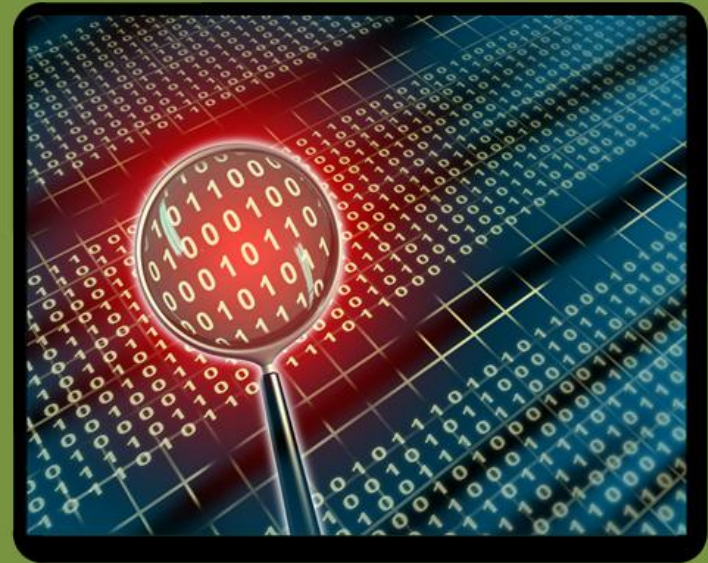
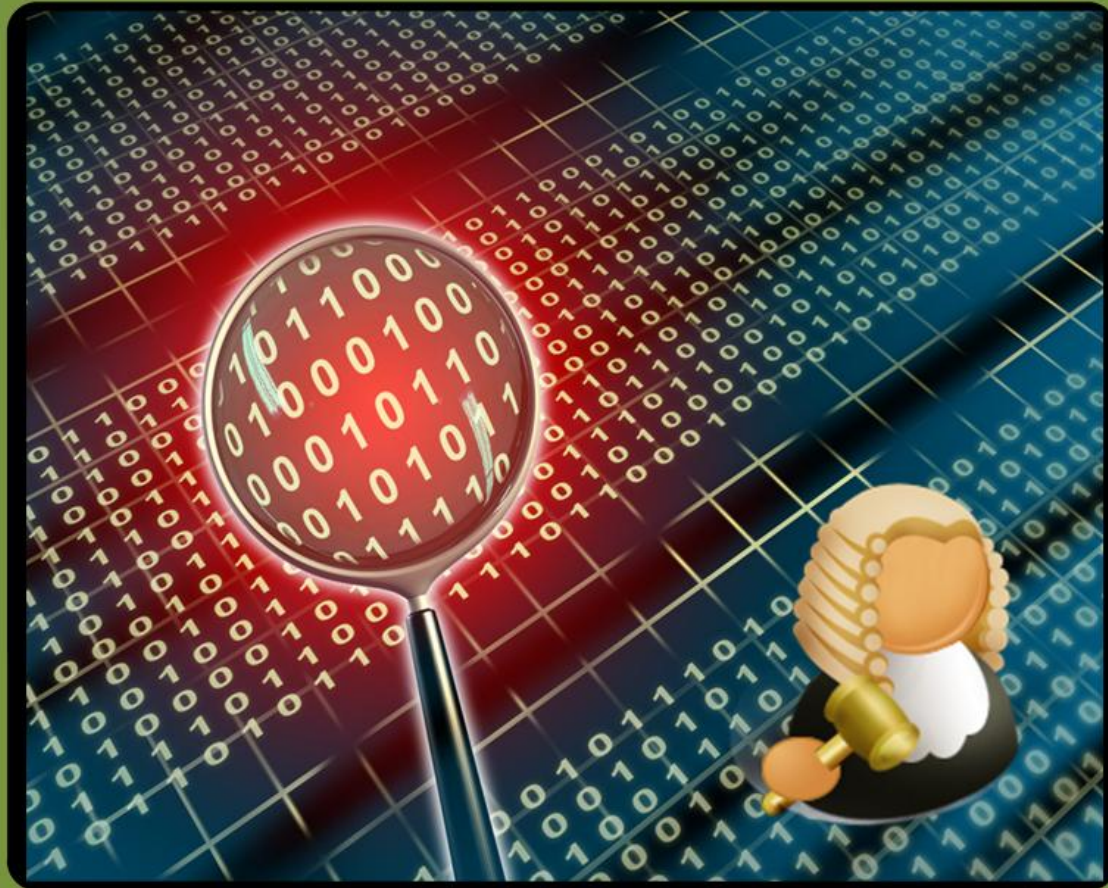


Network Forensics

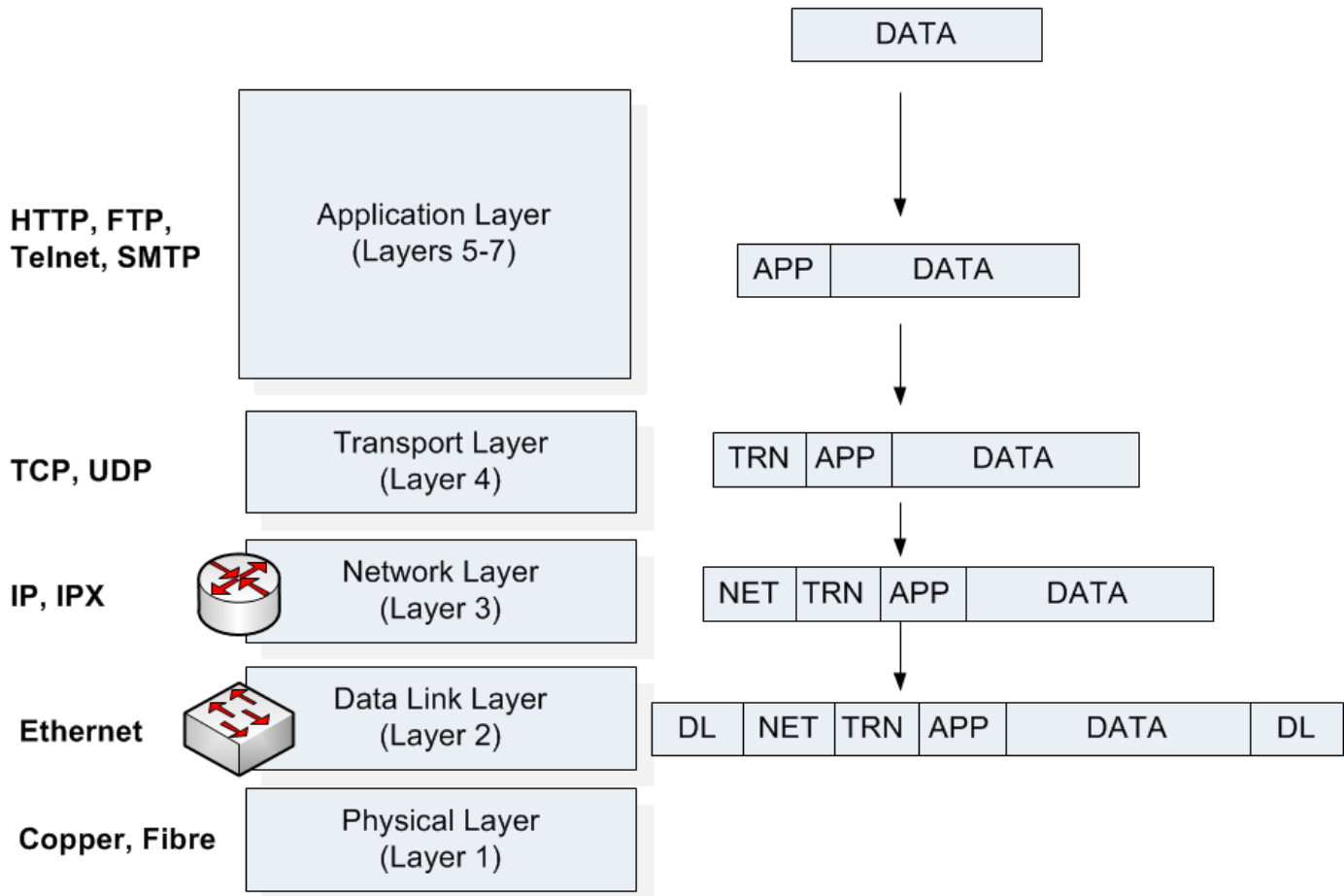
- Understand some of the methodologies used in network forensics.
- Provide an in-depth understanding of the key network protocols, including IP, TCP, ARP, ICMP, DNS, Application Layer protocols, and so on.
- Define a range of audit sources for network activity.

