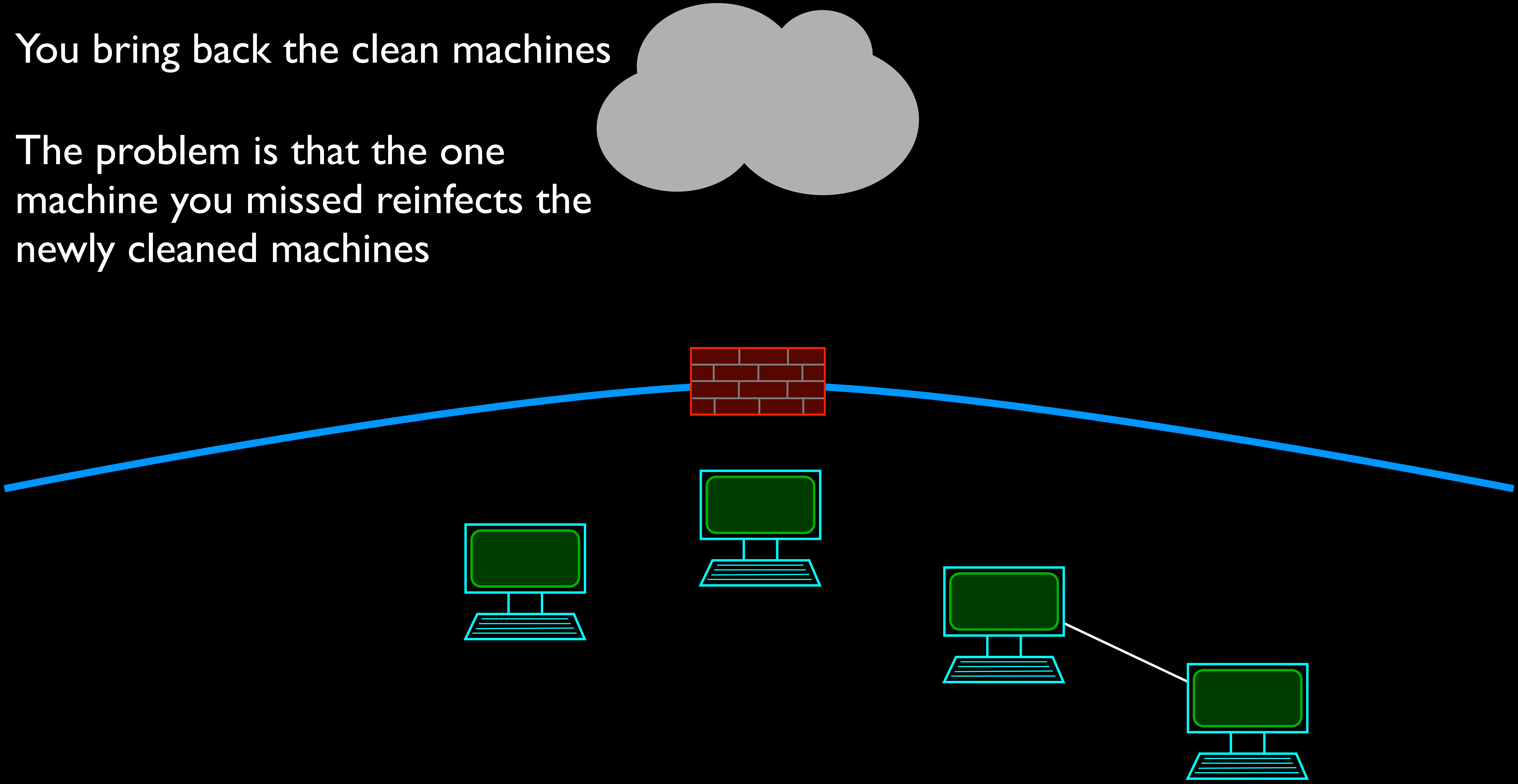


You bring back the clean machines



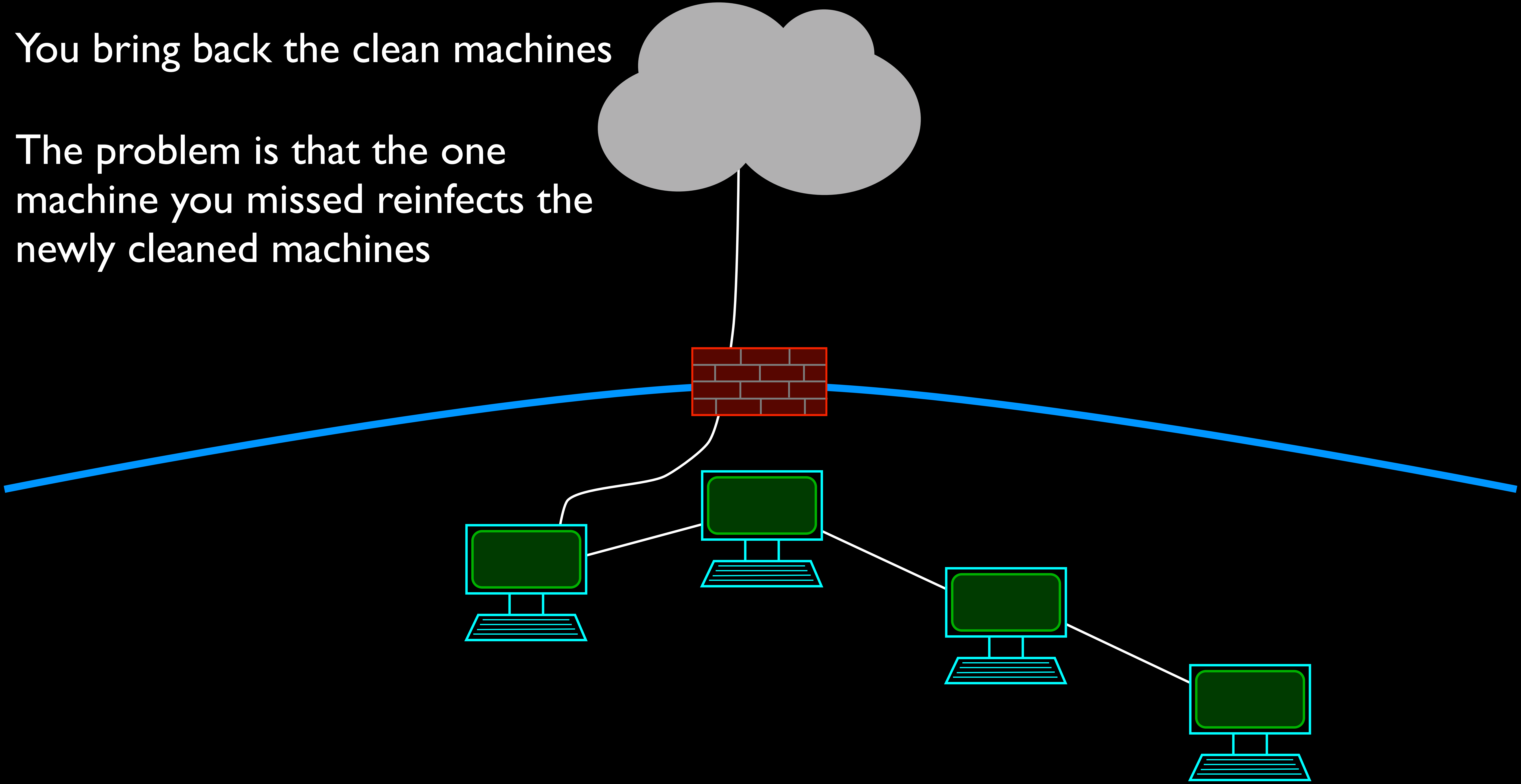
You bring back the clean machines

The problem is that the one machine you missed reinfects the newly cleaned machines

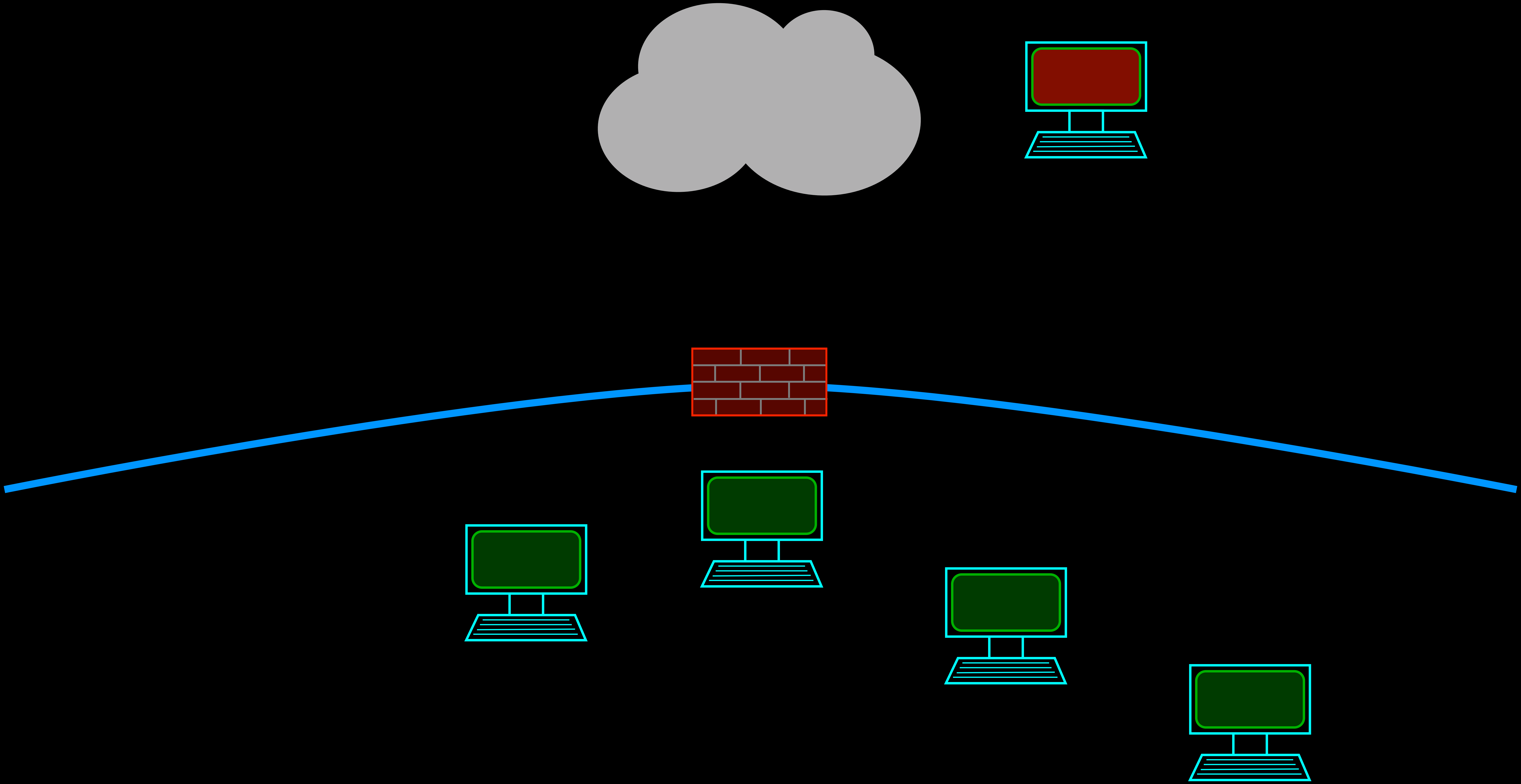


You bring back the clean machines

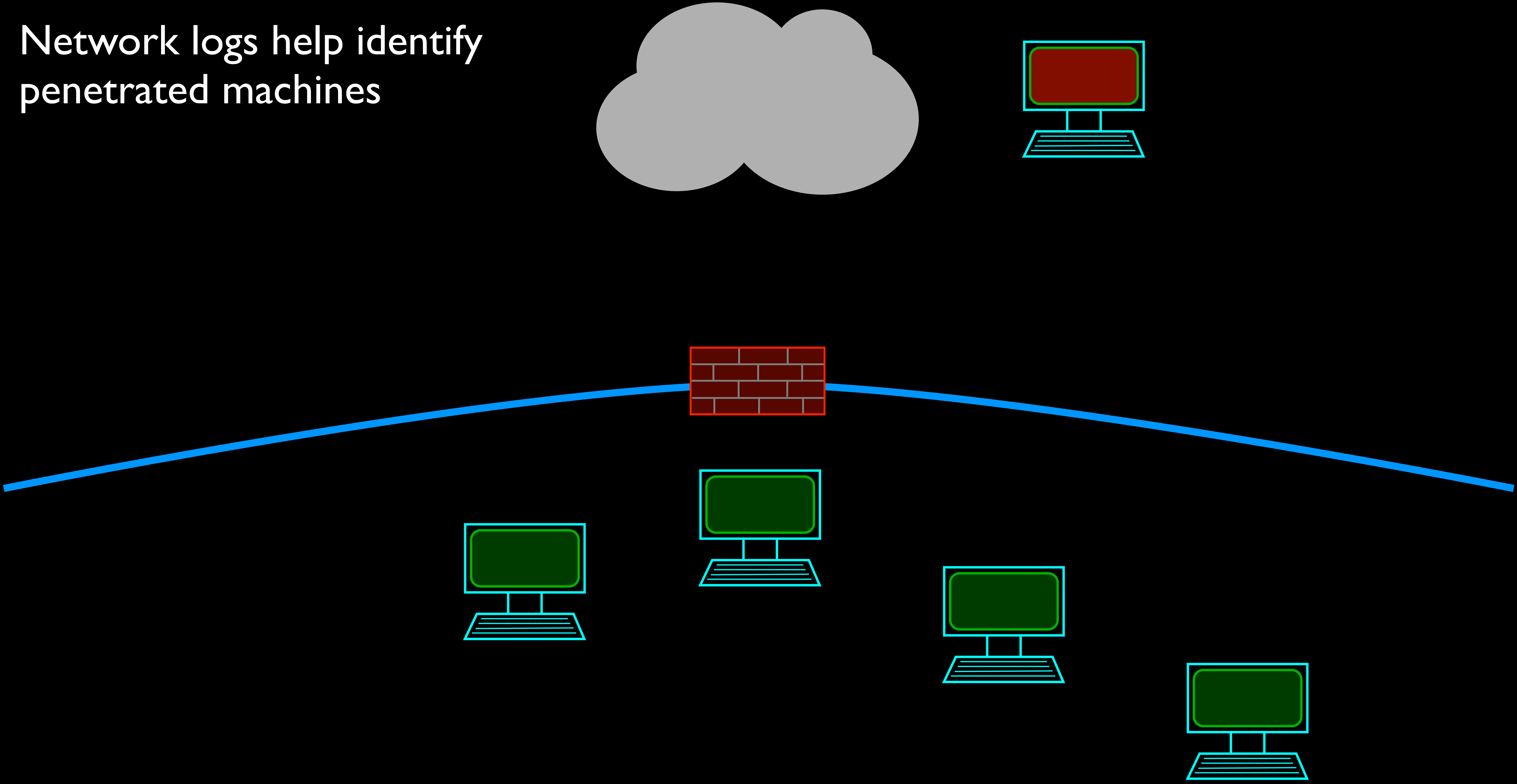
The problem is that the one machine you missed reinfects the newly cleaned machines



Using network logs to help spot infected systems

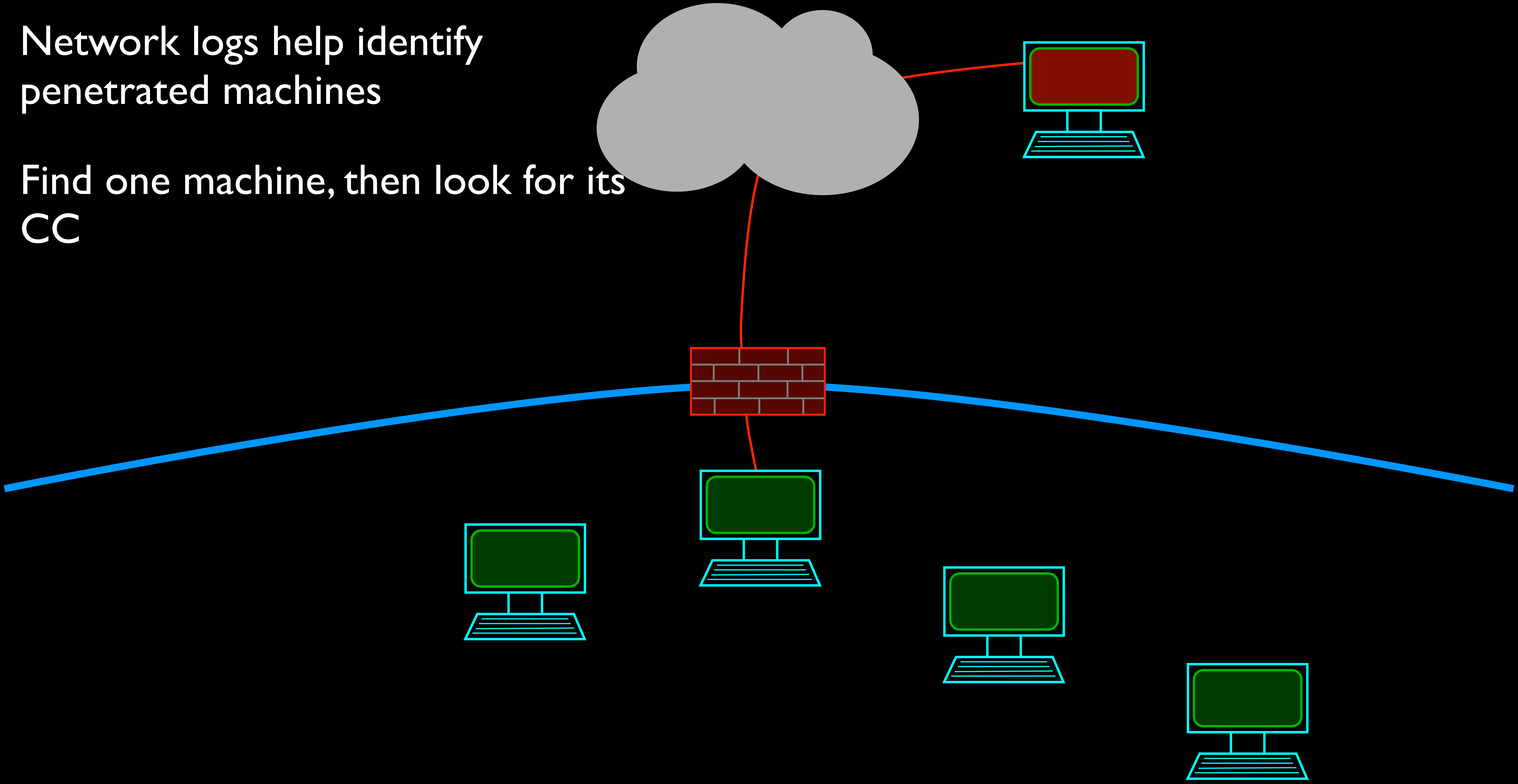


Network logs help identify penetrated machines



Network logs help identify penetrated machines

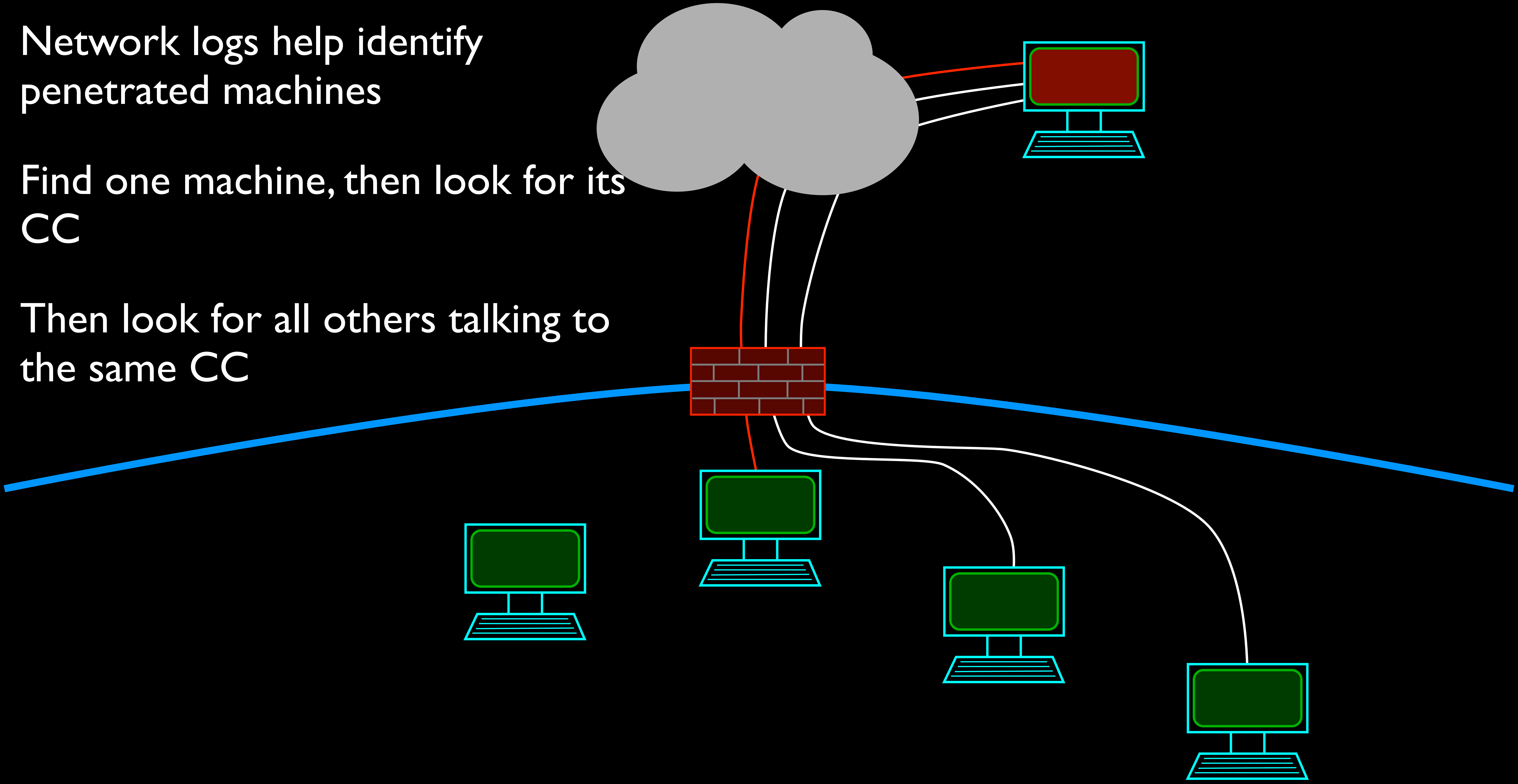
Find one machine, then look for its CC



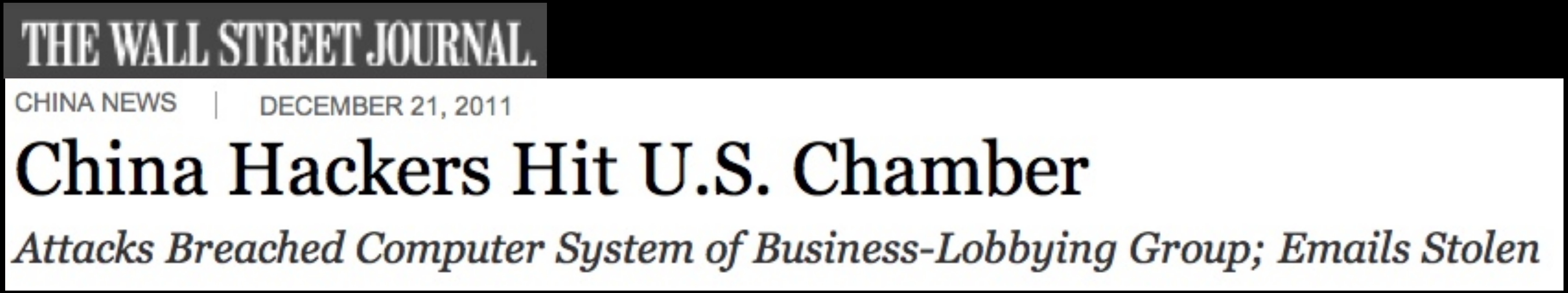
Network logs help identify penetrated machines

Find one machine, then look for its CC

Then look for all others talking to the same CC



Network logs may be your only detection & forensics source

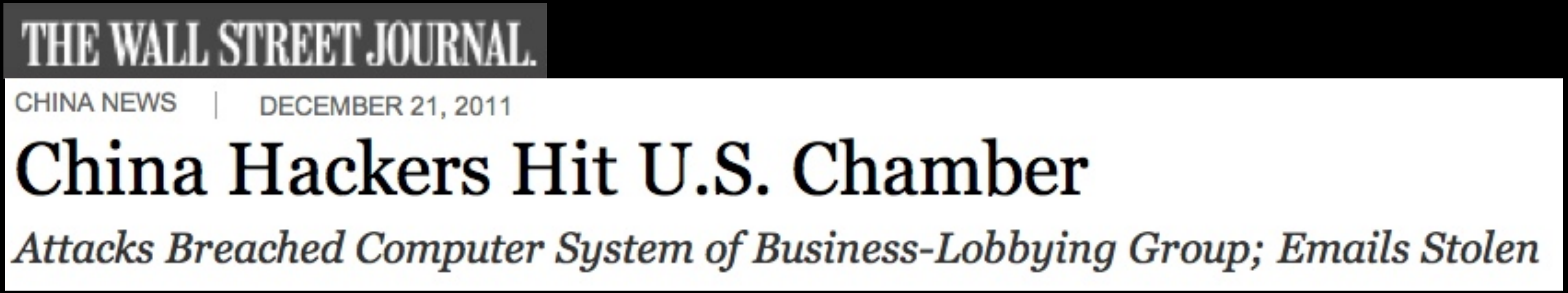


THE WALL STREET JOURNAL.

CHINA NEWS | DECEMBER 21, 2011

China Hackers Hit U.S. Chamber

Attacks Breached Computer System of Business-Lobbying Group; Emails Stolen



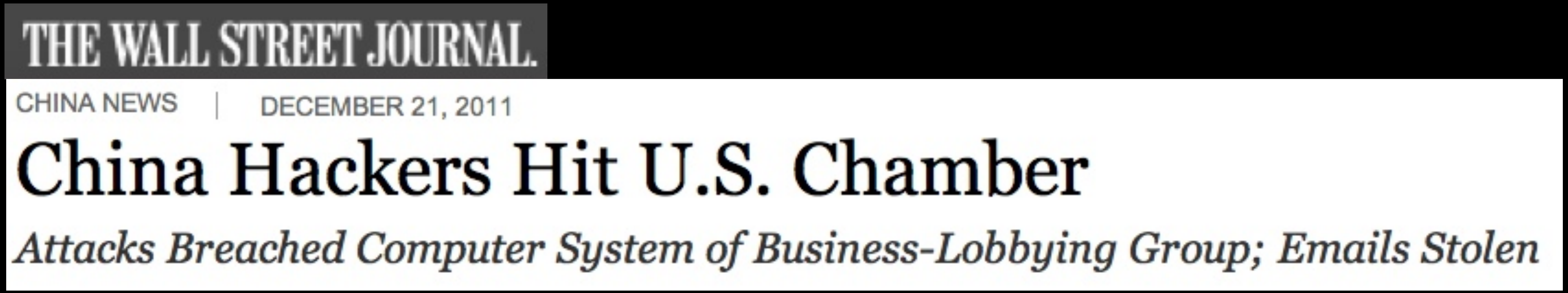
THE WALL STREET JOURNAL.

CHINA NEWS | DECEMBER 21, 2011

China Hackers Hit U.S. Chamber

Attacks Breached Computer System of Business-Lobbying Group; Emails Stolen

“The Chamber continues to see suspicious activity, they say. A thermostat at a town house the Chamber owns on Capitol Hill at one point was communicating with an Internet address in China”



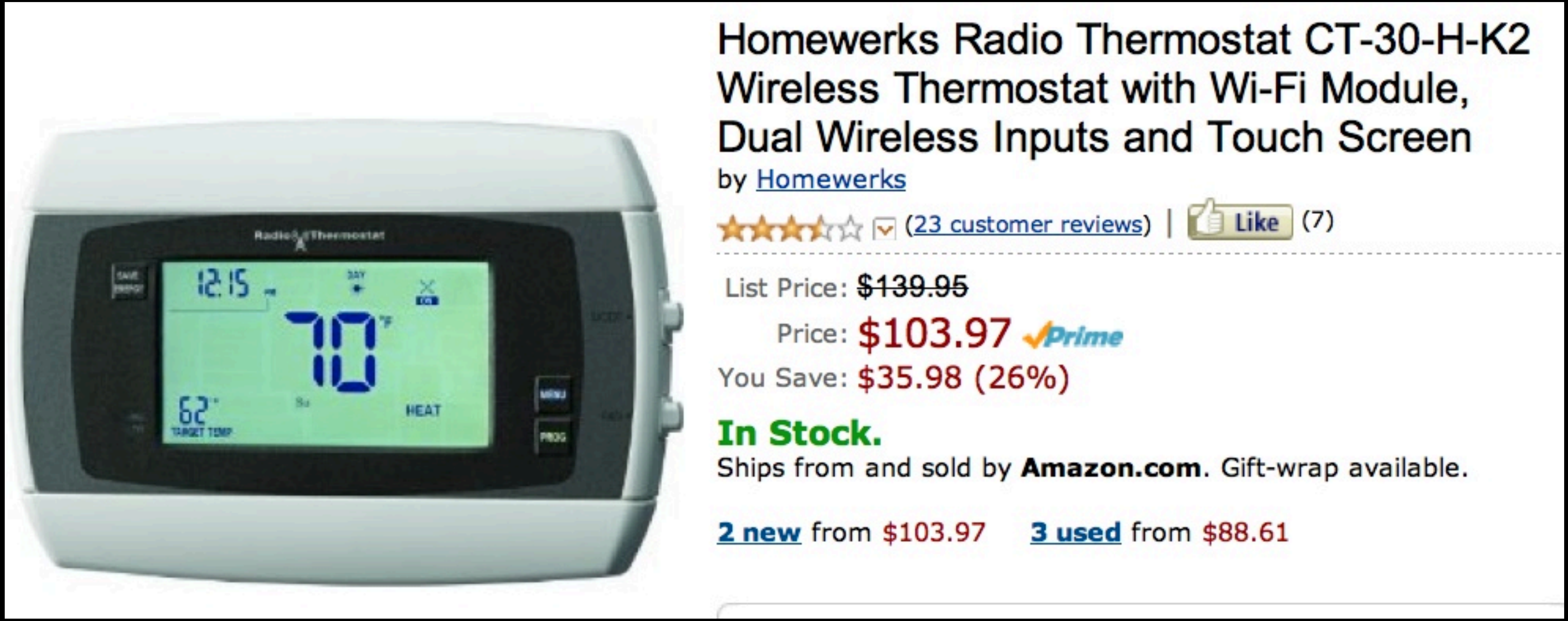
THE WALL STREET JOURNAL.

CHINA NEWS | DECEMBER 21, 2011

China Hackers Hit U.S. Chamber

Attacks Breached Computer System of Business-Lobbying Group; Emails Stolen

"The Chamber continues to see suspicious activity, they say. A thermostat at a town house the Chamber owns on Capitol Hill at one point was communicating with an Internet address in China"



Homewerks Radio Thermostat CT-30-H-K2 Wireless Thermostat with Wi-Fi Module, Dual Wireless Inputs and Touch Screen

by Homewerks

★★★½☆ (23 customer reviews) | Like (7)

List Price: ~~$139.95~~

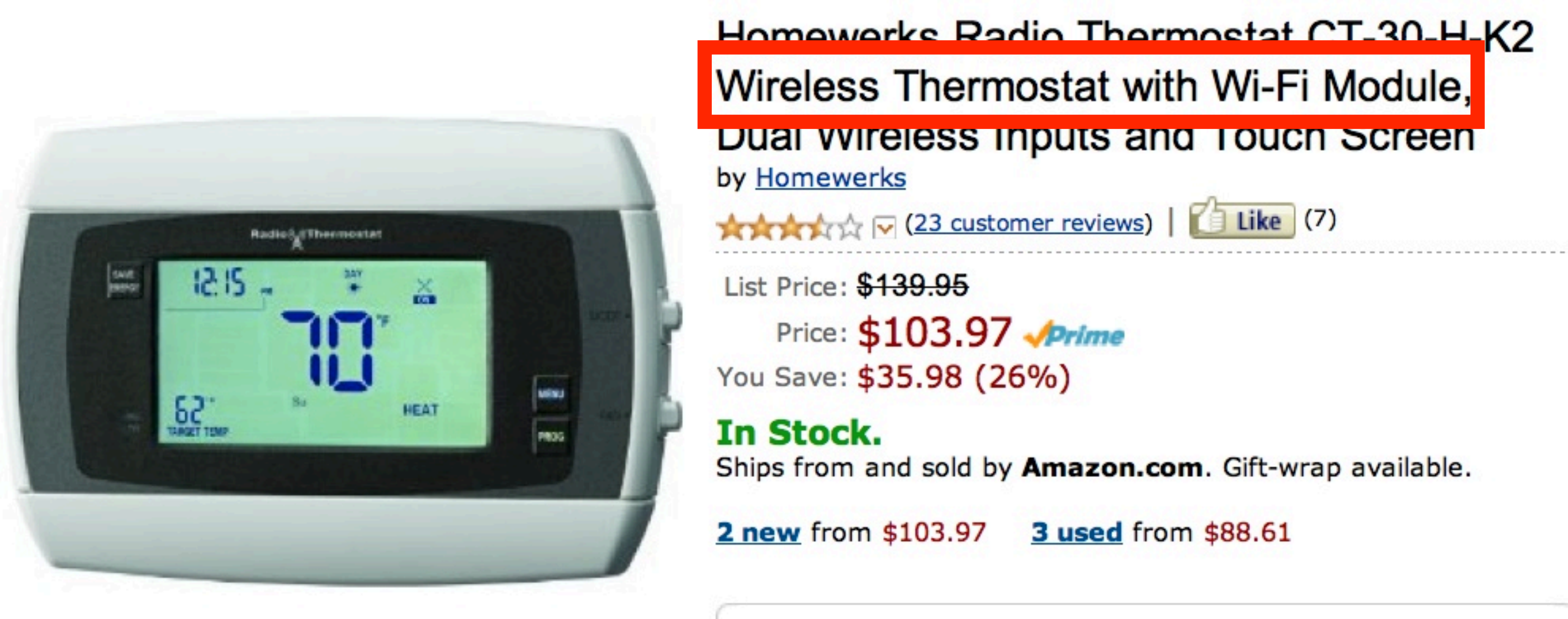
Price: $103.97 ✓Prime

You Save: $35.98 (26%)

In Stock.

Ships from and sold by **Amazon.com**. Gift-wrap available.

