

# cyber & data

---

“From bits to information”

Network  
Forensics and  
Protocols

# Outline

---

- The Core Protocols.
- ARP.
- SYN.
- FTP.
- ICMP.
- DNS.
- Port Scans.
- SYN Floods.
- Application Layer.



cyber  
& data

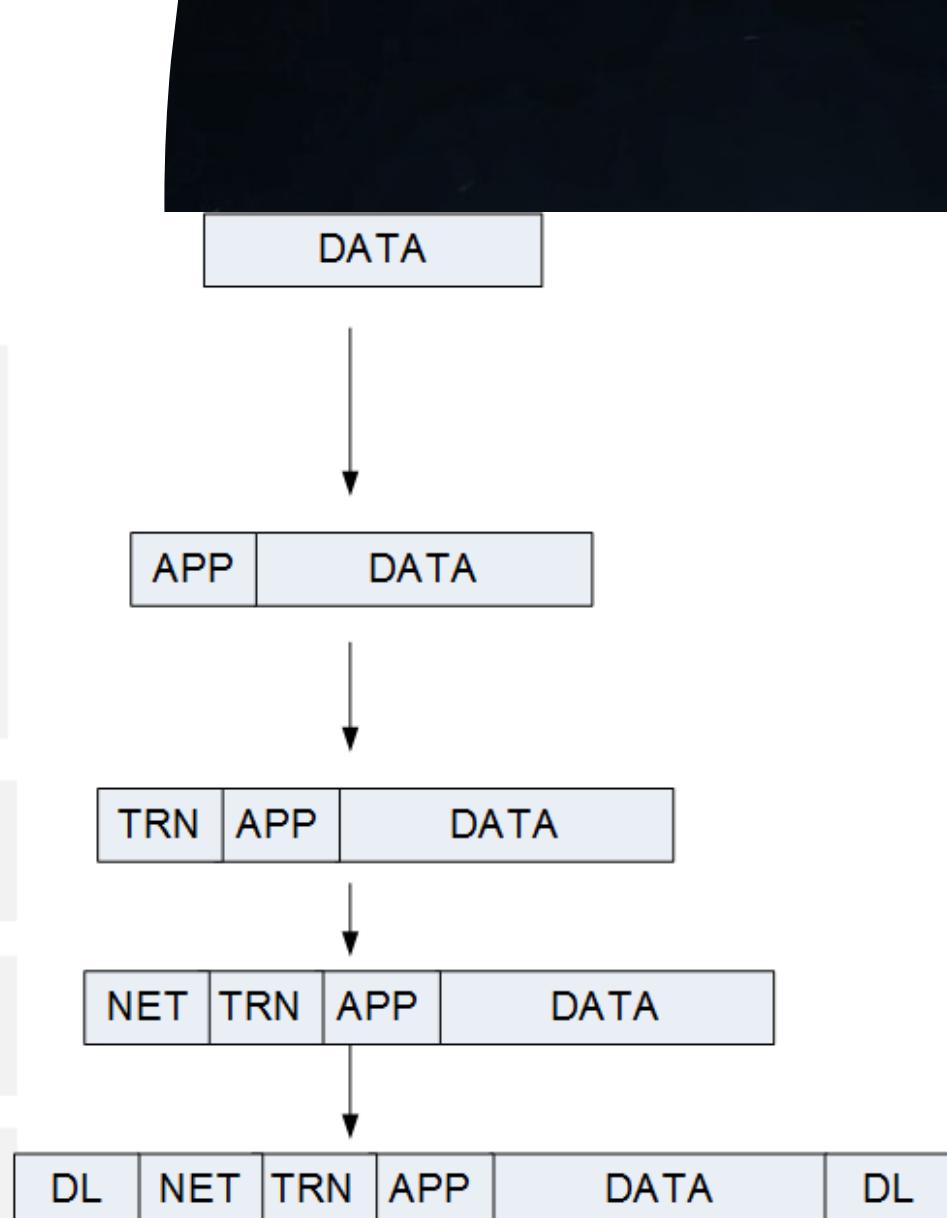
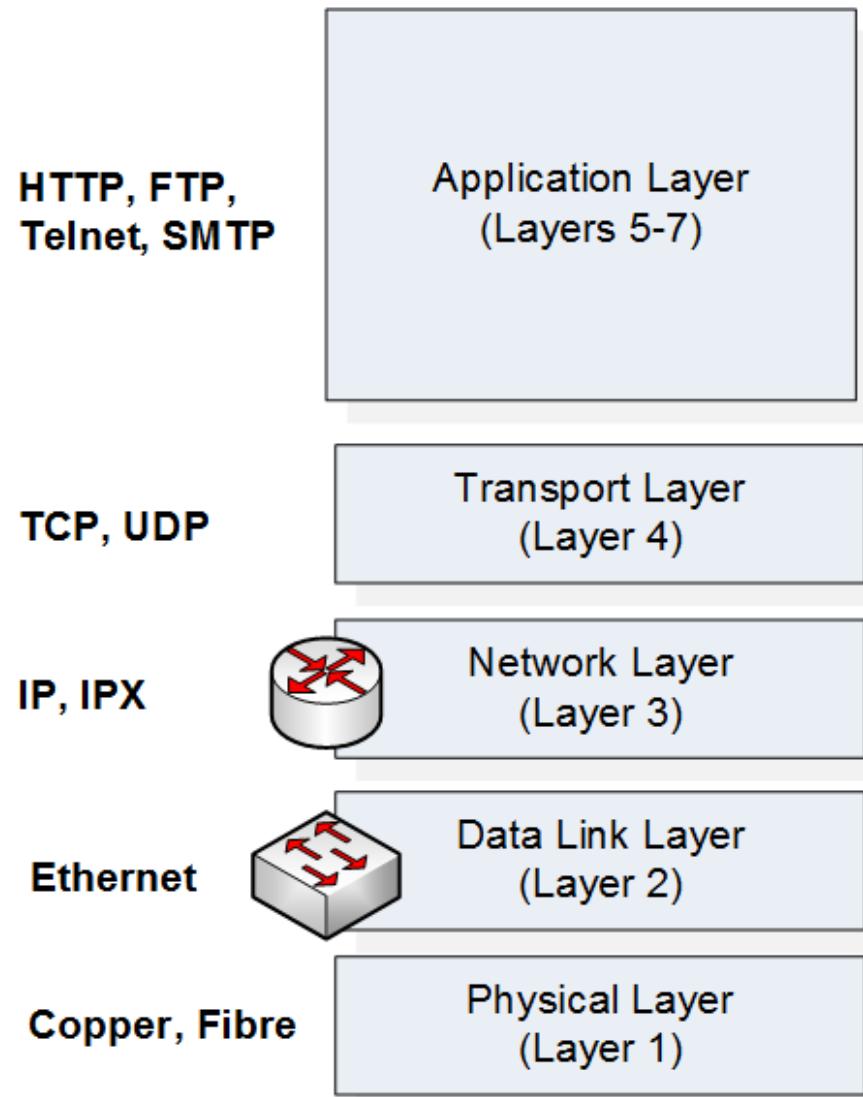
# cyber & data

---

“From bits to information”

## The Core Protocols

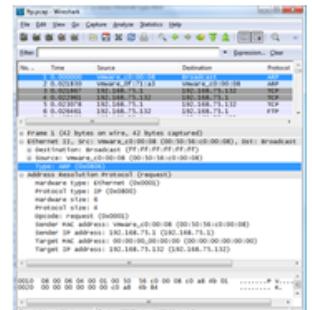
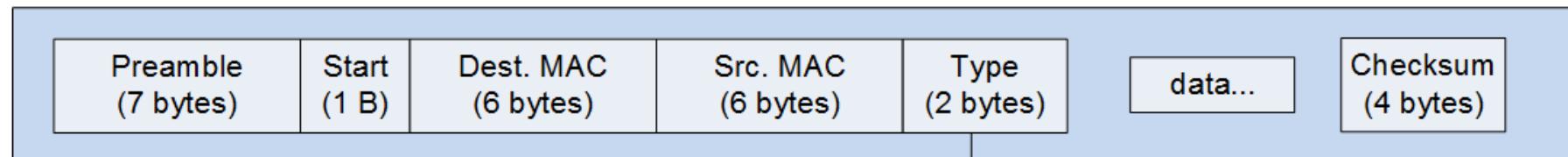
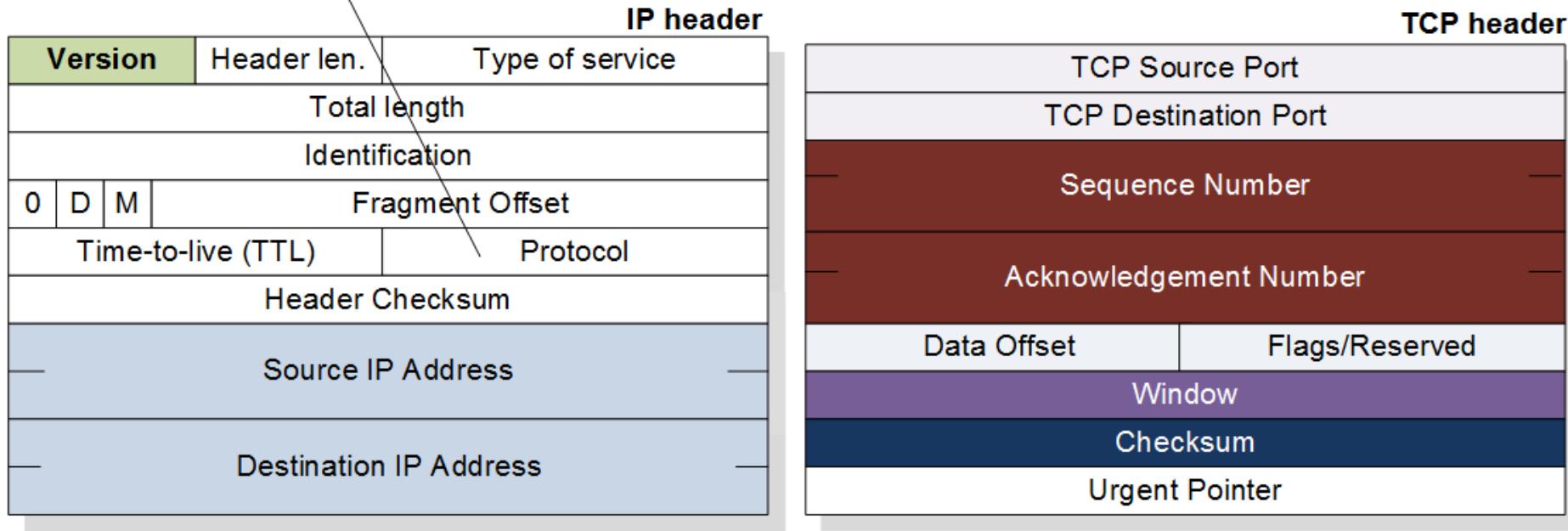
# Data Encapsulation