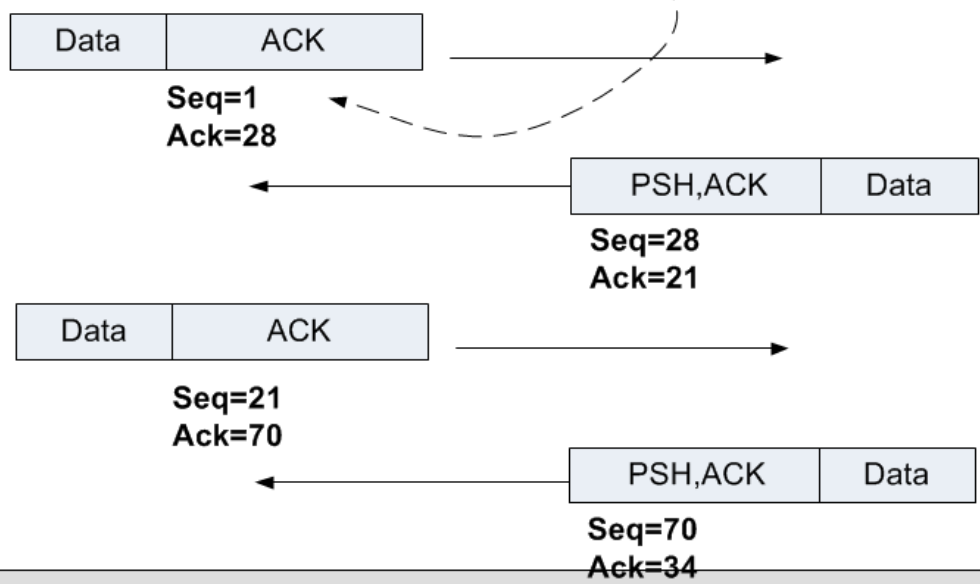
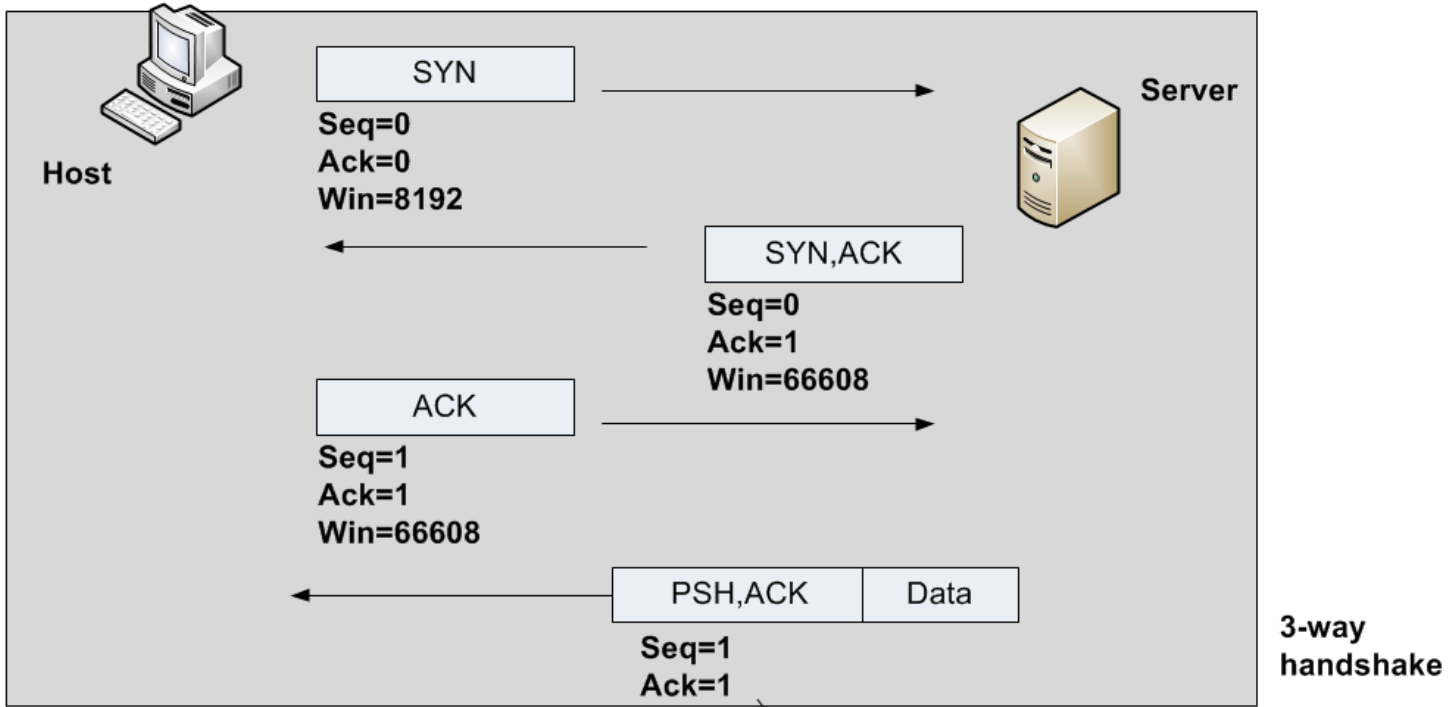


Network Forensics



Ethernet, IP and TCP





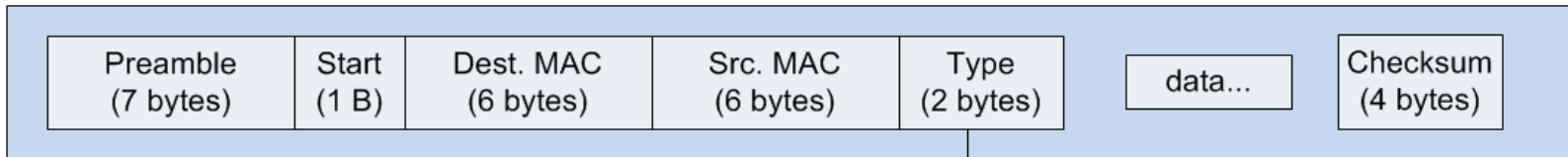
Protocol:
 1 – ICMP
 6 – TCP
 8 – EGP
 17 - UDP

IP header

Version		Header len.		Type of service	
Total length					
Identification					
0	D	M	Fragment Offset		
Time-to-live (TTL)			Protocol		
Header Checksum					
Source IP Address					
Destination IP Address					

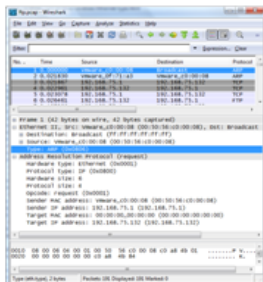
TCP header

TCP Source Port	
TCP Destination Port	
Sequence Number	
Acknowledgement Number	
Data Offset	Flags/Reserved
Window	
Checksum	
Urgent Pointer	