2 new from $103.97 **3 used** from $88.61



Homewerks Radio Thermostat CT-30-H-K2 Wireless Thermostat with Wi-Fi Module, Dual Wireless Inputs and Touch Screen

by Homewerks

★★★½☆ (23 customer reviews) | Like (7)

List Price: ~~$139.95~~

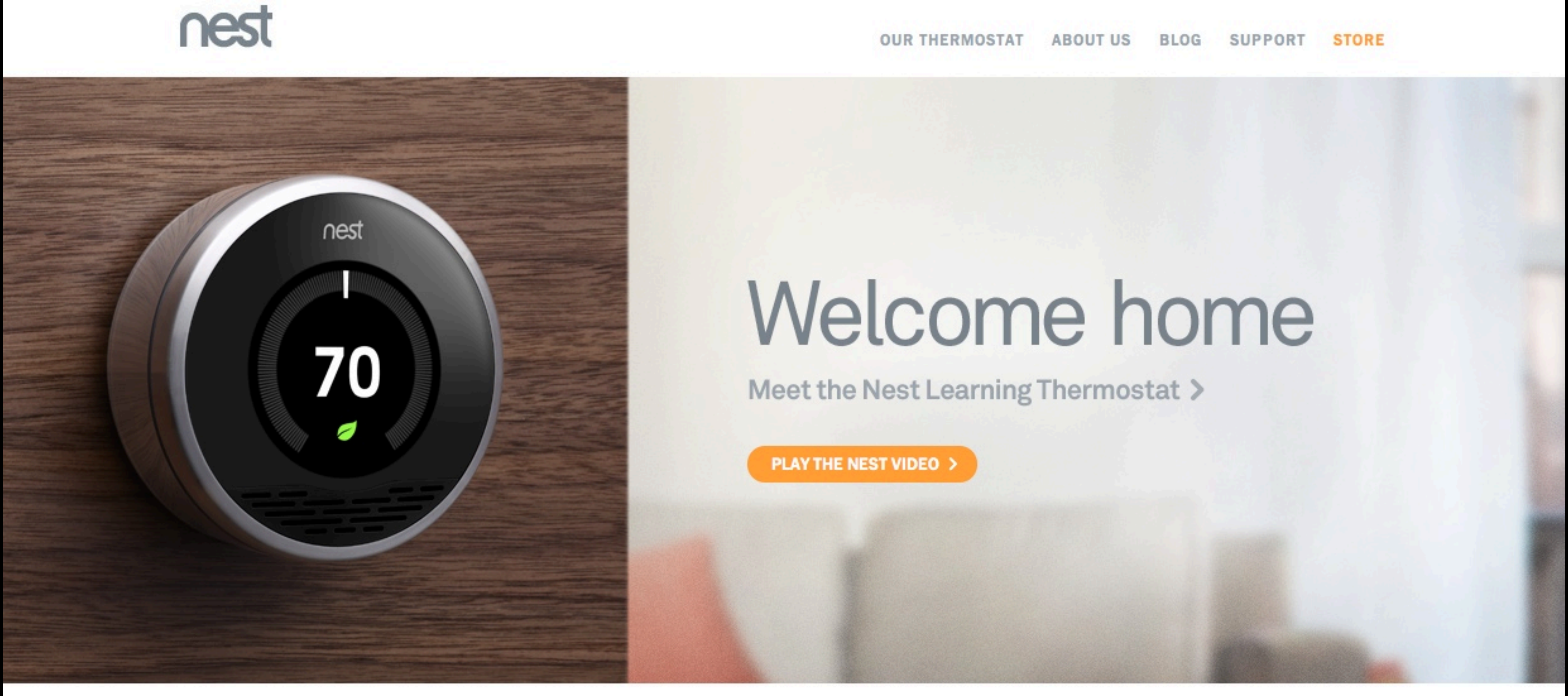
Price: $103.97 ✓Prime

You Save: $35.98 (26%)

In Stock.

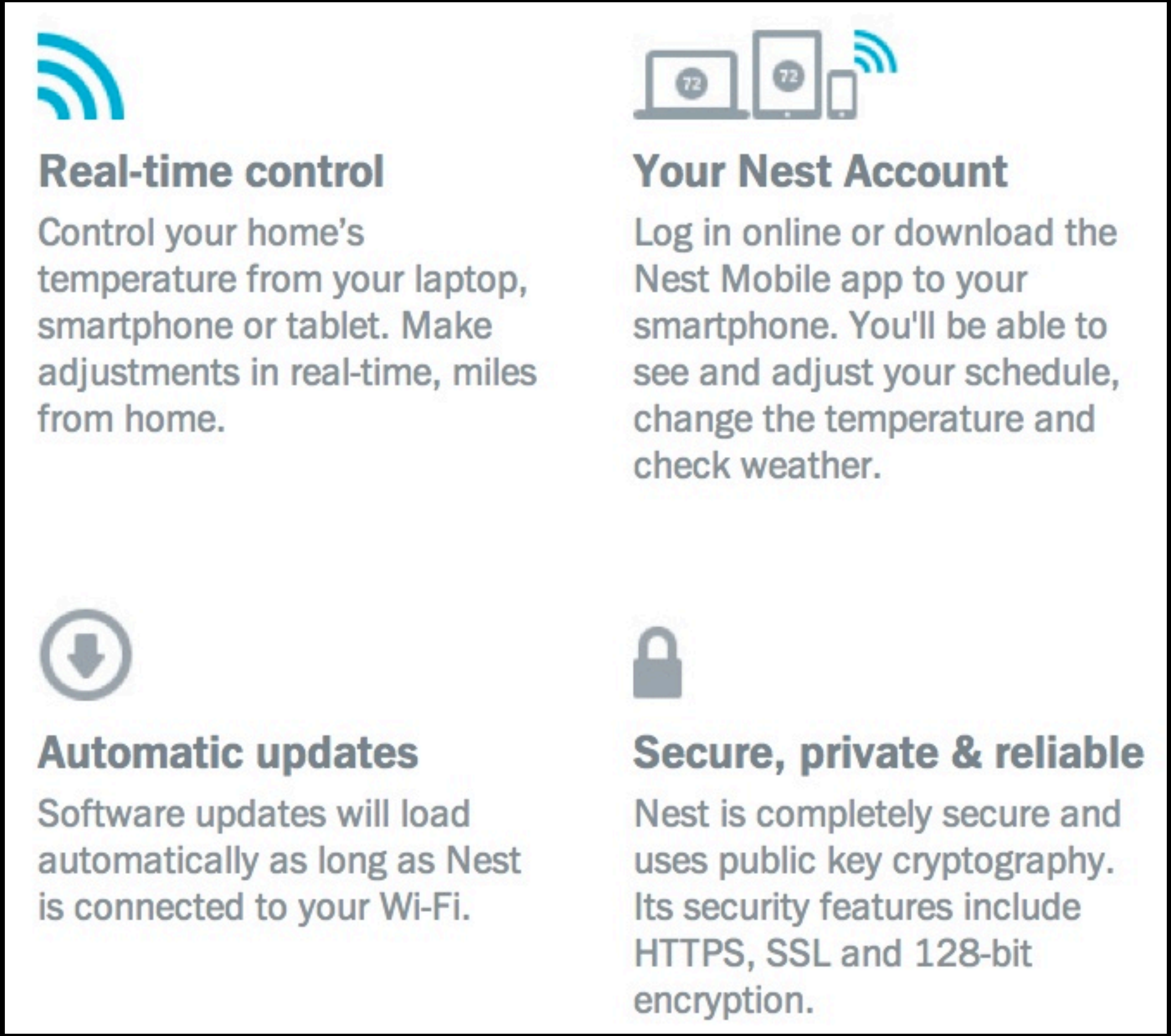
Ships from and sold by **Amazon.com**. Gift-wrap available.

2 new from $103.97 **3 used** from $88.61



Welcome home

Meet the Nest Learning Thermostat >



Real-time control

Control your home's temperature from your laptop, smartphone or tablet. Make adjustments in real-time, miles from home.

Your Nest Account

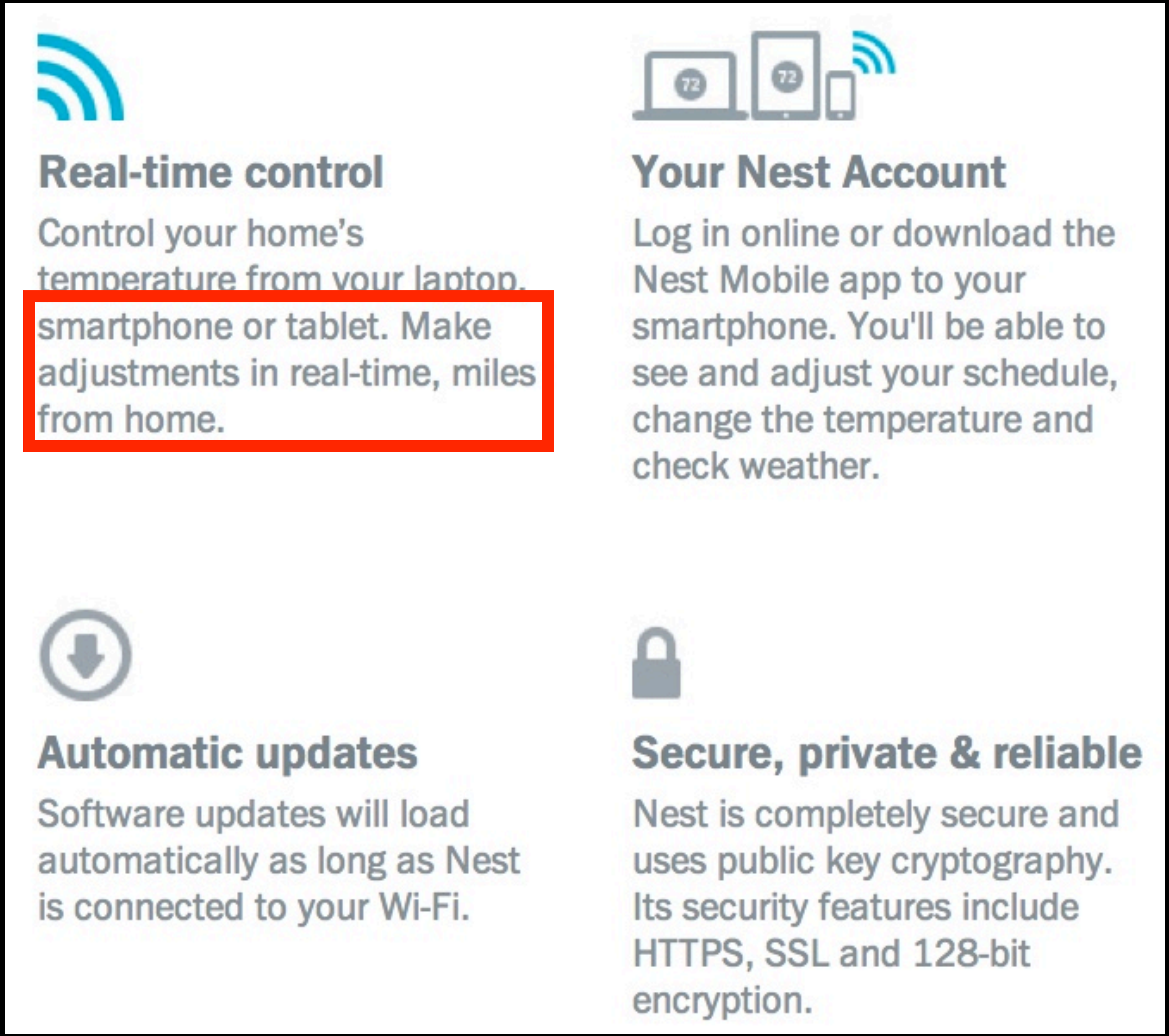
Log in online or download the Nest Mobile app to your smartphone. You'll be able to see and adjust your schedule, change the temperature and check weather.

Automatic updates

Software updates will load automatically as long as Nest is connected to your Wi-Fi.

Secure, private & reliable

Nest is completely secure and uses public key cryptography. Its security features include HTTPS, SSL and 128-bit encryption.



Real-time control

Control your home’s temperature from your laptop, smartphone or tablet. Make adjustments in real-time, miles from home.

Your Nest Account

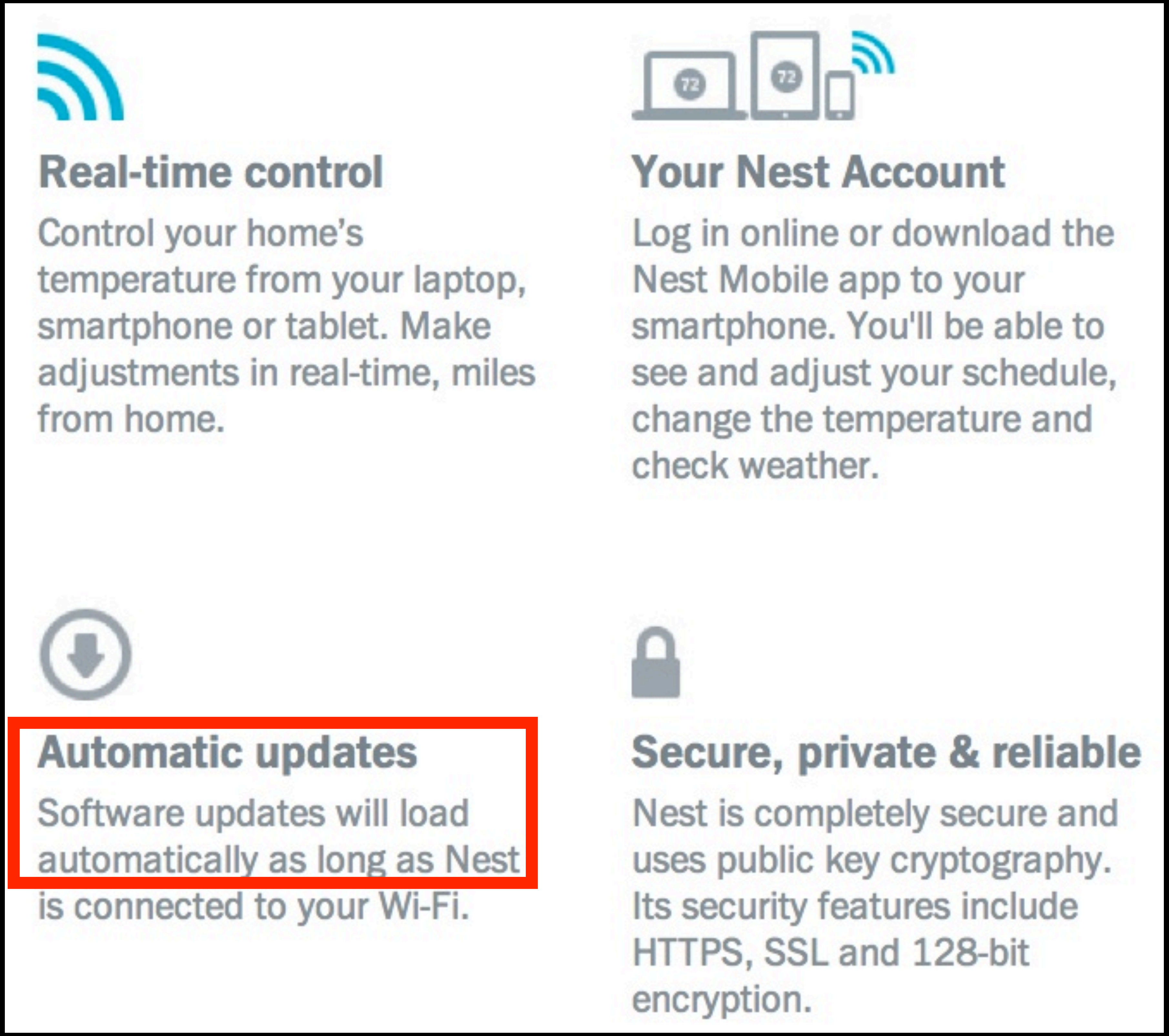
Log in online or download the Nest Mobile app to your smartphone. You'll be able to see and adjust your schedule, change the temperature and check weather.

Automatic updates

Software updates will load automatically as long as Nest is connected to your Wi-Fi.

Secure, private & reliable

Nest is completely secure and uses public key cryptography. Its security features include HTTPS, SSL and 128-bit encryption.



Real-time control

Control your home's temperature from your laptop, smartphone or tablet. Make adjustments in real-time, miles from home.

Your Nest Account

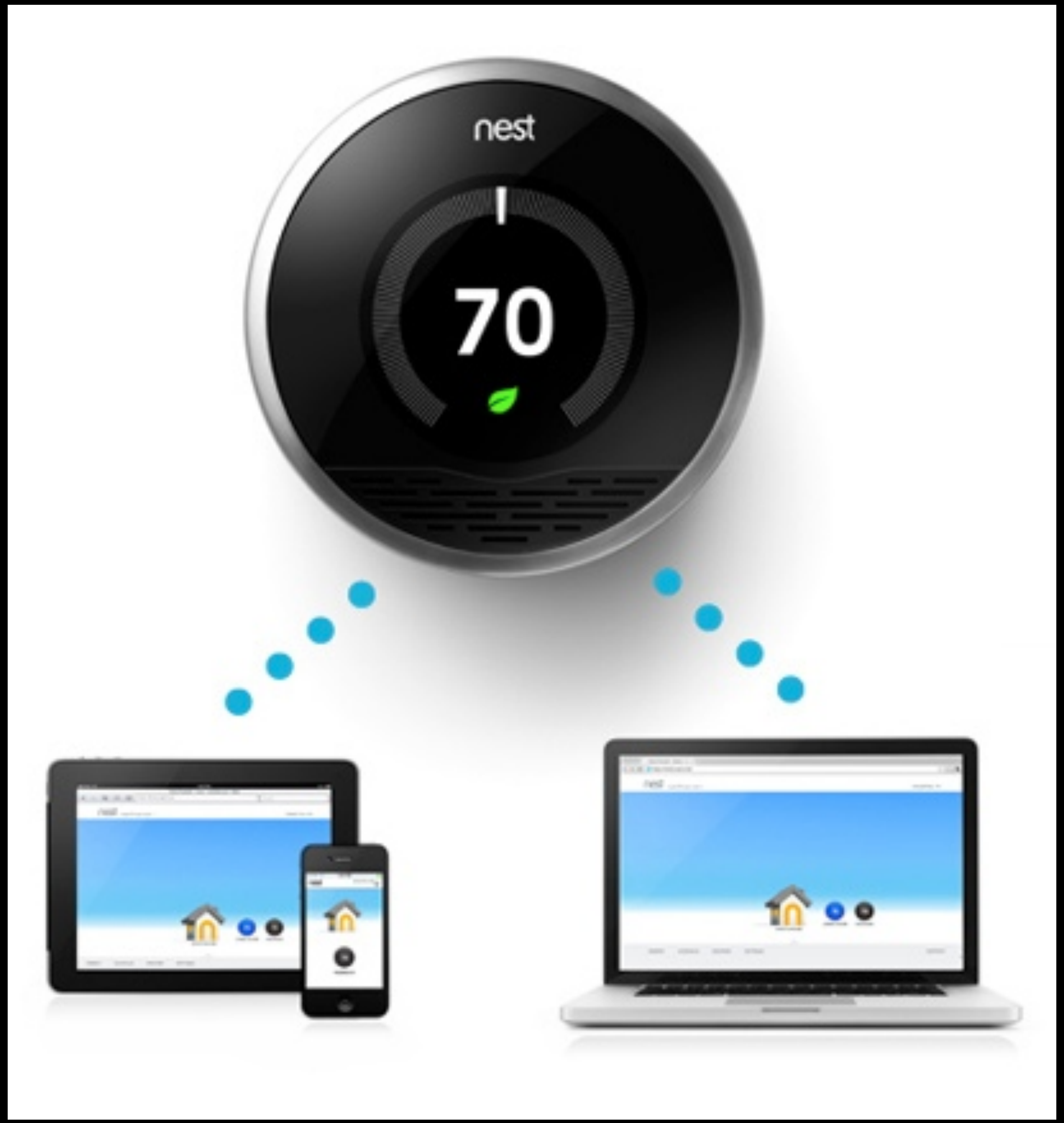
Log in online or download the Nest Mobile app to your smartphone. You'll be able to see and adjust your schedule, change the temperature and check weather.

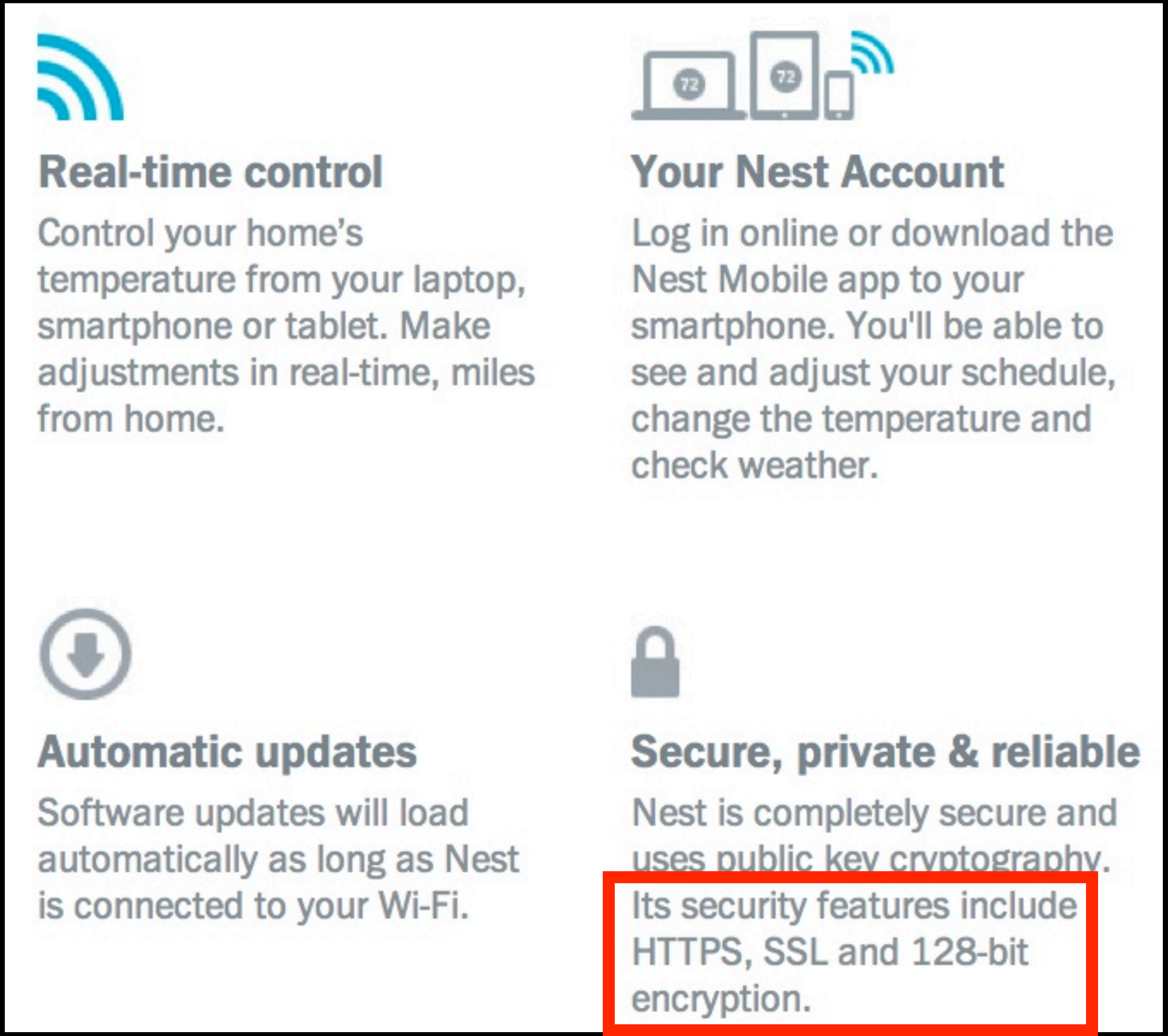
Automatic updates

Software updates will load automatically as long as Nest is connected to your Wi-Fi.

Secure, private & reliable

Nest is completely secure and uses public key cryptography. Its security features include HTTPS, SSL and 128-bit encryption.





Real-time control

Control your home's temperature from your laptop, smartphone or tablet. Make adjustments in real-time, miles from home.

Your Nest Account

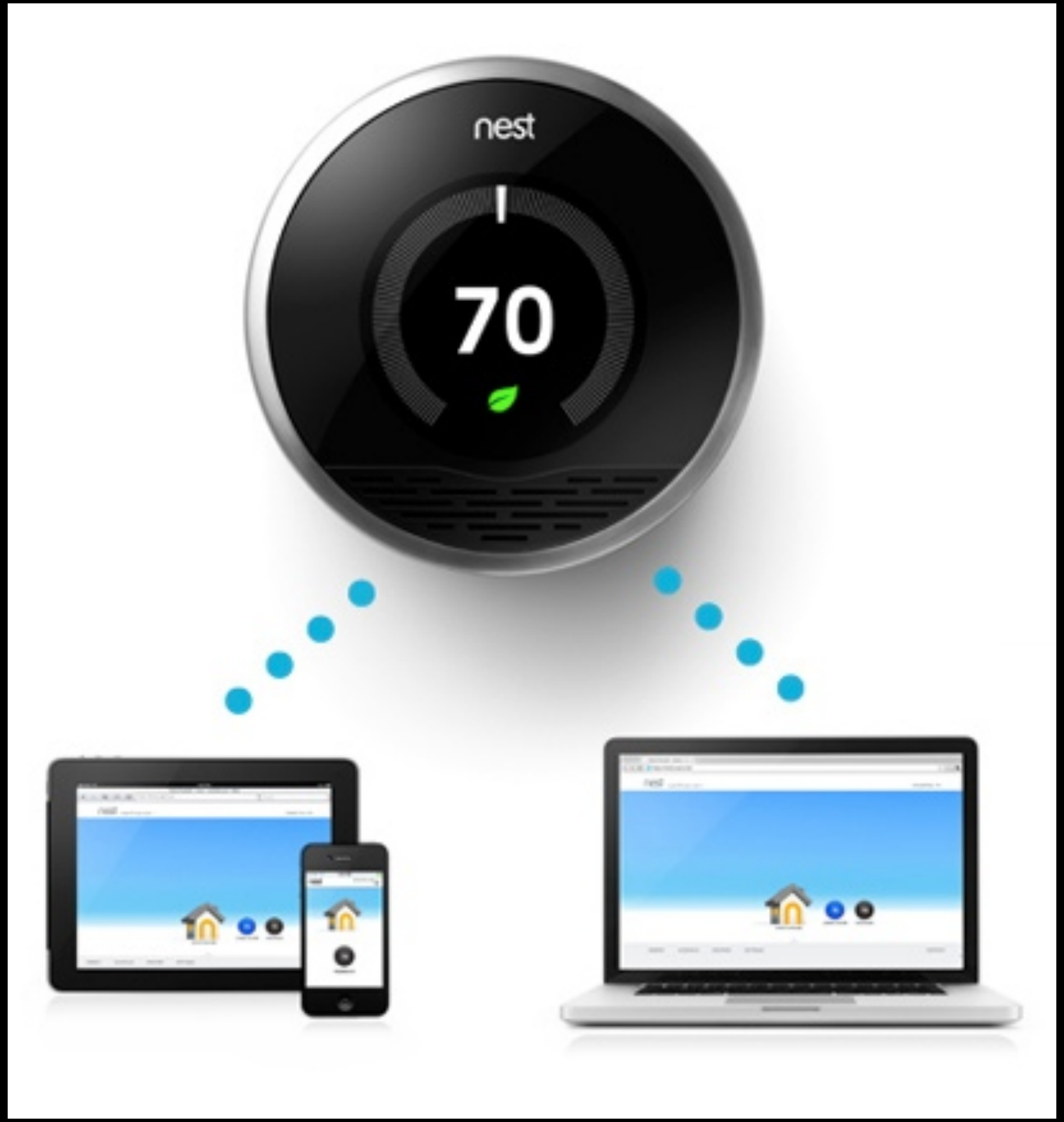
Log in online or download the Nest Mobile app to your smartphone. You'll be able to see and adjust your schedule, change the temperature and check weather.

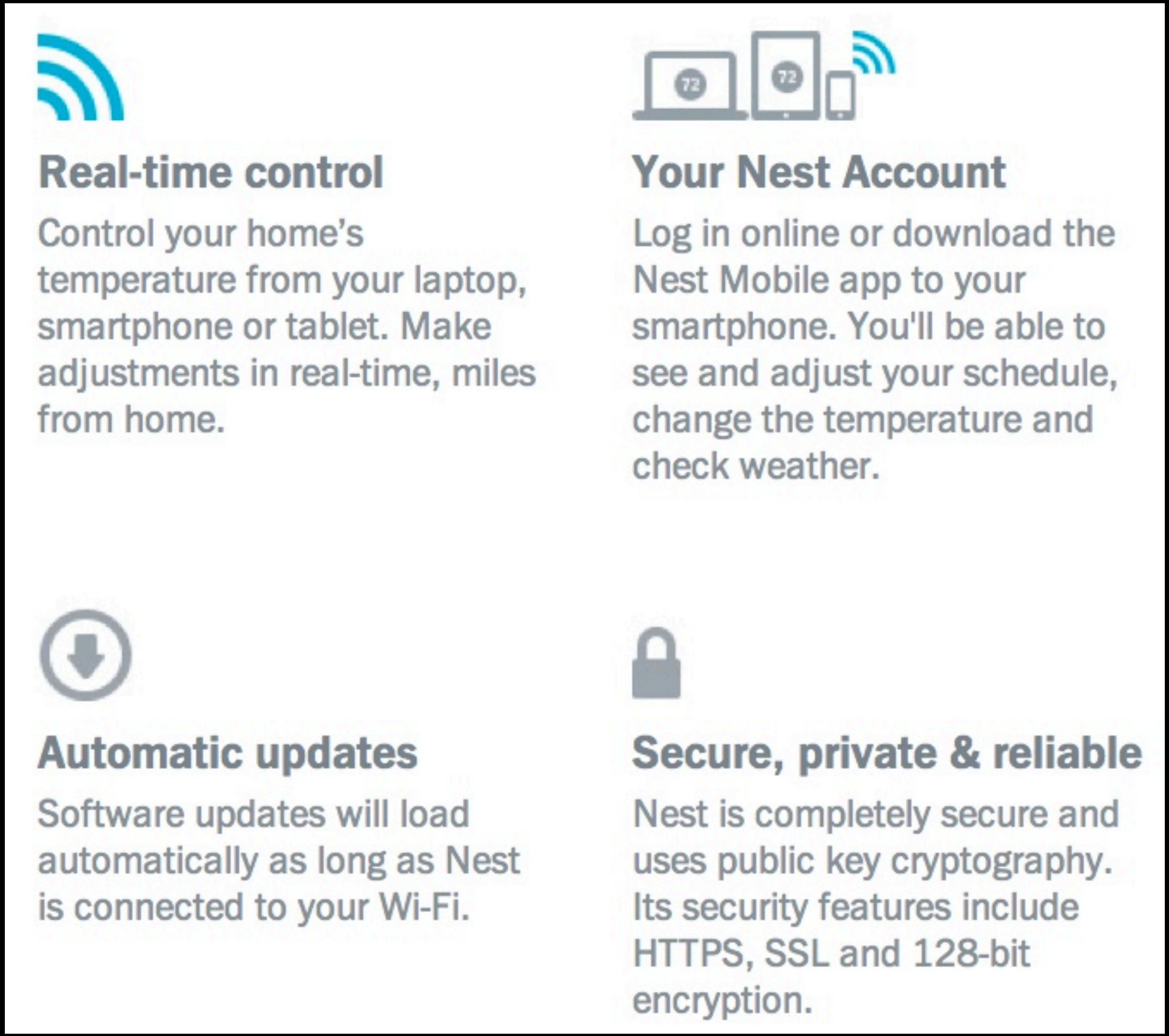
Automatic updates

Software updates will load automatically as long as Nest is connected to your Wi-Fi.

Secure, private & reliable

Nest is completely secure and uses public key cryptography. Its security features include HTTPS, SSL and 128-bit encryption.





Real-time control

Control your home's temperature from your laptop, smartphone or tablet. Make adjustments in real-time, miles from home.

Your Nest Account

Log in online or download the Nest Mobile app to your smartphone. You'll be able to see and adjust your schedule, change the temperature and check weather.

Automatic updates

Software updates will load automatically as long as Nest is connected to your Wi-Fi.

Secure, private & reliable

Nest is completely secure and uses public key cryptography. Its security features include HTTPS, SSL and 128-bit encryption.

The 88MZ100 ZigBee software stack features a set of host APIs that provide users full control of the light bulb via the Marvell Wi-Fi / ZigBee Gateway reference design. Using ZigBee's cost-effective green and global wireless networking standard, the 88MZ100 and Marvell Wi-Fi/ZigBee gateway enable consumers to seamlessly control their household devices from their mobile phone, connected consumer electronics device or dedicated website through an intuitive user interface (UI).

http://www.marketwatch.com/story/marvell-introduces-new-four-in-one-zigbee-microcontroller-soc-delivering-the-highest-level-of-integration-in-the-industry-2012-01-09

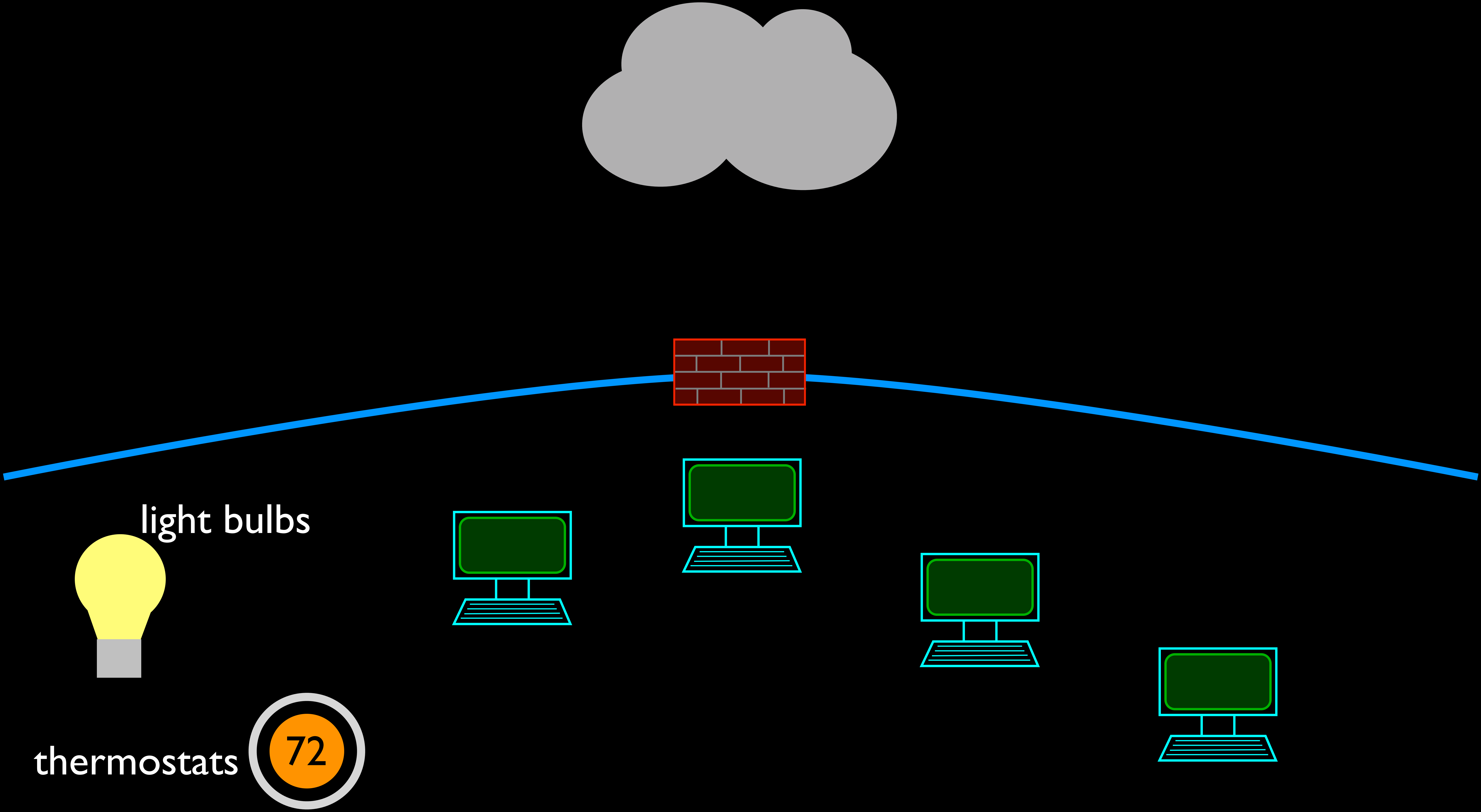
The 88MZ100 ZigBee software stack features a set of host APIs that provide users full control of the light bulb via the Marvell Wi-Fi / ZigBee Gateway reference design. Using ZigBee's cost-effective green and global wireless networking standard, the 88MZ100 and Marvell Wi-Fi/ZigBee gateway enable consumers to seamlessly control their household devices from their mobile phone, connected consumer electronics device or dedicated website through an intuitive user interface (UI).