cyber  
&  
data

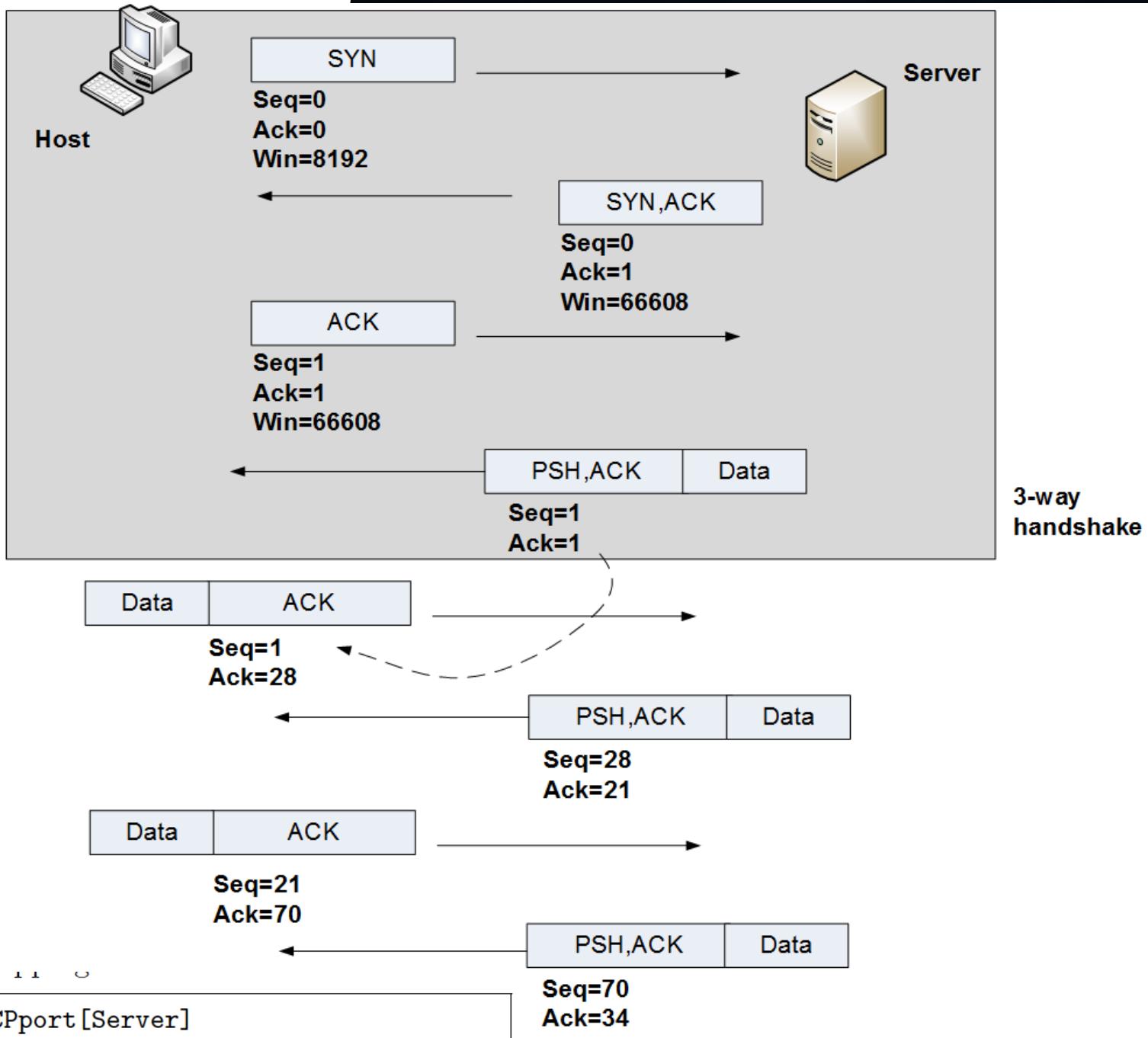
# Ethernet, IP and TCP

Protocol:  
1 – ICMP  
6 – TCP  
8 – EGP  
17 - UDP



Type:  
0x800 – IP  
0x806 – ARP

# Three-way handshake



cyber  
data

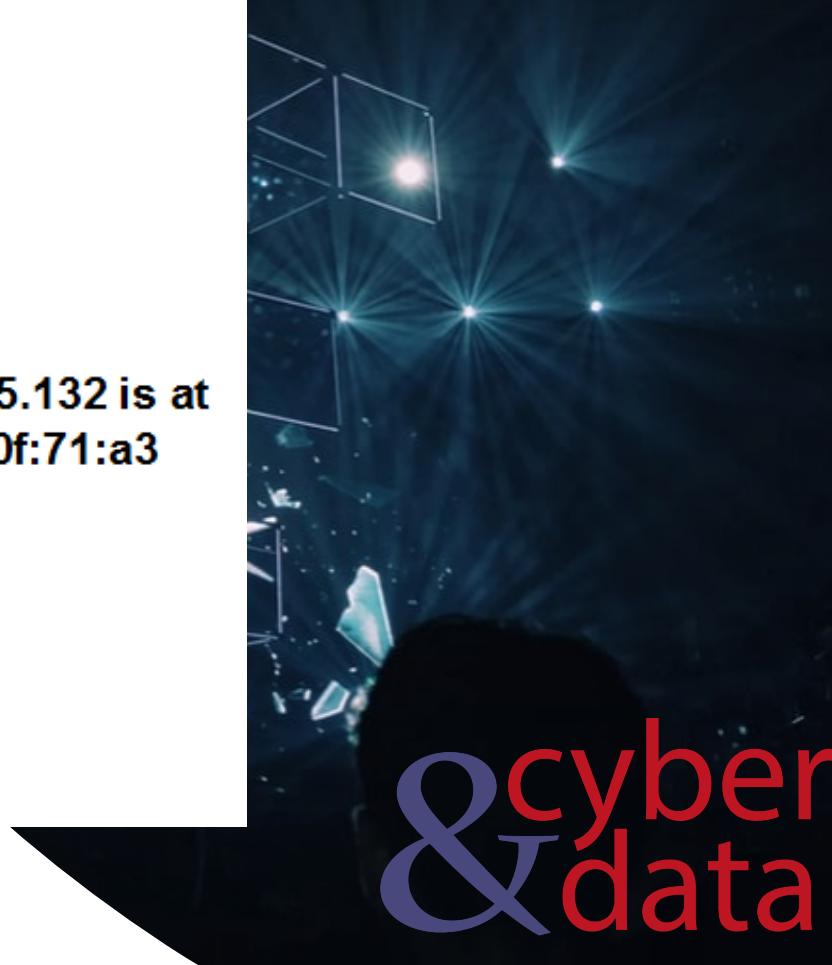
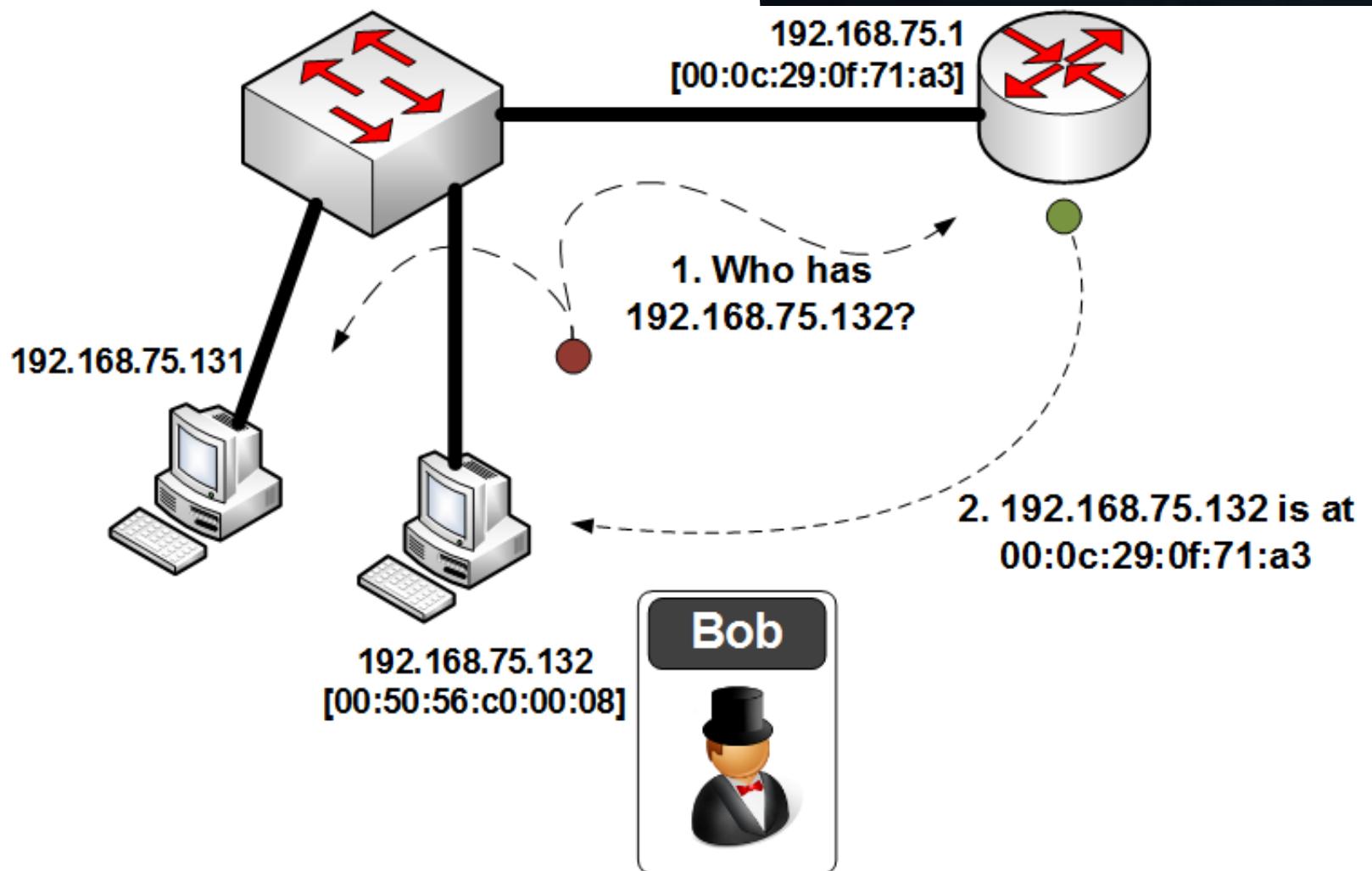
# cyber & data