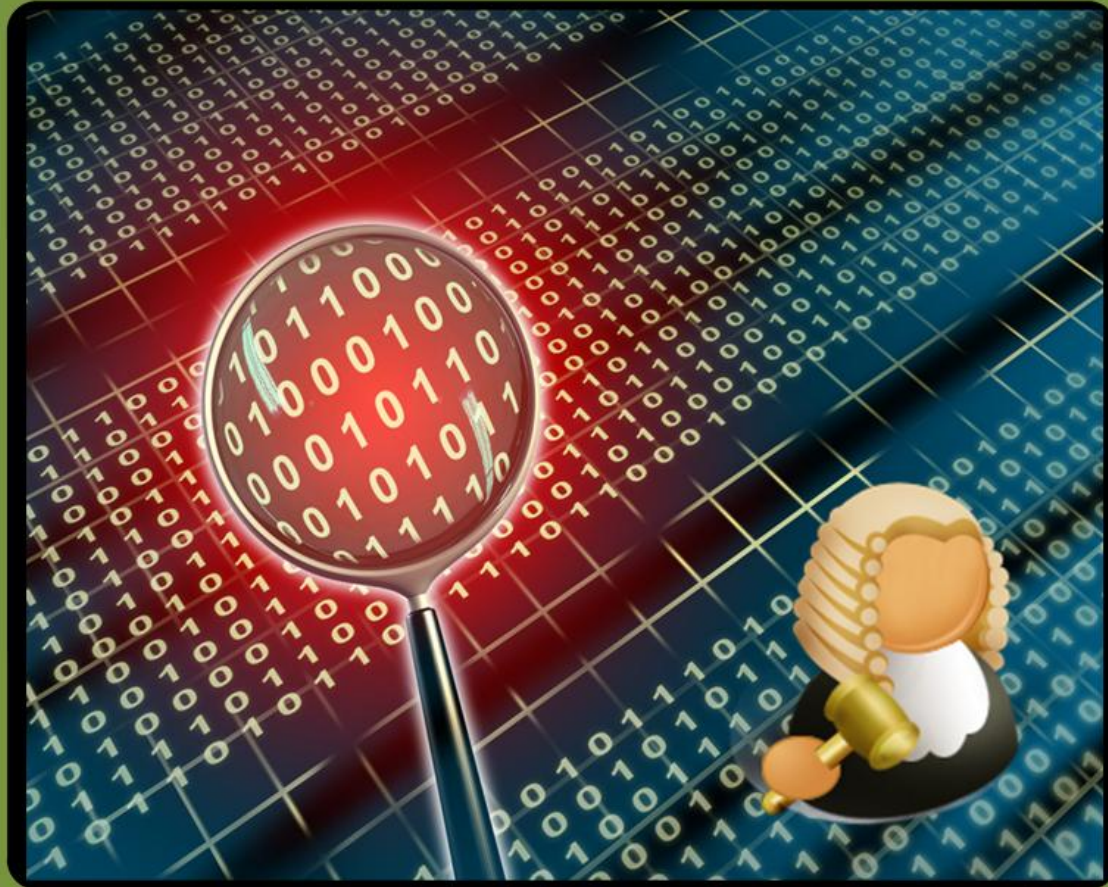


Type:
 0x800 – IP
 0x806 – ARP

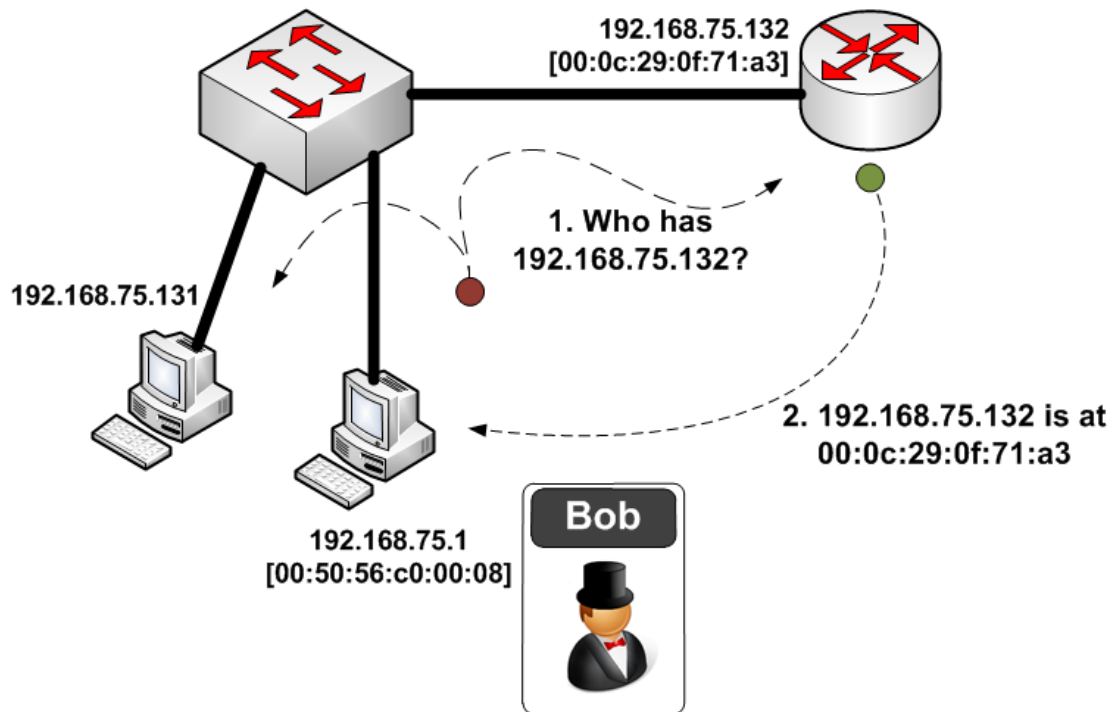
Ethernet frame



Network Forensics



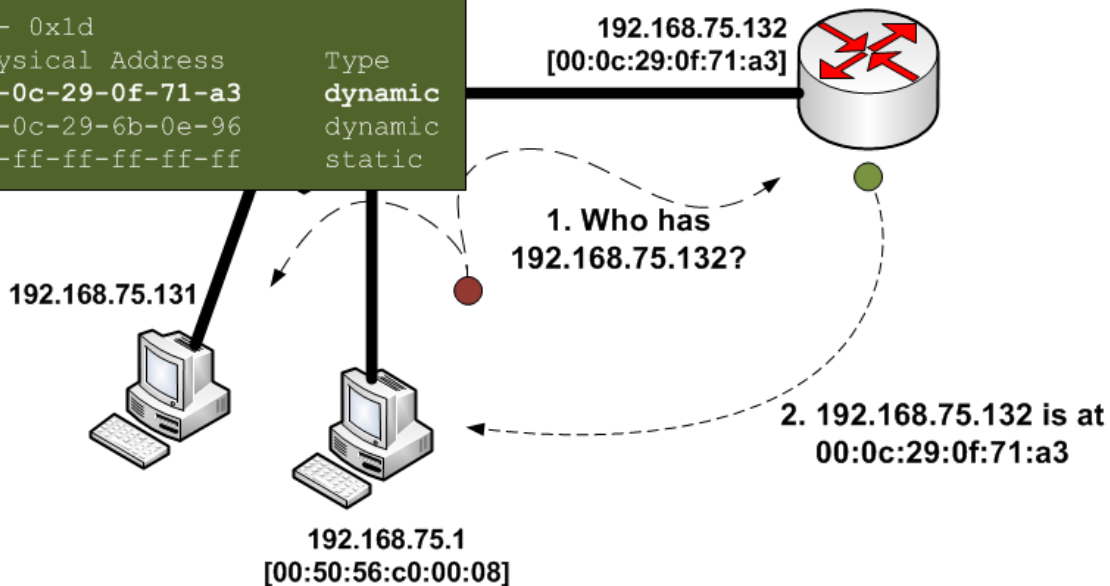
ARP



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

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)

Interface: 192.168.75.1 --- 0x1d	Internet Address	Physical Address	Type
	192.168.75.132	00-0c-29-0f-71-a3	dynamic
	192.168.75.138	00-0c-29-6b-0e-96	dynamic
	192.168.75.255	ff-ff-ff-ff-ff-ff	static

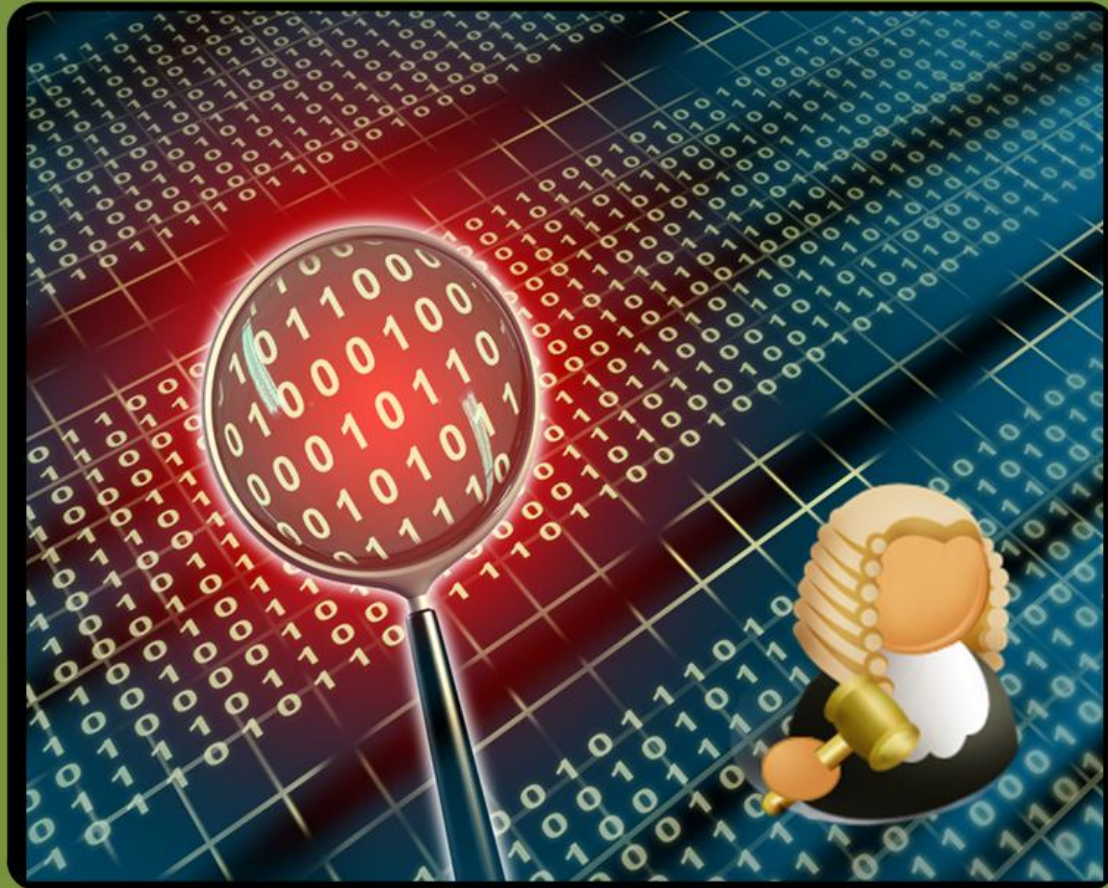


No.	Time	Source	Destination	Protocol	Info
2	0.021830	Vmware_0f:71:a3	Vmware_c0:00:08	ARP	192.168.75.132 is at 00:0c:29:0f:71:a3