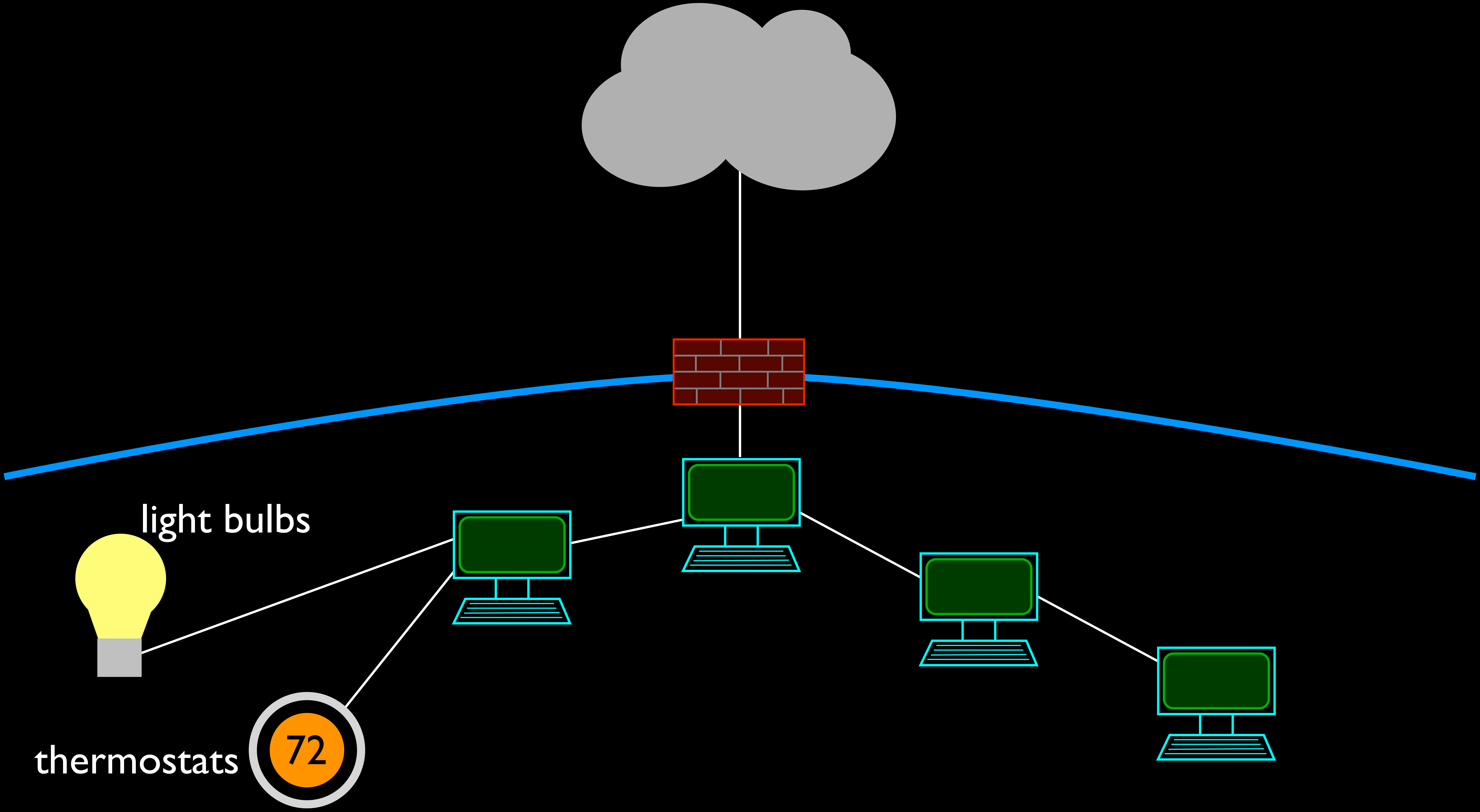
http://www.marketwatch.com/story/marvell-introduces-new-four-in-one-zigbee-microcontroller-soc-delivering-the-highest-level-of-integration-in-the-industry-2012-01-09

The 88MZ100 ZigBee software stack features a set of host APIs that
provide users full control of the light bulb via the Marvell Wi-Fi /
ZigBee ffective
green ar 100 and
Marve nlessly
control their household devices from their mobile phone, connected
consumer electronics device or dedicated website through an
intuitive user interface (UI).

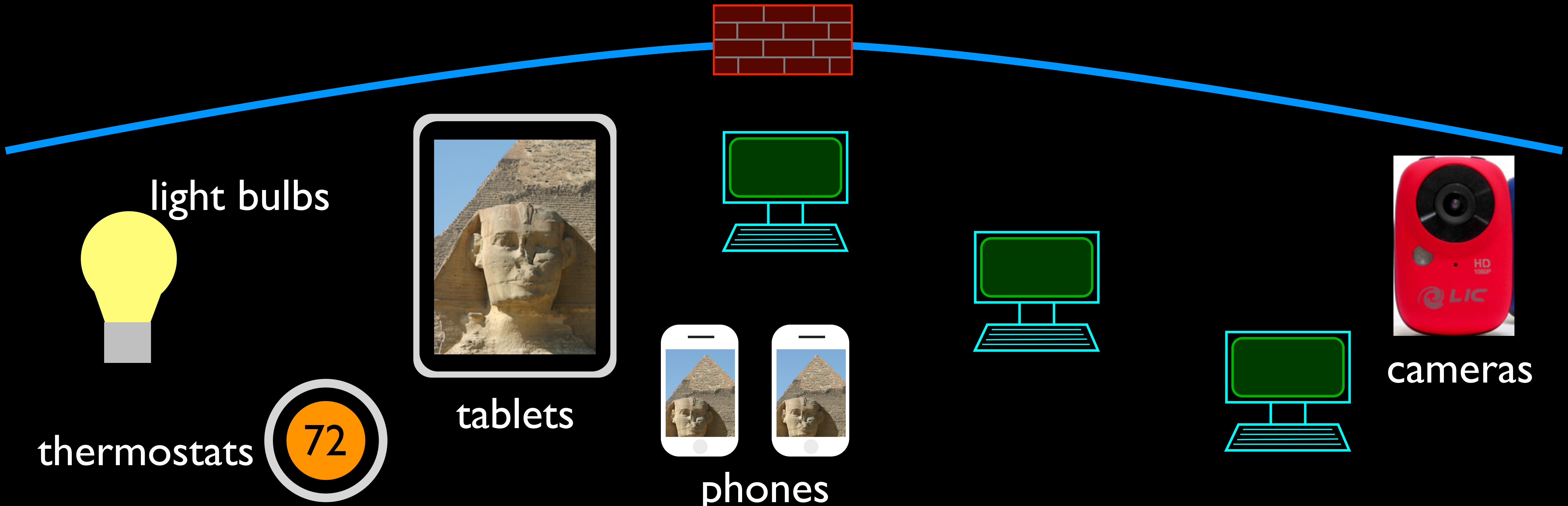
“full control of the light bulb”

http://www.marketwatch.com/story/marvell-introduces-new-four-in-one-zigbee-microcontroller-soc-delivering-the-highest-level-of-integration-in-the-industry-2012-01-09


light bulbs
thermostats
72


light bulbs
thermostats
72

Device-ification of the Enterprise



Device-ification of the Enterprise

Device-ification of the Enterprise

- Devices are fully Internet capable over Wi-Fi

Device-ification of the Enterprise

- Devices are fully Internet capable over Wi-Fi
- They are un-tethered from computers

Device-ification of the Enterprise

- Devices are fully Internet capable over Wi-Fi
- They are un-tethered from computers
- They are becoming ubiquitous

Device-ification of the Enterprise

- Devices are fully Internet capable over Wi-Fi
- They are un-tethered from computers
- They are becoming ubiquitous
- You have no visibility about what is going on inside the devices

Device-ification of the Enterprise

- Devices are fully Internet capable over Wi-Fi
- They are un-tethered from computers
- They are becoming ubiquitous
- You have no visibility about what is going on inside the devices
- They are potentially hackable or Trojaned to begin with

Device-ification of the Enterprise

- Devices are fully Internet capable over Wi-Fi
- They are un-tethered from computers
- They are becoming ubiquitous
- You have no visibility about what is going on inside the devices
- They are potentially hackable or Trojaned to begin with
- They may be owned by employees

Summary of Why Network Analysis

Summary of Why Network Analysis

- Standard protocol (TCP/IP) across OSes and devices

Summary of Why Network Analysis

- Standard protocol (TCP/IP) across OSes and devices
- Make sure your user are using secure version of services

Summary of Why Network Analysis

- Standard protocol (TCP/IP) across OSes and devices
- Make sure your user are using secure version of services
- Many/most attacks involve the network at some point

Summary of Why Network Analysis

- Standard protocol (TCP/IP) across OSes and devices
- Make sure your user are using secure version of services
- Many/most attacks involve the network at some point
- Can monitor a large number of hosts/devices from one location

Summary of Why Network Analysis

- Standard protocol (TCP/IP) across OSes and devices
- Make sure your user are using secure version of services
- Many/most attacks involve the network at some point
- Can monitor a large number of hosts/devices from one location
- Harder for the attacker to corrupt (unlike on-host logs)

Summary of Why Network Analysis

- Standard protocol (TCP/IP) across OSes and devices
- Make sure your user are using secure version of services
- Many/most attacks involve the network at some point
- Can monitor a large number of hosts/devices from one location
- Harder for the attacker to corrupt (unlike on-host logs)
- May be your only data source in some cases (e.g., thermostats)

Summary of Why Network Analysis

- Standard protocol (TCP/IP) across OSes and devices
- Make sure your user are using secure version of services
- Many/most attacks involve the network at some point
- Can monitor a large number of hosts/devices from one location
- Harder for the attacker to corrupt (unlike on-host logs)
- May be your only data source in some cases (e.g., thermostats)
- Extensive number of tools and documentation available

Act 3: Tools

tcpdump

Tcpdump Overview

Tcpdump Overview

- The basic, original packet sniffer

Tcpdump Overview

- The basic, original packet sniffer
- Ubiquitous. It is on your mac today

Tcpdump Overview

- The basic, original packet sniffer
- Ubiquitous. It is on your mac today
- Save raw network packets

Tcpdump Overview

- The basic, original packet sniffer
- Ubiquitous. It is on your mac today
- Save raw network packets
- Virtually all network analysis tools can read tcpdump data

Tcpdump Overview

- The basic, original packet sniffer
- Ubiquitous. It is on your mac today
- Save raw network packets
- Virtually all network analysis tools can read tcpdump data
- Strategy: login into remote system, run tcpdump, bring packets to analysis workstation

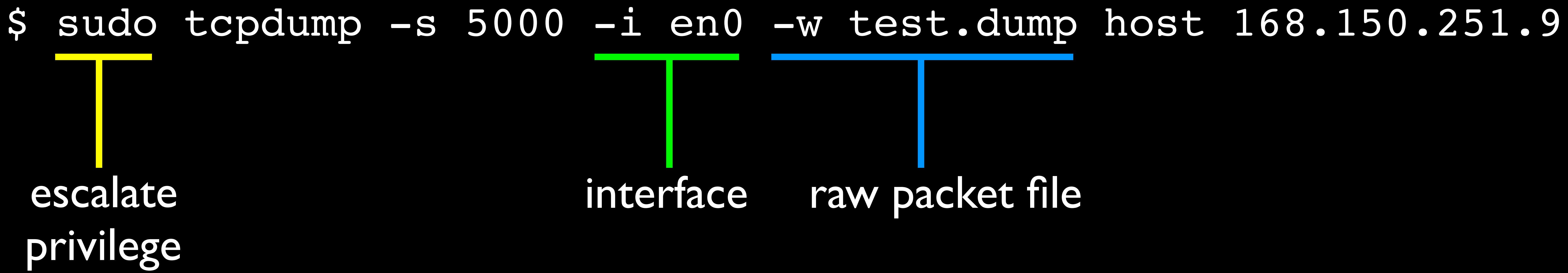
```
$ sudo tcpdump -s 5000 -i en0 -w test.dump host 168.150.251.9
$ sudo tcpdump -s 5000 -i en0 -w test.dump host 168.150.251.9
```

escalate
privilege

```
$ sudo tcpdump -s 5000 -i en0 -w test.dump host 168.150.251.9
```

escalate
privilege

interface

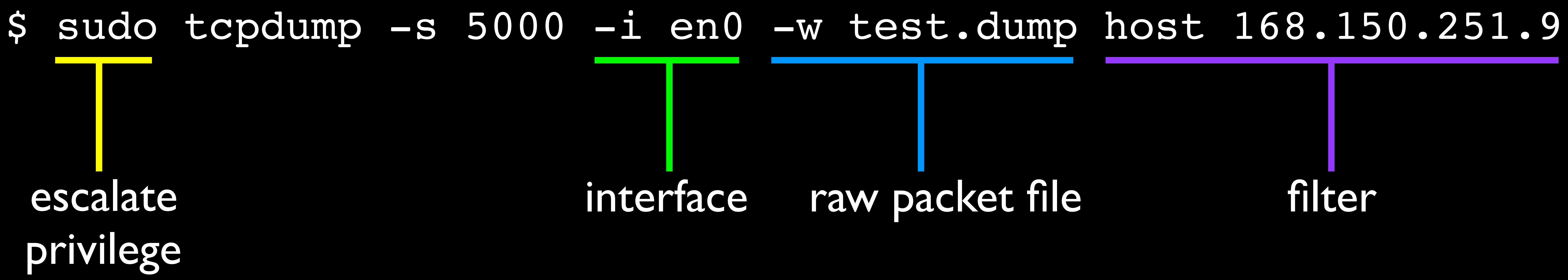


```
$ sudo tcpdump -s 5000 -i en0 -w test.dump host 168.150.251.9
```

escalate privilege

interface

raw packet file



```
$ sudo tcpdump -s 5000 -i en0 -w test.dump host 168.150.251.9
```

escalate
privilege

interface

raw packet file

filter

Wireshark

Wireshark Overview

Wireshark Overview

- Packet-oriented analysis

Wireshark Overview

- Packet-oriented analysis
- Assumes you understand networking and higher-level protocols

Wireshark Overview

- Packet-oriented analysis
- Assumes you understand networking and higher-level protocols
- Great for

Wireshark Overview

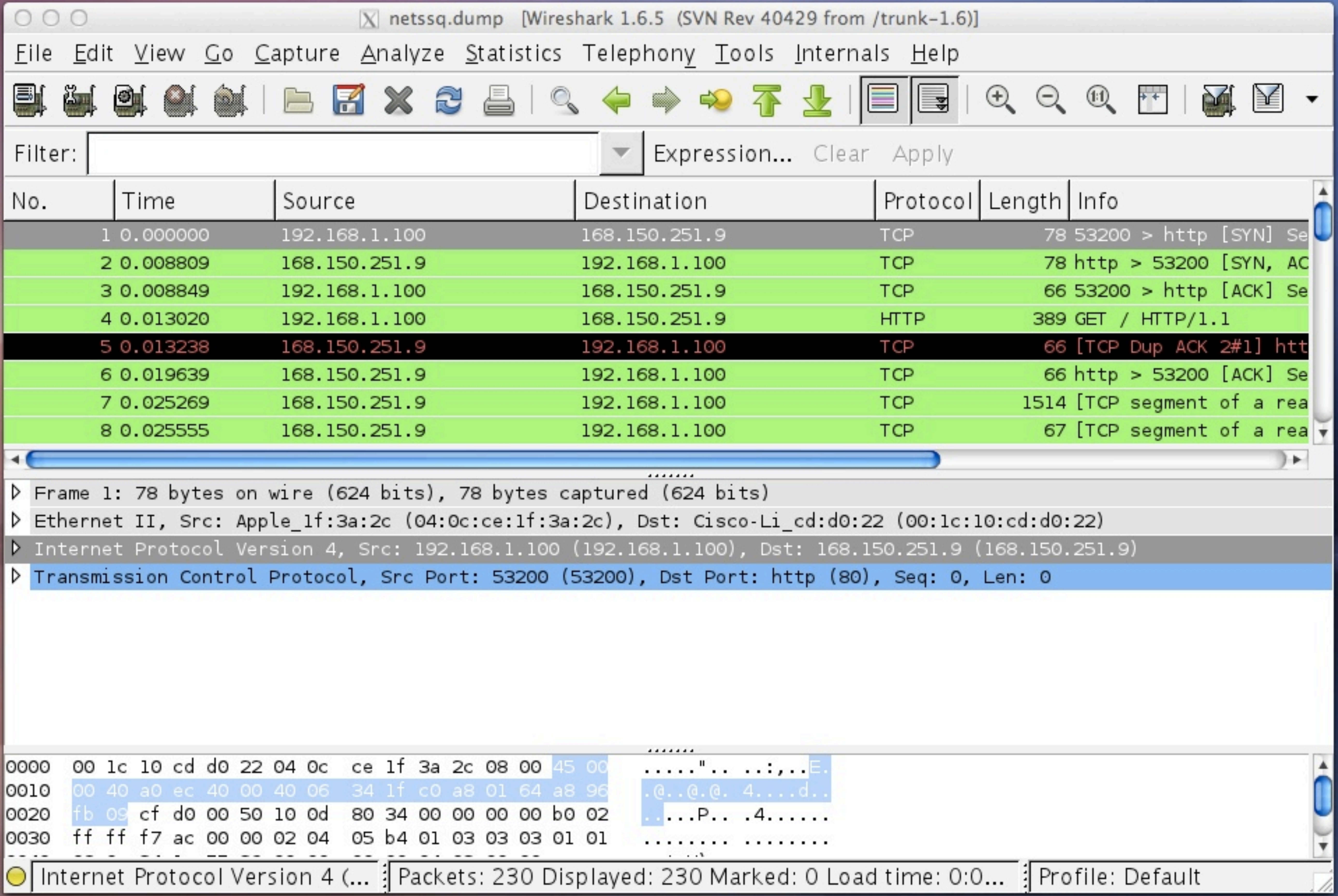
- Packet-oriented analysis
- Assumes you understand networking and higher-level protocols
- Great for
    - Learning networking

Wireshark Overview

- Packet-oriented analysis
- Assumes you understand networking and higher-level protocols
- Great for
  - Learning networking
  - Debugging network activity

Wireshark Overview

- Packet-oriented analysis
- Assumes you understand networking and higher-level protocols
- Great for
  - Learning networking
  - Debugging network activity
  - Network forensics



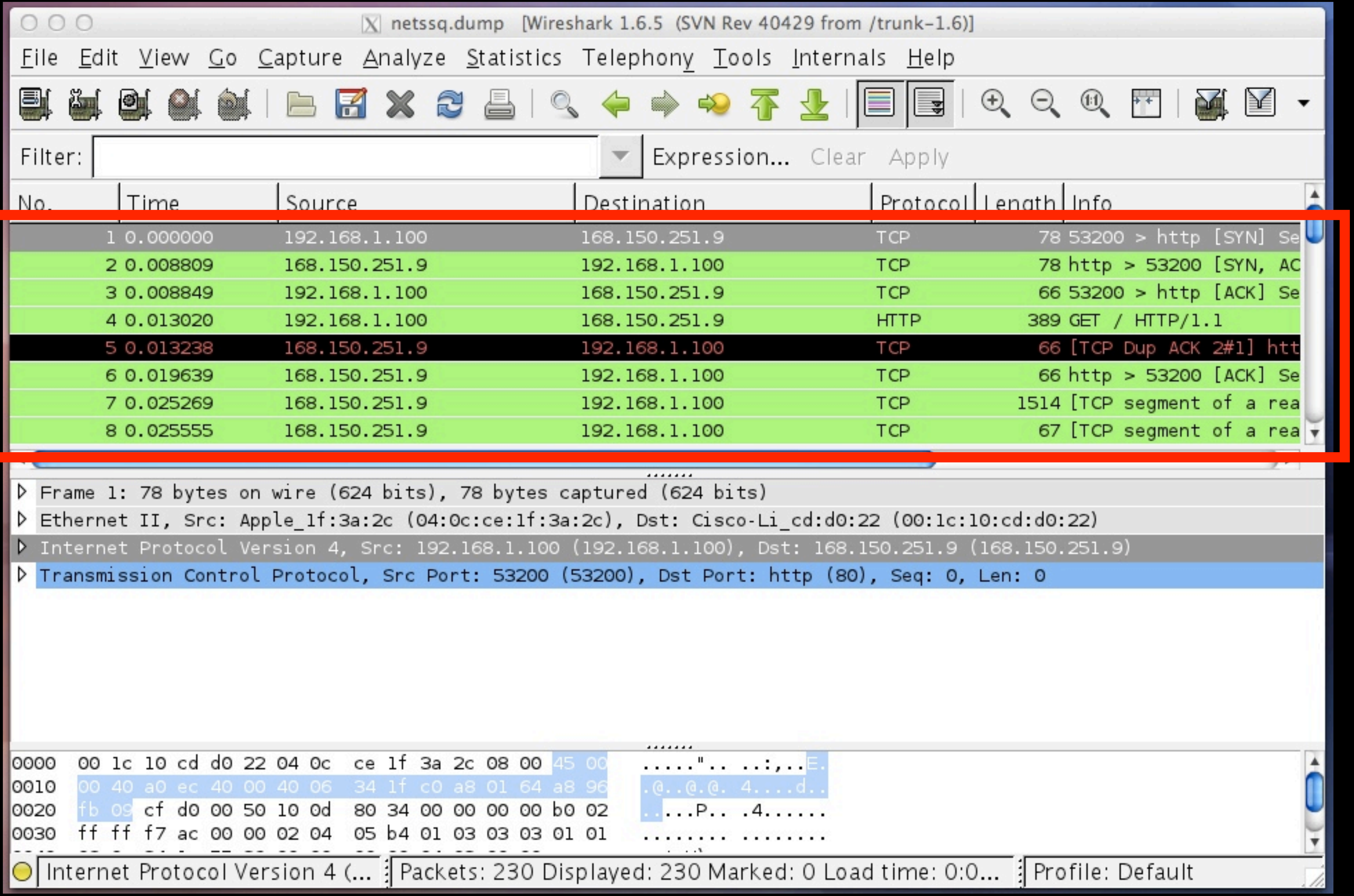
netssq.dump [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.   Time      Source           Destination      Protocol  Length Info
    1 0.000000  192.168.1.100    168.150.251.9    TCP           78 53200 > http [SYN] Se
    2 0.008809  168.150.251.9    192.168.1.100    TCP           78 http > 53200 [SYN, AC
    3 0.008849  192.168.1.100    168.150.251.9    TCP           66 53200 > http [ACK] Se
    4 0.013020  192.168.1.100    168.150.251.9    HTTP         389 GET / HTTP/1.1
    5 0.013238  168.150.251.9    192.168.1.100    TCP           66 [TCP Dup ACK 2#1] htt
    6 0.019639  168.150.251.9    192.168.1.100    TCP           66 http > 53200 [ACK] Se
    7 0.025269  168.150.251.9    192.168.1.100    TCP         1514 [TCP segment of a rea
    8 0.025555  168.150.251.9    192.168.1.100    TCP           67 [TCP segment of a rea
```

```
▷ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▷ Ethernet II, Src: Apple_1f:3a:2c (04:0c:ce:1f:3a:2c), Dst: Cisco-Li_cd:d0:22 (00:1c:10:cd:d0:22)
▷ Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 168.150.251.9 (168.150.251.9)
▷ Transmission Control Protocol, Src Port: 53200 (53200), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  00 1c 10 cd d0 22 04 0c  ce 1f 3a 2c 08 00 45 00   .....".. ..:,..E.
0010  00 40 a0 ec 40 00 40 06  34 1f c0 a8 01 64 a8 96   .@..@.@. 4....d..
0020  fb 09 cf d0 00 50 10 0d  80 34 00 00 00 00 b0 02   .....P.. .4......
0030  ff ff f7 ac 00 00 02 04  05 b4 01 03 03 03 01 01   ........ ........
```

Internet Protocol Version 4 (...
Packets: 230 Displayed: 230 Marked: 0 Load time: 0:0...
Profile: Default

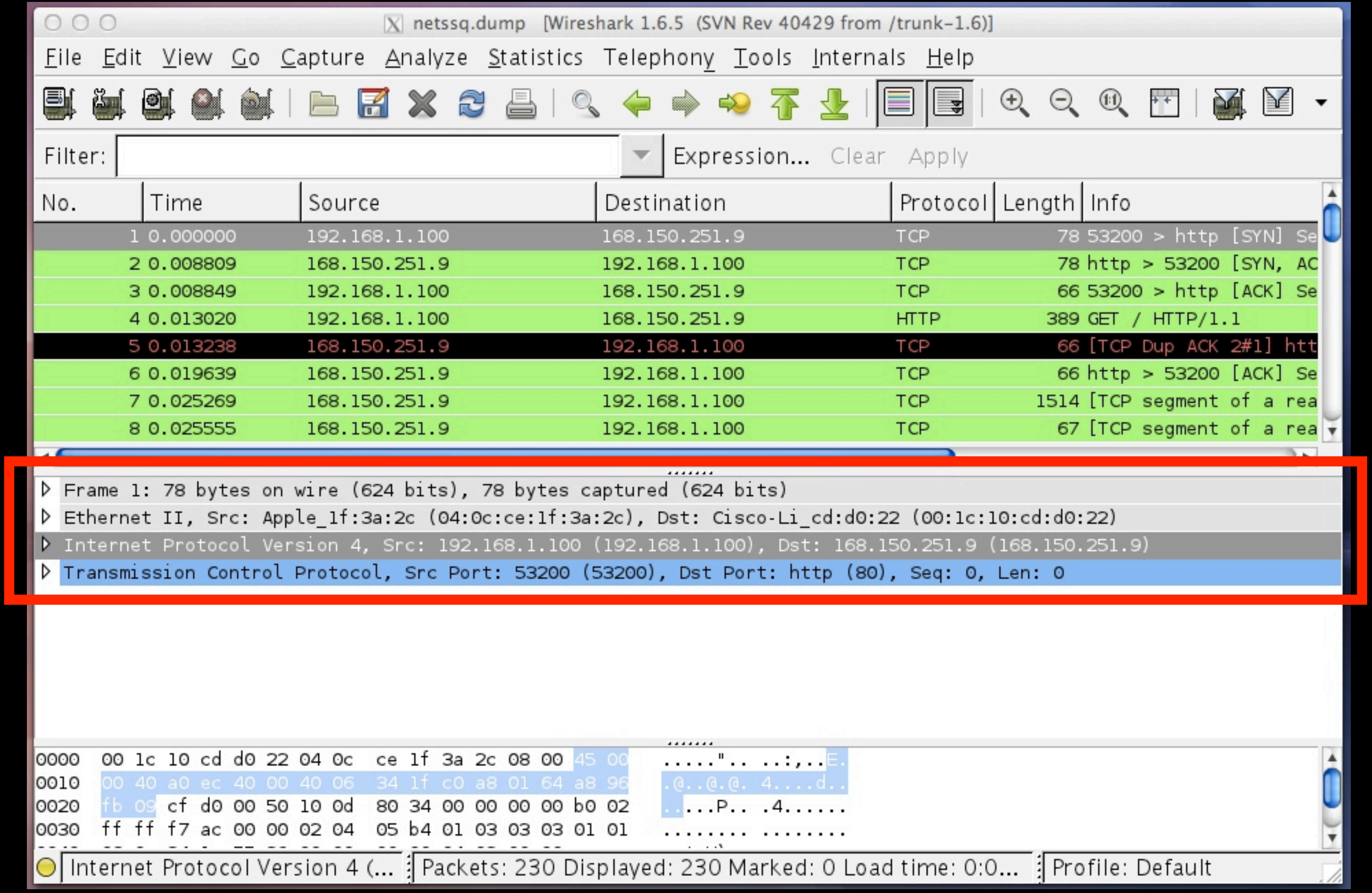

netssq.dump [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	168.150.251.9	TCP	78	53200 > http [SYN] Se
2	0.008809	168.150.251.9	192.168.1.100	TCP	78	http > 53200 [SYN, AC
3	0.008849	192.168.1.100	168.150.251.9	TCP	66	53200 > http [ACK] Se
4	0.013020	192.168.1.100	168.150.251.9	HTTP	389	GET / HTTP/1.1
5	0.013238	168.150.251.9	192.168.1.100	TCP	66	[TCP Dup ACK 2#1] htt
6	0.019639	168.150.251.9	192.168.1.100	TCP	66	http > 53200 [ACK] Se
7	0.025269	168.150.251.9	192.168.1.100	TCP	1514	[TCP segment of a rea
8	0.025555	168.150.251.9	192.168.1.100	TCP	67	[TCP segment of a rea

```
▷ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▷ Ethernet II, Src: Apple_1f:3a:2c (04:0c:ce:1f:3a:2c), Dst: Cisco-Li_cd:d0:22 (00:1c:10:cd:d0:22)
▷ Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 168.150.251.9 (168.150.251.9)
▷ Transmission Control Protocol, Src Port: 53200 (53200), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  00 1c 10 cd d0 22 04 0c  ce 1f 3a 2c 08 00 45 00   ....."..  ..:,..E.
0010  00 40 a0 ec 40 00 40 06  34 1f c0 a8 01 64 a8 96   .@..@.@.  4....d..
0020  fb 09 cf d0 00 50 10 0d  80 34 00 00 00 00 b0 02   .....P..  .4......
0030  ff ff f7 ac 00 00 02 04  05 b4 01 03 03 03 01 01   ........  ........
```

Internet Protocol Version 4 (... | Packets: 230 Displayed: 230 Marked: 0 Load time: 0:0... | Profile: Default

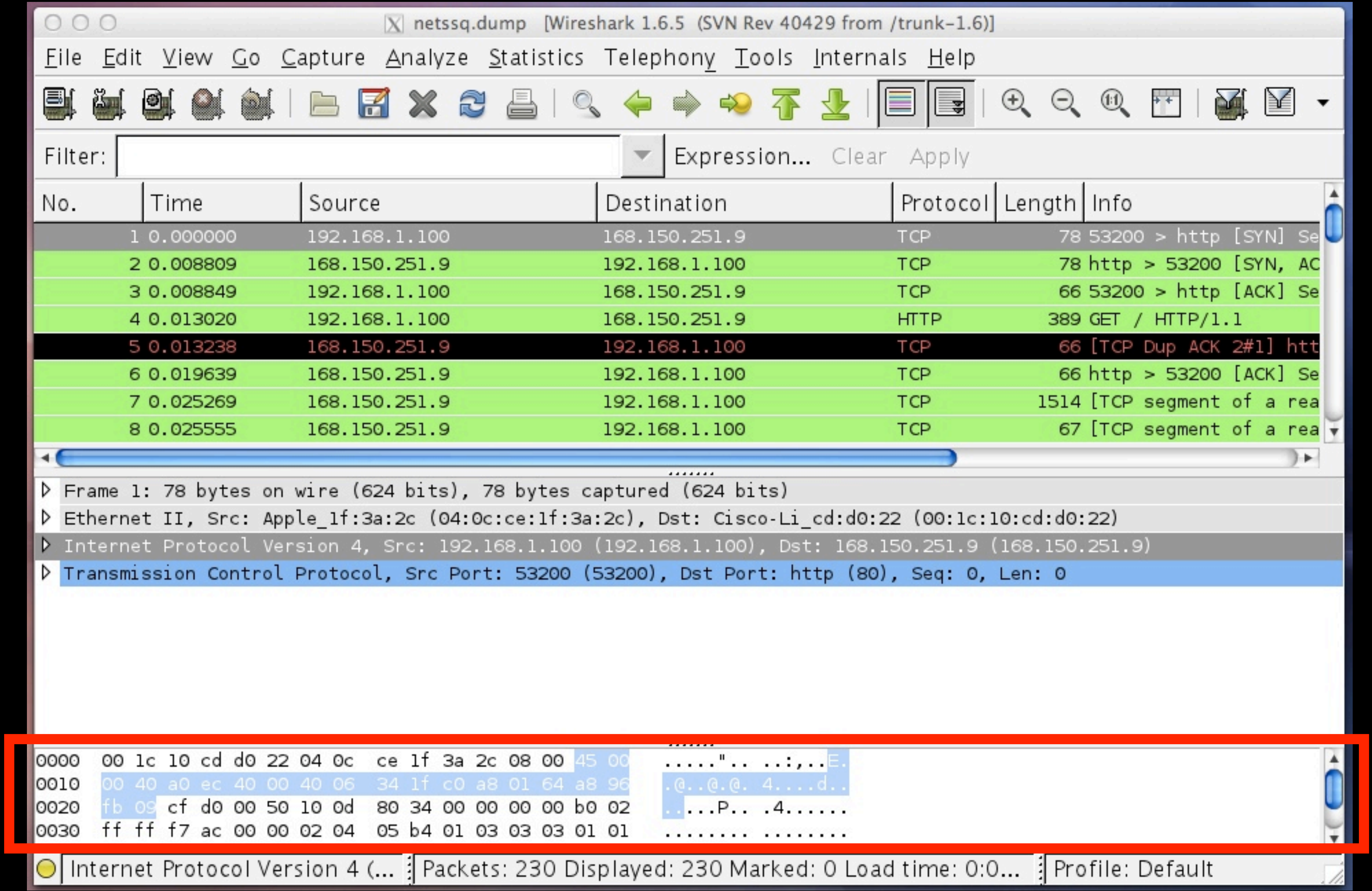

netssq.dump [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	168.150.251.9	TCP	78	53200 > http [SYN] Se
2	0.008809	168.150.251.9	192.168.1.100	TCP	78	http > 53200 [SYN, AC
3	0.008849	192.168.1.100	168.150.251.9	TCP	66	53200 > http [ACK] Se
4	0.013020	192.168.1.100	168.150.251.9	HTTP	389	GET / HTTP/1.1
5	0.013238	168.150.251.9	192.168.1.100	TCP	66	[TCP Dup ACK 2#1] htt
6	0.019639	168.150.251.9	192.168.1.100	TCP	66	http > 53200 [ACK] Se
7	0.025269	168.150.251.9	192.168.1.100	TCP	1514	[TCP segment of a rea
8	0.025555	168.150.251.9	192.168.1.100	TCP	67	[TCP segment of a rea