---

“From bits to information”

ARP

# ARP

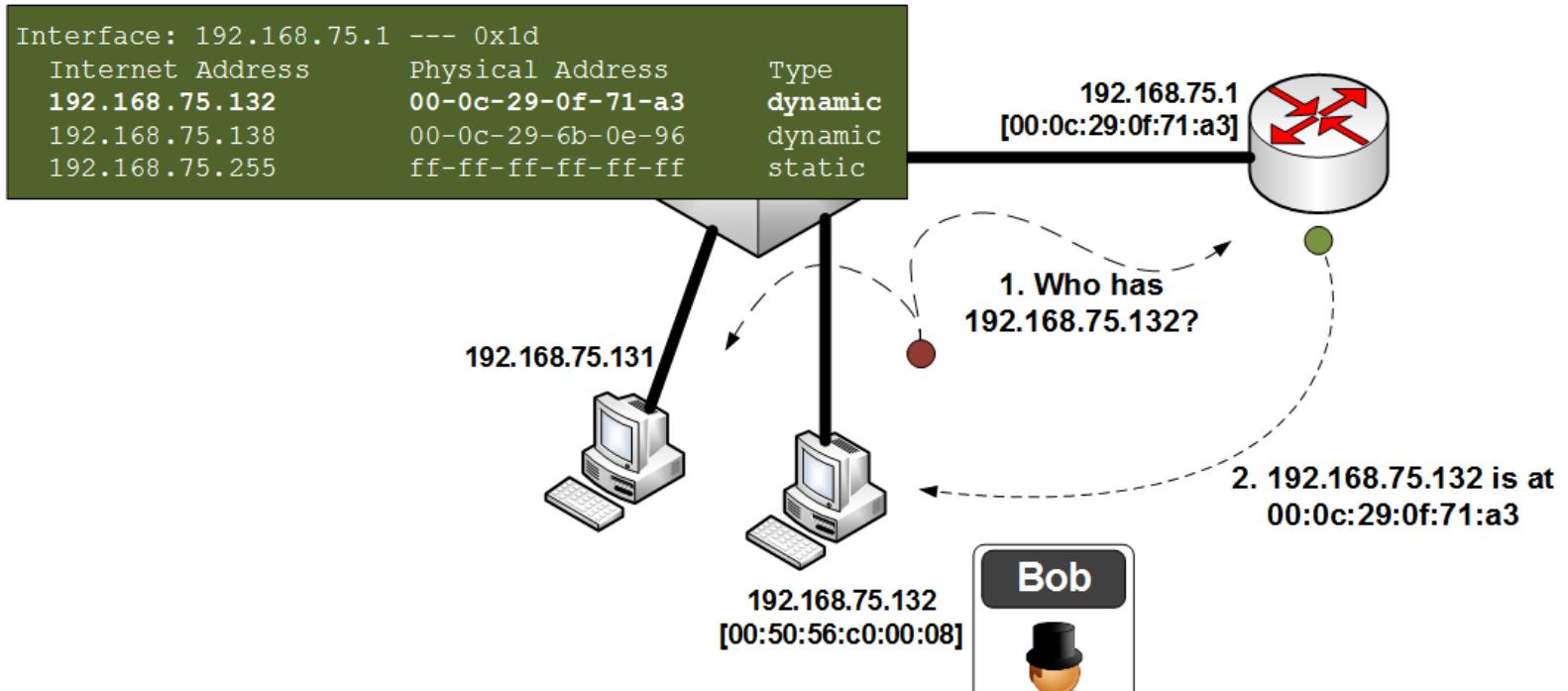


cyber  
& data

# ARP

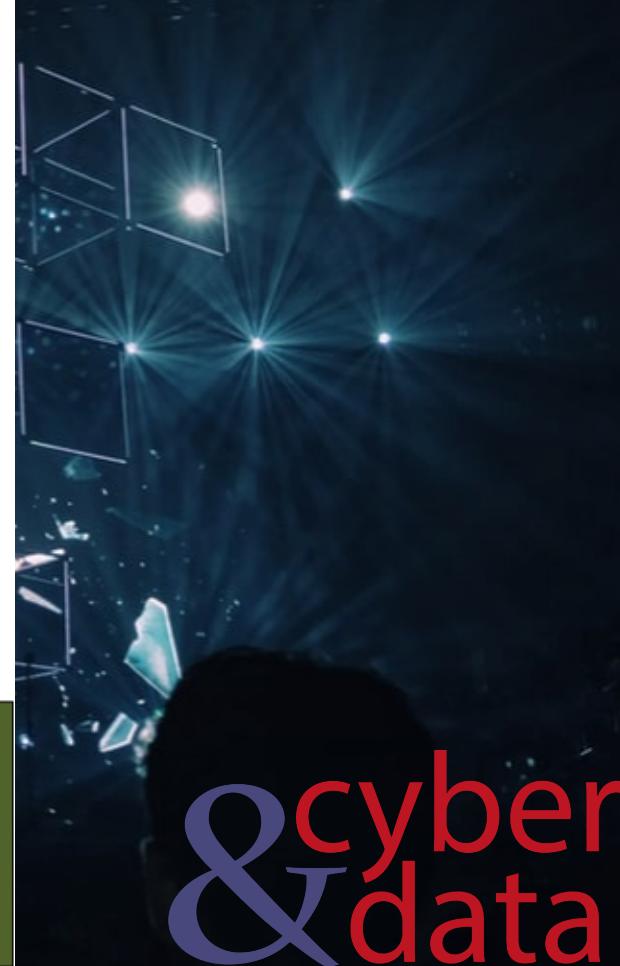
No.	Time	Source	Destination	Protocol Info
1	0.000000	Vmware_c0:00:08 192.168.75.132?	Broadcast Tell 192.168.75.1	ARP Who has

Frame 1 (42 bytes on wire, 42 bytes captured)  
Ethernet II, Src: Vmware\_c0:00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Address Resolution Protocol (request)



No.	Time	Source	Destination	Protocol Info
2	0.021830	Vmware_0f:71:a3 00:0c:29:0f:71:a3	Vmware_c0:00:08	ARP 192.168.75.132 is at