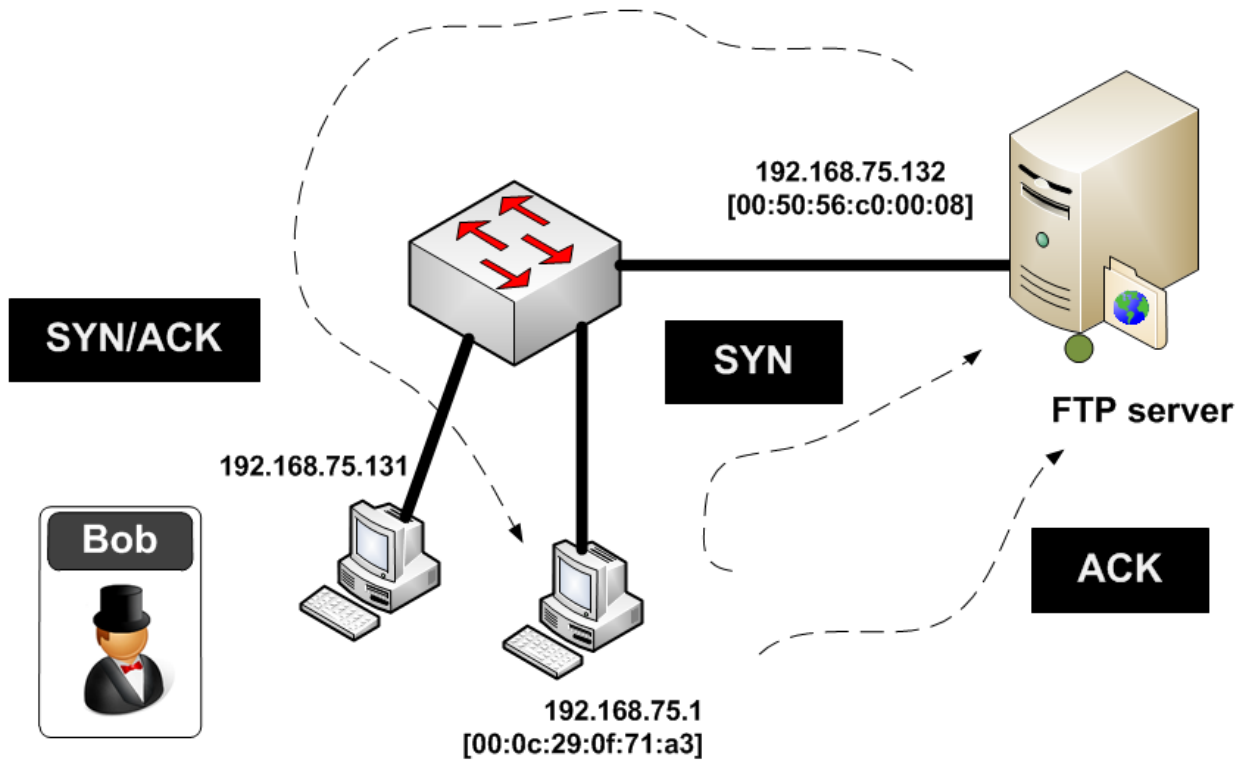
Frame 2 (42 bytes on wire, 42 bytes captured)
 Ethernet II, Src: Vmware_0f:71:a3 (00:0c:29:0f:71:a3), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
 Address Resolution Protocol (reply)

Author: Prof Bill Buchanan

Network Forensics



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

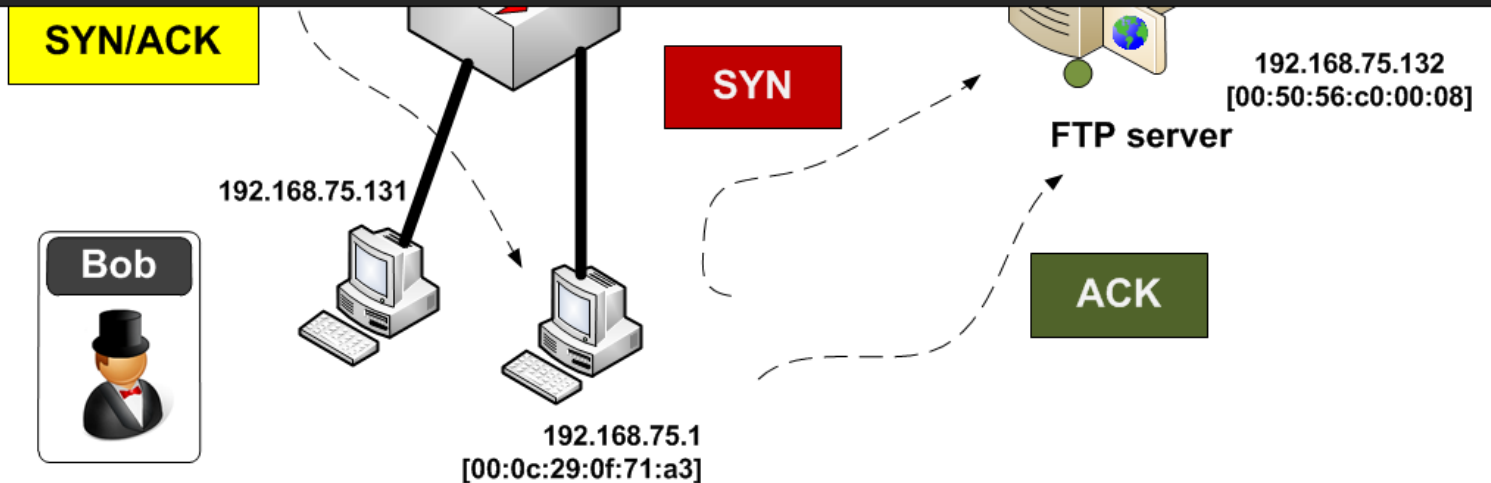
No.	Time	Source	Destination	Protocol	Info
5	0.023078	192.168.75.1	192.168.75.132	TCP	abatemgr > ftp [ACK] Seq=1 Ack=1 Win=66608 Len=0 TSV=683748 TSER=0

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

SYN

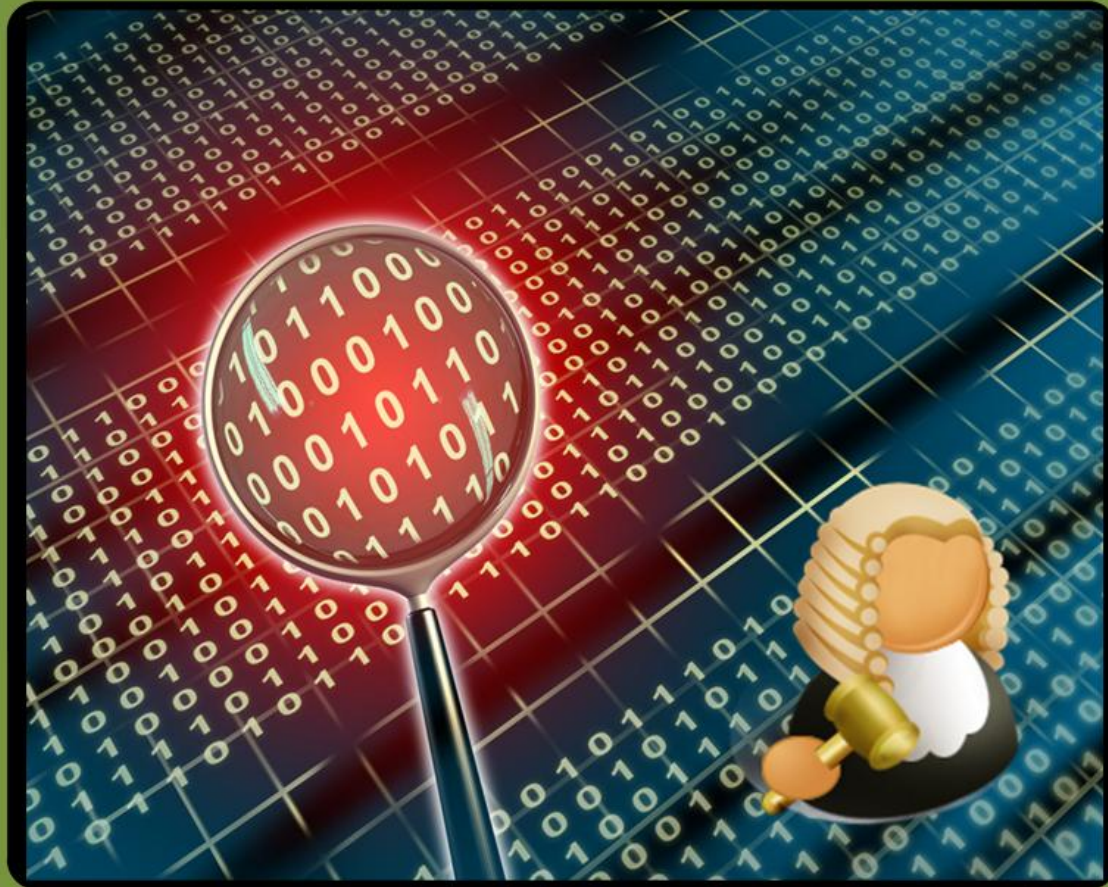
Net Forensics



Author: Prof Bill Buchanan

3-way handshake

Net Forensics



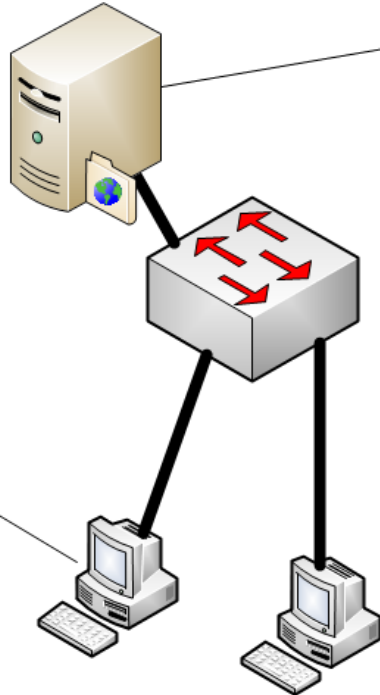
Application Protocol (FTP)

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.