```
▷ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▷ Ethernet II, Src: Apple_1f:3a:2c (04:0c:ce:1f:3a:2c), Dst: Cisco-Li_cd:d0:22 (00:1c:10:cd:d0:22)
▷ Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 168.150.251.9 (168.150.251.9)
▷ Transmission Control Protocol, Src Port: 53200 (53200), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  00 1c 10 cd d0 22 04 0c  ce 1f 3a 2c 08 00 45 00   ....."..  ..:,..E.
0010  00 40 a0 ec 40 00 40 06  34 1f c0 a8 01 64 a8 96   .@..@.@.  4....d..
0020  fb 09 cf d0 00 50 10 0d  80 34 00 00 00 00 b0 02   .....P..  .4......
0030  ff ff f7 ac 00 00 02 04  05 b4 01 03 03 03 01 01   ........  ........
```

Internet Protocol Version 4 (...
Packets: 230 Displayed: 230 Marked: 0 Load time: 0:0...
Profile: Default

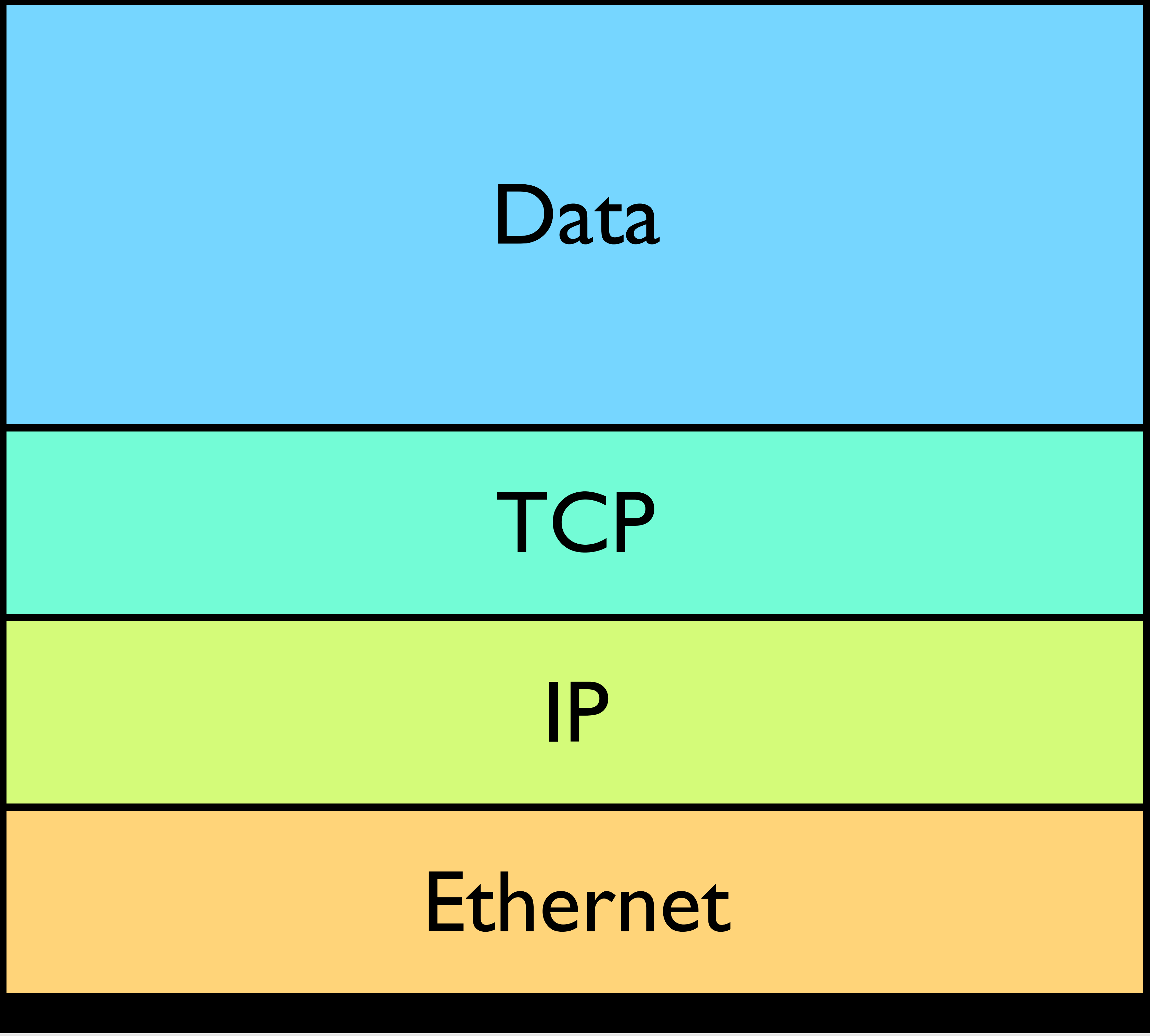


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	168.150.251.9	TCP	78	53200 > http [SYN] Se
2	0.008809	168.150.251.9	192.168.1.100	TCP	78	http > 53200 [SYN, AC
3	0.008849	192.168.1.100	168.150.251.9	TCP	66	53200 > http [ACK] Se
4	0.013020	192.168.1.100	168.150.251.9	HTTP	389	GET / HTTP/1.1
5	0.013238	168.150.251.9	192.168.1.100	TCP	66	[TCP Dup ACK 2#1] htt
6	0.019639	168.150.251.9	192.168.1.100	TCP	66	http > 53200 [ACK] Se
7	0.025269	168.150.251.9	192.168.1.100	TCP	1514	[TCP segment of a rea
8	0.025555	168.150.251.9	192.168.1.100	TCP	67	[TCP segment of a rea

```
▷ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▷ Ethernet II, Src: Apple_1f:3a:2c (04:0c:ce:1f:3a:2c), Dst: Cisco-Li_cd:d0:22 (00:1c:10:cd:d0:22)
▷ Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 168.150.251.9 (168.150.251.9)
▷ Transmission Control Protocol, Src Port: 53200 (53200), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  00 1c 10 cd d0 22 04 0c  ce 1f 3a 2c 08 00 45 00   ....."..  ..:,..E.
0010  00 40 a0 ec 40 00 40 06  34 1f c0 a8 01 64 a8 96   .@..@.@.  4....d..
0020  fb 09 cf d0 00 50 10 0d  80 34 00 00 00 00 b0 02   .....P..  .4......
0030  ff ff f7 ac 00 00 02 04  05 b4 01 03 03 03 01 01   ........  ........
```

Internet Protocol Version 4 (... Packets: 230 Displayed: 230 Marked: 0 Load time: 0:0... Profile: Default

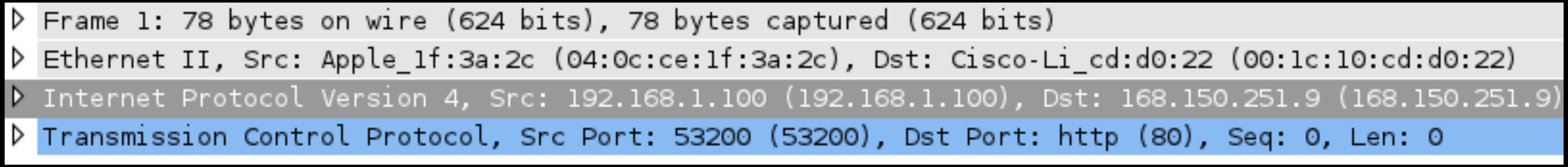


Data

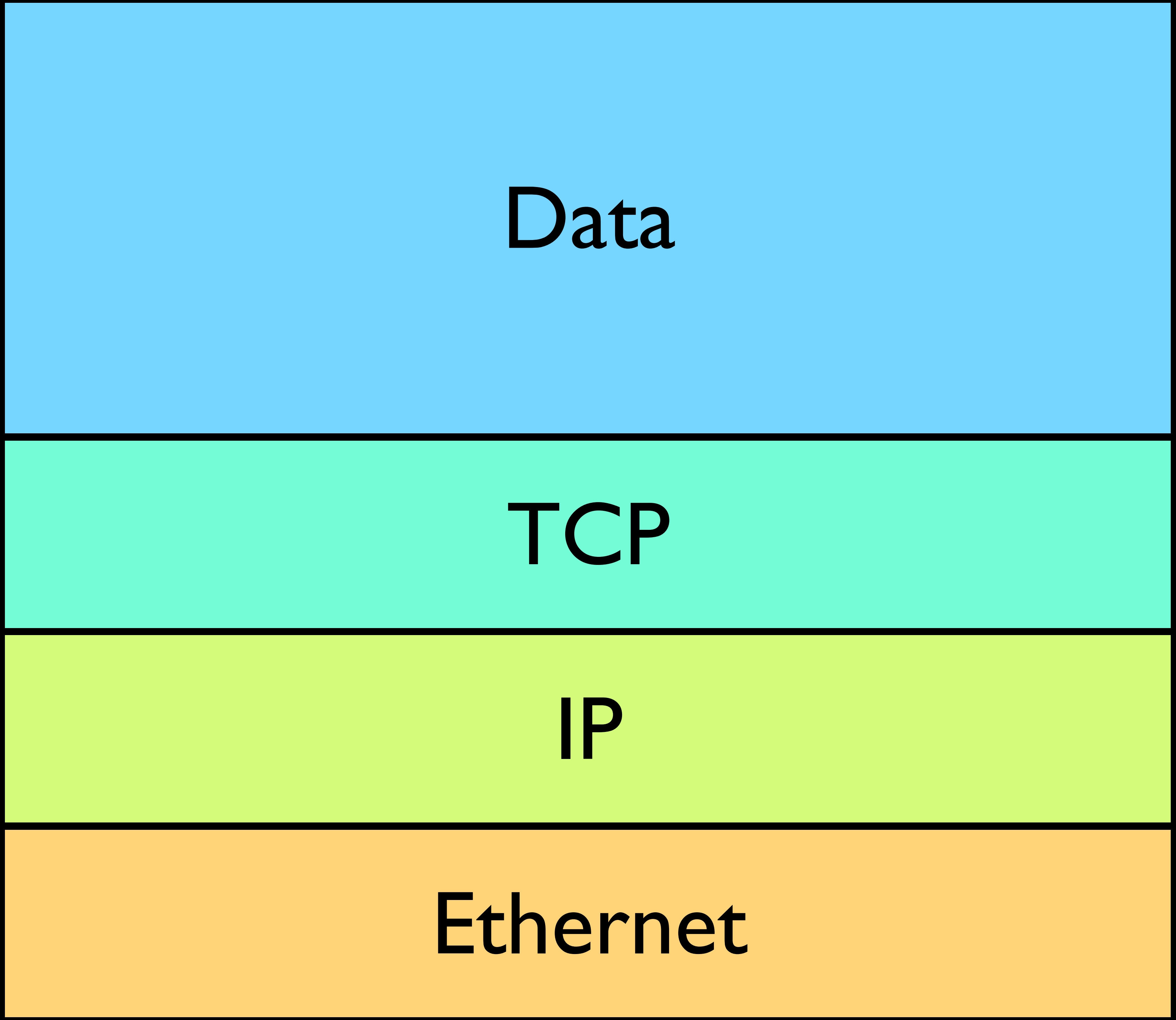
TCP

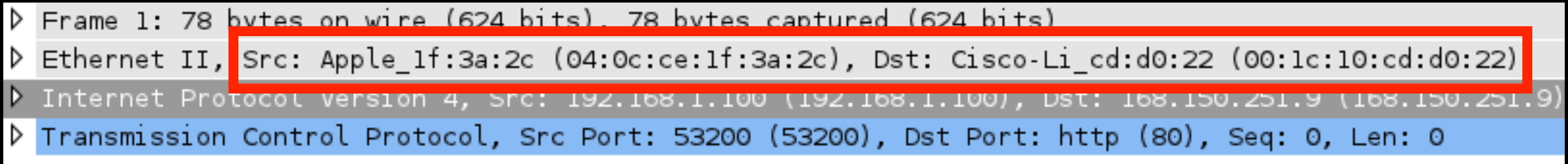
IP

Ethernet

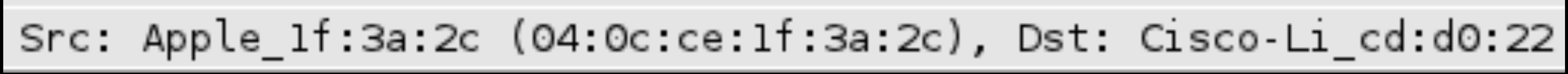


```
▷ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▷ Ethernet II, Src: Apple_1f:3a:2c (04:0c:ce:1f:3a:2c), Dst: Cisco-Li_cd:d0:22 (00:1c:10:cd:d0:22)
▷ Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 168.150.251.9 (168.150.251.9)
▷ Transmission Control Protocol, Src Port: 53200 (53200), Dst Port: http (80), Seq: 0, Len: 0
```

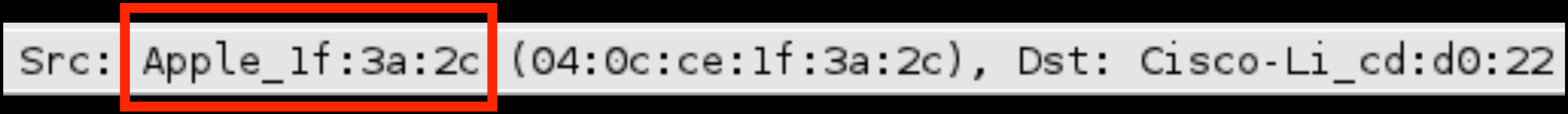




```
▷ Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▷ Ethernet II, Src: Apple_1f:3a:2c (04:0c:ce:1f:3a:2c), Dst: Cisco-Li_cd:d0:22 (00:1c:10:cd:d0:22)
▷ Internet Protocol Version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 168.150.251.9 (168.150.251.9)
▷ Transmission Control Protocol, Src Port: 53200 (53200), Dst Port: http (80), Seq: 0, Len: 0
```

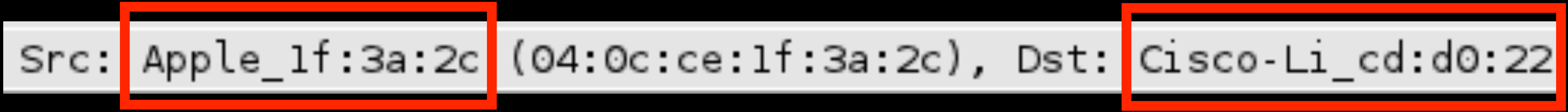


```
Src: Apple_1f:3a:2c (04:0c:ce:1f:3a:2c), Dst: Cisco-Li_cd:d0:22
```



```
Src: Apple_1f:3a:2c (04:0c:ce:1f:3a:2c), Dst: Cisco-Li_cd:d0:22
```

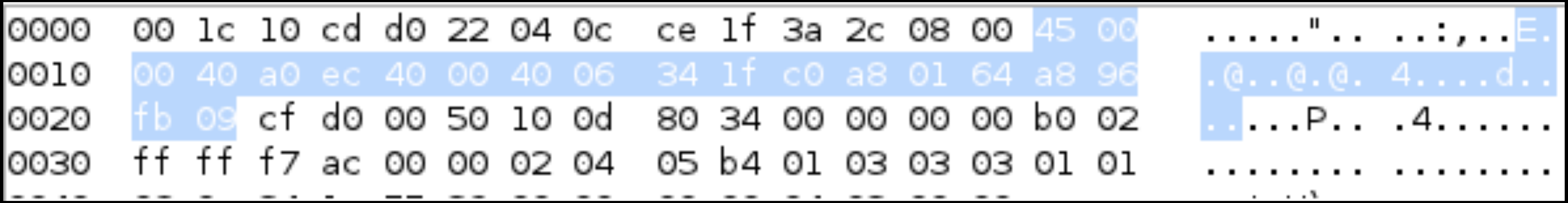
Apple
MacBook Air



```
Src: Apple_1f:3a:2c (04:0c:ce:1f:3a:2c), Dst: Cisco-Li_cd:d0:22
```

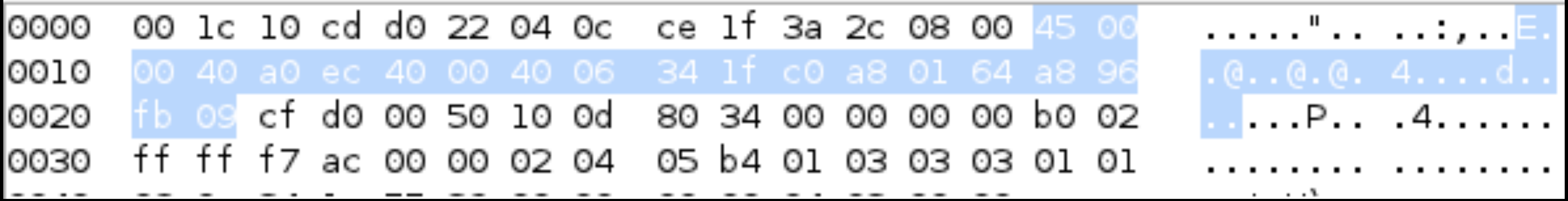
Apple
MacBook Air

Cisco
Linksys WiFi
Router

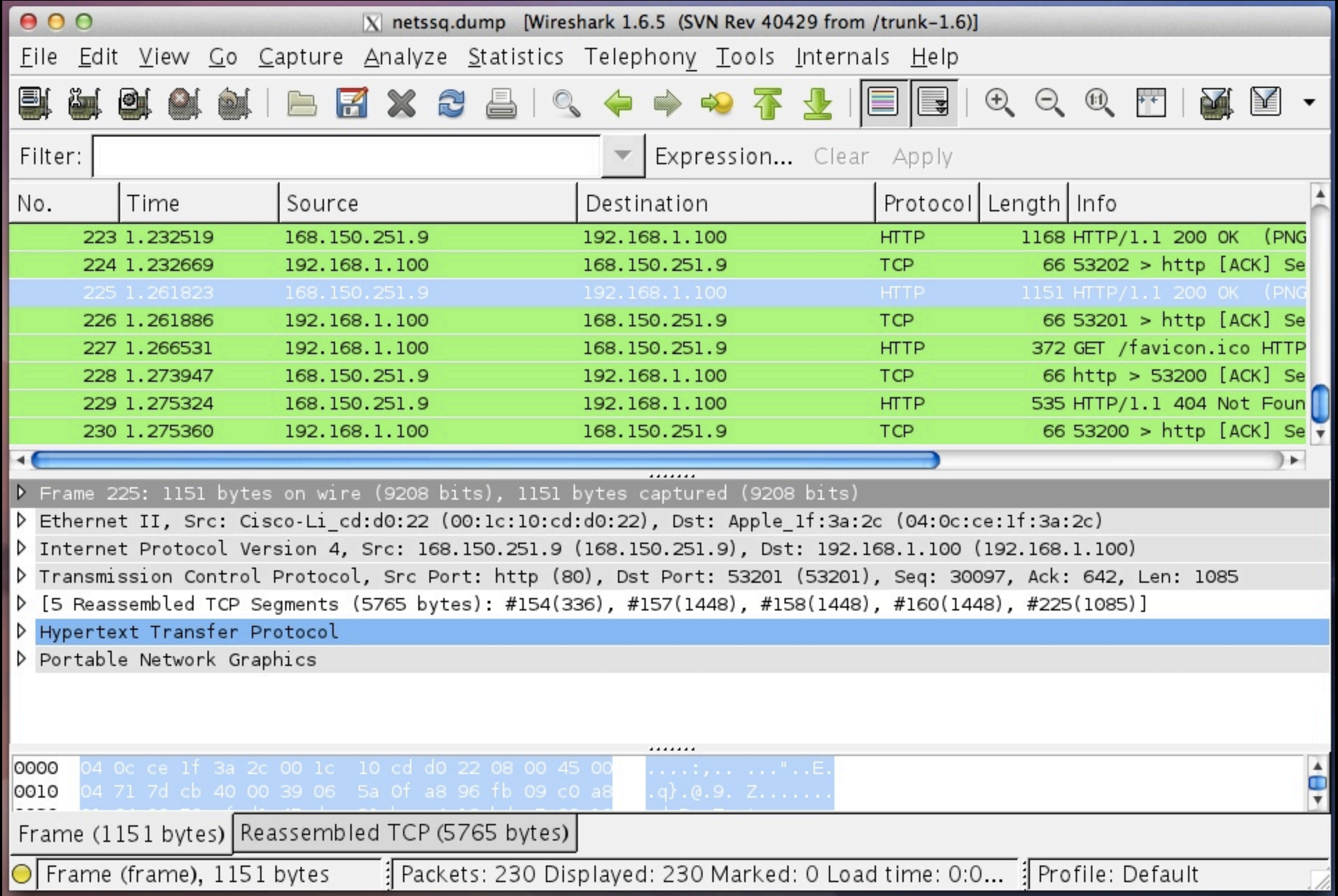


```
0000  00 1c 10 cd d0 22 04 0c  ce 1f 3a 2c 08 00 45 00   ....."..  ..:,..E.
0010  00 40 a0 ec 40 00 40 06  34 1f c0 a8 01 64 a8 96   .@..@.@.  4....d..
0020  fb 09 cf d0 00 50 10 0d  80 34 00 00 00 00 b0 02   .....P..  .4......
0030  ff ff f7 ac 00 00 02 04  05 b4 01 03 03 03 01 01   ........  ........
```

IP Header



```
0000  00 1c 10 cd d0 22 04 0c  ce 1f 3a 2c 08 00 45 00   ....."..  ..:,..E.
0010  00 40 a0 ec 40 00 40 06  34 1f c0 a8 01 64 a8 96   .@..@.@.  4....d..
0020  fb 09 cf d0 00 50 10 0d  80 34 00 00 00 00 b0 02   .....P..  .4......
0030  ff ff f7 ac 00 00 02 04  05 b4 01 03 03 03 01 01   ........  ........
```



No.	Time	Source	Destination	Protocol	Length	Info
223	1.232519	168.150.251.9	192.168.1.100	HTTP	1168	HTTP/1.1 200 OK (PNG
224	1.232669	192.168.1.100	168.150.251.9	TCP	66	53202 > http [ACK] Se
225	1.261823	168.150.251.9	192.168.1.100	HTTP	1151	HTTP/1.1 200 OK (PNG
226	1.261886	192.168.1.100	168.150.251.9	TCP	66	53201 > http [ACK] Se
227	1.266531	192.168.1.100	168.150.251.9	HTTP	372	GET /favicon.ico HTTP
228	1.273947	168.150.251.9	192.168.1.100	TCP	66	http > 53200 [ACK] Se
229	1.275324	168.150.251.9	192.168.1.100	HTTP	535	HTTP/1.1 404 Not Foun
230	1.275360	192.168.1.100	168.150.251.9	TCP	66	53200 > http [ACK] Se

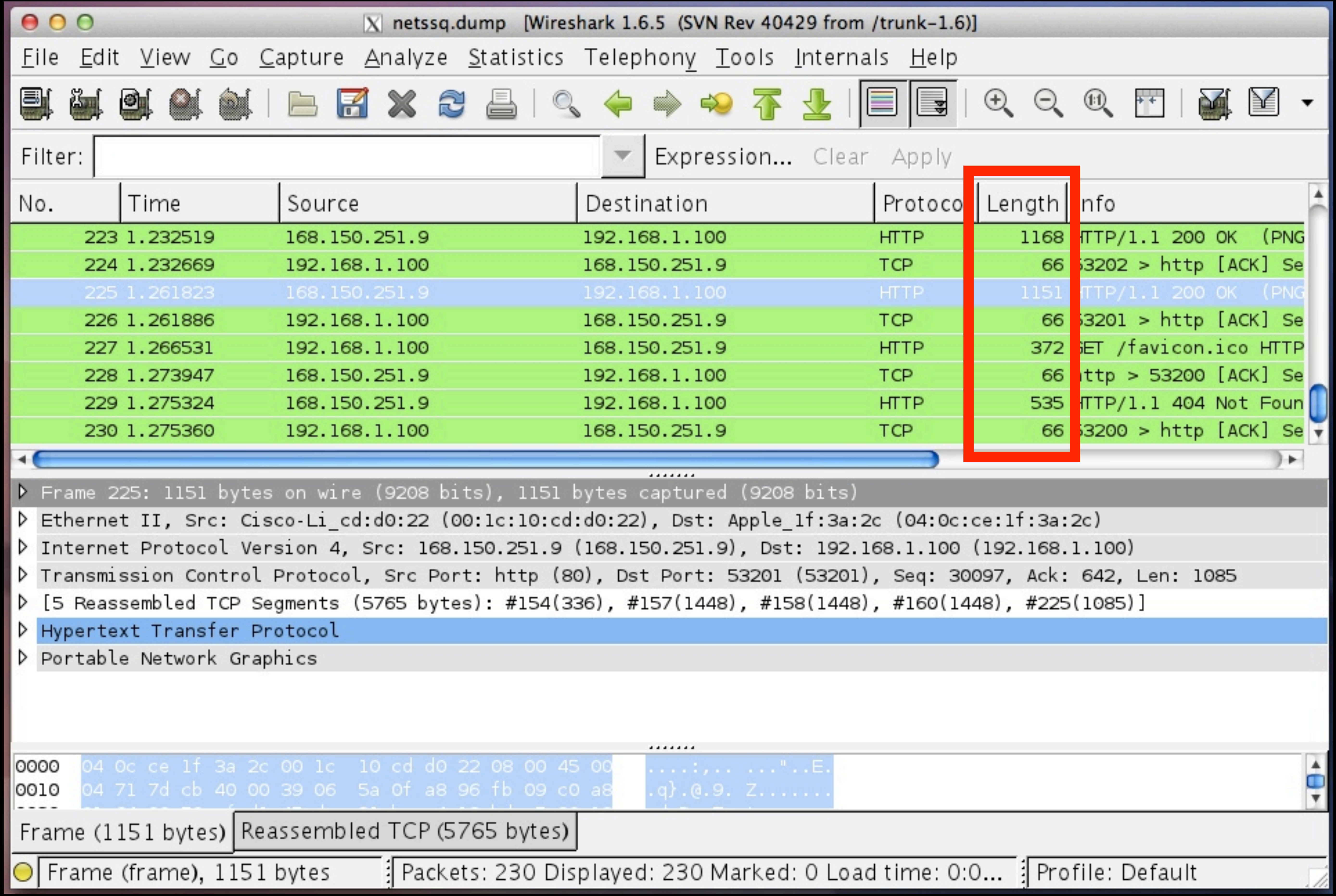
```
▷ Frame 225: 1151 bytes on wire (9208 bits), 1151 bytes captured (9208 bits)
▷ Ethernet II, Src: Cisco-Li_cd:d0:22 (00:1c:10:cd:d0:22), Dst: Apple_1f:3a:2c (04:0c:ce:1f:3a:2c)
▷ Internet Protocol Version 4, Src: 168.150.251.9 (168.150.251.9), Dst: 192.168.1.100 (192.168.1.100)
▷ Transmission Control Protocol, Src Port: http (80), Dst Port: 53201 (53201), Seq: 30097, Ack: 642, Len: 1085
▷ [5 Reassembled TCP Segments (5765 bytes): #154(336), #157(1448), #158(1448), #160(1448), #225(1085)]
▷ Hypertext Transfer Protocol
▷ Portable Network Graphics
```

```
0000  04 0c ce 1f 3a 2c 00 1c  10 cd d0 22 08 00 45 00   ....:,.. ..."..E.
0010  04 71 7d cb 40 00 39 06  5a 0f a8 96 fb 09 c0 a8   .q}.@.9. Z.......
```

Frame (frame), 1151 bytes

Packets: 230 Displayed: 230 Marked: 0 Load time: 0:0...

Profile: Default



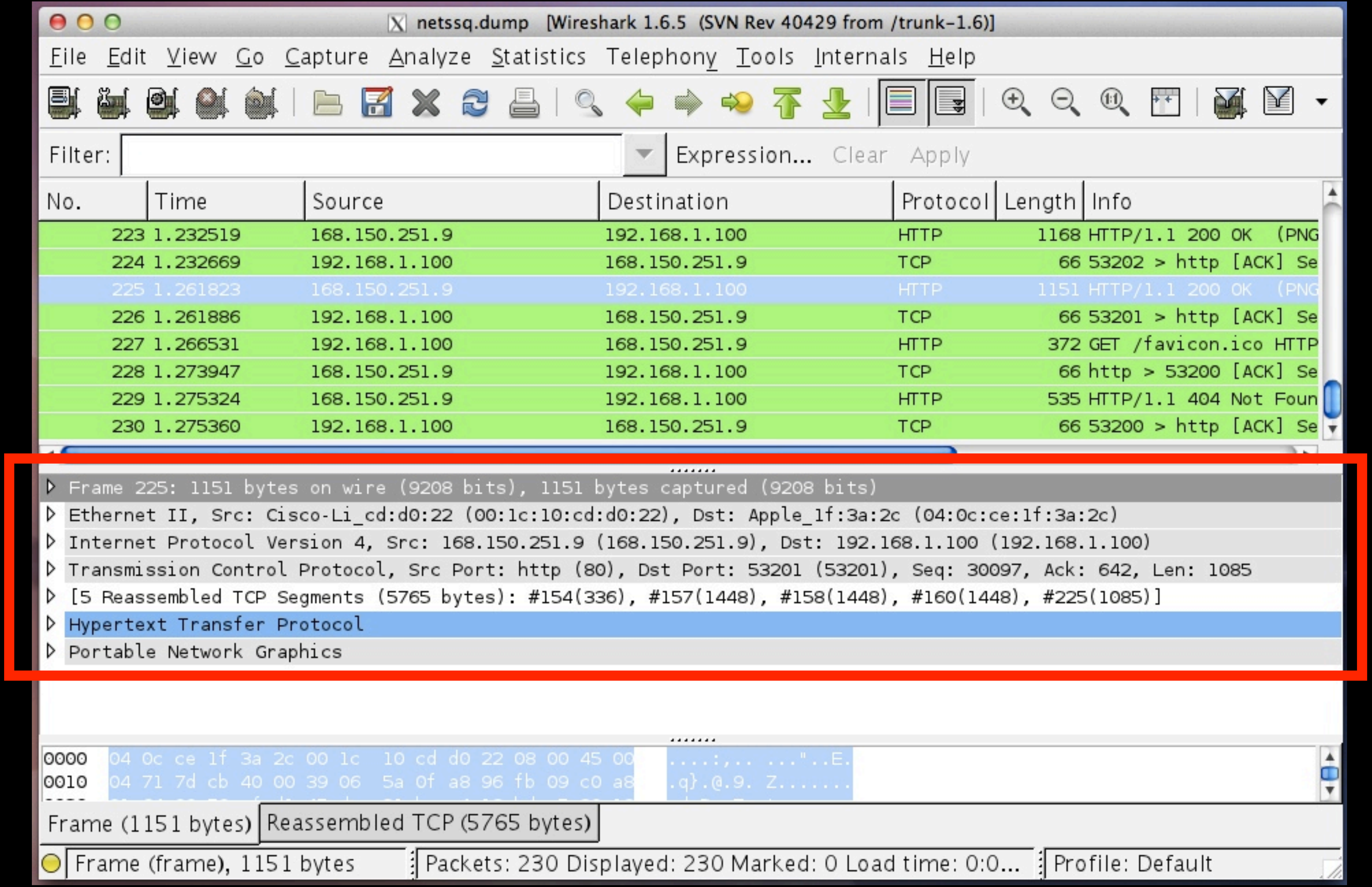
netssq.dump [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protoco	Length	nfo
223	1.232519	168.150.251.9	192.168.1.100	HTTP	1168	TTP/1.1 200 OK (PNG
224	1.232669	192.168.1.100	168.150.251.9	TCP	66	3202 > http [ACK] Se
225	1.261823	168.150.251.9	192.168.1.100	HTTP	1151	TTP/1.1 200 OK (PNG
226	1.261886	192.168.1.100	168.150.251.9	TCP	66	3201 > http [ACK] Se
227	1.266531	192.168.1.100	168.150.251.9	HTTP	372	ET /favicon.ico HTTP
228	1.273947	168.150.251.9	192.168.1.100	TCP	66	ttp > 53200 [ACK] Se
229	1.275324	168.150.251.9	192.168.1.100	HTTP	535	TTP/1.1 404 Not Foun
230	1.275360	192.168.1.100	168.150.251.9	TCP	66	3200 > http [ACK] Se

```
▷ Frame 225: 1151 bytes on wire (9208 bits), 1151 bytes captured (9208 bits)
▷ Ethernet II, Src: Cisco-Li_cd:d0:22 (00:1c:10:cd:d0:22), Dst: Apple_1f:3a:2c (04:0c:ce:1f:3a:2c)
▷ Internet Protocol Version 4, Src: 168.150.251.9 (168.150.251.9), Dst: 192.168.1.100 (192.168.1.100)
▷ Transmission Control Protocol, Src Port: http (80), Dst Port: 53201 (53201), Seq: 30097, Ack: 642, Len: 1085
▷ [5 Reassembled TCP Segments (5765 bytes): #154(336), #157(1448), #158(1448), #160(1448), #225(1085)]
▷ Hypertext Transfer Protocol
▷ Portable Network Graphics
```

```
0000  04 0c ce 1f 3a 2c 00 1c  10 cd d0 22 08 00 45 00   ....:,.. ..."..E.
0010  04 71 7d cb 40 00 39 06  5a 0f a8 96 fb 09 c0 a8   .q}.@.9. Z.......
```

```
Frame (frame), 1151 bytes   Packets: 230 Displayed: 230 Marked: 0 Load time: 0:0...   Profile: Default
```


netssq.dump [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

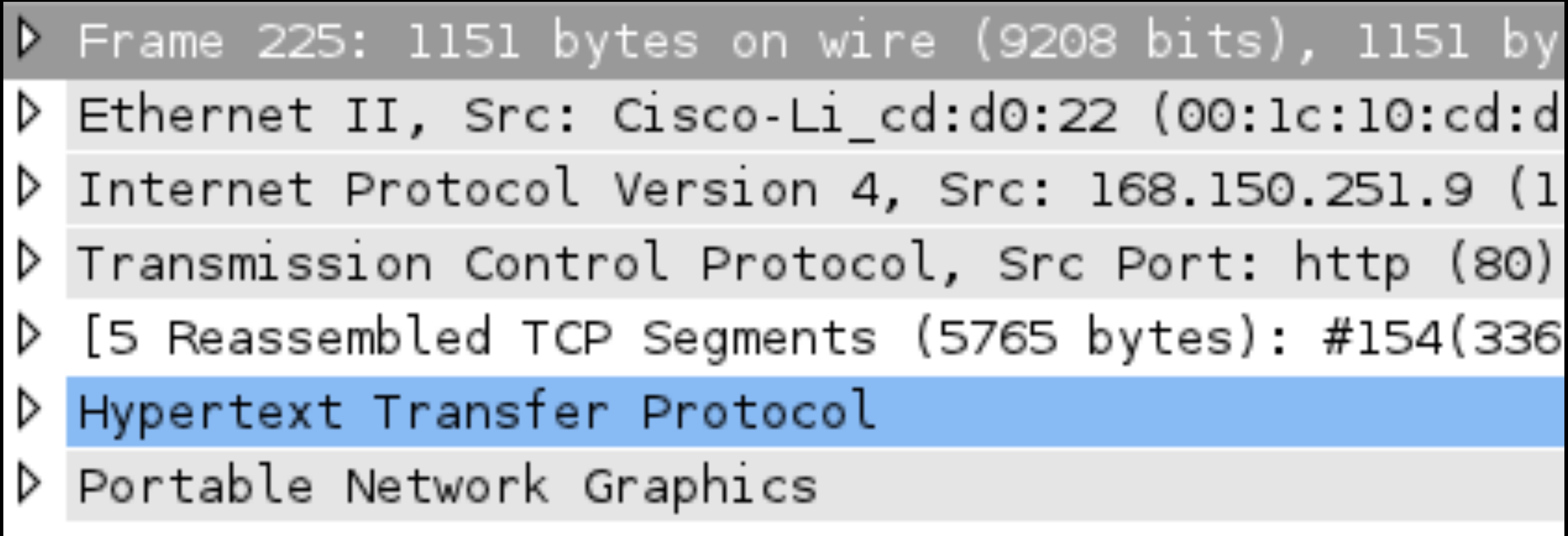
```
No.     Time      Source          Destination     Protocol Length Info
    223 1.232519  168.150.251.9   192.168.1.100   HTTP      1168 HTTP/1.1 200 OK  (PNG
    224 1.232669  192.168.1.100   168.150.251.9   TCP         66 53202 > http [ACK] Se
    225 1.261823  168.150.251.9   192.168.1.100   HTTP      1151 HTTP/1.1 200 OK  (PNG
    226 1.261886  192.168.1.100   168.150.251.9   TCP         66 53201 > http [ACK] Se
    227 1.266531  192.168.1.100   168.150.251.9   HTTP       372 GET /favicon.ico HTTP
    228 1.273947  168.150.251.9   192.168.1.100   TCP         66 http > 53200 [ACK] Se
    229 1.275324  168.150.251.9   192.168.1.100   HTTP       535 HTTP/1.1 404 Not Foun
    230 1.275360  192.168.1.100   168.150.251.9   TCP         66 53200 > http [ACK] Se
```