Frame 2 (42 bytes on wire, 42 bytes captured)  
Ethernet II, Src: Vmware\_0f:71:a3 (00:0c:29:0f:71:a3), Dst: Vmware\_c0:00:08 (00:50:56:c0:00:08)  
Address Resolution Protocol (reply)



cyber  
&  
data

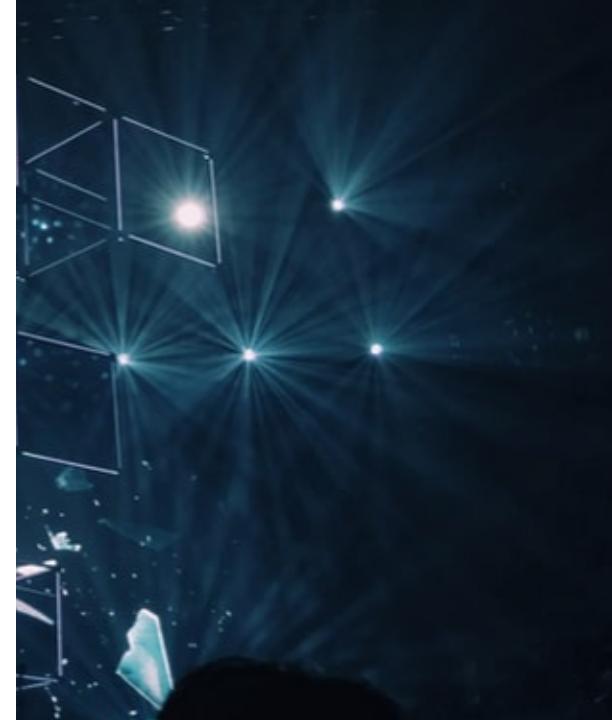
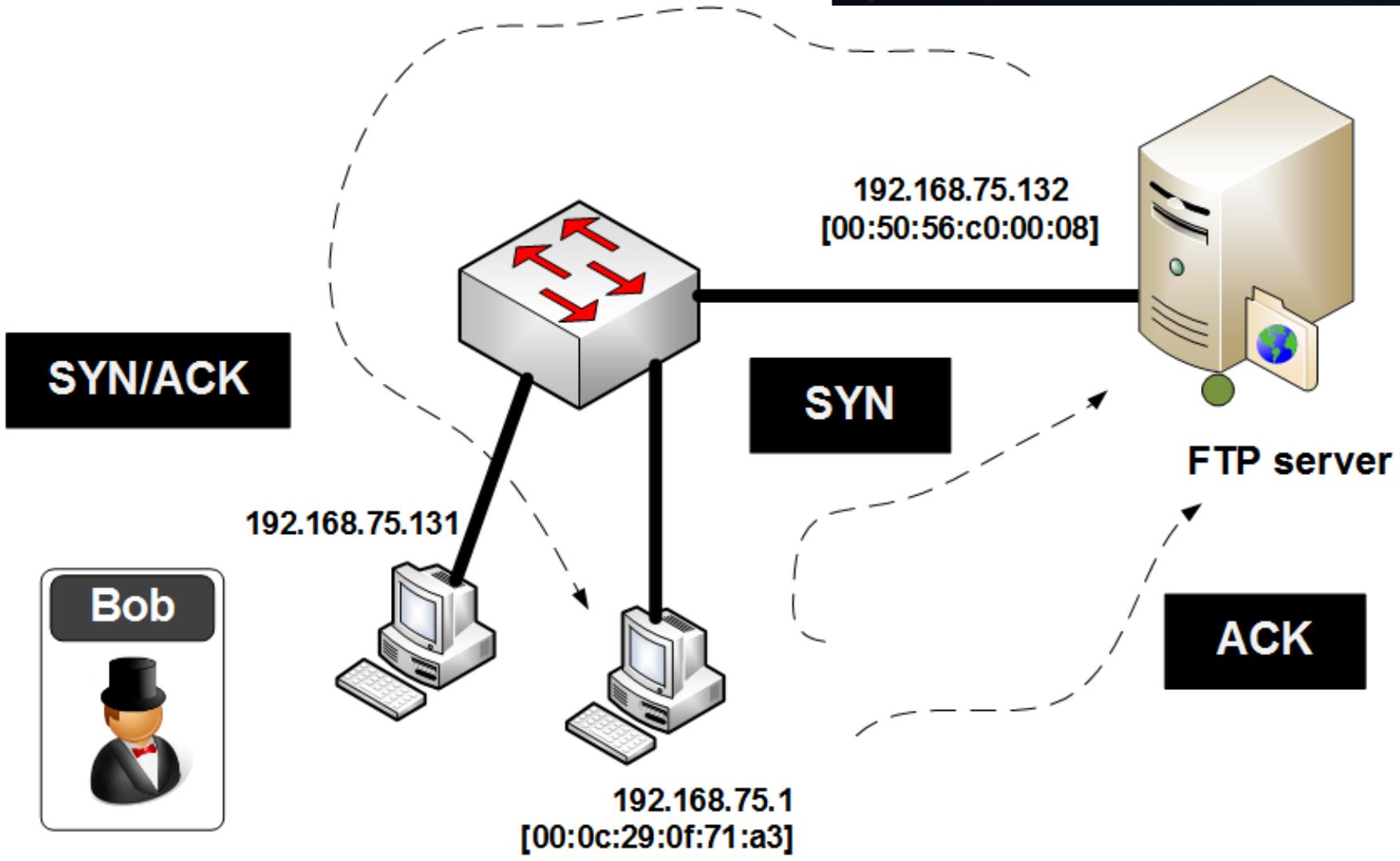
# cyber & data

---

“From bits to information”

SYN

# SYN



cyber  
& data

# SYN

No.	Time	Source	Destination	Protocol	Info
3	0.021867	192.168.75.1	192.168.75.132	TCP	abatemgr > ftp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 TSV=683746 TSER=0

Frame 3 (74 bytes on wire, 74 bytes captured)

Internet Protocol, Src: 192.168.75.1 (192.168.75.1), Dst: 192.168.75.132 (192.168.75.132)

Transmission Control Protocol, Src Port: abatemgr (3655), Dst Port: ftp (21), Seq: 0, Len: 0

No.	Time	Source	Destination	Protocol	Info
4	0.022961	192.168.75.132	192.168.75.1	TCP	ftp > abatemgr [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=0 TSV=0 TSER=0

Frame 4 (78 bytes on wire, 78 bytes captured)

Internet Protocol, Src: 192.168.75.132 (192.168.75.132), Dst: 192.168.75.1 (192.168.75.1)

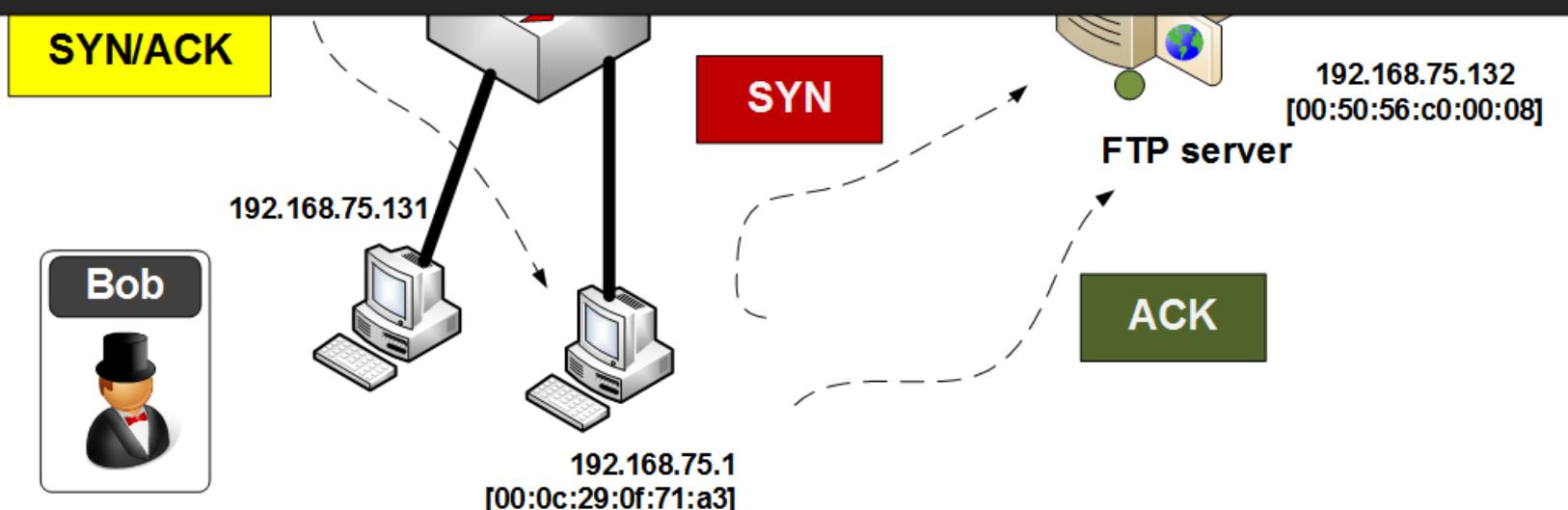
Transmission Control Protocol, Src Port: ftp (21), Dst Port: abatemgr (3655), Seq: 0, Ack: 1, Len: 0

No.	Time	Source	Destination	Protocol	Info
5	0.023078	192.168.75.1	192.168.75.132	TCP	abatemgr > ftp [ACK] Seq=1 Ack=1 Win=66608 Len=0 TSV=683748 TSER=0

Frame 5 (66 bytes on wire, 66 bytes captured)

Internet Protocol, Src: 192.168.75.1 (192.168.75.1), Dst: 192.168.75.132 (192.168.75.132)

Transmission Control Protocol, Src Port: abatemgr (3655), Dst Port: ftp (21), Seq: 1, Ack: 1, Len: 0



# cyber & data

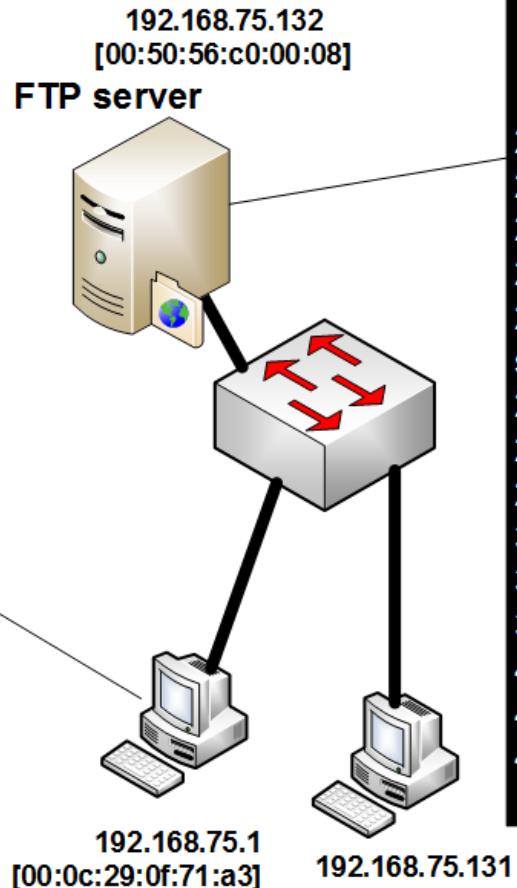
---

“From bits to information”