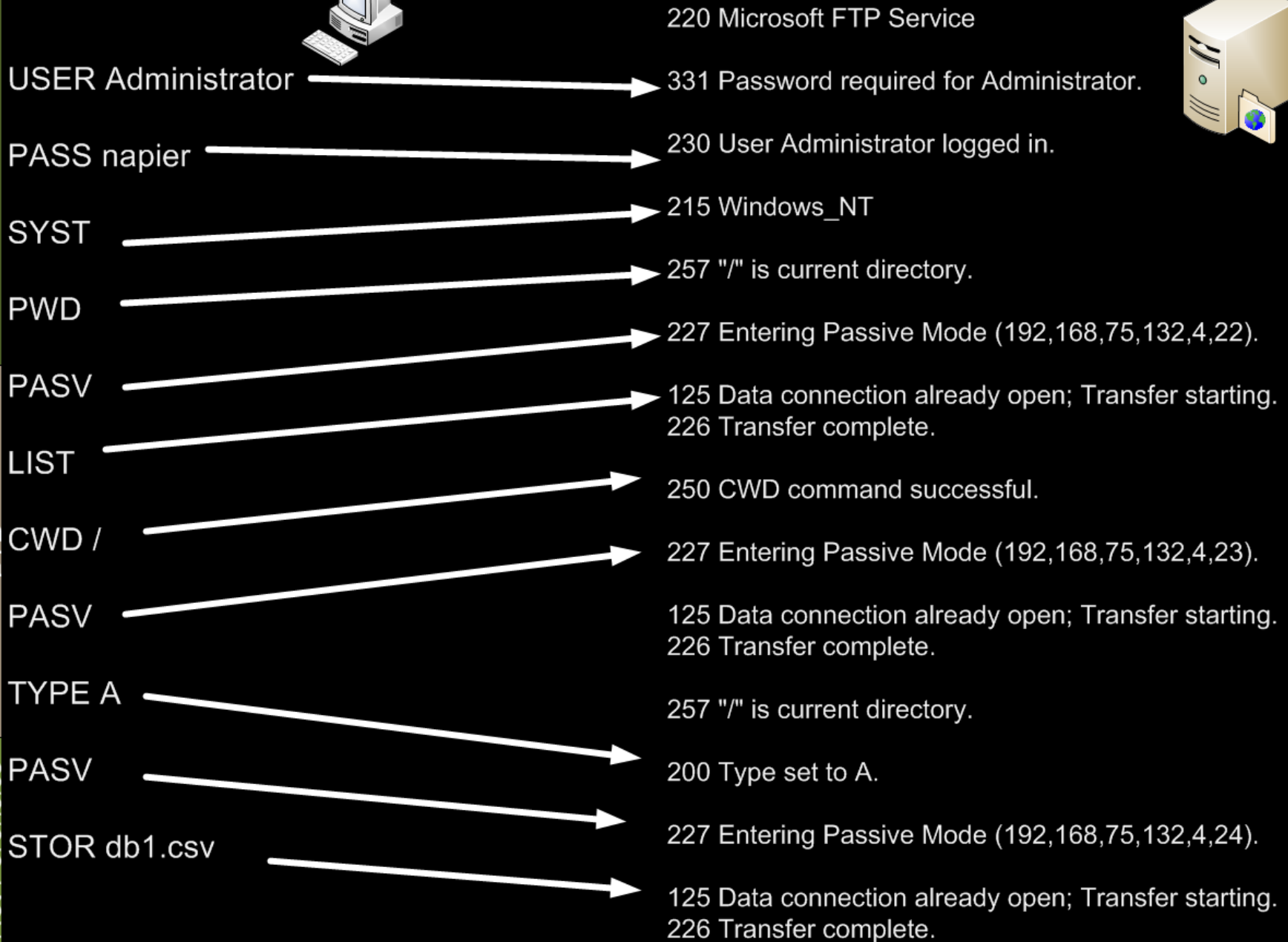
ascii
 binary
 bye
 cd
 close
 delete
 get
 help
 lcd
 ls
 mkdir
 mget
 mput
 open
 put
 pwd
 quit
 rmdir

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

FTP server



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.



ETD

Net Forensics

FTP commands and responses

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



CWD /
PASV
LIST

192.168.75.132
[00:50:56:c0:00:08]



250 CWD command successful

227 Entering Passive Mode (192,168,75,132,4,23).

SYN

SYN/ACK

ACK

Transfer on port
1047

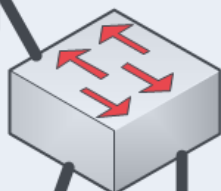
Server
port
created:
1047

FIN/ACK

FIN/ACK

226 Transfer complete.

192.168.75.132
[00:50:56:c0:00:08]

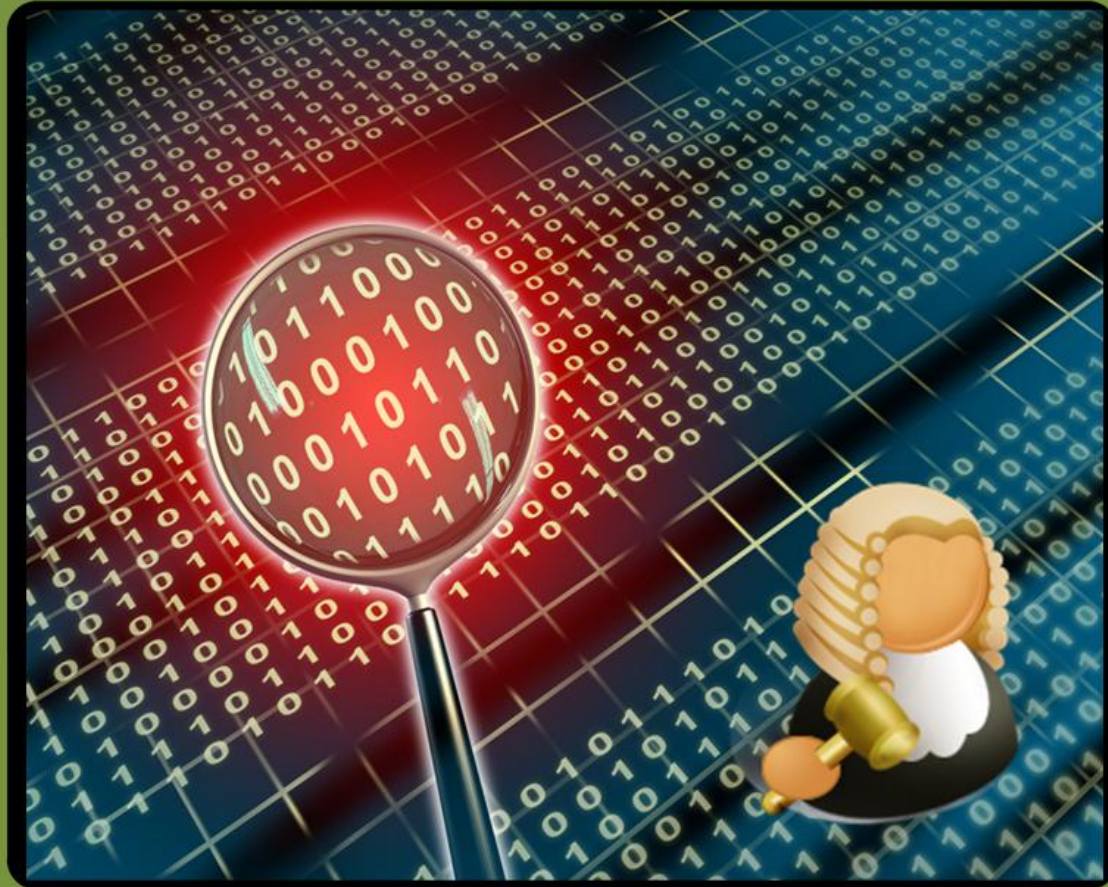


192.168.75.1
[00:0c:29:0f:71:a3]