```
▷ Frame 225: 1151 bytes on wire (9208 bits), 1151 bytes captured (9208 bits)
▷ Ethernet II, Src: Cisco-Li_cd:d0:22 (00:1c:10:cd:d0:22), Dst: Apple_1f:3a:2c (04:0c:ce:1f:3a:2c)
▷ Internet Protocol Version 4, Src: 168.150.251.9 (168.150.251.9), Dst: 192.168.1.100 (192.168.1.100)
▷ Transmission Control Protocol, Src Port: http (80), Dst Port: 53201 (53201), Seq: 30097, Ack: 642, Len: 1085
▷ [5 Reassembled TCP Segments (5765 bytes): #154(336), #157(1448), #158(1448), #160(1448), #225(1085)]
▷ Hypertext Transfer Protocol
▷ Portable Network Graphics
```

```
0000  04 0c ce 1f 3a 2c 00 1c  10 cd d0 22 08 00 45 00   ....:,.. ..."..E.
0010  04 71 7d cb 40 00 39 06  5a 0f a8 96 fb 09 c0 a8   .q}.@.9. Z.......
```

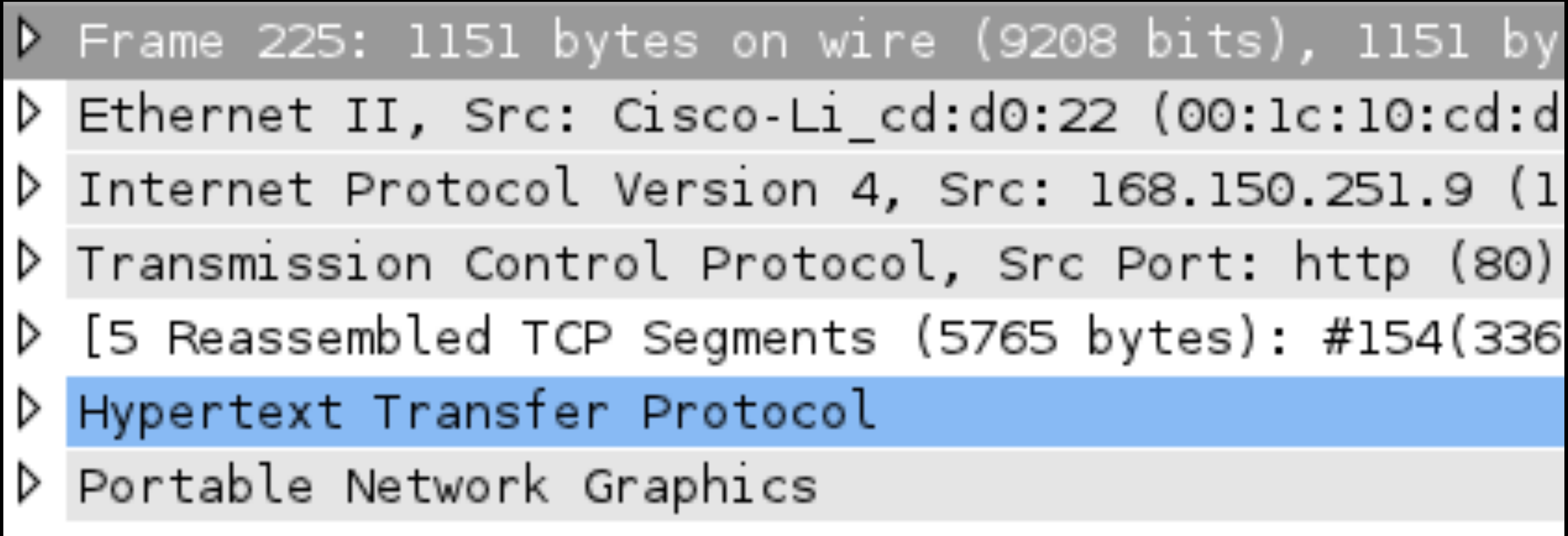
Frame (frame), 1151 bytes   Packets: 230 Displayed: 230 Marked: 0 Load time: 0:0...   Profile: Default

Deep Packet Inspection



```
▷ Frame 225: 1151 bytes on wire (9208 bits), 1151 by
▷ Ethernet II, Src: Cisco-Li_cd:d0:22 (00:1c:10:cd:d
▷ Internet Protocol Version 4, Src: 168.150.251.9 (1
▷ Transmission Control Protocol, Src Port: http (80)
▷ [5 Reassembled TCP Segments (5765 bytes): #154(336
▷ Hypertext Transfer Protocol
▷ Portable Network Graphics
```

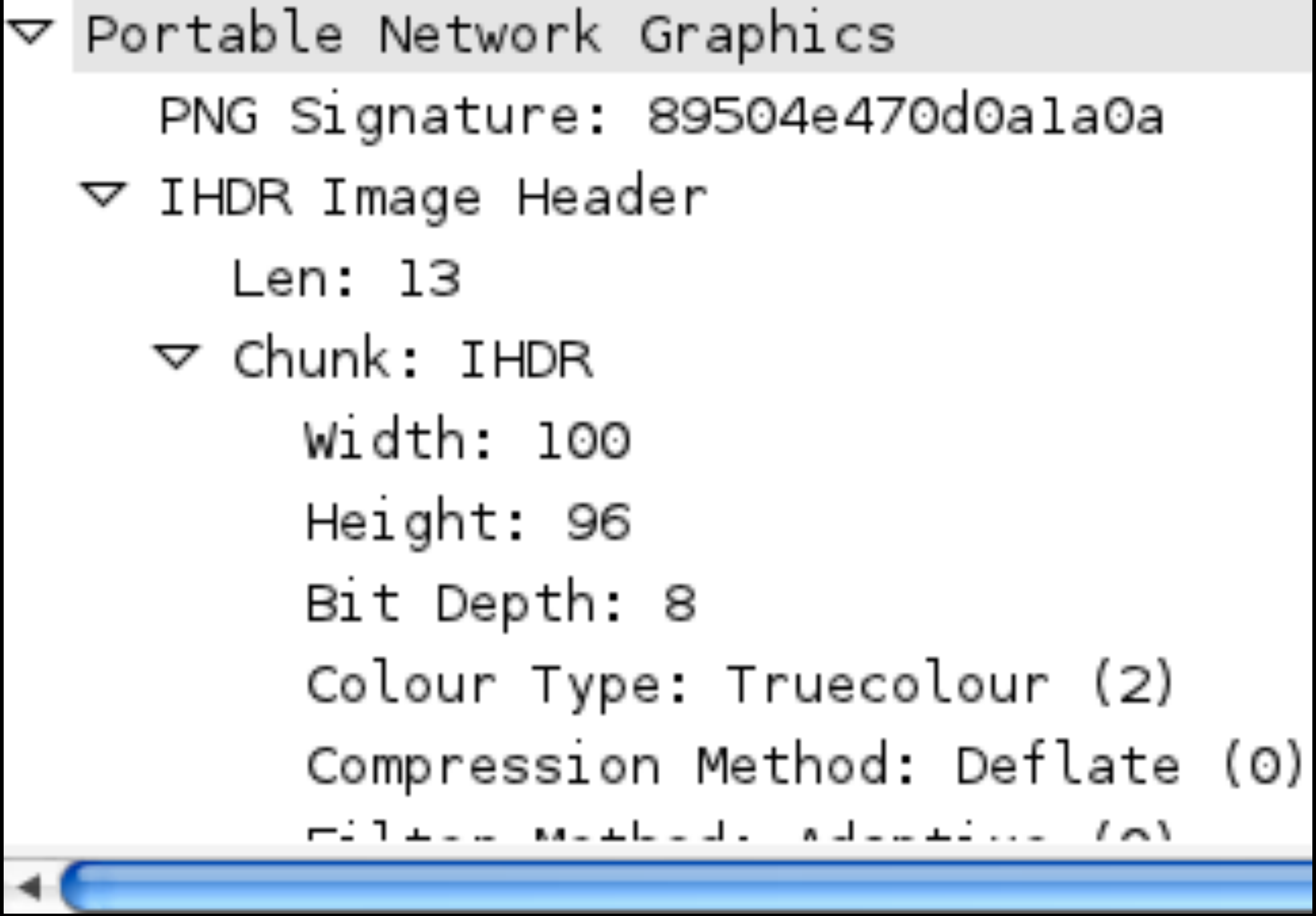
Deep Packet Inspection



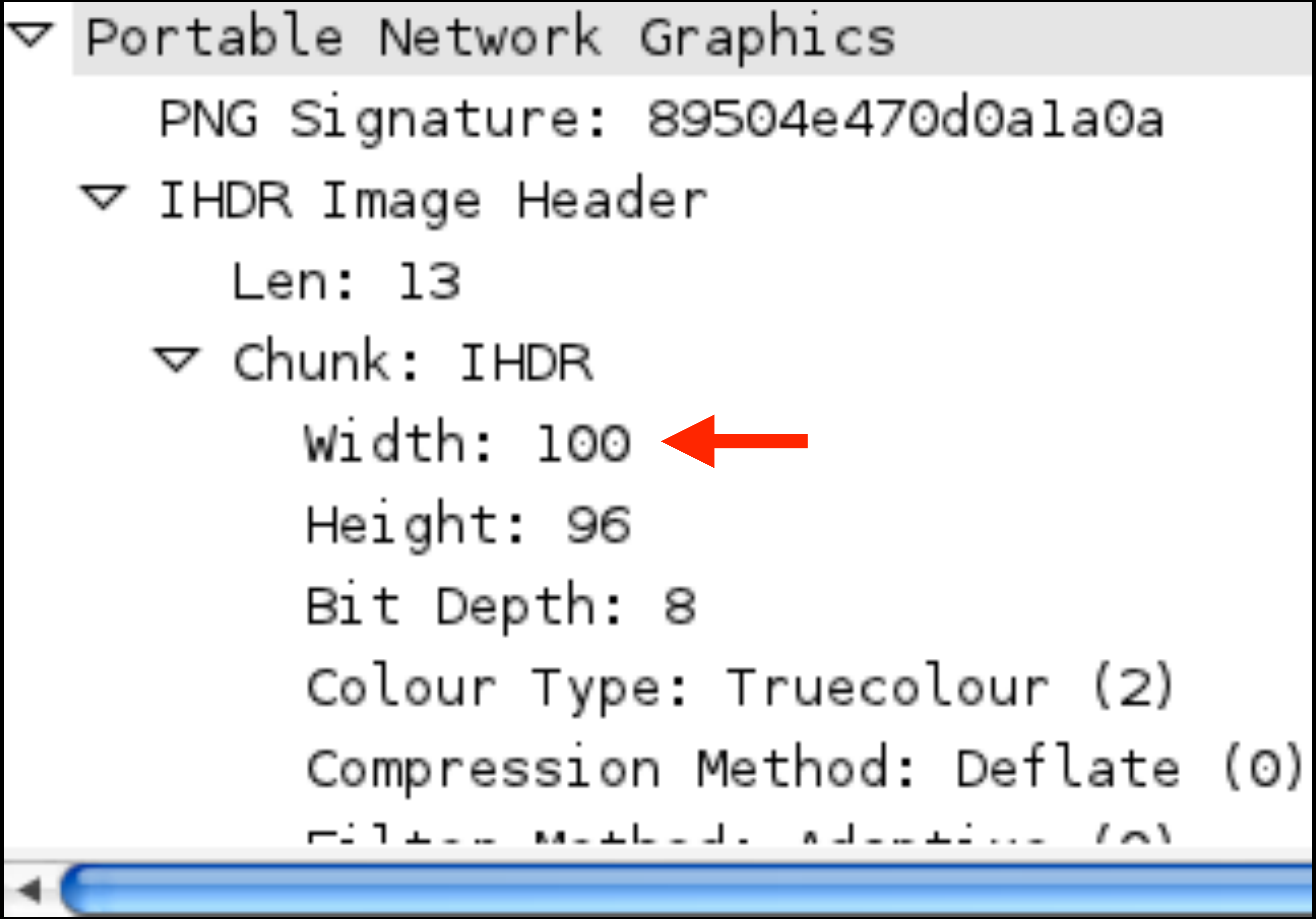
```
▷ Frame 225: 1151 bytes on wire (9208 bits), 1151 by
▷ Ethernet II, Src: Cisco-Li_cd:d0:22 (00:1c:10:cd:d
▷ Internet Protocol Version 4, Src: 168.150.251.9 (1
▷ Transmission Control Protocol, Src Port: http (80)
▷ [5 Reassembled TCP Segments (5765 bytes): #154(336
▷ Hypertext Transfer Protocol
▷ Portable Network Graphics
```

↑

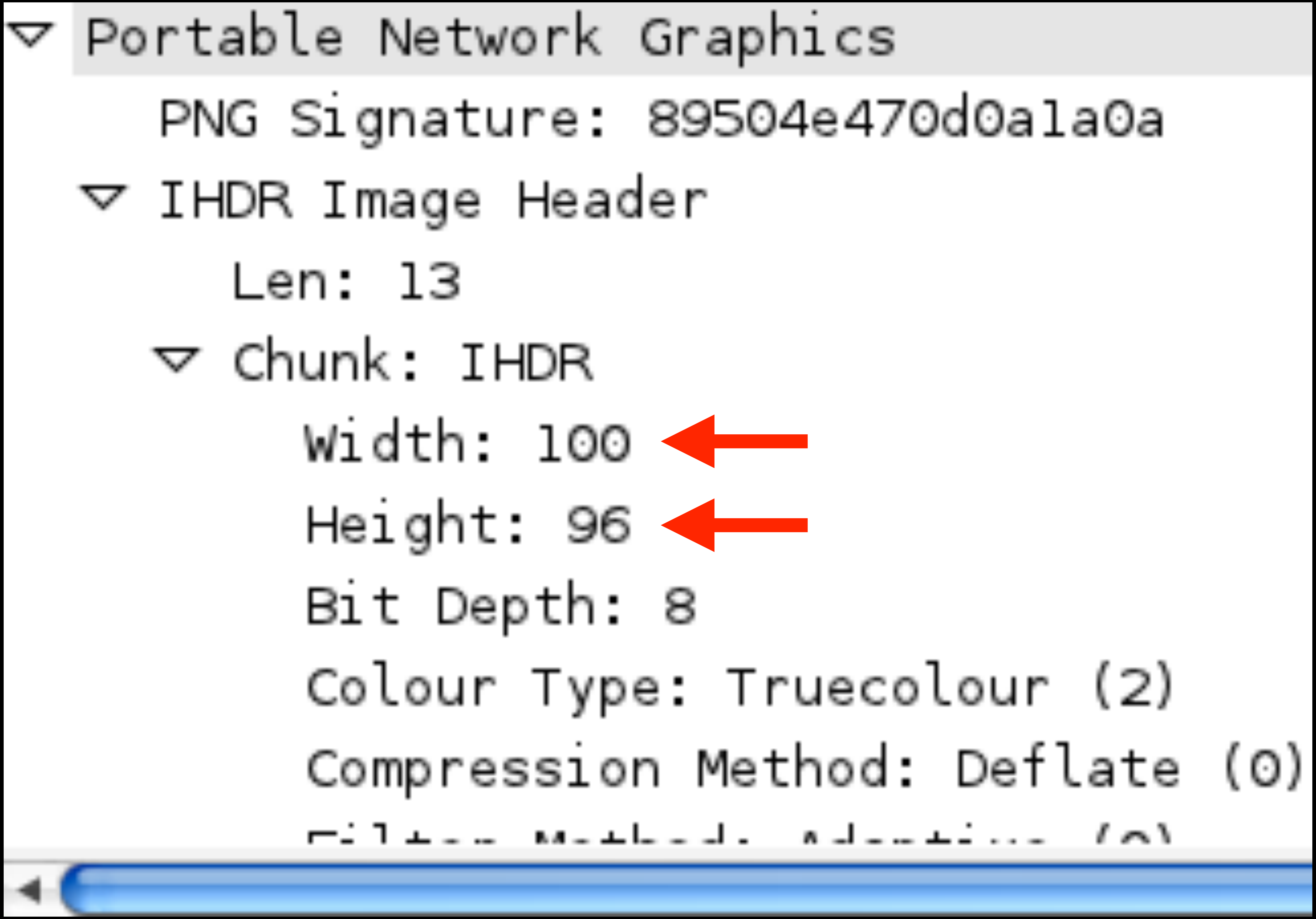
PNG over HTTP



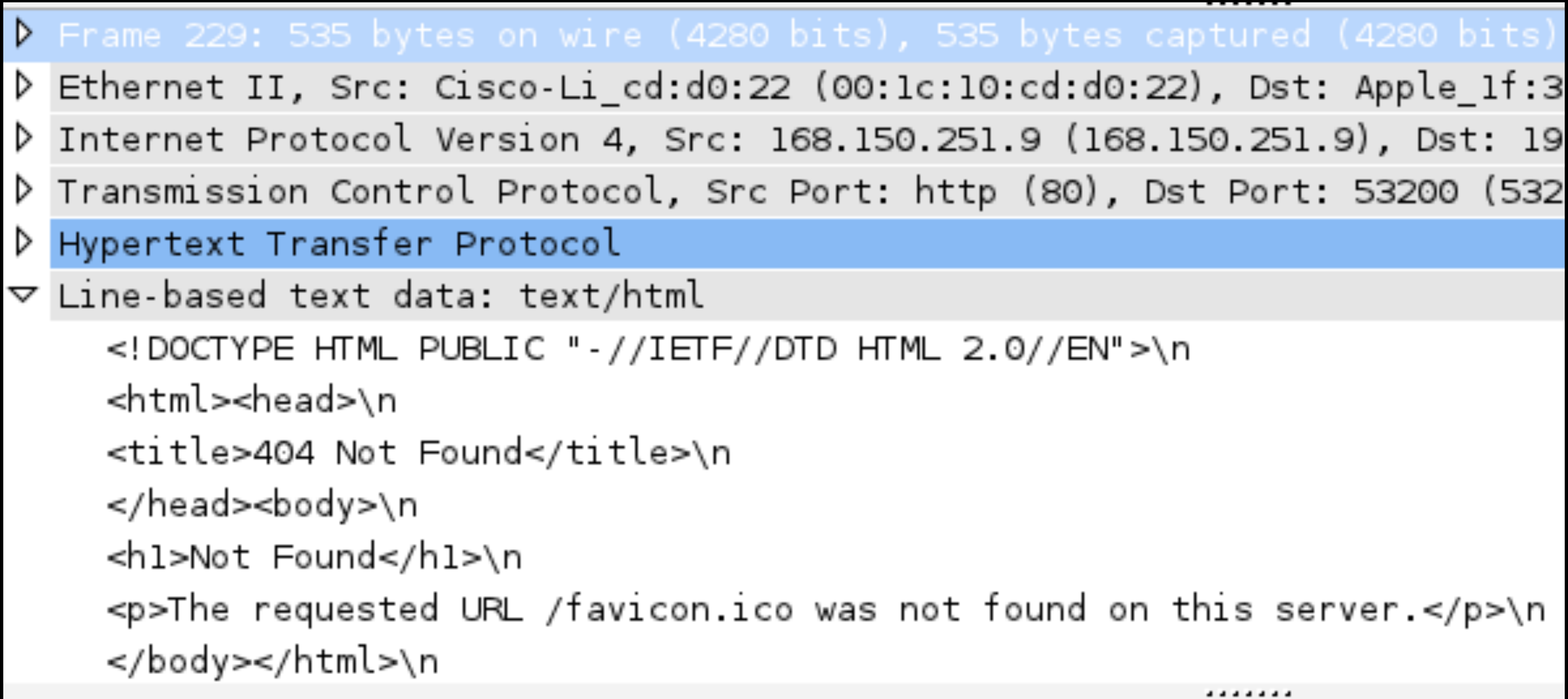
```
▽ Portable Network Graphics
    PNG Signature: 89504e470d0a1a0a
  ▽ IHDR Image Header
      Len: 13
    ▽ Chunk: IHDR
        Width: 100
        Height: 96
        Bit Depth: 8
        Colour Type: Truecolour (2)
        Compression Method: Deflate (0)
        Filter Method: Adaptive (0)
```



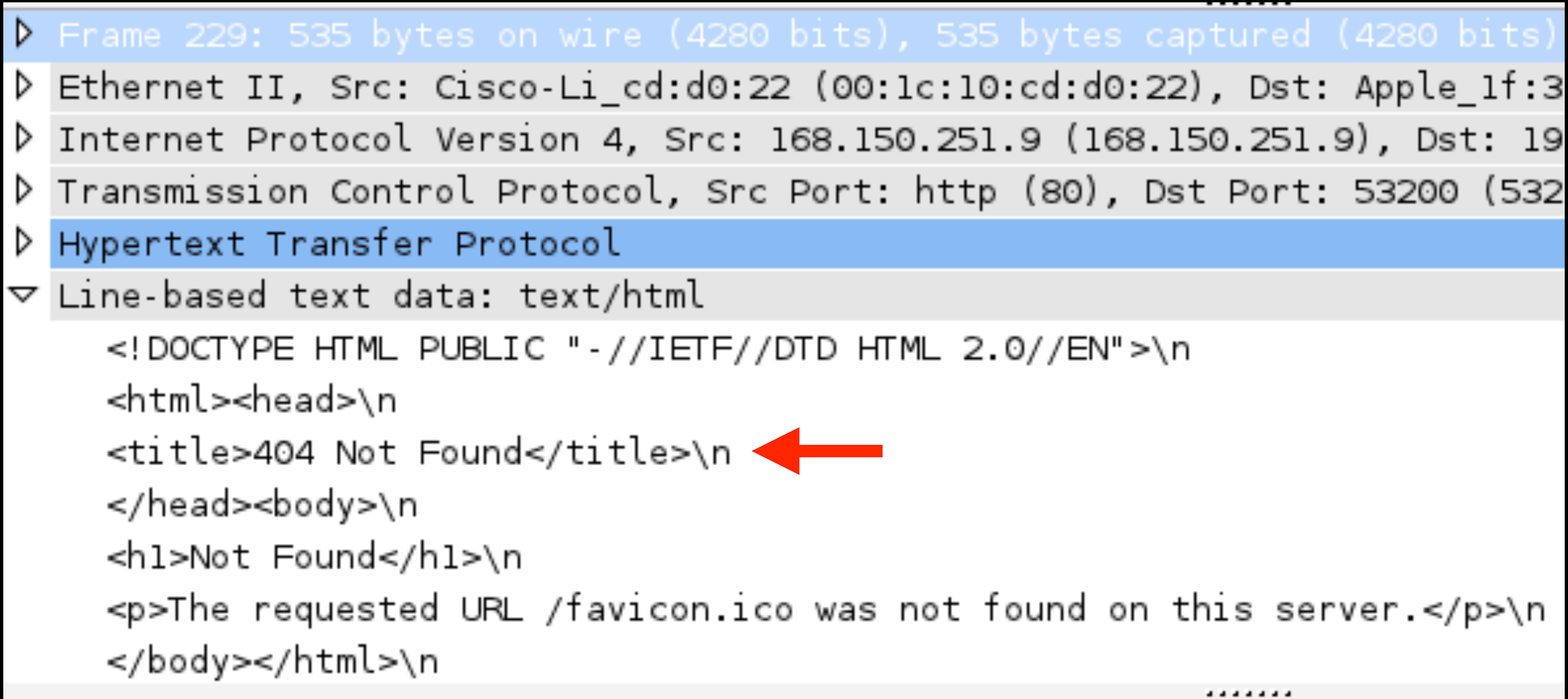
```
▽ Portable Network Graphics
    PNG Signature: 89504e470d0a1a0a
  ▽ IHDR Image Header
      Len: 13
    ▽ Chunk: IHDR
        Width: 100
        Height: 96
        Bit Depth: 8
        Colour Type: Truecolour (2)
        Compression Method: Deflate (0)
        Filter Method: Adaptive (0)
```



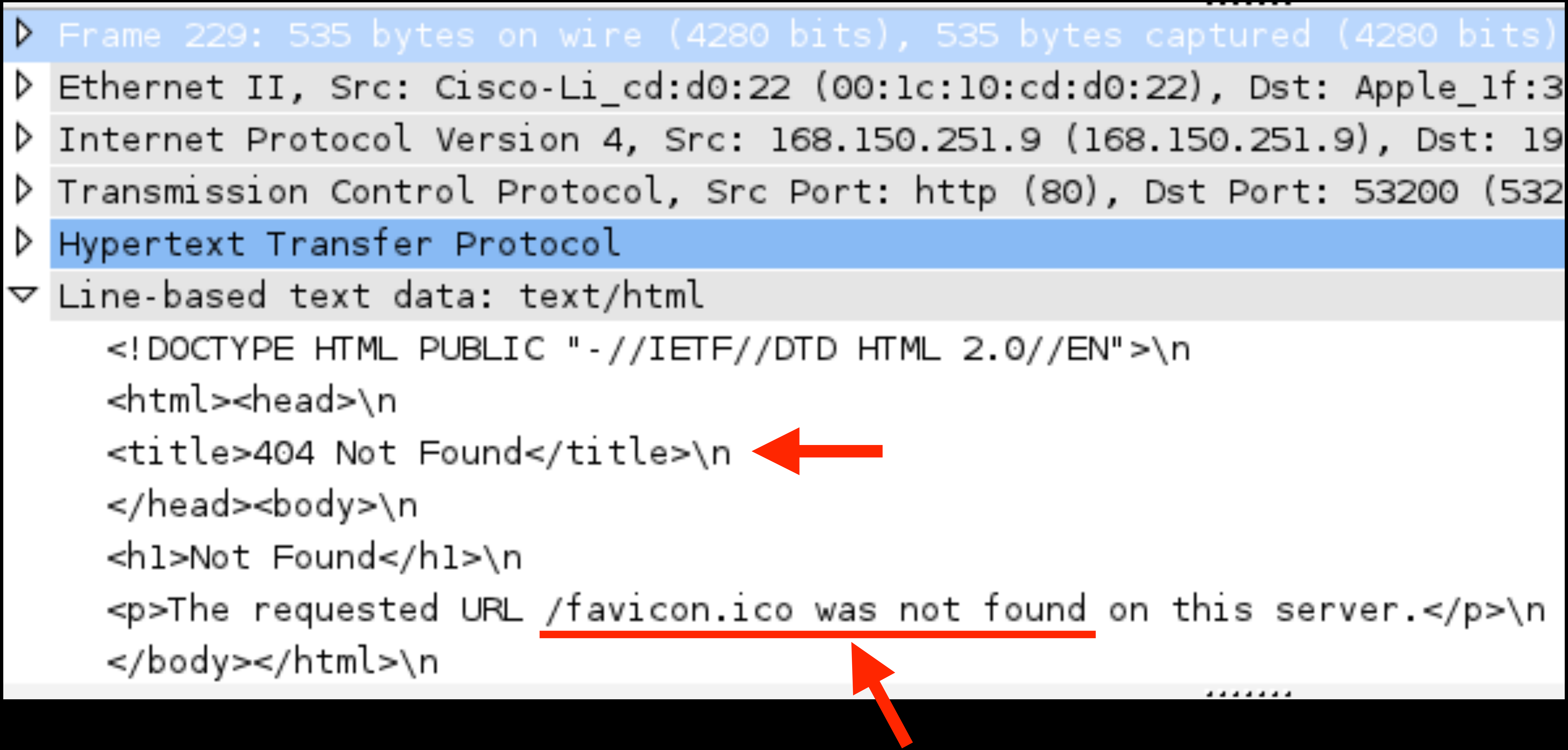
```
▽ Portable Network Graphics
    PNG Signature: 89504e470d0a1a0a
  ▽ IHDR Image Header
      Len: 13
    ▽ Chunk: IHDR
        Width: 100
        Height: 96
        Bit Depth: 8
        Colour Type: Truecolour (2)
        Compression Method: Deflate (0)
        Filter Method: Adaptive (0)
```



```
▷ Frame 229: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits)
▷ Ethernet II, Src: Cisco-Li_cd:d0:22 (00:1c:10:cd:d0:22), Dst: Apple_1f:3
▷ Internet Protocol Version 4, Src: 168.150.251.9 (168.150.251.9), Dst: 19
▷ Transmission Control Protocol, Src Port: http (80), Dst Port: 53200 (532
▷ Hypertext Transfer Protocol
▽ Line-based text data: text/html
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>404 Not Found</title>\n
    </head><body>\n
    <h1>Not Found</h1>\n
    <p>The requested URL /favicon.ico was not found on this server.</p>\n
    </body></html>\n
```



```
▷ Frame 229: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits)
▷ Ethernet II, Src: Cisco-Li_cd:d0:22 (00:1c:10:cd:d0:22), Dst: Apple_1f:3
▷ Internet Protocol Version 4, Src: 168.150.251.9 (168.150.251.9), Dst: 19
▷ Transmission Control Protocol, Src Port: http (80), Dst Port: 53200 (532
▷ Hypertext Transfer Protocol
▽ Line-based text data: text/html
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>404 Not Found</title>\n
    </head><body>\n
    <h1>Not Found</h1>\n
    <p>The requested URL /favicon.ico was not found on this server.</p>\n
    </body></html>\n
```



```
▷ Frame 229: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits)
▷ Ethernet II, Src: Cisco-Li_cd:d0:22 (00:1c:10:cd:d0:22), Dst: Apple_1f:3
▷ Internet Protocol Version 4, Src: 168.150.251.9 (168.150.251.9), Dst: 19
▷ Transmission Control Protocol, Src Port: http (80), Dst Port: 53200 (532
▷ Hypertext Transfer Protocol
▽ Line-based text data: text/html
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>404 Not Found</title>\n
    </head><body>\n
    <h1>Not Found</h1>\n
    <p>The requested URL /favicon.ico was not found on this server.</p>\n
    </body></html>\n
```

Snort

Snort Overview

Snort Overview

- Network-based Intrusion Detection System (IDS)

Snort Overview

- Network-based Intrusion Detection System (IDS)
- Can be Intrusion Prevention System (IPS)

Snort Overview

- Network-based Intrusion Detection System (IDS)
- Can be Intrusion Prevention System (IPS)
- Highly Linux-centric

Snort Overview

- Network-based Intrusion Detection System (IDS)
- Can be Intrusion Prevention System (IPS)
- Highly Linux-centric
- Controlled by Sourcefire

The good news

The good news

There is an installation manual for Lion

Building Snort for Mac OS X 10.7 Lion (Server)

Author : Christoph Murauer
Date : 11.11.2011
Version : 1.1
Created using : Apple´s Wiki 3 Server
E - Mail : christoph_murauer@mac.com
Website : http://www.mac.ph

The bad news

The bad news

It is 17 pages

Download the “Latest” Rules

```
cd $HOME/Source/snort
openssl md5 snortrules-snapshot-2912.tar.gz
more snortrules-snapshot-2912.tar.gz.md5.txt
tar -xzvf snortrules-snapshot-2912.tar.gz
sudo mv ./etc /etc/snort
sudo mv ./preproc_rules /etc/snort/preproc_rules
sudo mv ./rules /etc/snort/rules
sudo mv ./so_rules /etc/snort/so_rules
sudo chown -R root:wheel /etc/snort
```

Modify Configuration File