FTP

# FTP

ascii  
binary  
bye  
cd  
close  
delete  
get  
help  
lcd  
ls  
mkdir  
mget  
mput  
open  
put  
pwd  
quit  
rmdir



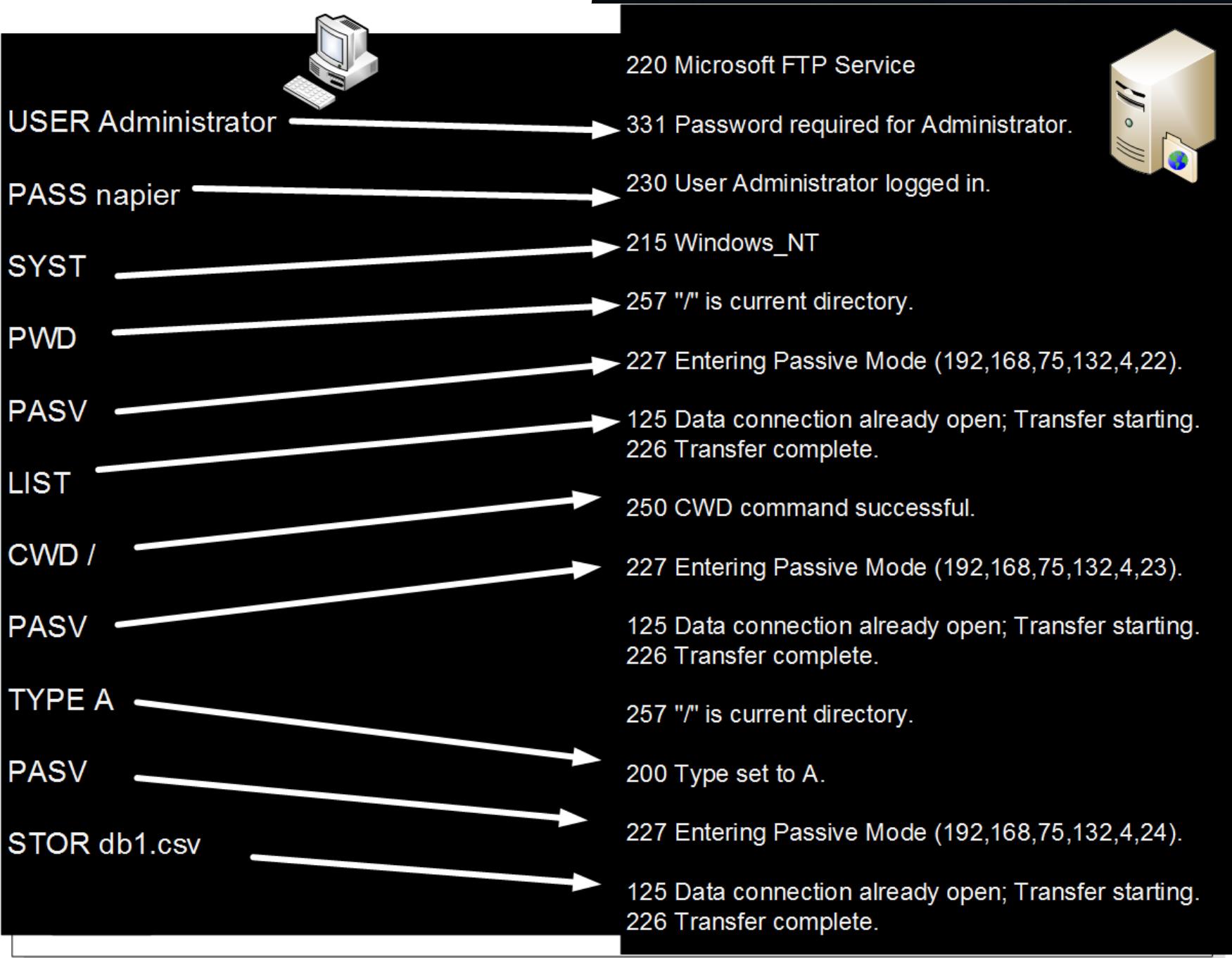
100 Codes The requested action is being taken.  
200 Codes The requested action has been successfully completed.  
300 Codes The command has been accepted, but the requested action is being held pending receipt of further information.  
400 Codes The command was not accepted and the requested action did not take place.  
500 Codes The command was not accepted and the requested action did not take place.

125 Data connection already open, transfer starting.  
150 File status okay, about to open data connection.  
200 Command okay.  
202 Command not implemented  
211 System status, or system help reply.  
212 Directory status.  
226 Closing data connection. Requested file action successful (file transfer, abort, etc.).  
227 Entering Passive Mode  
230 User logged in, proceed.  
250 Requested file action okay, completed.  
331 User name okay, need password.  
332 Need account for login.  
350 Requested file action pending further information.  
421 Service not available, closing control connection.  
425 Can't open data connection.  
426 Connection closed, transfer aborted.