192.168.75.131

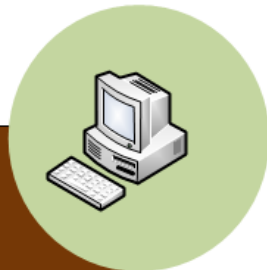
Bob

Net Forensics



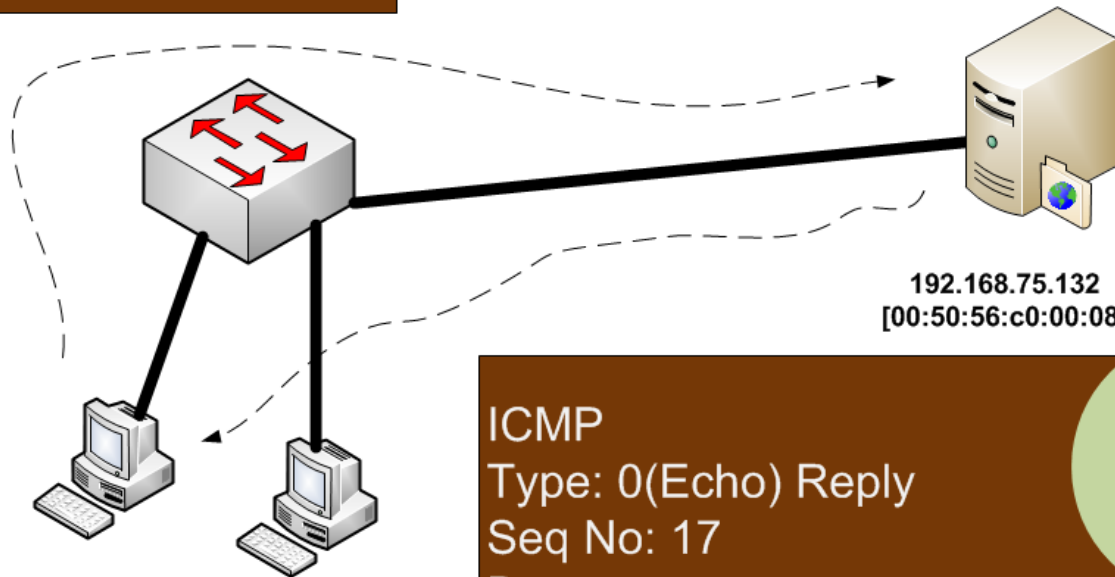
ICMP

ICMP
Type: 8 (Echo) Request
Seq No: 17
Data:
abcdefghijklmnopqrstuvwabcdefghi



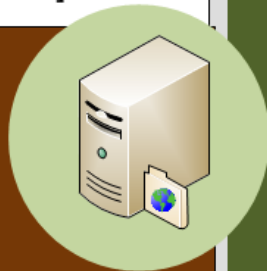
192.168.75.1
[00:0c:29:0f:71:a3]

192.168.75.131

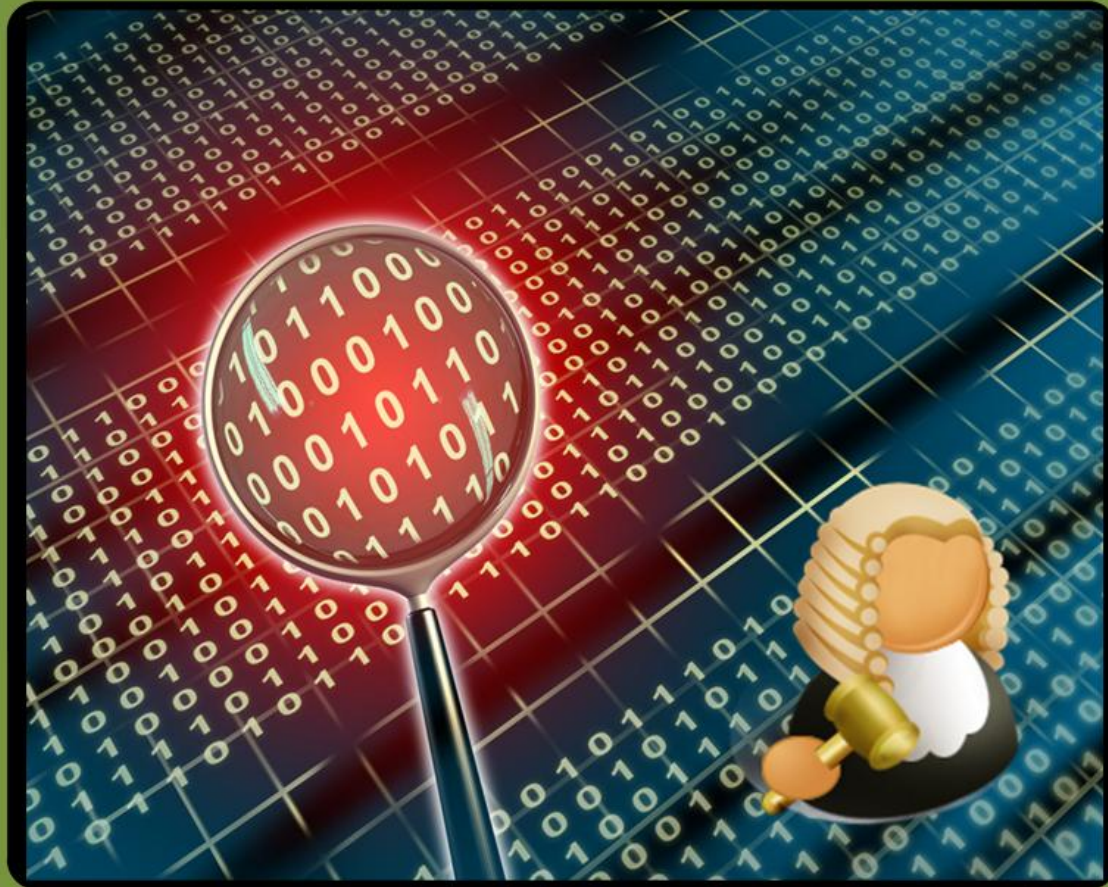


192.168.75.132
[00:50:56:c0:00:08]

ICMP
Type: 0(Echo) Reply
Seq No: 17
Data:
abcdefghijklmnopqrstuvwabcdefghi



Net Forensics



DNS

DNS (UDP)

Flags:

- Response (Query)
- Opcode (Standard Query (0))
- Recursive lookup
- No non-authenticated..

Query:

- www.intel.com: type A, class IN

DNS (UDP)

Flags:

- Response (Reply)
- Opcode (Standard Query (0))
- Recursive lookup
- No non-authenticated..

Query:

- www.intel.com: type A, class IN
- Authoritative ans:**
Server: n6g.akamai.net
IP: 92.122.208.217