```
sudo pico /etc/snort/snort.conf
```

Line 101 : var RULE_PATH /etc/snort/rules
Line 102 : var SO_RULE_PATH /etc/snort/so_rules
Line 103 : var PREPROC_RULE_PATH /etc/snort/preproc_rules
Line 403 : preprocessor sfportscan: proto { all } memcap { 10000000 } sense_level { low }
Line 406 : preprocessor arpspoof
Line 505 : output alert_syslog: LOG_LOCAL5 LOG_ALERT
Line 593 - 595 : remove the # and the space at the beginning of the line.
Line 603 - 620 : remove the # and the space at the beginning of the line.

More bad news

More bad news

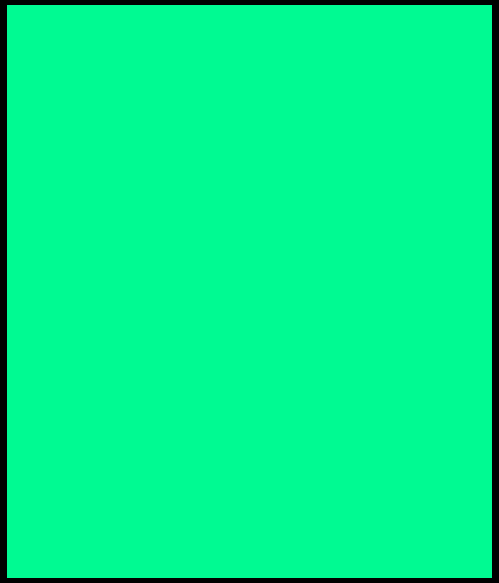
It is open source

More bad news

It is open source–ish

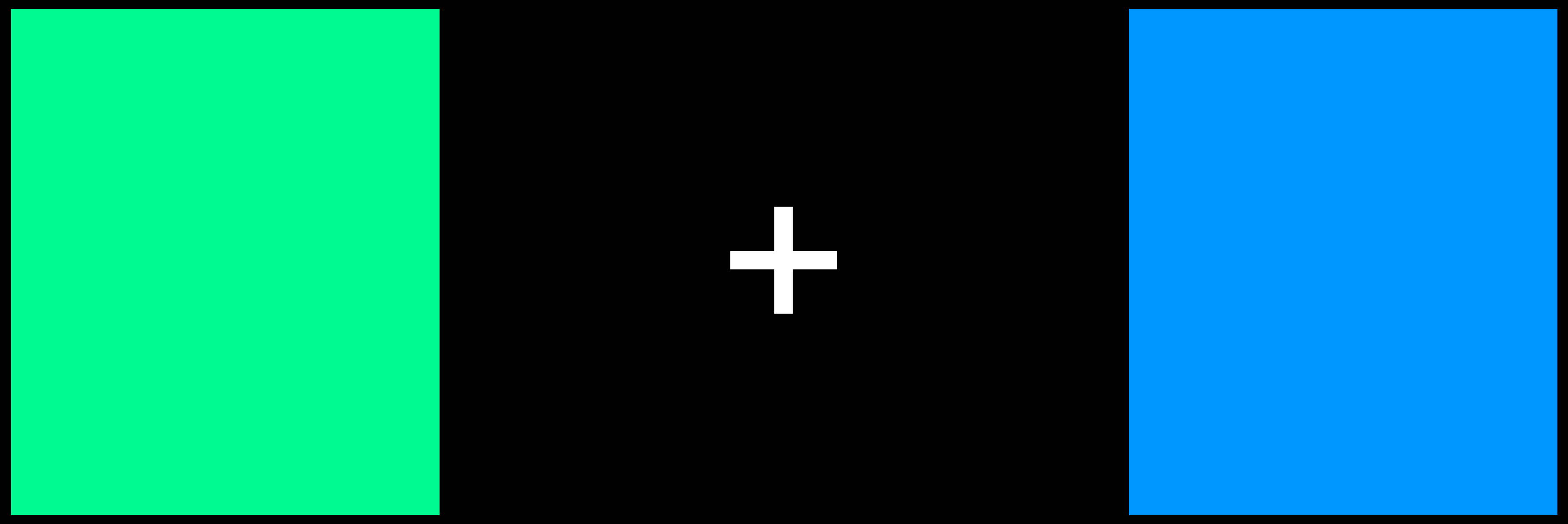
IDS / AV Approach

IDS / AV Approach



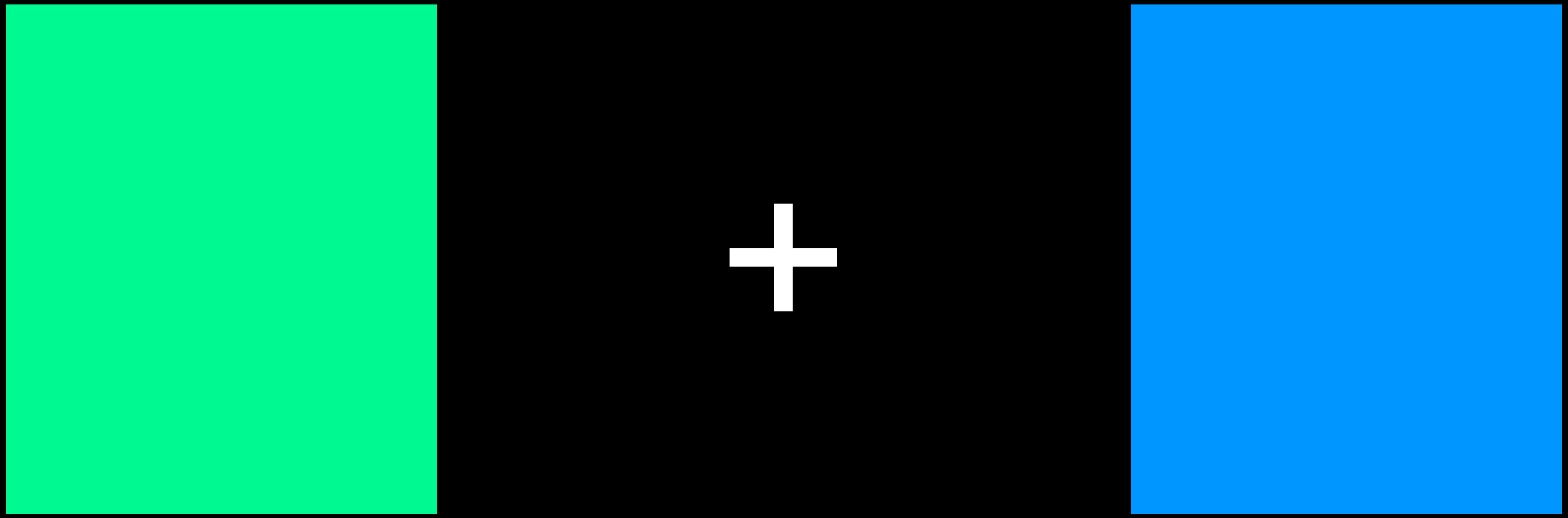
Detection Engine

IDS / AV Approach



Detection Engine + Signatures / Rules

IDS / AV Approach

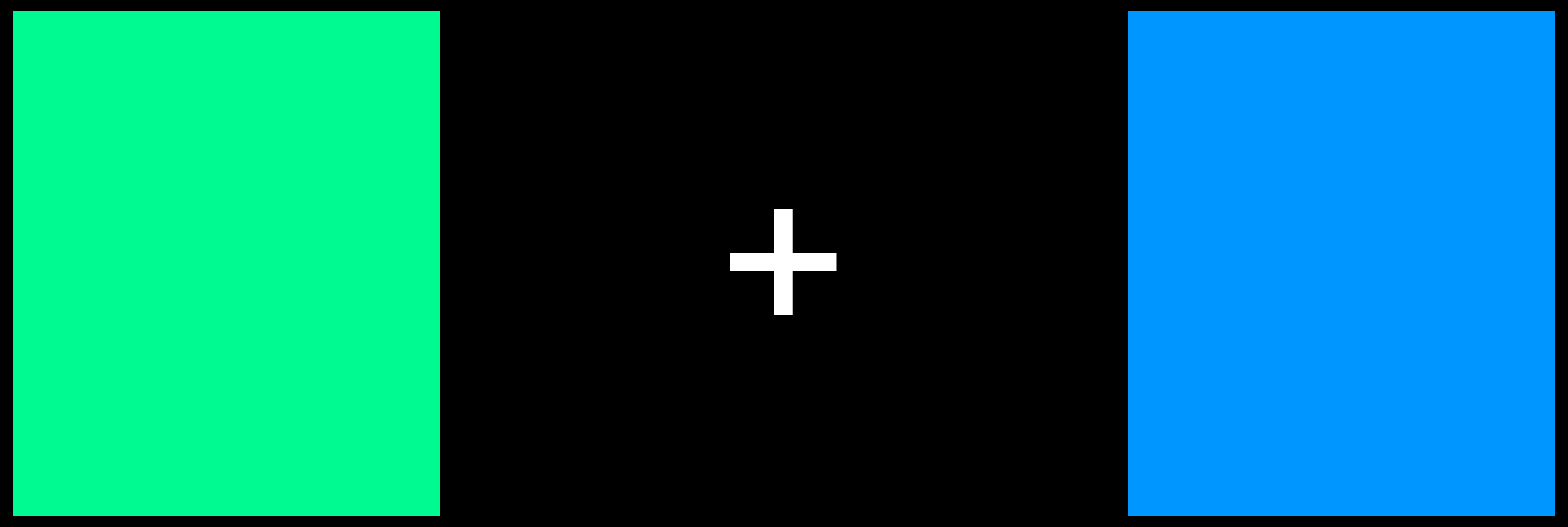


Detection Engine

Open Source

Signatures / Rules

IDS / AV Approach



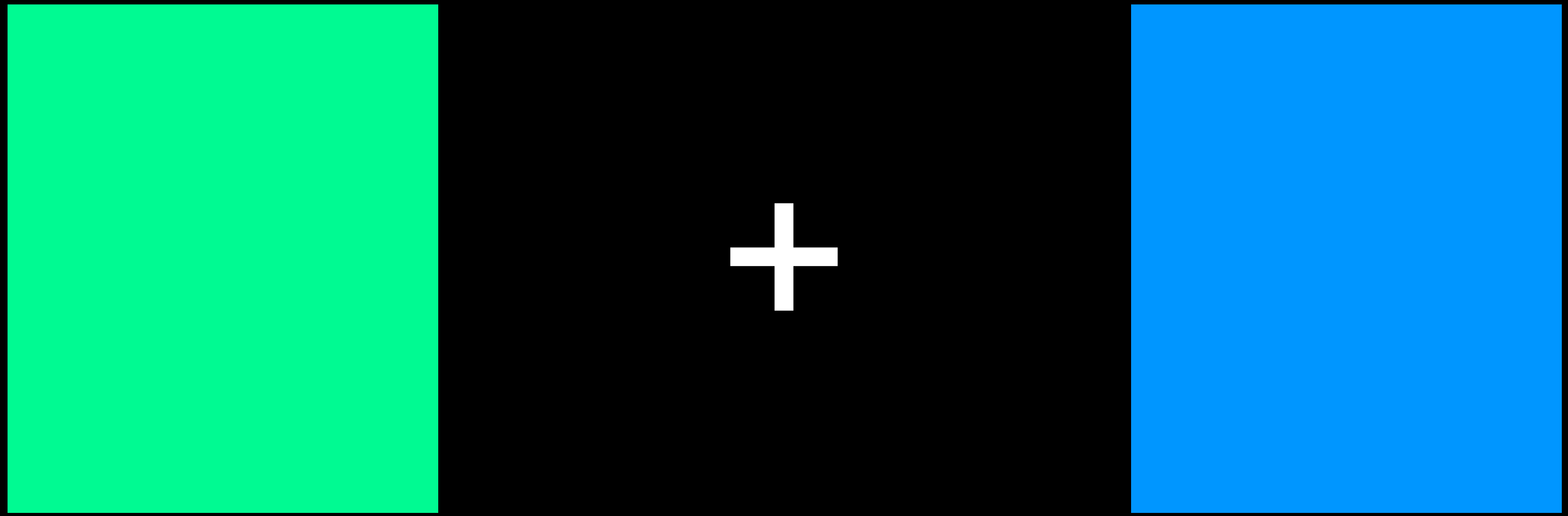
Detection Engine

Open Source

Signatures / Rules

Proprietary

IDS / AV Approach



Detection Engine

Open Source

Signatures / Rules

Proprietary

$$$

Rules Access

Rules Access

Access Level	When

Rules Access

Access Level	When
Unregistered	Good luck (at point Snort releases)

Rules Access

Access Level	When
Unregistered	Good luck (at point Snort releases)
Registered (free)	30 days late

Rules Access

Access Level	When
Unregistered	Good luck (at point Snort releases)
Registered (free)	30 days late
Subscription ($$$)	Up to date

Subscription Costs

Subscription Costs

Subscription Type	Pricing	Sensor(s)

Subscription Costs

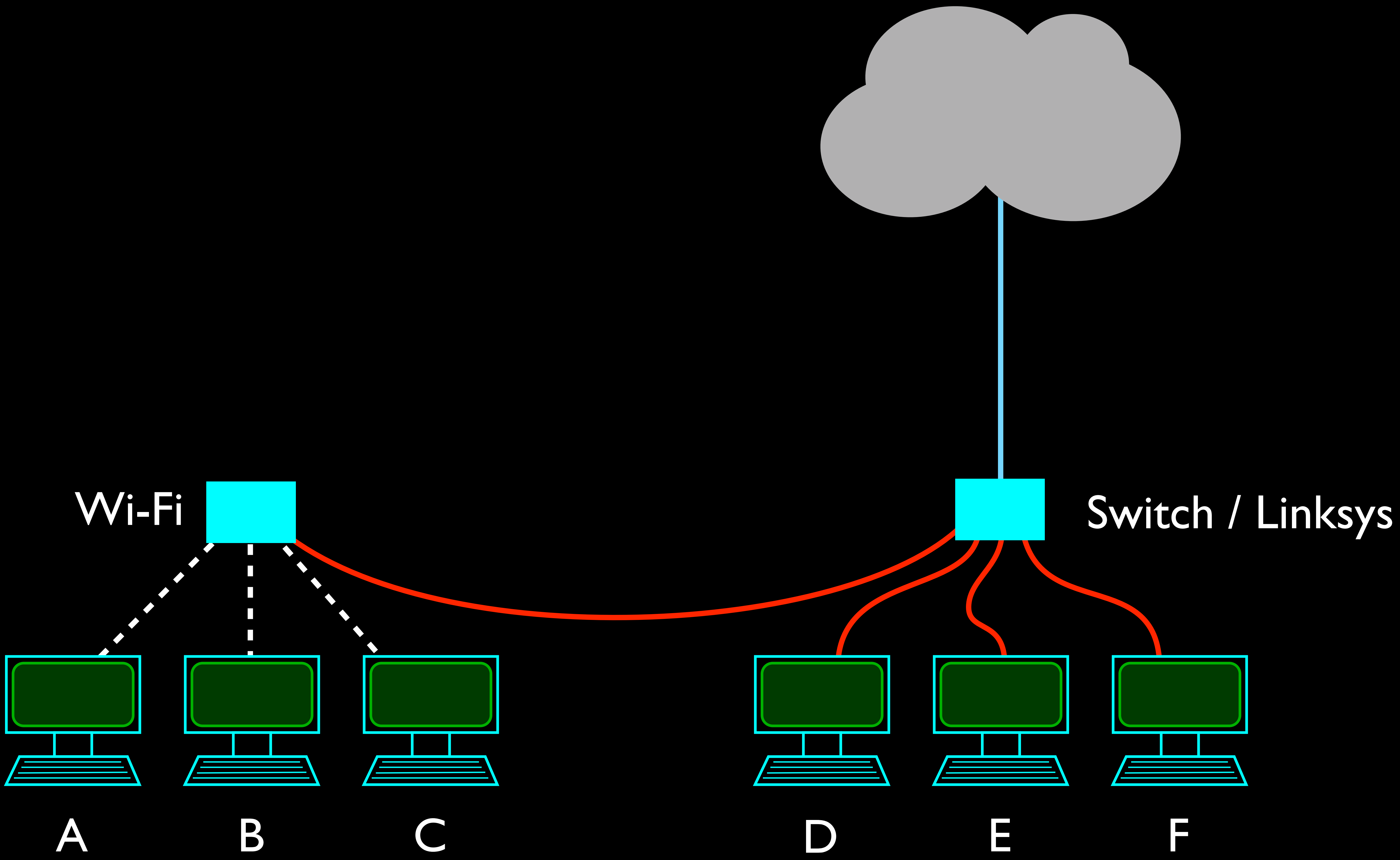
Subscription Type	Pricing	Sensor(s)
Personal	$30 / sensor	1

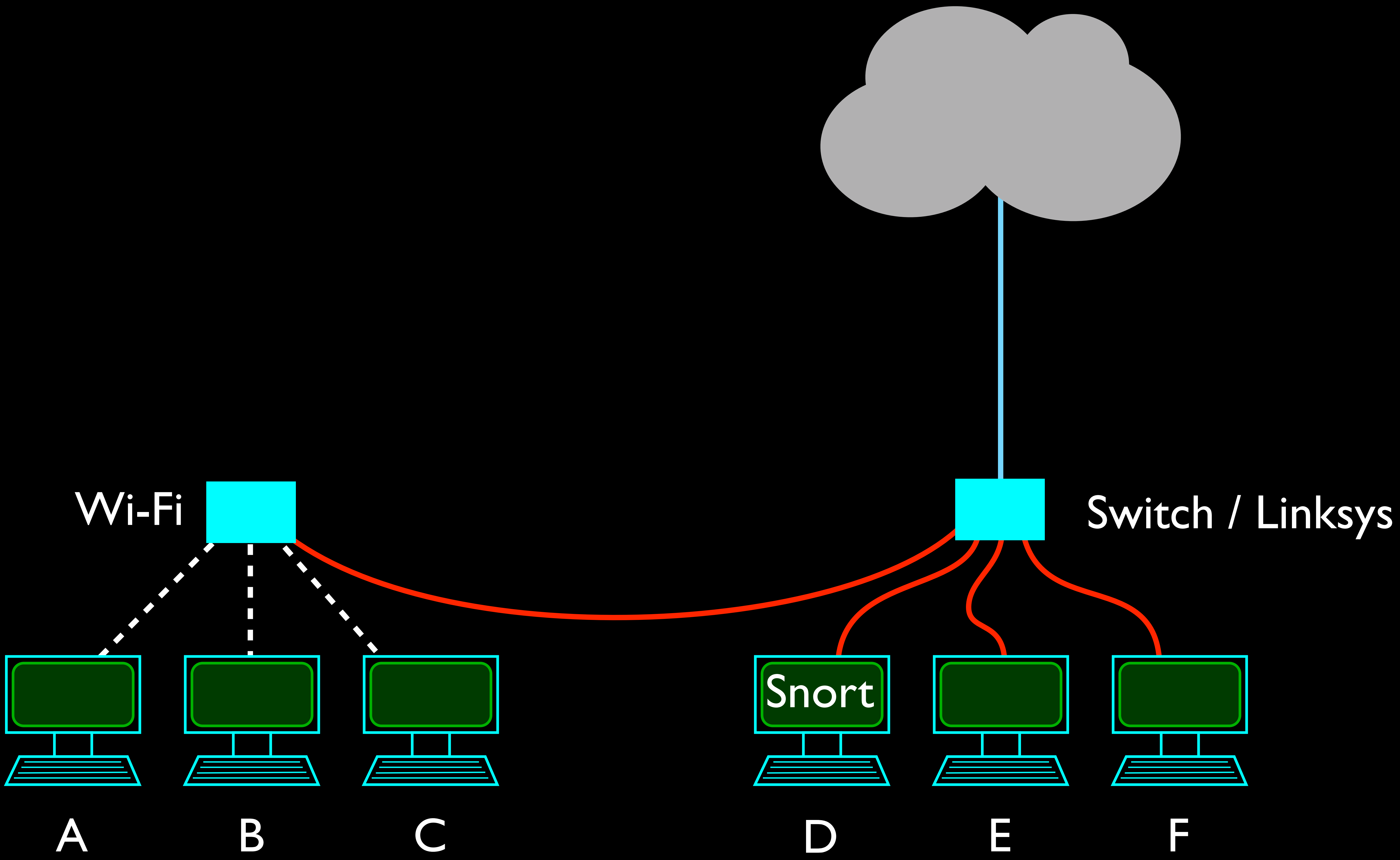
Subscription Costs

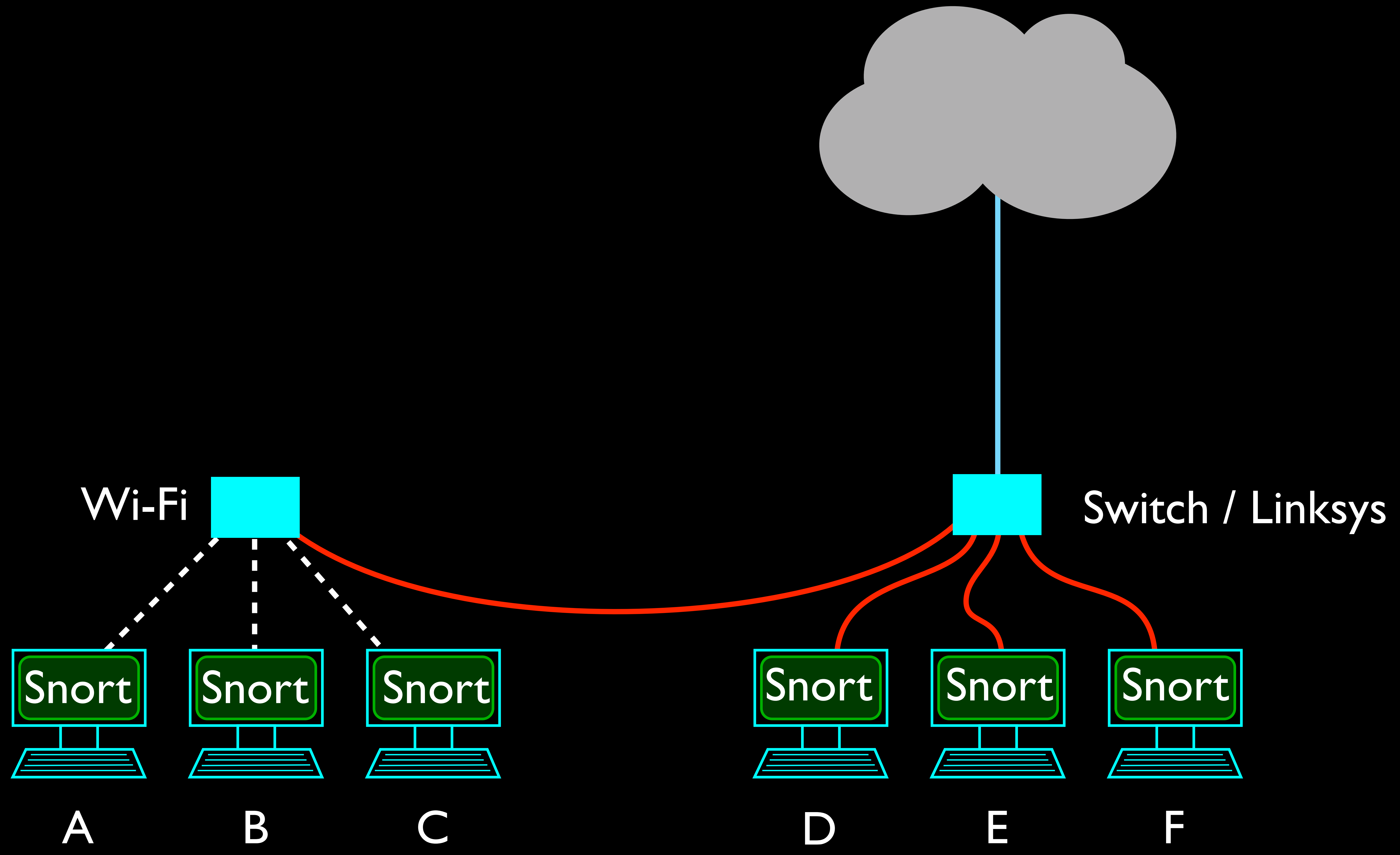
Subscription Type	Pricing	Sensor(s)
Personal	$30 / sensor	1
Business	$500 / sensor	1-5

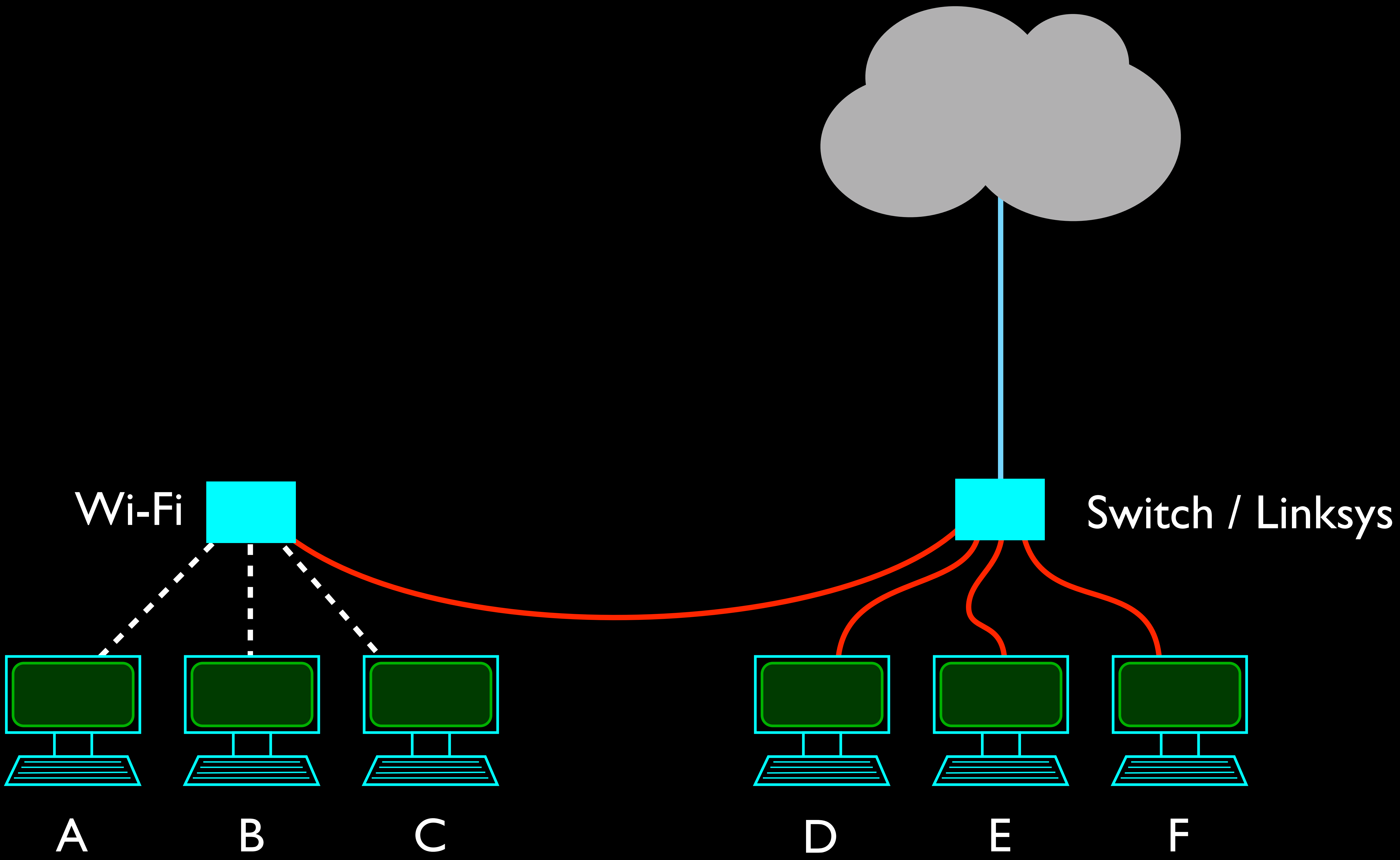
Subscription Costs

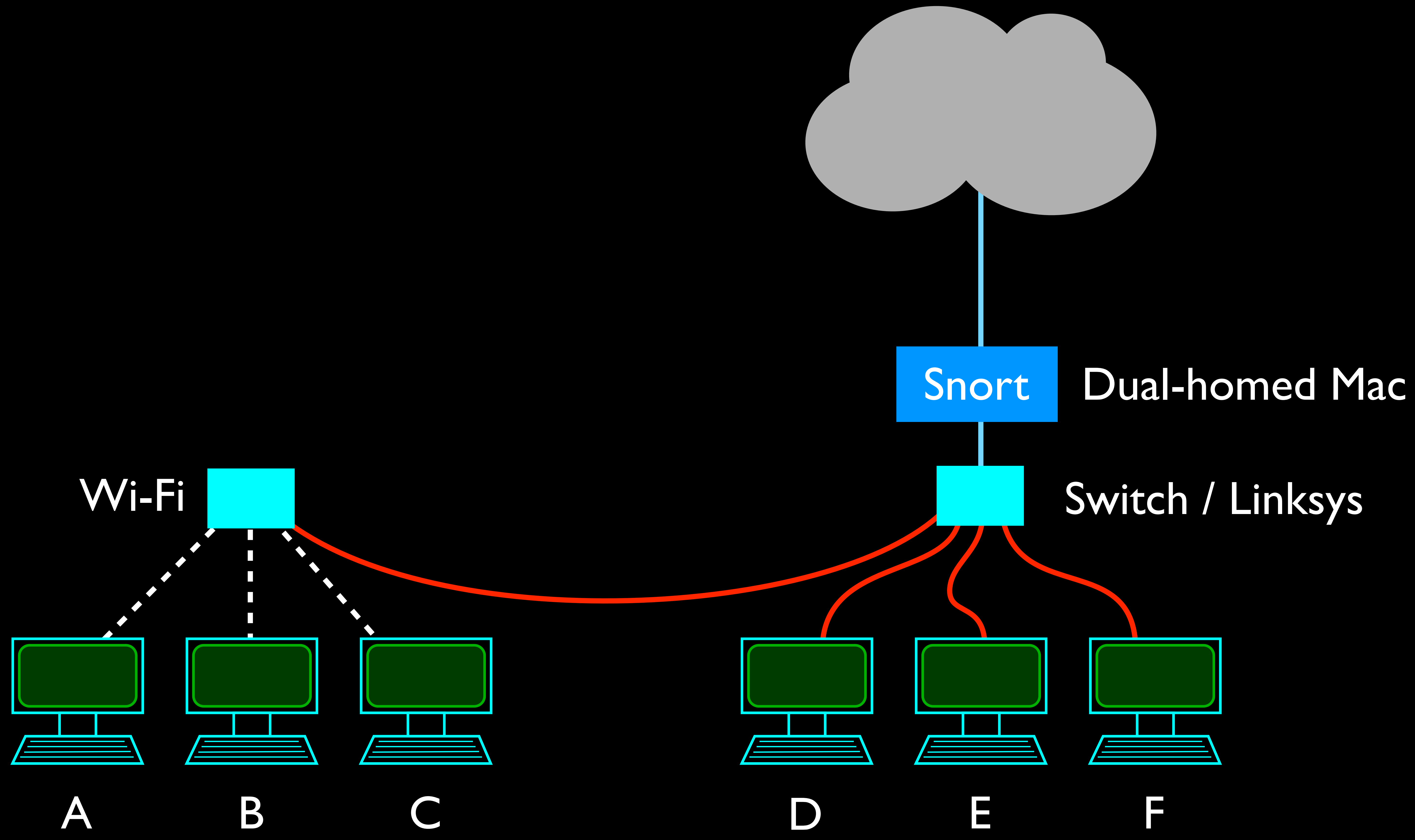
Subscription Type	Pricing	Sensor(s)
Personal	$30 / sensor	1
Business	$500 / sensor	1-5
Business	$400 / sensor	6+

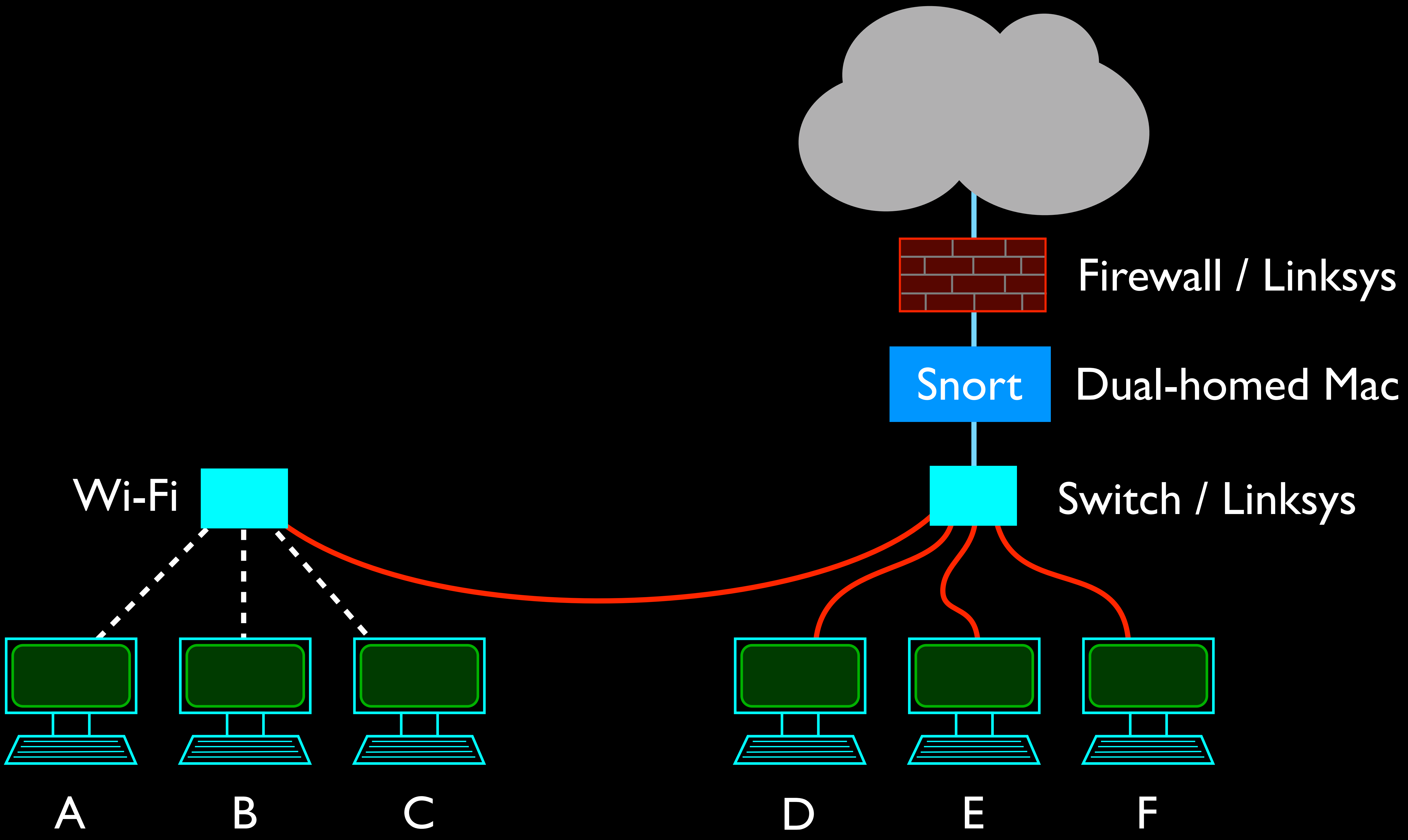

Wi-Fi
Switch / Linksys
A
B
C
D
E
F


Wi-Fi
Switch / Linksys
Snort
A
B
C
D
E
F


Wi-Fi
Switch / Linksys
Snort
Snort
Snort
Snort
Snort
Snort
A
B
C
D
E
F


Wi-Fi
Switch / Linksys
A
B
C
D
E
F


Snort
Dual-homed Mac
Wi-Fi
Switch / Linksys
A
B
C
D
E
F


Firewall / Linksys
Snort
Dual-homed Mac
Wi-Fi
Switch / Linksys
A
B
C
D
E
F

Nmap

Nmap Overview

Nmap Overview

- Maps out your network (not a sniffer)

Nmap Overview

- Maps out your network (not a sniffer)
- Identifies assets on your network (ping sweep)

Nmap Overview

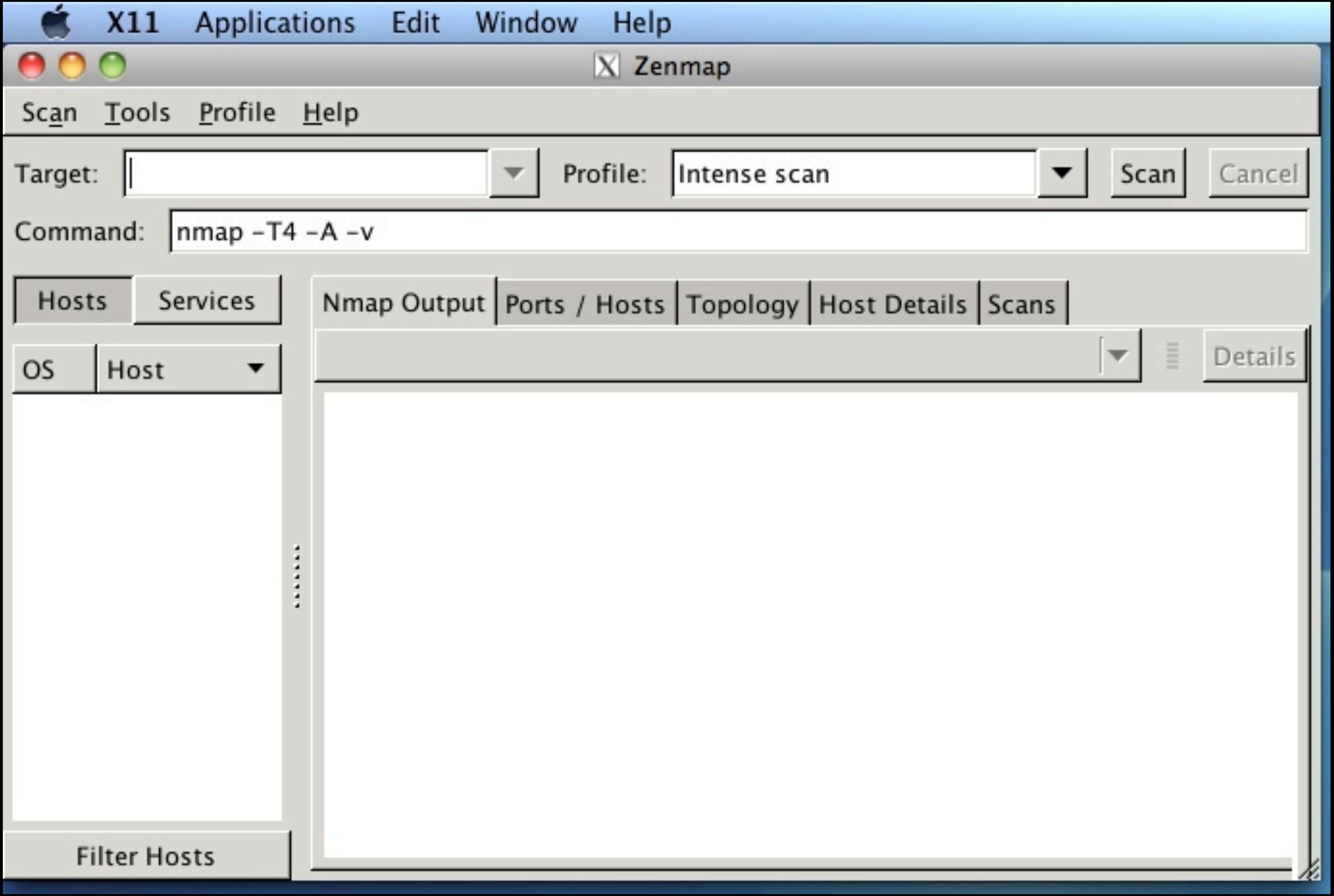
- Maps out your network (not a sniffer)
- Identifies assets on your network (ping sweep)
- Identifies services running on each asset

Nmap Overview

- Maps out your network (not a sniffer)
- Identifies assets on your network (ping sweep)
- Identifies services running on each asset
- “Determines” the type of machine / OS on for each asset

Nmap Overview

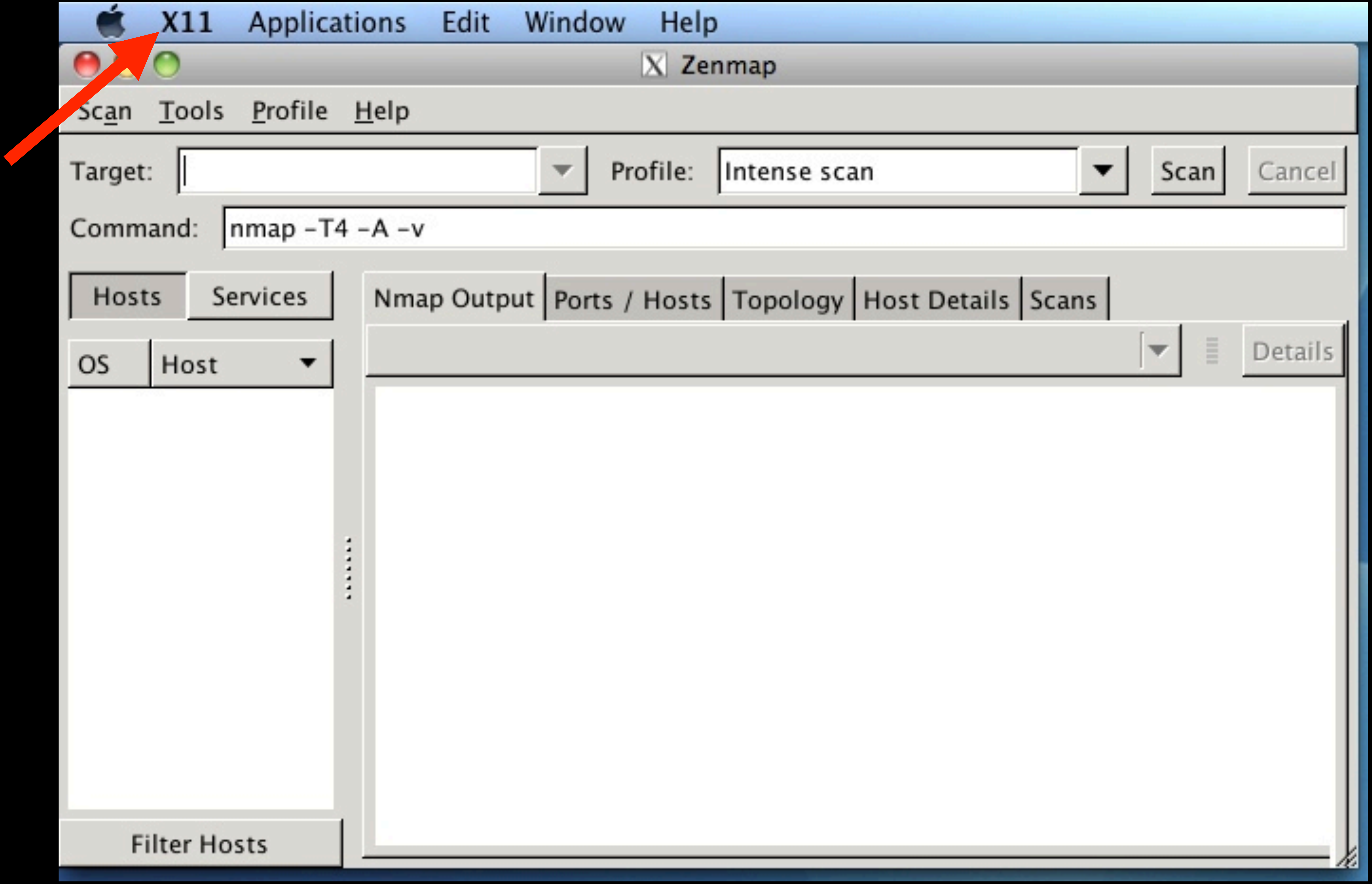
- Maps out your network (not a sniffer)
- Identifies assets on your network (ping sweep)
- Identifies services running on each asset
- “Determines” the type of machine / OS on for each asset
- Zenmap GUI front-end does not run on Lion
  (command line tool does)



Target:

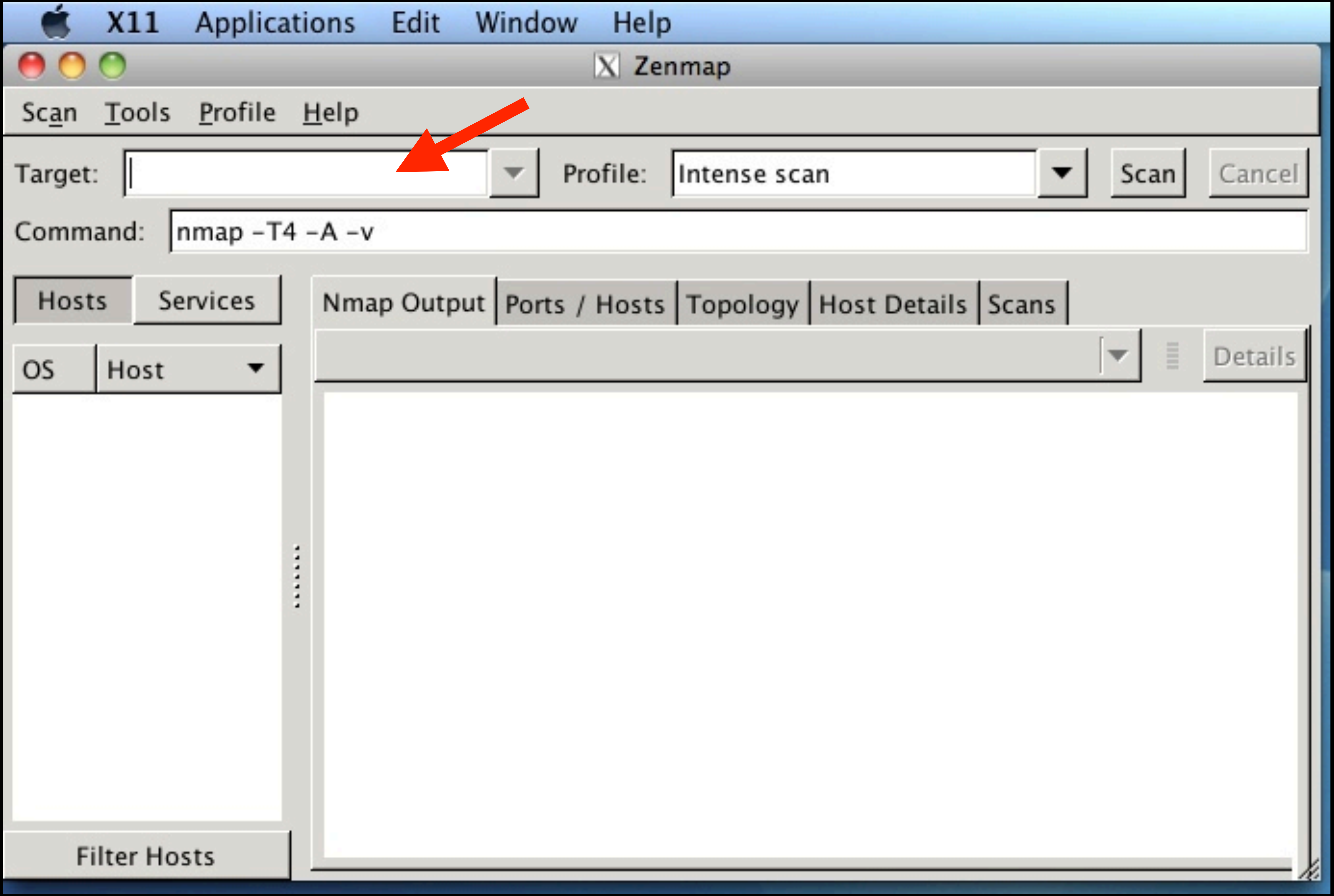
Profile: Intense scan

Command: nmap -T4 -A -v



Profile: Intense scan

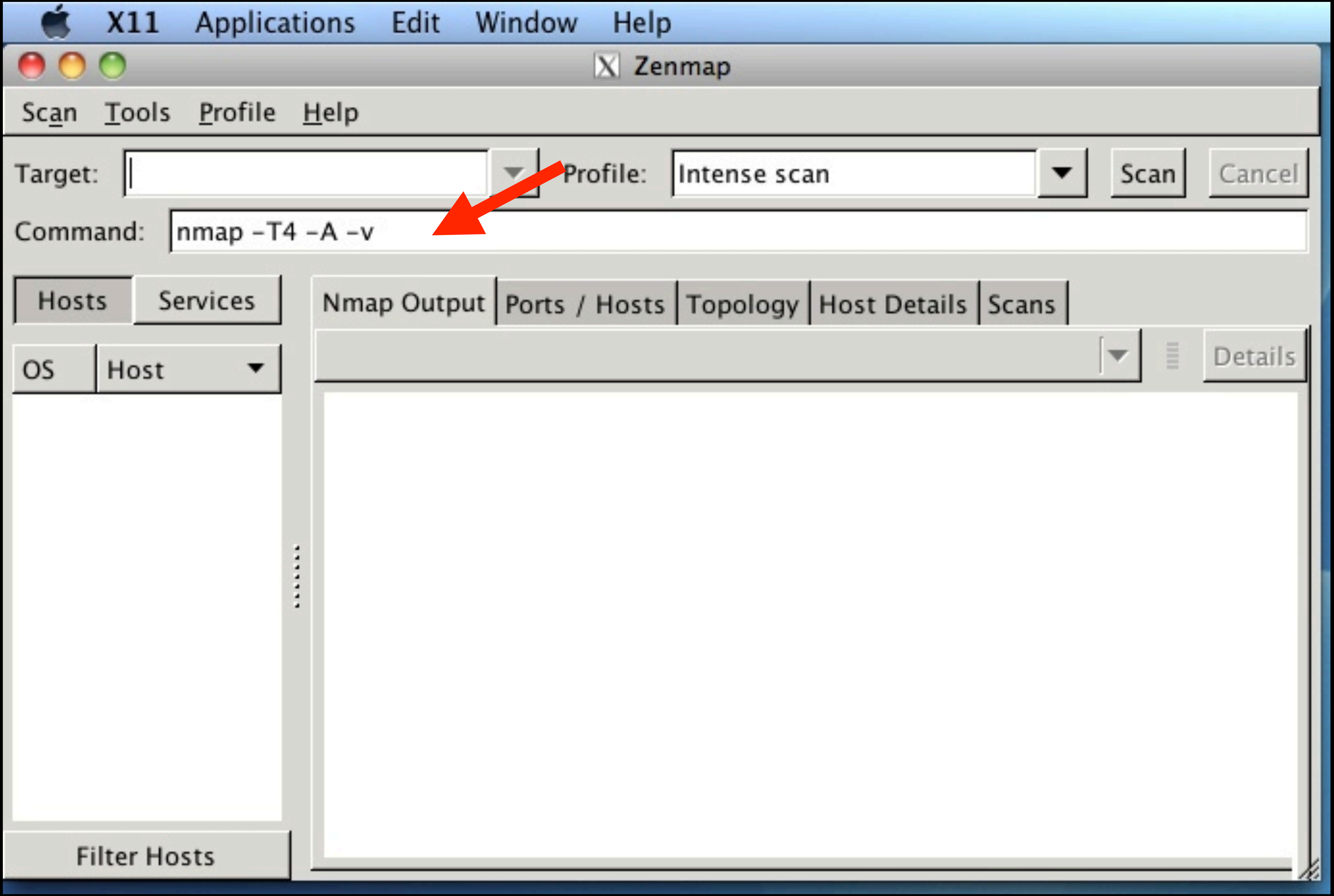
Command: nmap -T4 -A -v



Target:

Profile: Intense scan

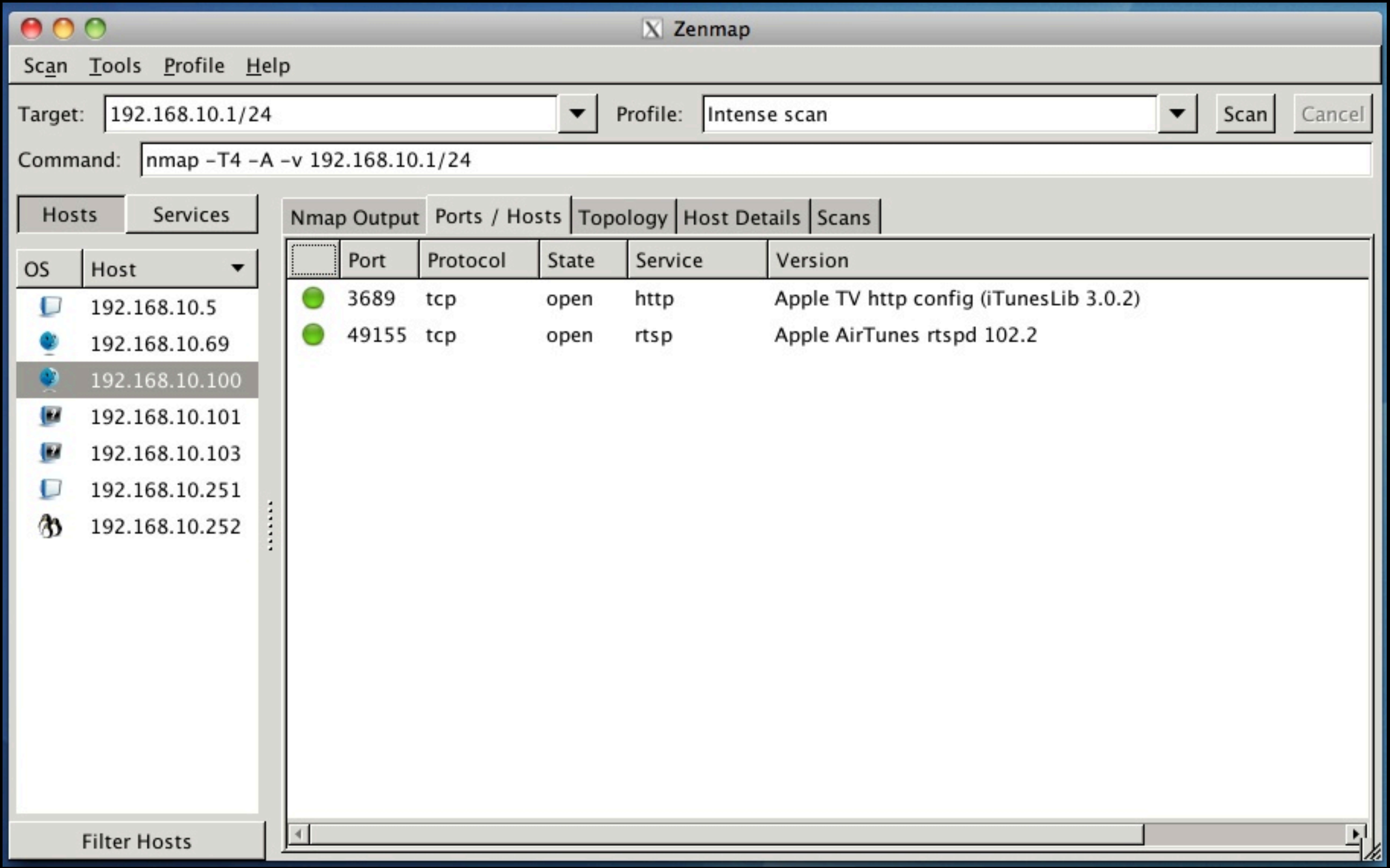
Command: nmap -T4 -A -v



Target:

Profile: Intense scan

Command: nmap -T4 -A -v



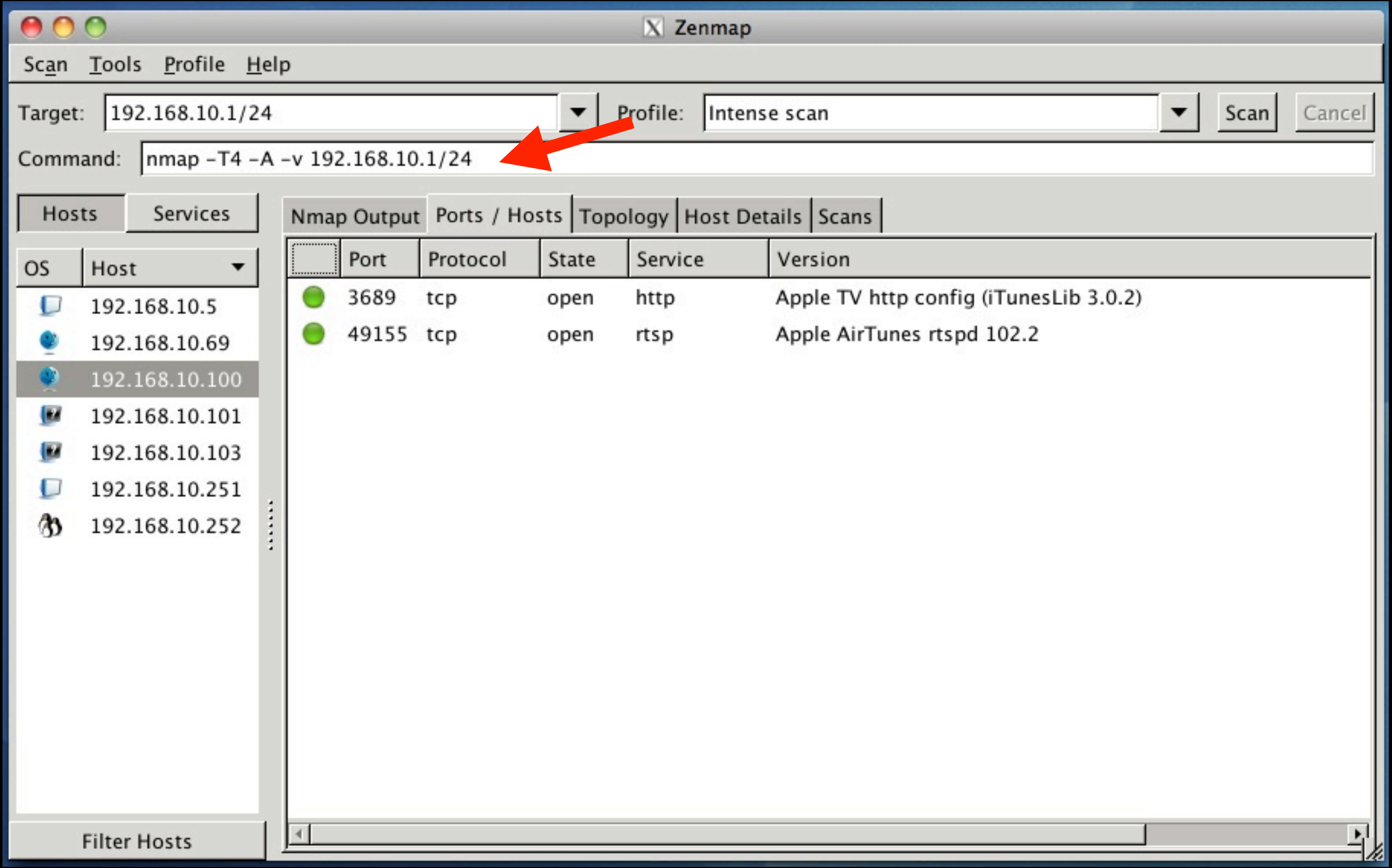