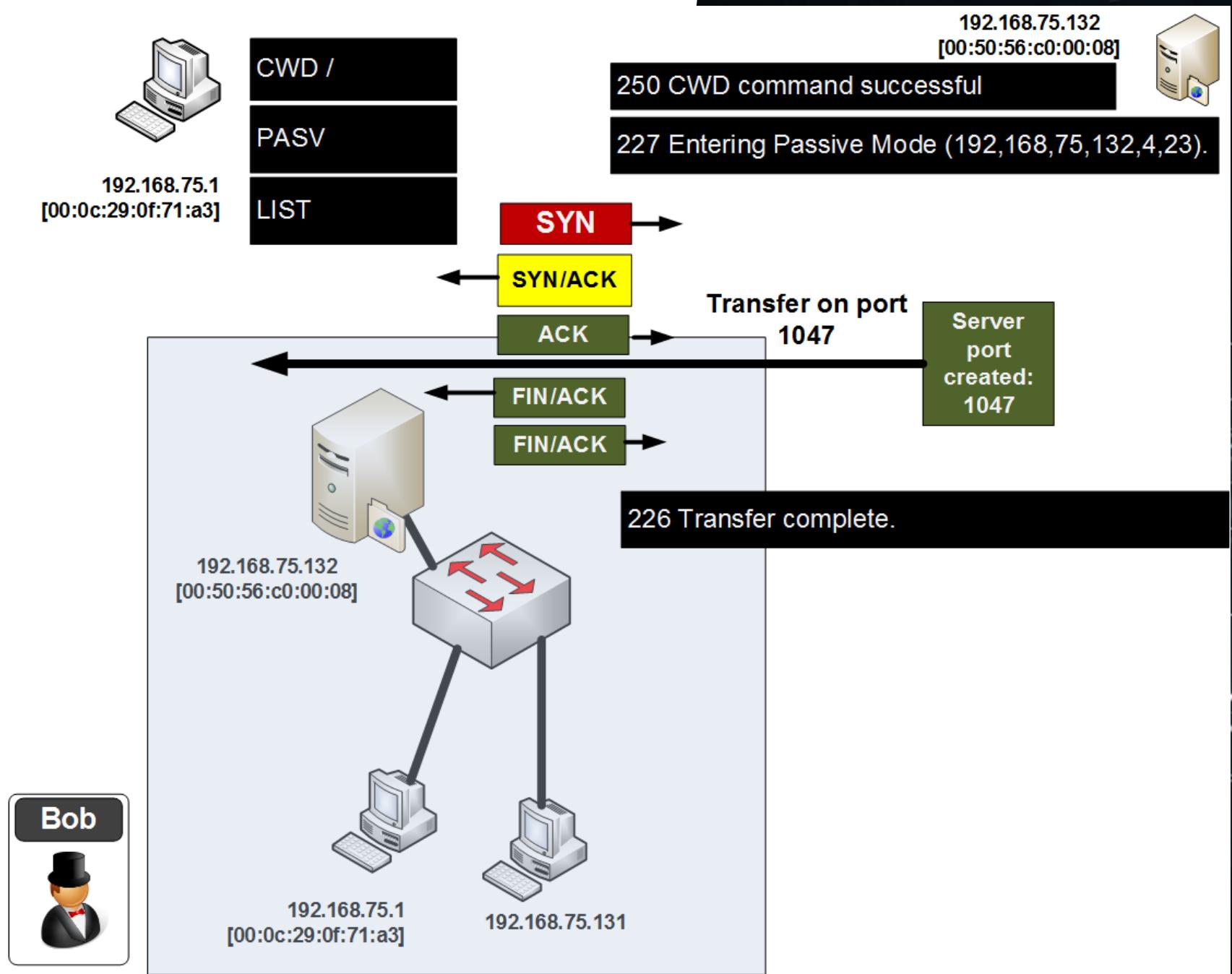


cyber  
&  
data

# FTP



# FTP



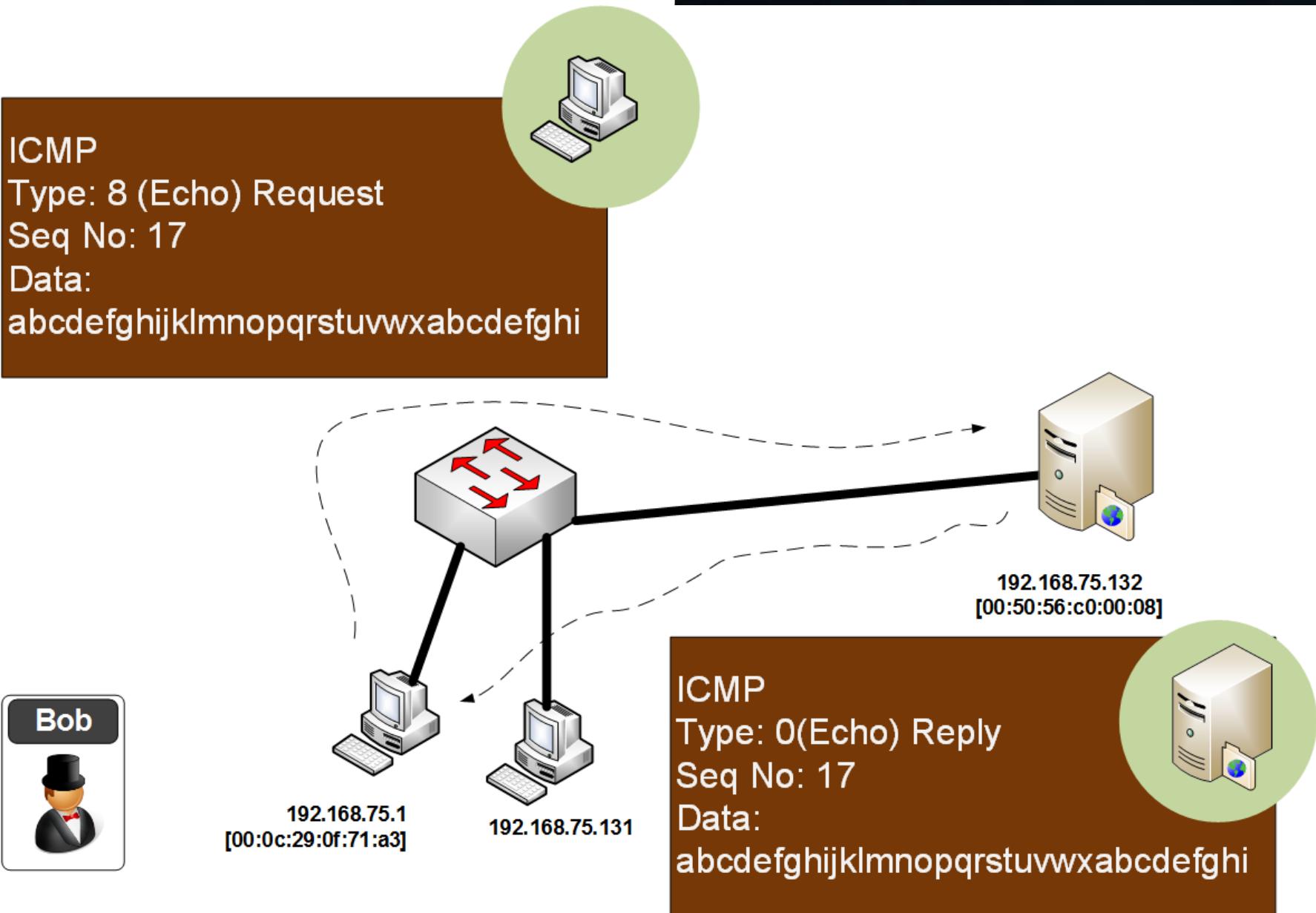
# cyber & data

---

“From bits to information”

# ICMP

# ICMP



cyber  
& data

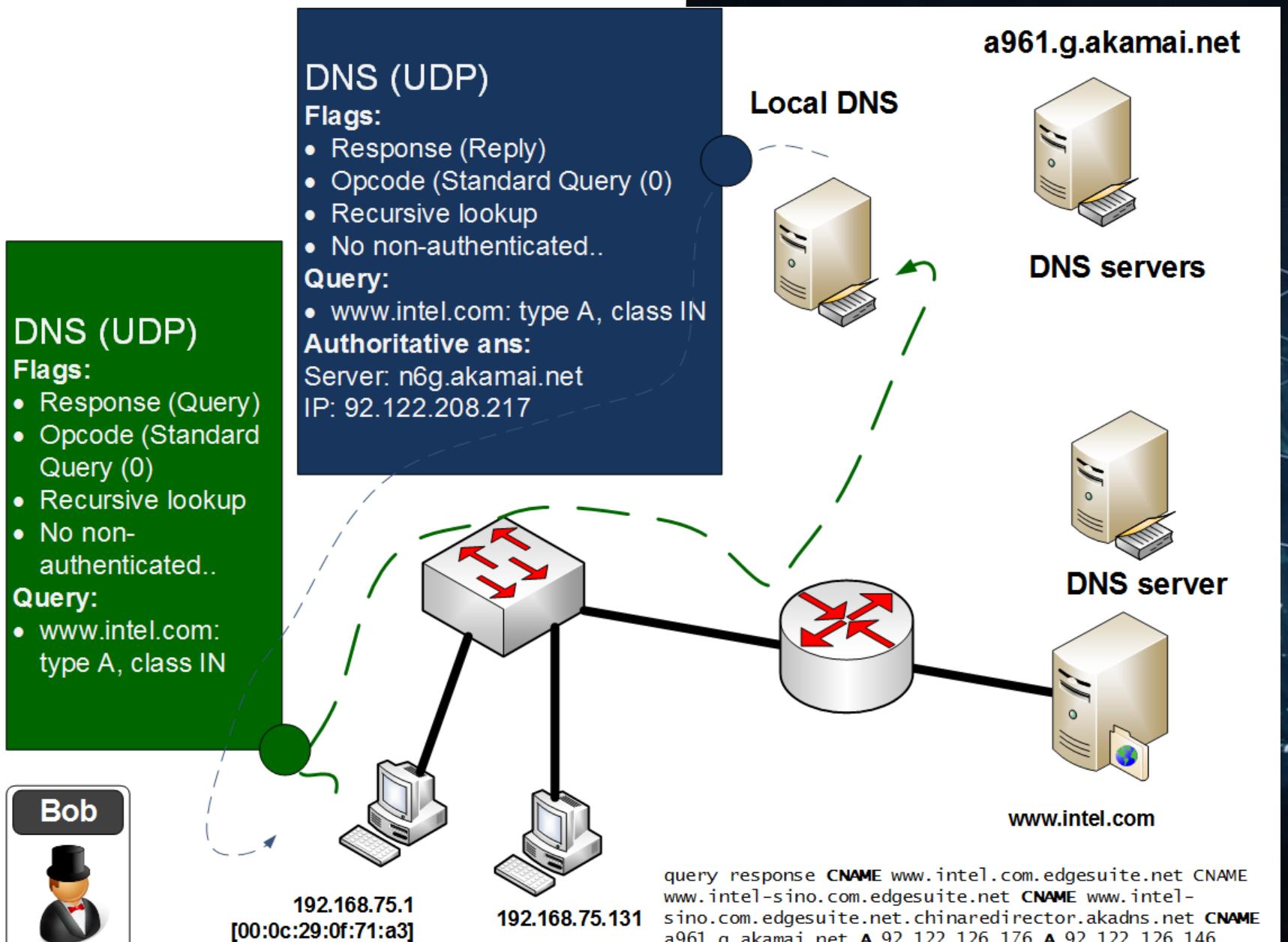
# cyber & data

---

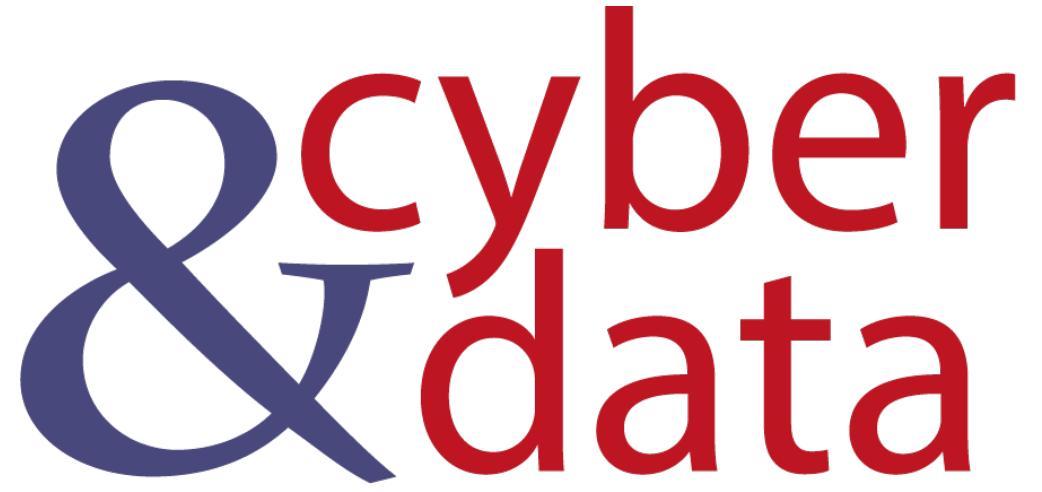
“From bits to information”