Local DNS

a961.g.akamai.net



DNS servers



DNS server

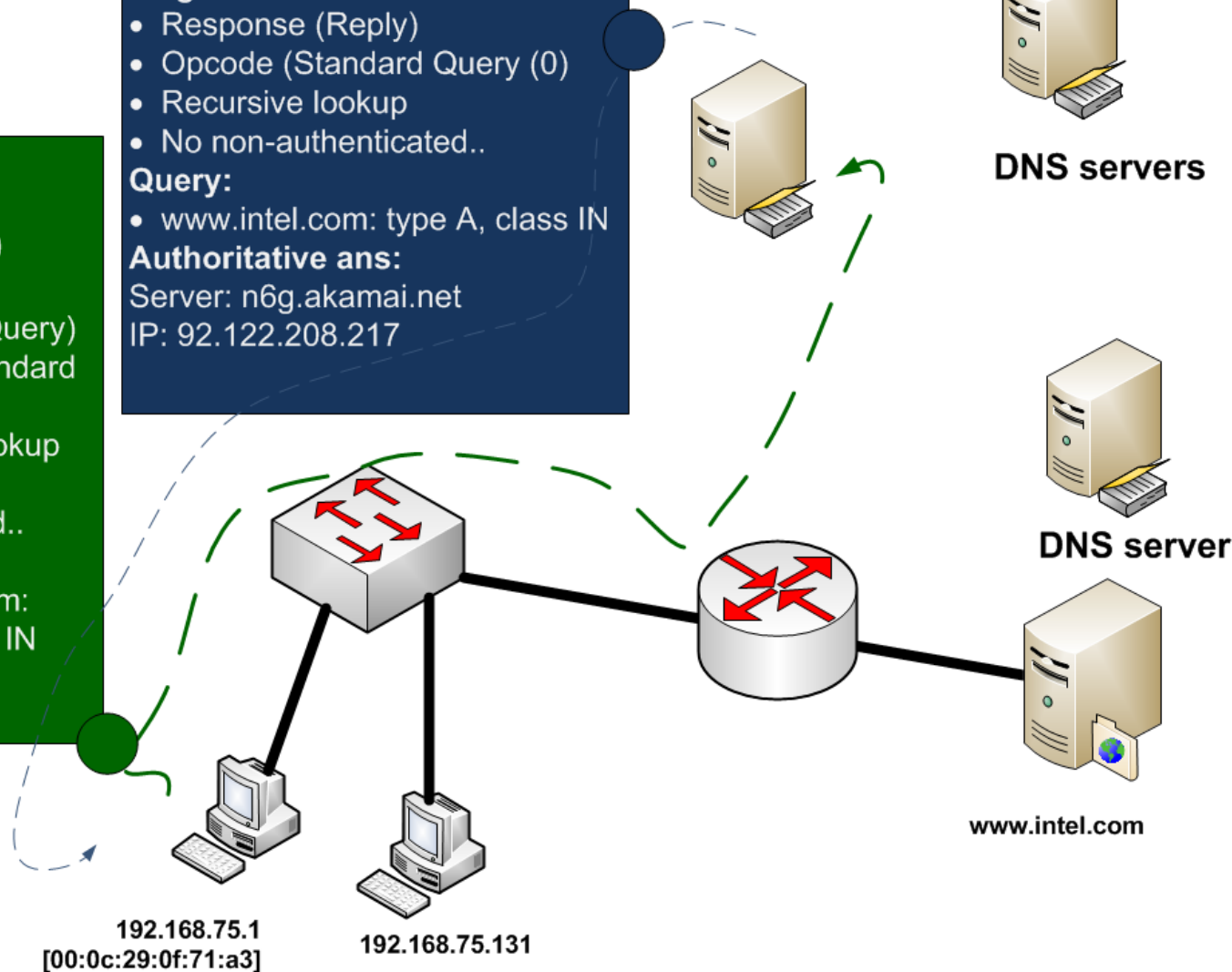


www.intel.com

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

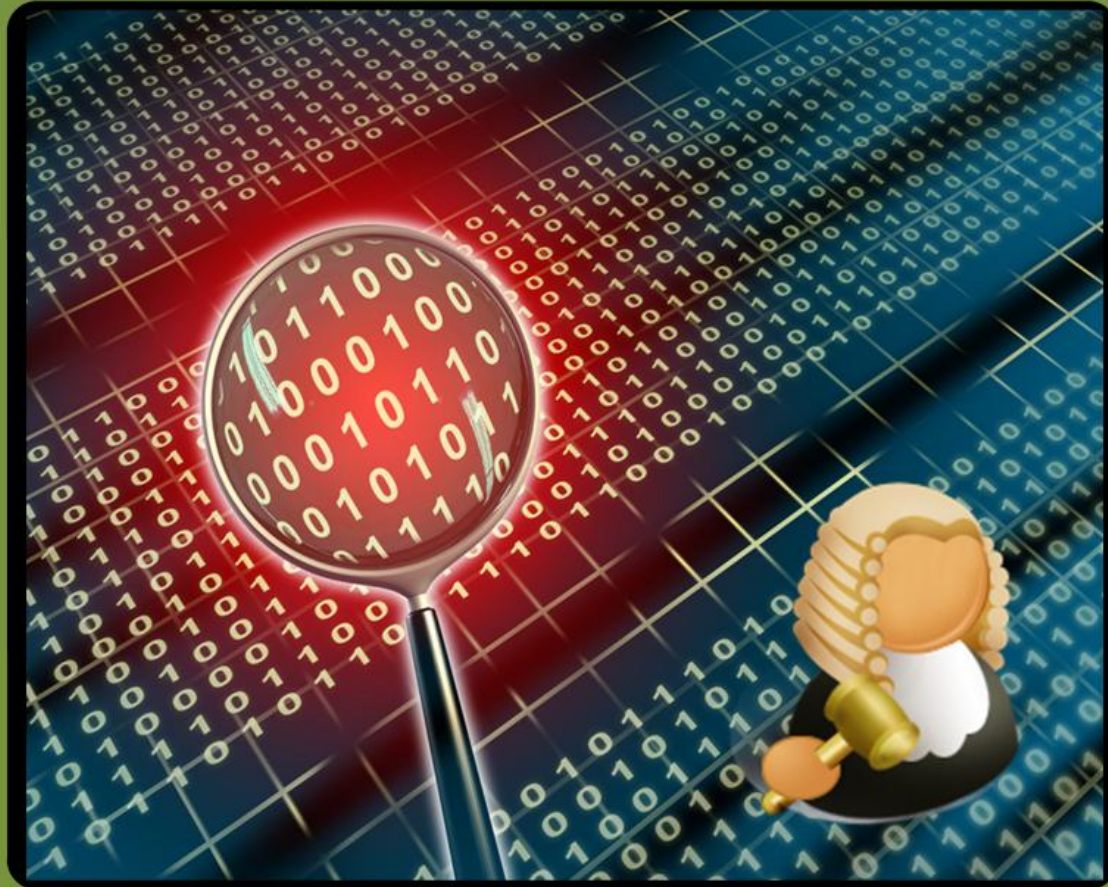
192.168.75.131

Bob



Author: Prof Bill Buchanan

Net Forensics



Port Scan

No.	Time	Source	Destination	Protocol	Info
85	25.420710	192.168.75.1	192.168.75.132	TCP	54370 > telnet