Target: 192.168.10.1/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.1/24

OS	Host
	192.168.10.5
	192.168.10.69
	192.168.10.100
	192.168.10.101
	192.168.10.103
	192.168.10.251
	192.168.10.252

	Port	Protocol	State	Service	Version
●	3689	tcp	open	http	Apple TV http config (iTunesLib 3.0.2)
●	49155	tcp	open	rtsp	Apple AirTunes rtspd 102.2



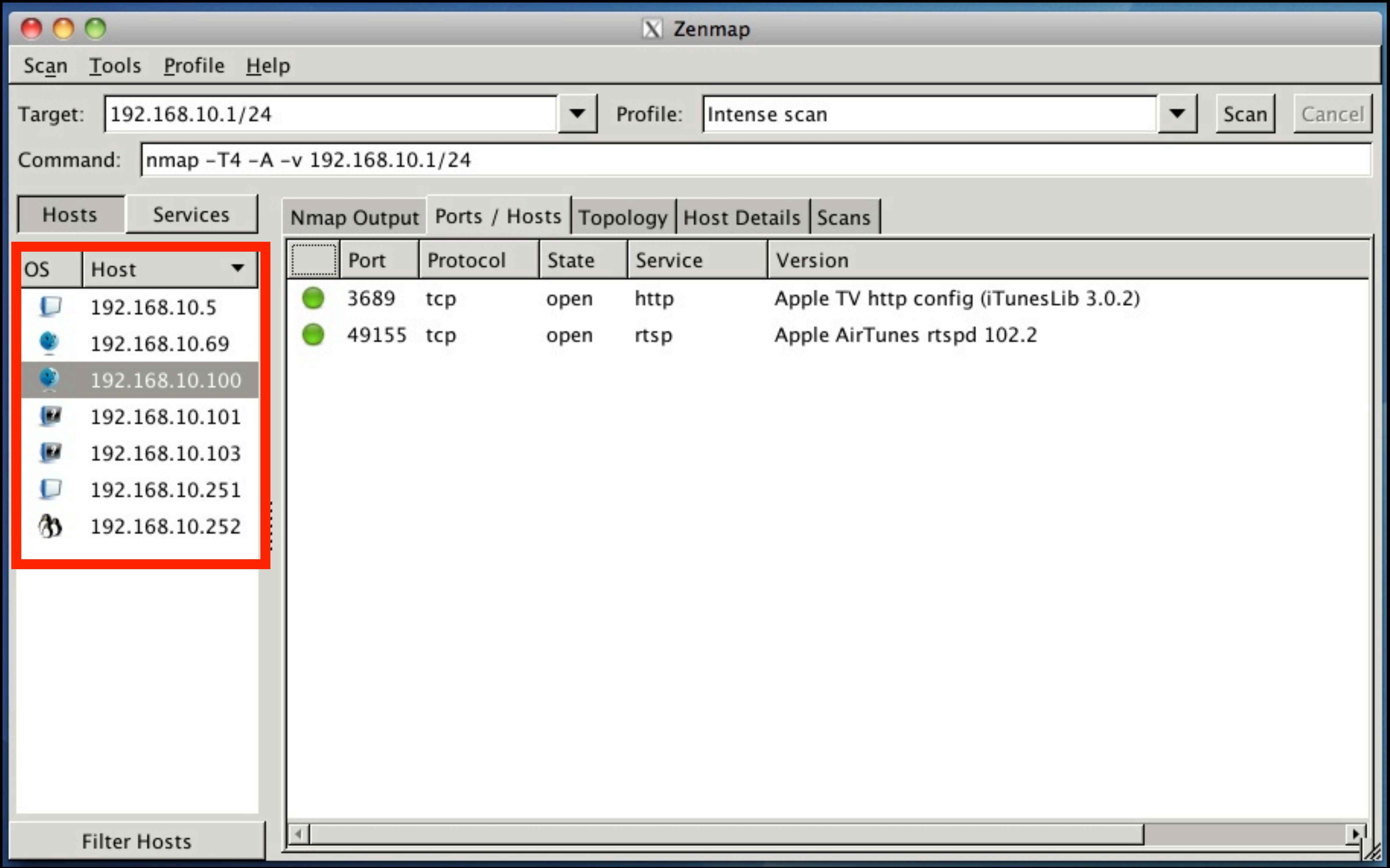
Target: 192.168.10.1/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.1/24

OS	Host
	192.168.10.5
	192.168.10.69
	192.168.10.100
	192.168.10.101
	192.168.10.103
	192.168.10.251
	192.168.10.252

	Port	Protocol	State	Service	Version
●	3689	tcp	open	http	Apple TV http config (iTunesLib 3.0.2)
●	49155	tcp	open	rtsp	Apple AirTunes rtspd 102.2



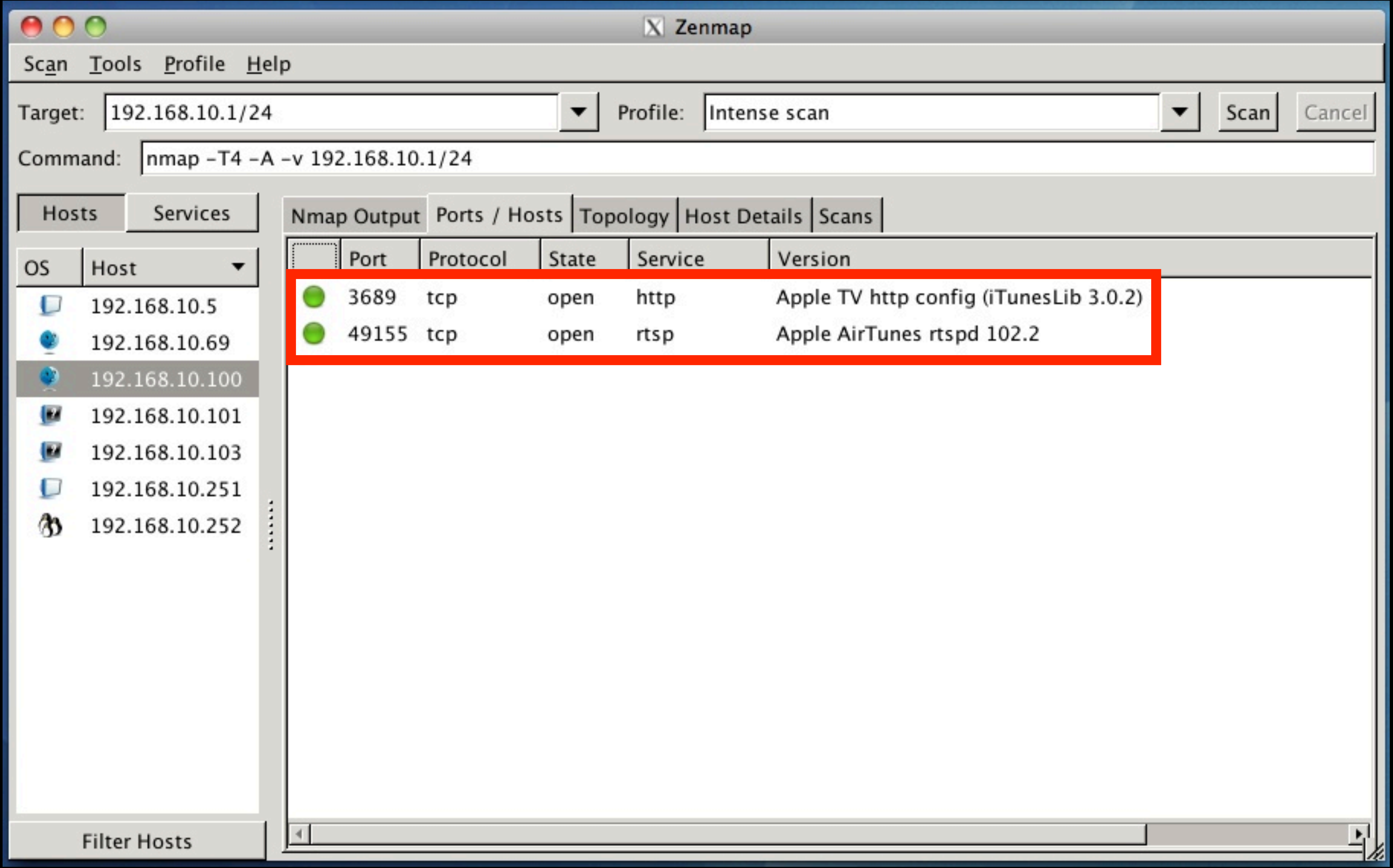
Target: 192.168.10.1/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.10.1/24

OS	Host
	192.168.10.5
	192.168.10.69
	192.168.10.100
	192.168.10.101
	192.168.10.103
	192.168.10.251
	192.168.10.252

	Port	Protocol	State	Service	Version
●	3689	tcp	open	http	Apple TV http config (iTunesLib 3.0.2)
●	49155	tcp	open	rtsp	Apple AirTunes rtspd 102.2



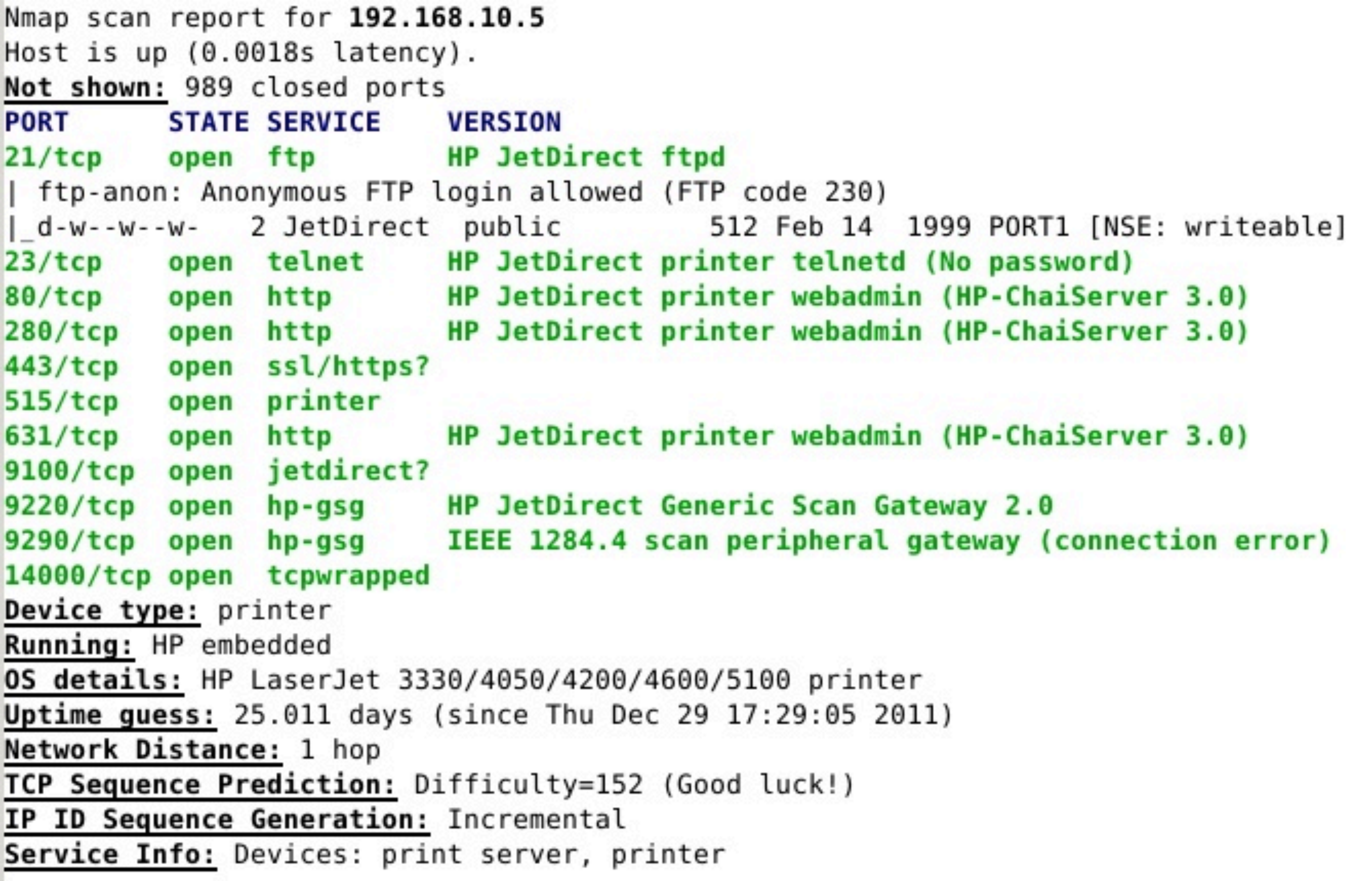
Target: 192.168.10.1/24

Profile: Intense scan

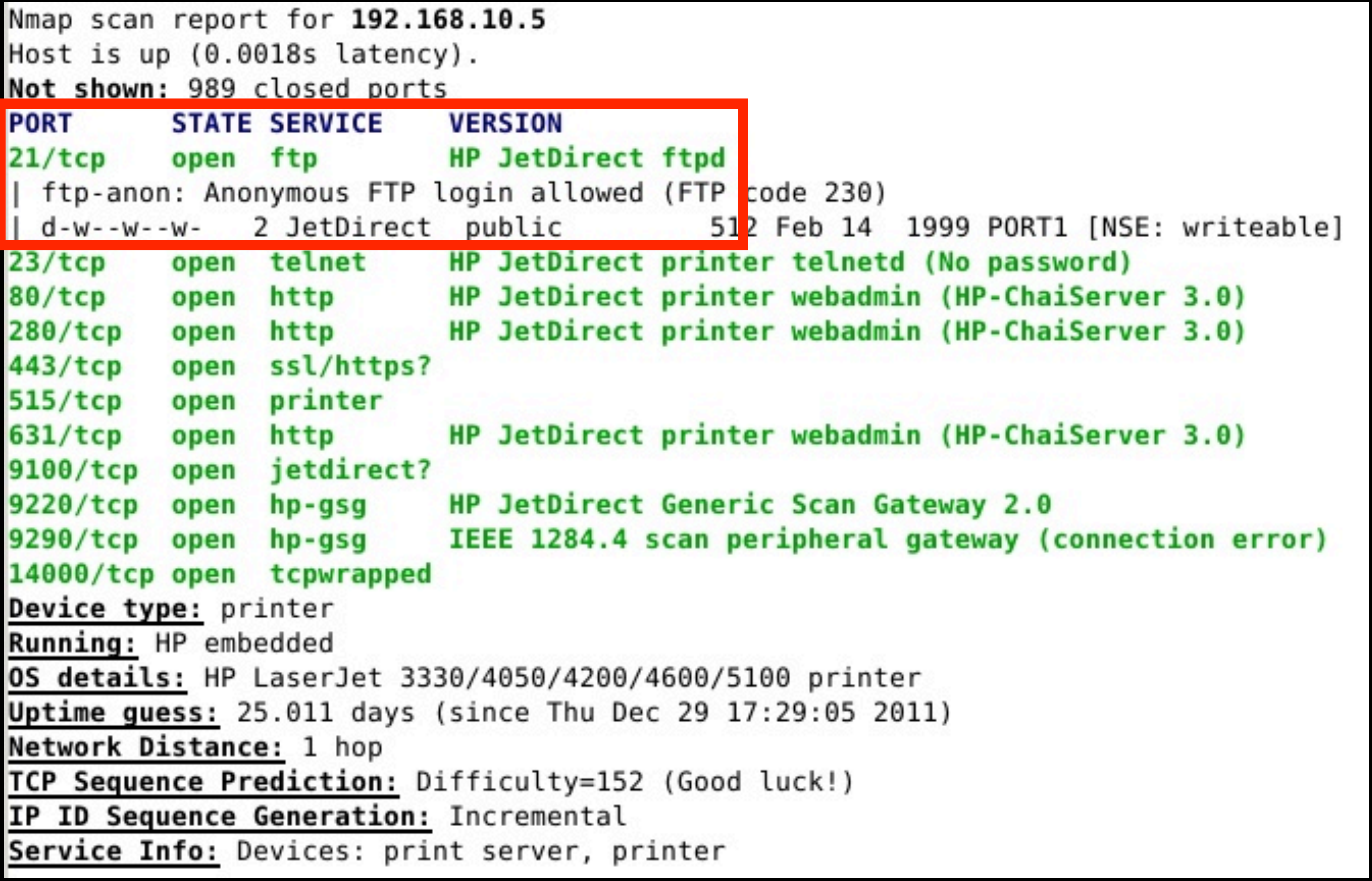
Command: nmap -T4 -A -v 192.168.10.1/24

OS	Host
	192.168.10.5
	192.168.10.69
	192.168.10.100
	192.168.10.101
	192.168.10.103
	192.168.10.251
	192.168.10.252

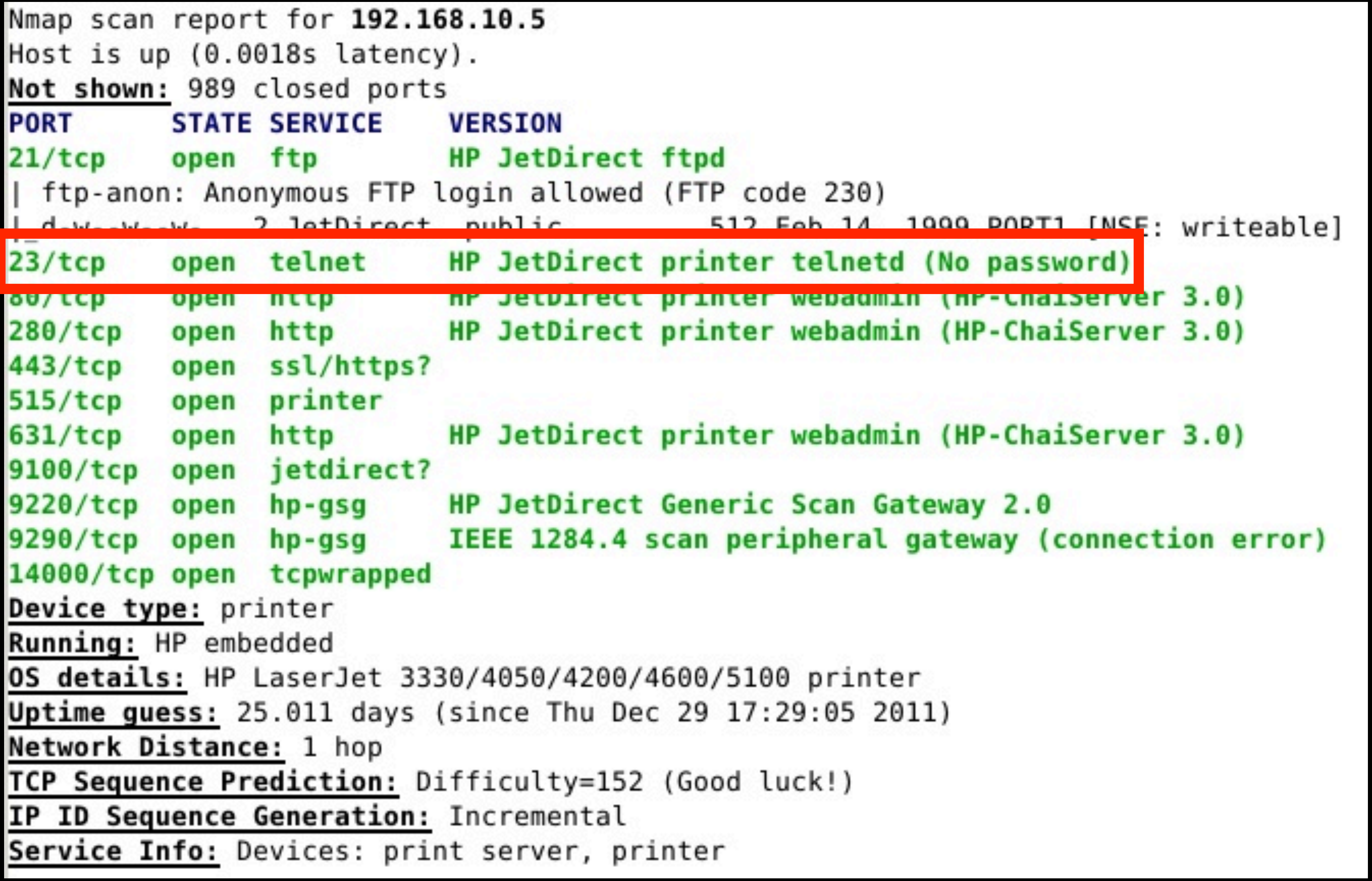
	Port	Protocol	State	Service	Version
●	3689	tcp	open	http	Apple TV http config (iTunesLib 3.0.2)
●	49155	tcp	open	rtsp	Apple AirTunes rtspd 102.2



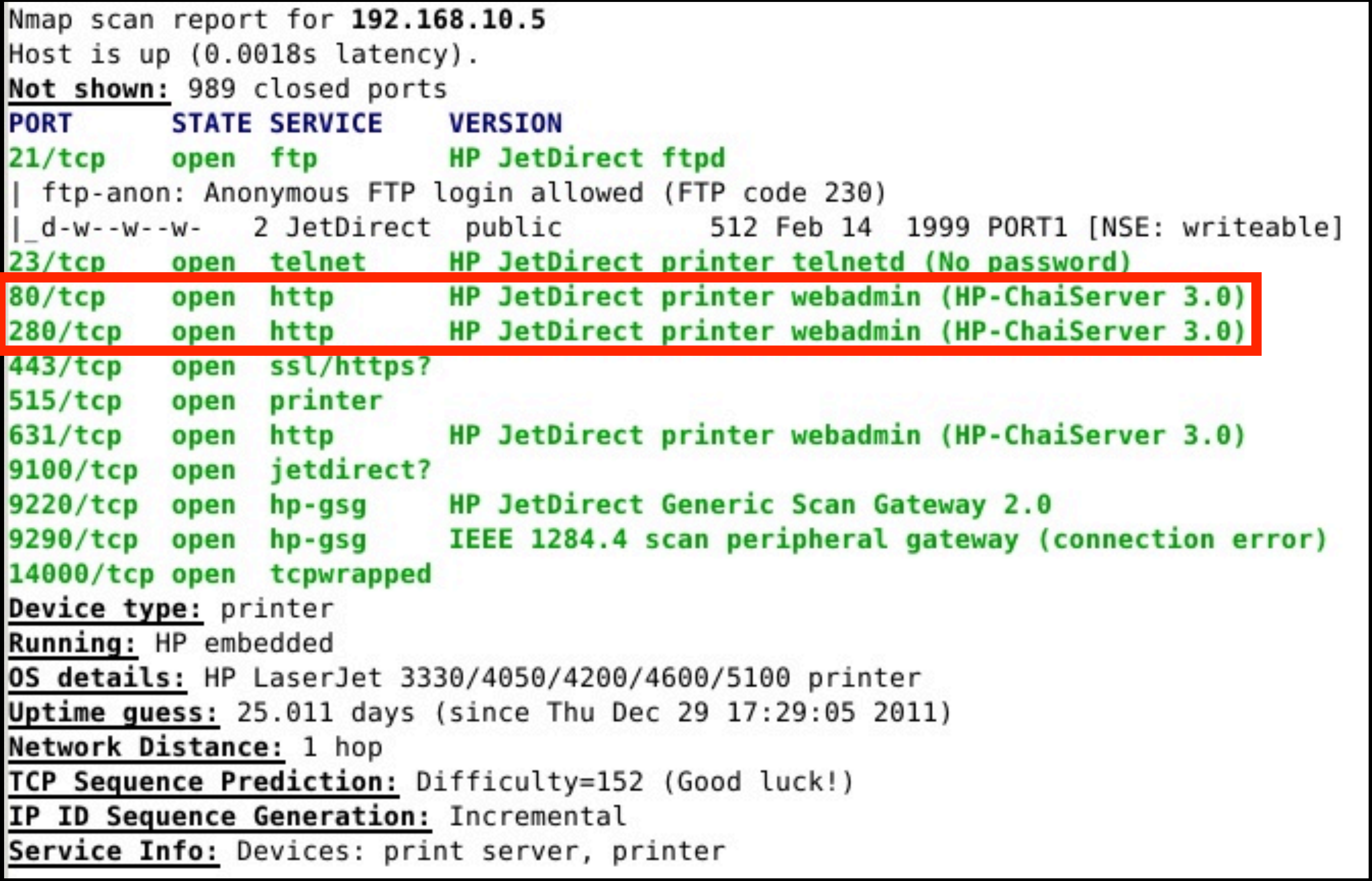
```
Nmap scan report for 192.168.10.5
Host is up (0.0018s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        HP JetDirect ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_d-w--w--w-   2 JetDirect  public         512 Feb 14  1999 PORT1 [NSE: writeable]
23/tcp    open  telnet     HP JetDirect printer telnetd (No password)
80/tcp    open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
280/tcp   open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
443/tcp   open  ssl/https?
515/tcp   open  printer
631/tcp   open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
9100/tcp  open  jetdirect?
9220/tcp  open  hp-gsg     HP JetDirect Generic Scan Gateway 2.0
9290/tcp  open  hp-gsg     IEEE 1284.4 scan peripheral gateway (connection error)
14000/tcp open  tcpwrapped
Device type: printer
Running: HP embedded
OS details: HP LaserJet 3330/4050/4200/4600/5100 printer
Uptime guess: 25.011 days (since Thu Dec 29 17:29:05 2011)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=152 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Devices: print server, printer
```



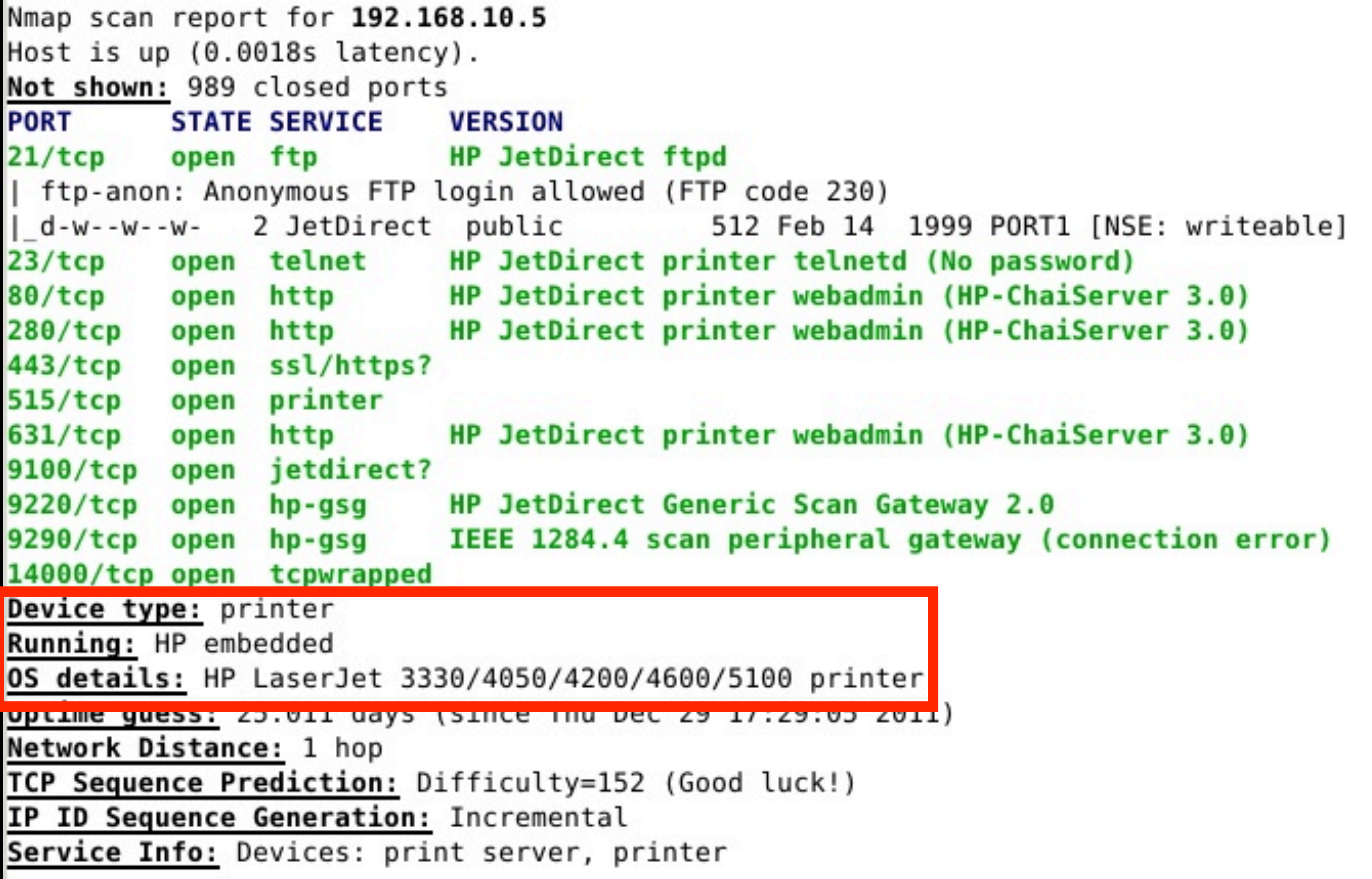
```
Nmap scan report for 192.168.10.5
Host is up (0.0018s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        HP JetDirect ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| d-w--w--w-   2 JetDirect  public         512 Feb 14  1999 PORT1 [NSE: writeable]
23/tcp    open  telnet     HP JetDirect printer telnetd (No password)
80/tcp    open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
280/tcp   open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
443/tcp   open  ssl/https?
515/tcp   open  printer
631/tcp   open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
9100/tcp  open  jetdirect?
9220/tcp  open  hp-gsg     HP JetDirect Generic Scan Gateway 2.0
9290/tcp  open  hp-gsg     IEEE 1284.4 scan peripheral gateway (connection error)
14000/tcp open  tcpwrapped
Device type: printer
Running: HP embedded
OS details: HP LaserJet 3330/4050/4200/4600/5100 printer
Uptime guess: 25.011 days (since Thu Dec 29 17:29:05 2011)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=152 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Devices: print server, printer
```