## DNS

# DNS



cyber & data

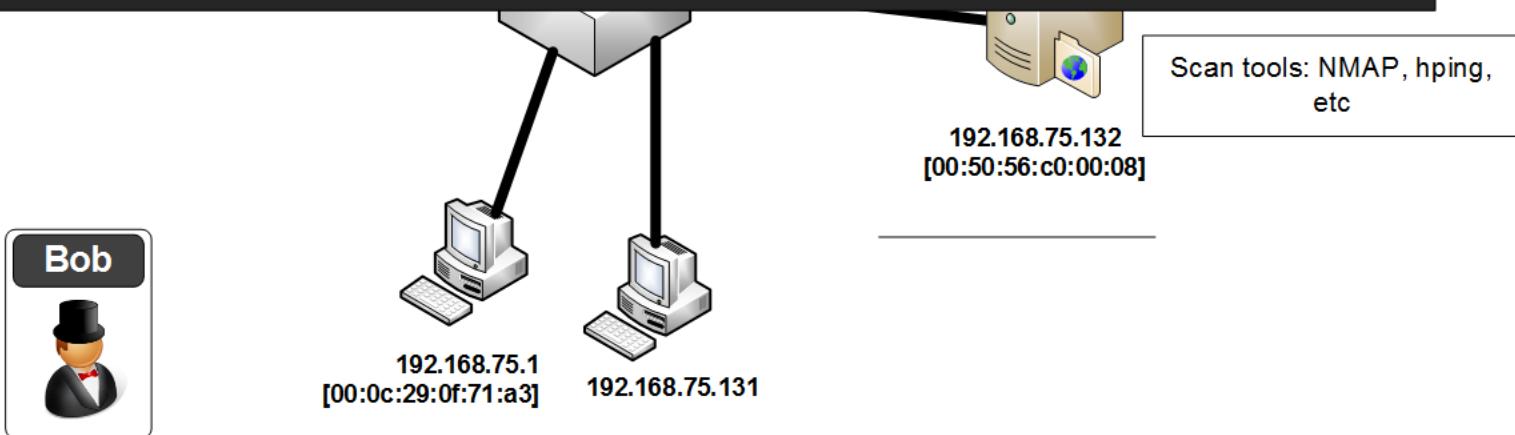


"From bits to information"

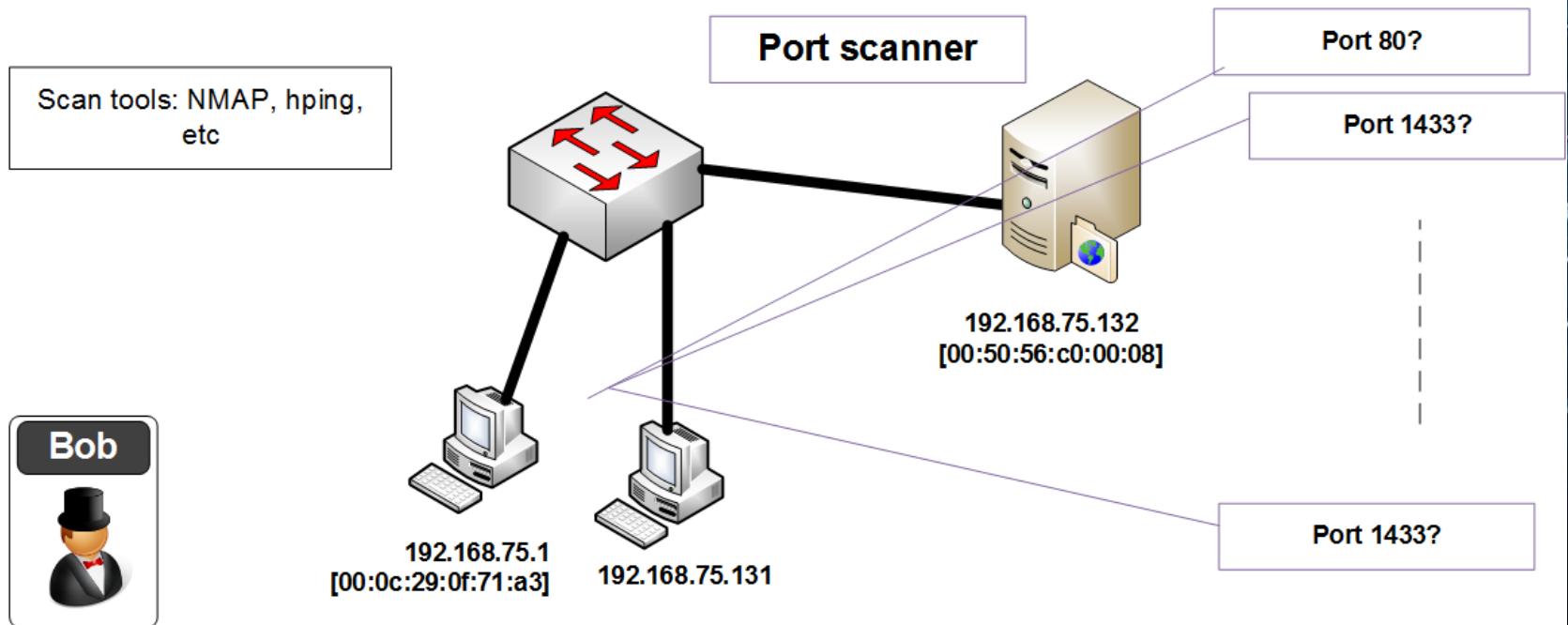
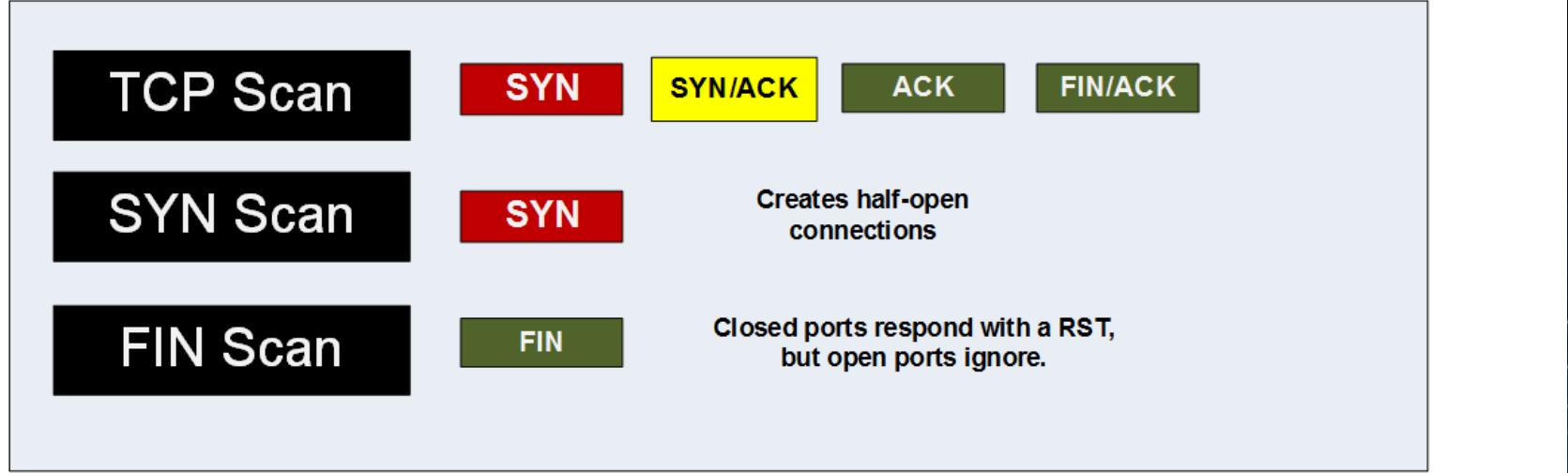
# Port Scans

# Port Scans

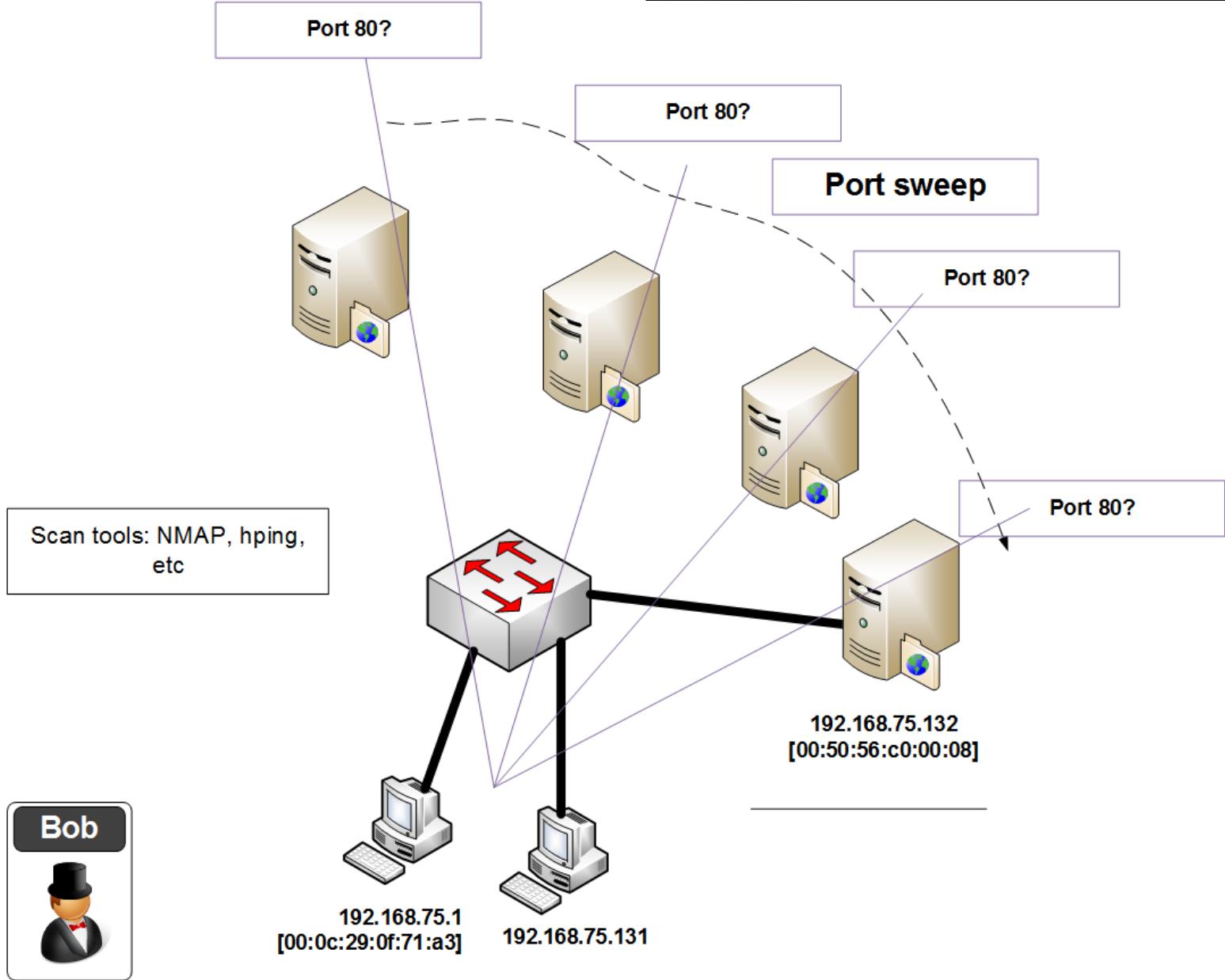
```
No.      Time      Source          Destination        Protocol Info  
85 25.420710  192.168.75.1    192.168.75.132    TCP      54370 > telnet  
[SYN] Seq=0 Win=1024 Len=0 MSS=1460  
  
Frame 85 (58 bytes on wire, 58 bytes captured)  
Internet Protocol, Src: 192.168.75.1 (192.168.75.1), Dst: 192.168.75.132  
(192.168.75.132)  
Transmission Control Protocol, Src Port: 54370 (54370), Dst Port: telnet (23), Seq: 0,  
Len: 0  
  
No.      Time      Source          Destination        Protocol Info  
86 25.420836  192.168.75.1    192.168.75.132    TCP      54370 > rap  
[SYN] Seq=0 Win=2048 Len=0 MSS=1460  
  
Frame 86 (58 bytes on wire, 58 bytes captured)  
Internet Protocol, Src: 192.168.75.1 (192.168.75.1), Dst: 192.168.75.132  
(192.168.75.132)  
Transmission Control Protocol, Src Port: 54370 (54370), Dst Port: rap (256), Seq: 0,  
Len: 0
```