```
Nmap scan report for 192.168.10.5
Host is up (0.0018s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        HP JetDirect ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx   2 JetDirect  public         512 Feb 14  1999 PORT1 [NSE: writeable]
23/tcp    open  telnet     HP JetDirect printer telnetd (No password)
80/tcp    open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
280/tcp   open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
443/tcp   open  ssl/https?
515/tcp   open  printer
631/tcp   open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
9100/tcp  open  jetdirect?
9220/tcp  open  hp-gsg     HP JetDirect Generic Scan Gateway 2.0
9290/tcp  open  hp-gsg     IEEE 1284.4 scan peripheral gateway (connection error)
14000/tcp open  tcpwrapped
Device type: printer
Running: HP embedded
OS details: HP LaserJet 3330/4050/4200/4600/5100 printer
Uptime guess: 25.011 days (since Thu Dec 29 17:29:05 2011)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=152 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Devices: print server, printer
```



```
Nmap scan report for 192.168.10.5
Host is up (0.0018s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        HP JetDirect ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_d-w--w--w-   2 JetDirect  public         512 Feb 14  1999 PORT1 [NSE: writeable]
23/tcp    open  telnet     HP JetDirect printer telnetd (No password)
80/tcp    open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
280/tcp   open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
443/tcp   open  ssl/https?
515/tcp   open  printer
631/tcp   open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
9100/tcp  open  jetdirect?
9220/tcp  open  hp-gsg     HP JetDirect Generic Scan Gateway 2.0
9290/tcp  open  hp-gsg     IEEE 1284.4 scan peripheral gateway (connection error)
14000/tcp open  tcpwrapped
Device type: printer
Running: HP embedded
OS details: HP LaserJet 3330/4050/4200/4600/5100 printer
Uptime guess: 25.011 days (since Thu Dec 29 17:29:05 2011)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=152 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Devices: print server, printer
```



```
Nmap scan report for 192.168.10.5
Host is up (0.0018s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        HP JetDirect ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_d-w--w--w-   2 JetDirect  public         512 Feb 14  1999 PORT1 [NSE: writeable]
23/tcp    open  telnet     HP JetDirect printer telnetd (No password)
80/tcp    open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
280/tcp   open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
443/tcp   open  ssl/https?
515/tcp   open  printer
631/tcp   open  http       HP JetDirect printer webadmin (HP-ChaiServer 3.0)
9100/tcp  open  jetdirect?
9220/tcp  open  hp-gsg     HP JetDirect Generic Scan Gateway 2.0
9290/tcp  open  hp-gsg     IEEE 1284.4 scan peripheral gateway (connection error)
14000/tcp open  tcpwrapped
Device type: printer
Running: HP embedded
OS details: HP LaserJet 3330/4050/4200/4600/5100 printer
Uptime guess: 25.011 days (since Thu Dec 29 17:29:05 2011)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=152 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Devices: print server, printer
```

Date: Wed, 8 Aug 2001 20:33:56 -0400
From: John Hilker
Subject: Code Red Worm

Our HP 4000 series LaserJet printers were affected by the Code Red "hits" as described by Dave Martin.

The fix resulting from a call to HP tech support is to run a couple of files (only from a PC) which check the firmware version on the printer and then update it.

The two files are called: BPJ05054 and gmswine.exe

Instructions are enclosed with the files.

Date: Wed, 8 Aug 2001 20:33:56 -0400
From: John Hilker
Subject: Code Red Worm

Our HP 4000 series LaserJet printers were affected by the Code Red "hits" as described by Dave Martin.

The fix resulting from a call to HP tech support is to run a couple of files (only from a PC) which check the firmware version on the printer and then update it.

The two files are called: BPJ05054 and gmswine.exe

Instructions are enclosed with the files.

Exclusive: Millions of printers open to devastating hack attack, researchers say

By Bob Sullivan

Printers can be remotely controlled by computer criminals over the Internet, with the potential to steal personal information, attack otherwise secure networks and even cause physical damage, the researchers argue in a vulnerability warning first reported by msnbc.com. They say there's no easy fix for the flaw they've identified in some Hewlett-Packard LaserJet printer lines – and perhaps on other firms' printers, too – and there's no way to tell if hackers have already exploited it.

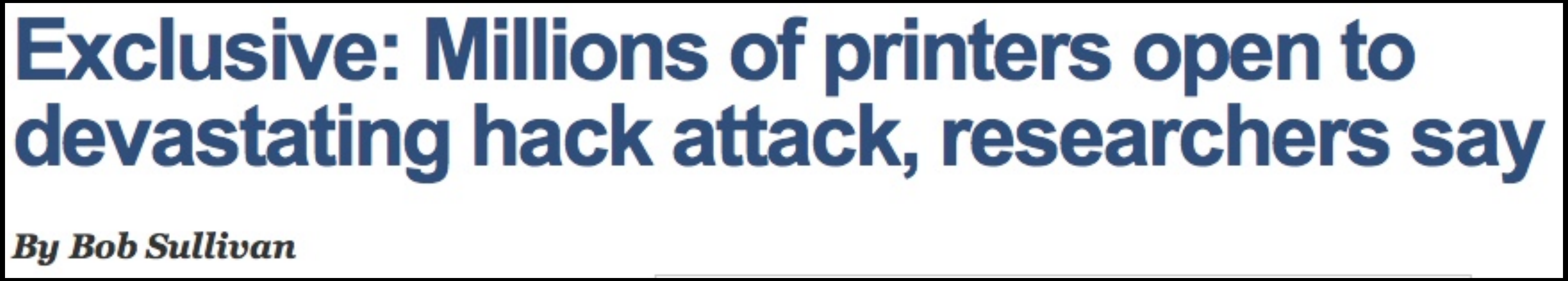
http://redtape.msnbc.msn.com/_news/2011/11/29/9076395-exclusive-millions-of-printers-open-to-devastating-hack-attack-researchers-say

Exclusive: Millions of printers open to devastating hack attack, researchers say

By Bob Sullivan

Printers can be remotely controlled by computer criminals over the Internet, with the potential to steal personal information, attack otherwise secure networks and even cause physical damage, the researchers argue in a vulnerability warning first reported by msnbc.com. They say there's no easy fix for the flaw they've identified in some Hewlett-Packard LaserJet printer lines – and perhaps on other firms' printers, too – and there's no way to tell if hackers have already exploited it.

http://redtape.msnbc.msn.com/_news/2011/11/29/9076395-exclusive-millions-of-printers-open-to-devastating-hack-attack-researchers-say



Exclusive: Millions of printers open to devastating hack attack, researchers say

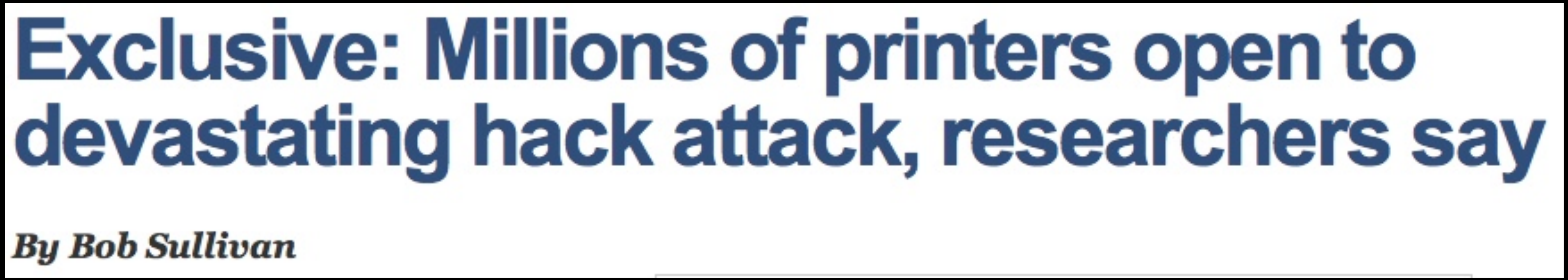
By Bob Sullivan

In one demonstration of an attack based on the flaw, Stolfo and fellow researcher Ang Cui showed how a hijacked computer could be given instructions that would continuously heat up the printer's fuser – which is designed to dry the ink once it's applied to paper – eventually causing the paper to turn brown and smoke.

Exclusive: Millions of printers open to devastating hack attack, researchers say

By Bob Sullivan

In one demonstration of an attack based on the flaw, Stolfo and fellow researcher Ang Cui showed how a hijacked computer could be given instructions that would continuously heat up the printer’s fuser – which is designed to dry the ink once it’s applied to paper – eventually causing the paper to turn brown and smoke.

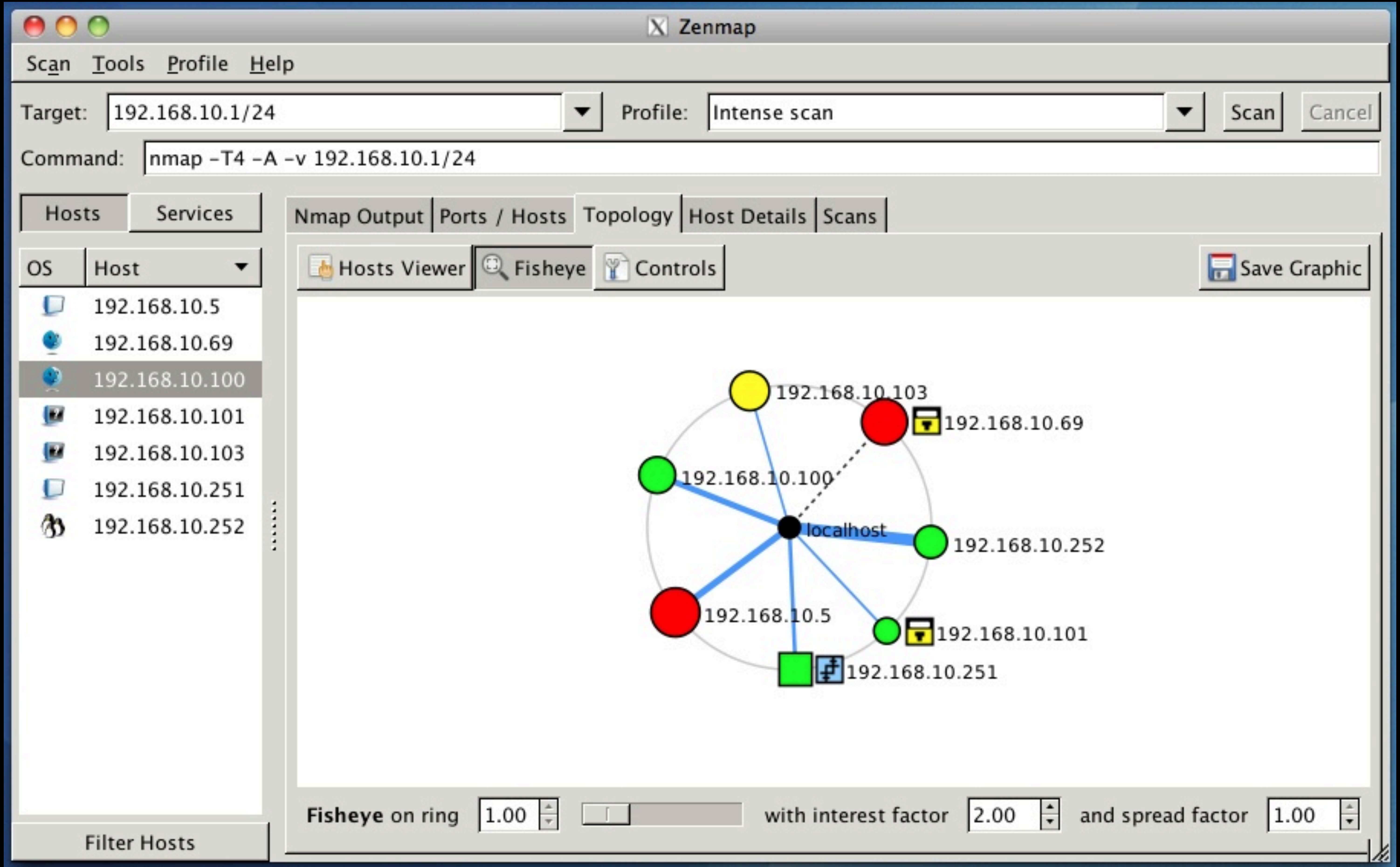


Exclusive: Millions of printers open to devastating hack attack, researchers say

By Bob Sullivan

[Hewlett-Packard LaserJet printers] allow firmware upgrades through a process called "Remote Firmware Update."

anyone can instruct the printer to erase its operating software and install a booby-trapped version



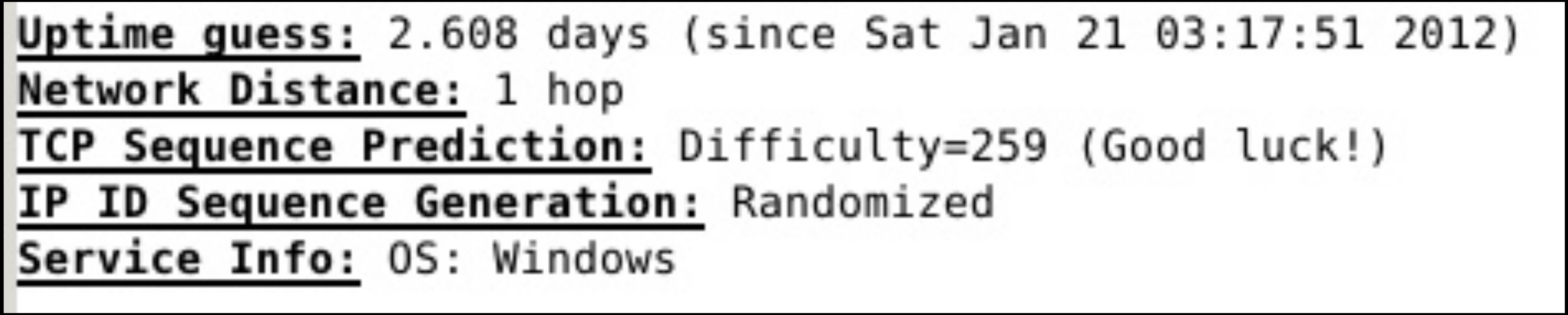
Target: 192.168.10.1/24

Profile: Intense scan

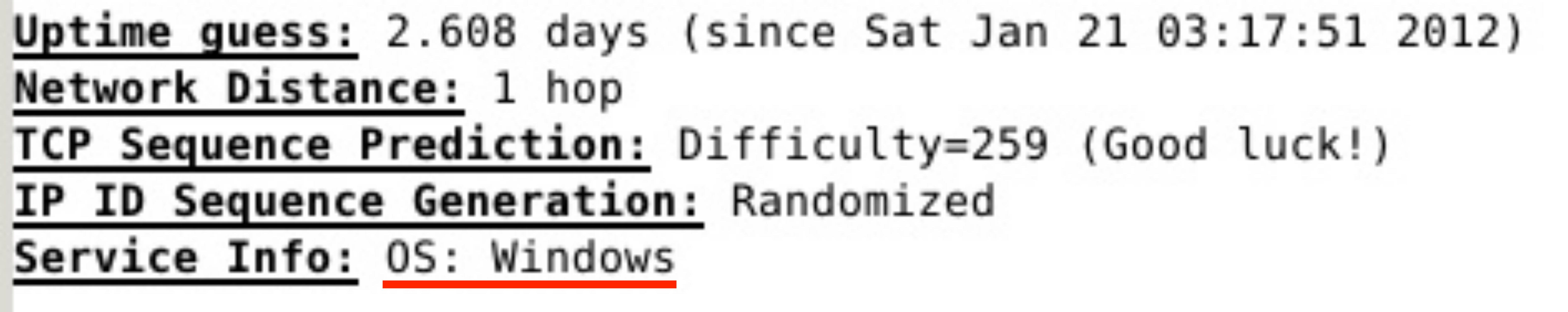
Command: nmap -T4 -A -v 192.168.10.1/24

OS	Host
	192.168.10.5
	192.168.10.69
	192.168.10.100
	192.168.10.101
	192.168.10.103
	192.168.10.251
	192.168.10.252

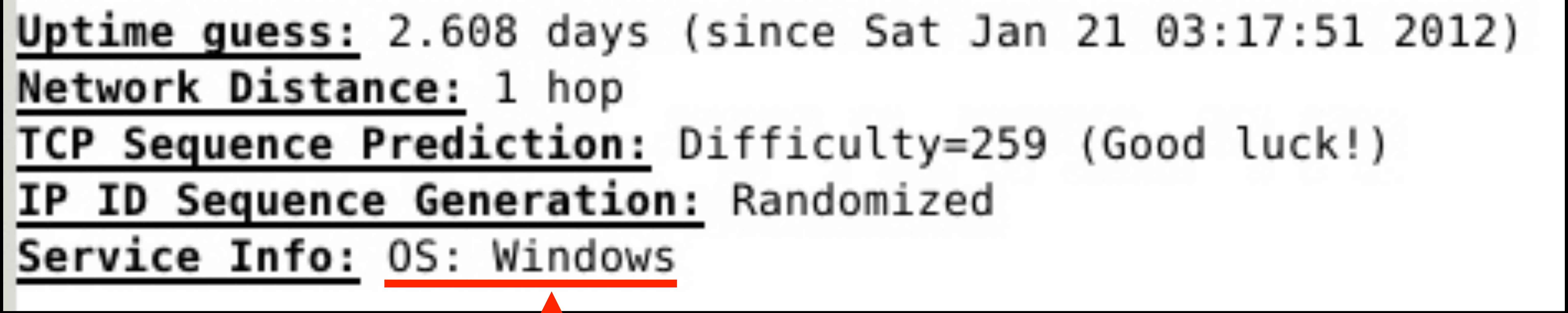
Fisheye on ring 1.00 with interest factor 2.00 and spread factor 1.00



```
Uptime guess: 2.608 days (since Sat Jan 21 03:17:51 2012)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: Windows
```



```
Uptime guess: 2.608 days (since Sat Jan 21 03:17:51 2012)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: Windows
```



```
Uptime guess: 2.608 days (since Sat Jan 21 03:17:51 2012)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: Windows
```

Mac Pro running Lion

Conclusions

Conclusions

- Range of network-based analysis tools for the Mac:

Conclusions

- Range of network-based analysis tools for the Mac:
  - Wireshark – packet-oriented forensics

Conclusions

- Range of network-based analysis tools for the Mac:
  - Wireshark – packet-oriented forensics
  - Snort – intrusion detection

Conclusions

- Range of network-based analysis tools for the Mac:
  - Wireshark – packet-oriented forensics
  - Snort – intrusion detection
  - Nmap – general network surveyor

Conclusions

- Range of network-based analysis tools for the Mac:
  - Wireshark – packet-oriented forensics
  - Snort – intrusion detection
  - Nmap – general network surveyor
- Come out of the UNIX world; not very Mac-like

Conclusions

- Range of network-based analysis tools for the Mac:
    - Wireshark – packet-oriented forensics
    - Snort – intrusion detection
    - Nmap – general network surveyor
- Come out of the UNIX world; not very Mac-like
- Most were started when networking world was much different

Conclusions

- Range of network-based analysis tools for the Mac:
    - Wireshark – packet-oriented forensics
    - Snort – intrusion detection
    - Nmap – general network surveyor
- Come out of the UNIX world; not very Mac-like
- Most were started when networking world was much different
- In many cases, they may your best or only tools available