# Port Scans



# Port Scans



cyber  
&  
data

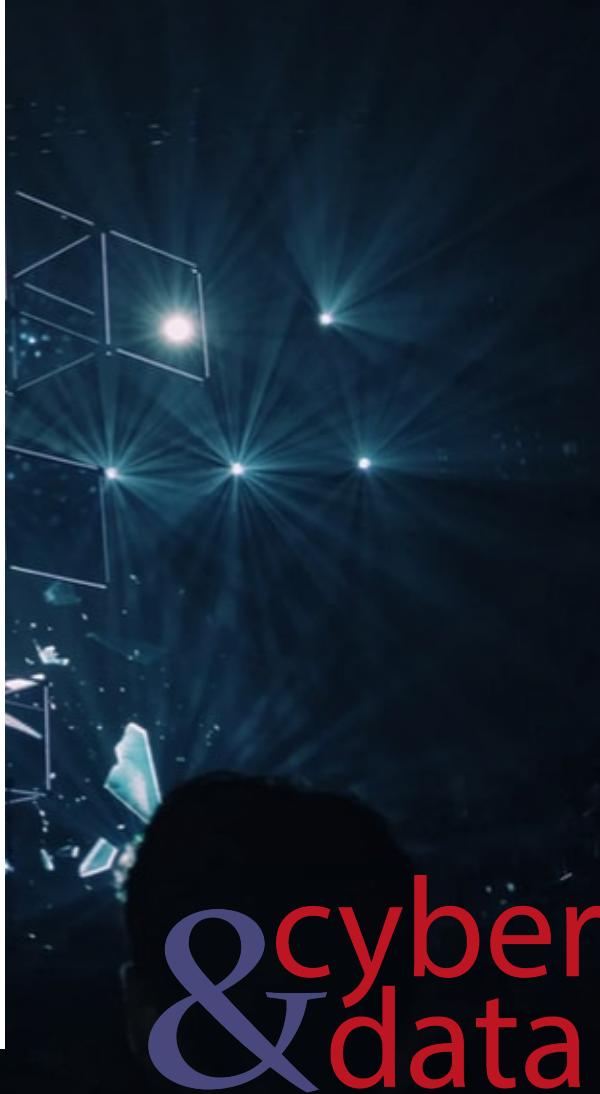
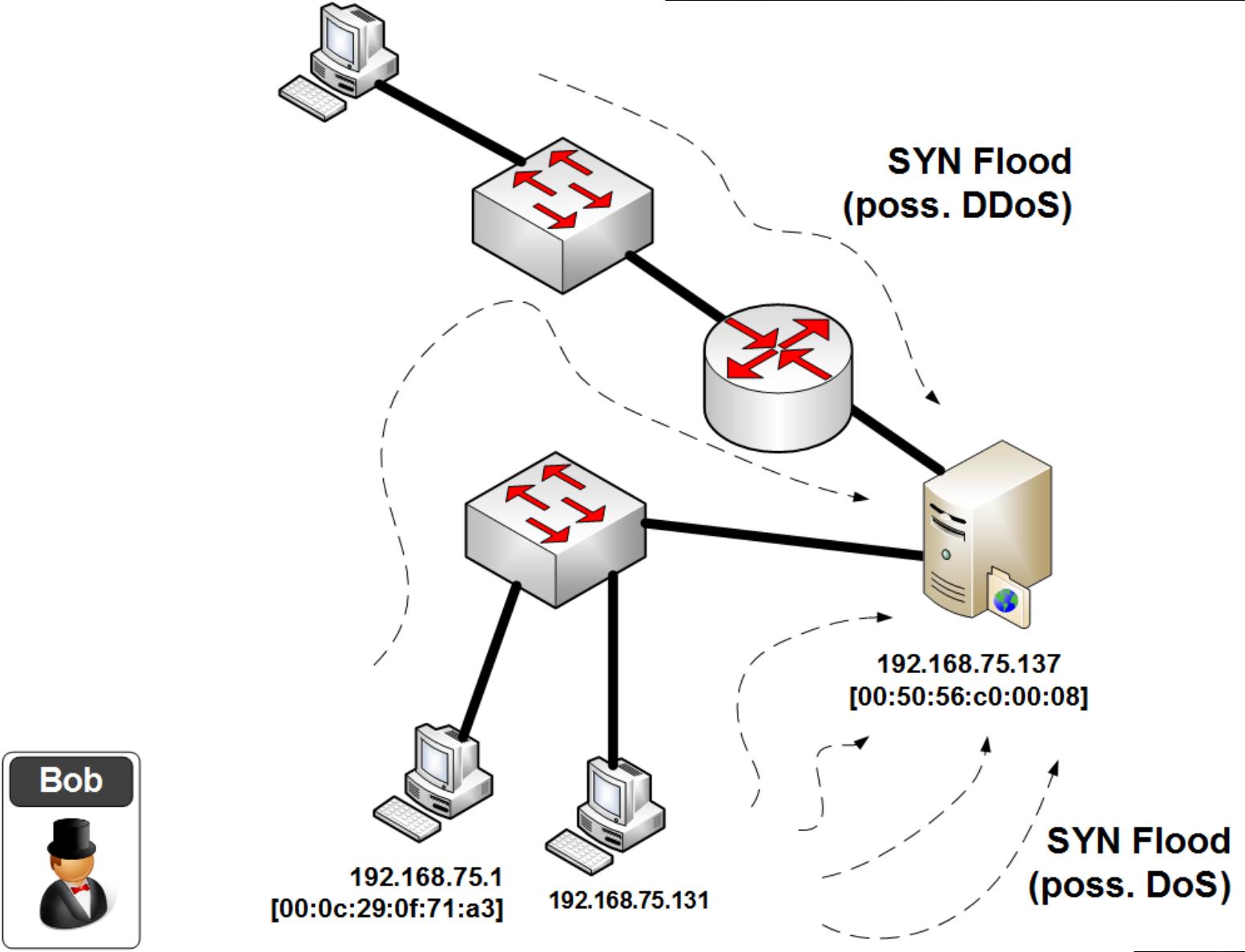
# cyber & data

---

“From bits to information”

## SYN Flood

# SYN Flood



# cyber & data

---

“From bits to information”

Application Layer

# Application Layer (HTTP)

```
GET / HTTP/1.1
User-Agent: Opera/9.80 (Windows NT 6.0; U; en) Presto/
2.2.15 Version/10.01
Host: 192.168.75.132
Accept: text/html, application/xml;q=0.9, application/
xhtml+xml, image/png, image/jpeg, image/gif, image/x-
bitmap, */*;q=0.1 Accept-Language: en-GB,en;q=0.9
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Connection: Keep-Alive...
```

```
HTTP/1.1 200 OK
Content-Length: 2606
Content-Type: text/html
Content-Location: http://192.168.75.132/iisstart.htm
Last-Modified: Sun, 13 Dec 2009 15:16:14 GMT
Accept-Ranges: bytes ETag: "fc31243677cc41:745" Server: Microsoft-IIS/
6.0 X-Powered-By: ASP.NET
Date: Sat, 02 Jan 2010 22:33:01 GMT
<HTML> <HEAD> <TITLE>SFC (Final Test)</TITLE> <META http-equiv=Content-
Type content="text/html; charset=iso-8859-1"> <LINK href="2.css"
type=text/css rel=stylesheet> <style type="text/css"> ...
```

Bob



192.168.75.1  
[00:0c:29:0f:71:a3] 192.168.75.131

cyber  
&  
data

# cyber & data

---

“From bits to information”

Network  
Forensics and  
Protocols