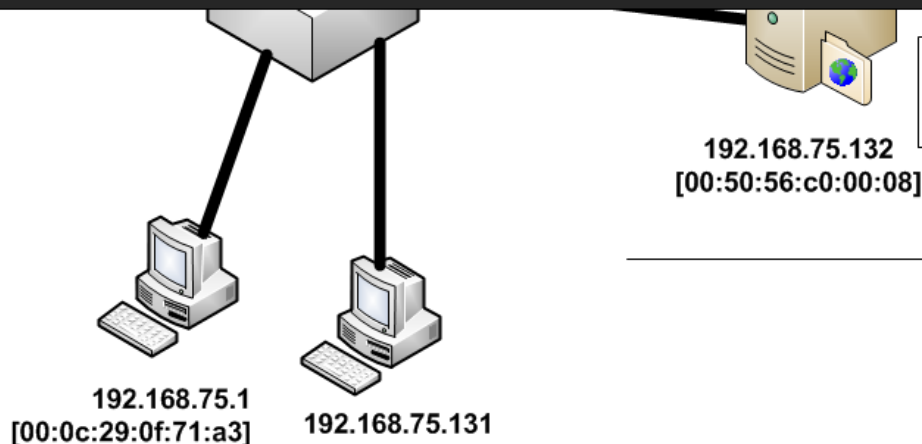
[SYN] Seq=0 Win=1024 Len=0 MSS=1460

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



Scan tools: NMAP, hping, etc

TCP Scan

SYN

SYN/ACK

ACK

FIN/ACK

SYN Scan

SYN

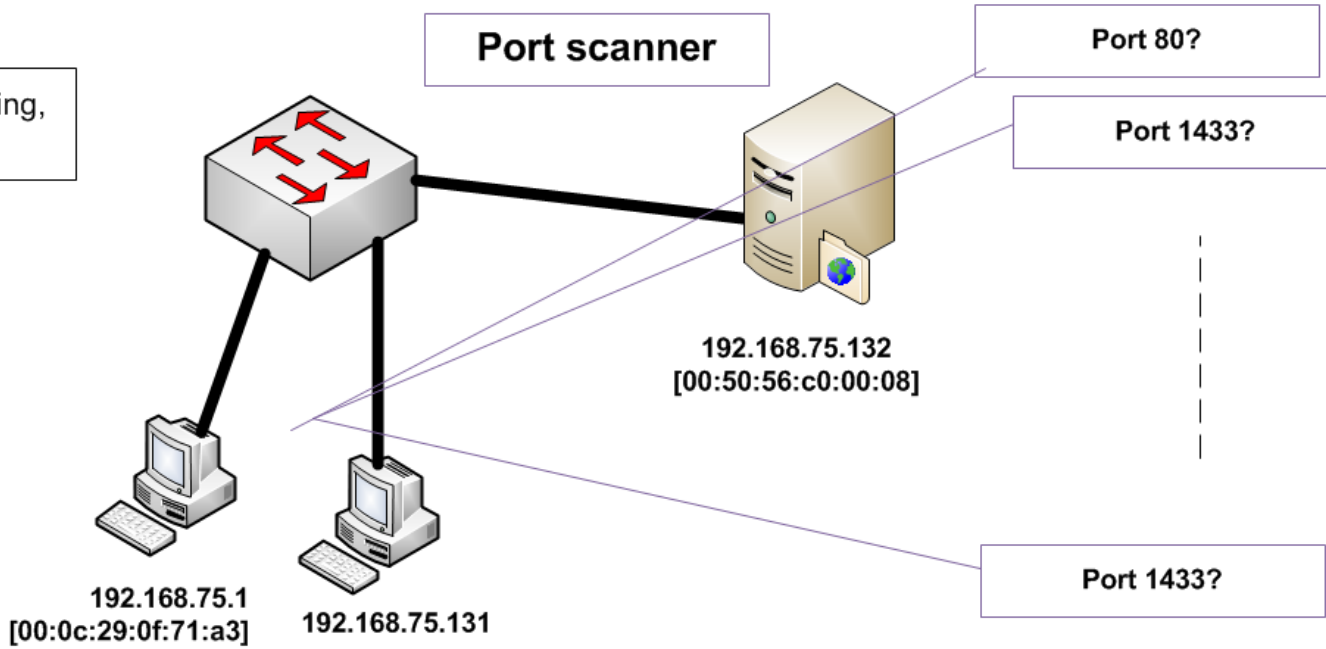
Creates half-open connections

FIN Scan

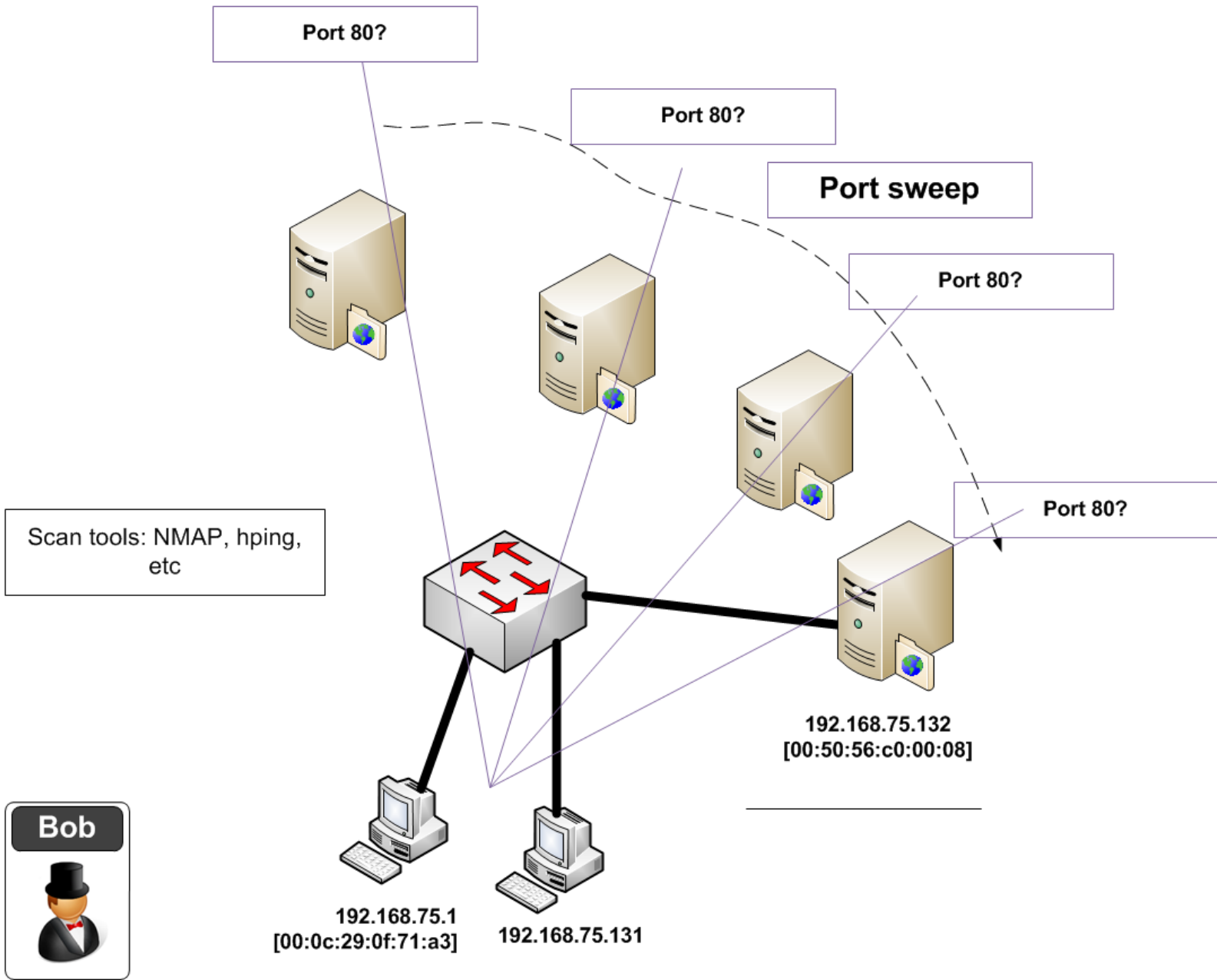
FIN

Closed ports respond with a RST, but open ports ignore.

Scan tools: NMAP, hping, etc



Author: Prof Bill Buchanan



Wireshark: 2149 Expert Infos

Errors: 0 Warnings: 0 Notes: 0 Chats: 2149 Severity filter: Error+Warn+Note+Chat

No.	Sever.	Group	Protocol	Summary
116	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port netbios-ssn
117	Chat	Sequence	TCP	Connection reset (RST)
118	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port ftp
119	Chat	Sequence	TCP	Connection reset (RST)
120	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port smtp
121	Chat	Sequence	TCP	Connection reset (RST)
122	Chat	Sequence	TCP	Connection reset (RST)
123	Chat	Sequence	TCP	Connection establish request (SYN): server port http
124	Chat	Sequence	TCP	Connection establish request (SYN): server port epmap
125	Chat	Sequence	TCP	Connection establish request (SYN): server port domain
126	Chat	Sequence	TCP	Connection establish request (SYN): server port h323hostcall
127	Chat	Sequence	TCP	Connection establish request (SYN): server port imap
128	Chat	Sequence	TCP	Connection establish request (SYN): server port pop3
129	Chat	Sequence	TCP	Connection establish request (SYN): server port ident
130	Chat	Sequence	TCP	Connection establish request (SYN): server port https
131	Chat	Sequence	TCP	Connection establish request (SYN): server port 65129
132	Chat	Sequence	TCP	Connection establish request (SYN): server port 1007
133	Chat	Sequence	TCP	Connection establish request (SYN): server port encrypted_admin
134	Chat	Sequence	TCP	Connection establish request (SYN): server port 8011
135	Chat	Sequence	TCP	Connection establish request (SYN): server port sbl
136	Chat	Sequence	TCP	Connection establish request (SYN): server port 3404
137	Chat	Sequence	TCP	Connection establish request (SYN): server port 49163
138	Chat	Sequence	TCP	Connection establish request (SYN): server port activesync
139	Chat	Sequence	TCP	Connection establish request (SYN): server port klogin
140	Chat	Sequence	TCP	Connection establish request (SYN): server port esro-gen
141	Chat	Sequence	TCP	Connection establish request (SYN): server port dnp
142	Chat	Sequence	TCP	Connection establish request (SYN): server port presence
143	Chat	Sequence	TCP	Connection establish request (SYN): server port 6129
144	Chat	Sequence	TCP	Connection establish request (SYN): server port ii-admin

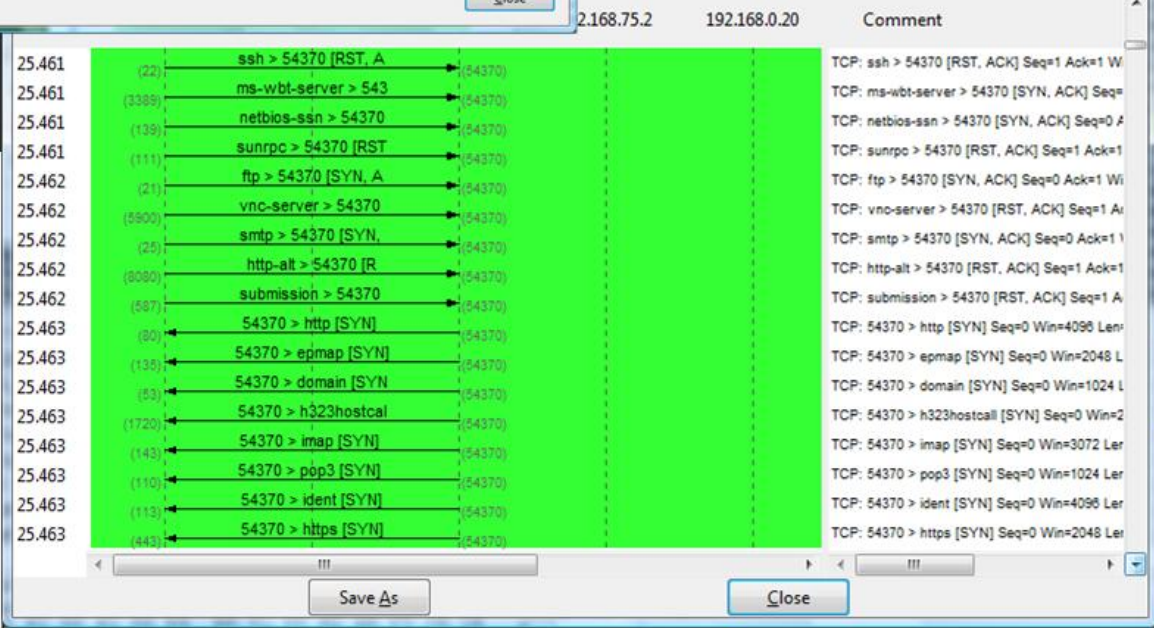
Endpoints: nmap.pcap

Ethernet: 4 Fibre Channel FDDI IPv4: 5 IPX JXTA NCP RSVP SCTP **TCP: 1003** Token Ring UDP: 9 USB WLAN

TCP Endpoints

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
192.168.75.1	54370	1967	110518	1000	58000	967	52518
192.168.75.1	54371	166	9296	83	4814	83	4482
192.168.0.20	netbios-ssn	124	14756	76	7928	48	6828
192.168.75.132	sbl	33	3801	13	1761	20	2040
192.168.75.132	netarx	33	3801	13	1761	20	2040
192.168.75.132	danf-ak2	33	3801	13	1761	20	2040
192.168.75.132	afrog	33	3801	13	1761	20	2040
192.168.75.132	telnet	4	232	3	174	1	58
192.168.75.132	microsoft-ds	4	232	3	174	1	58
192.168.75.132	blackjack	4	232	3	174	1	58
192.168.75.132	ms-wbt-server	4	232	3	174	1	58
192.168.75.132	netbios-ssn	4	232	3	174	1	58
192.168.75.132	ftp	4	232	3	174	1	58
192.168.75.132	smtp	4	232	3	174	1	58
192.168.75.132	http	4	232	3	174	1	58
192.168.75.132	epmap	4	232	3	174	1	58
192.168.75.132	domain	4	232	3	174	1	58

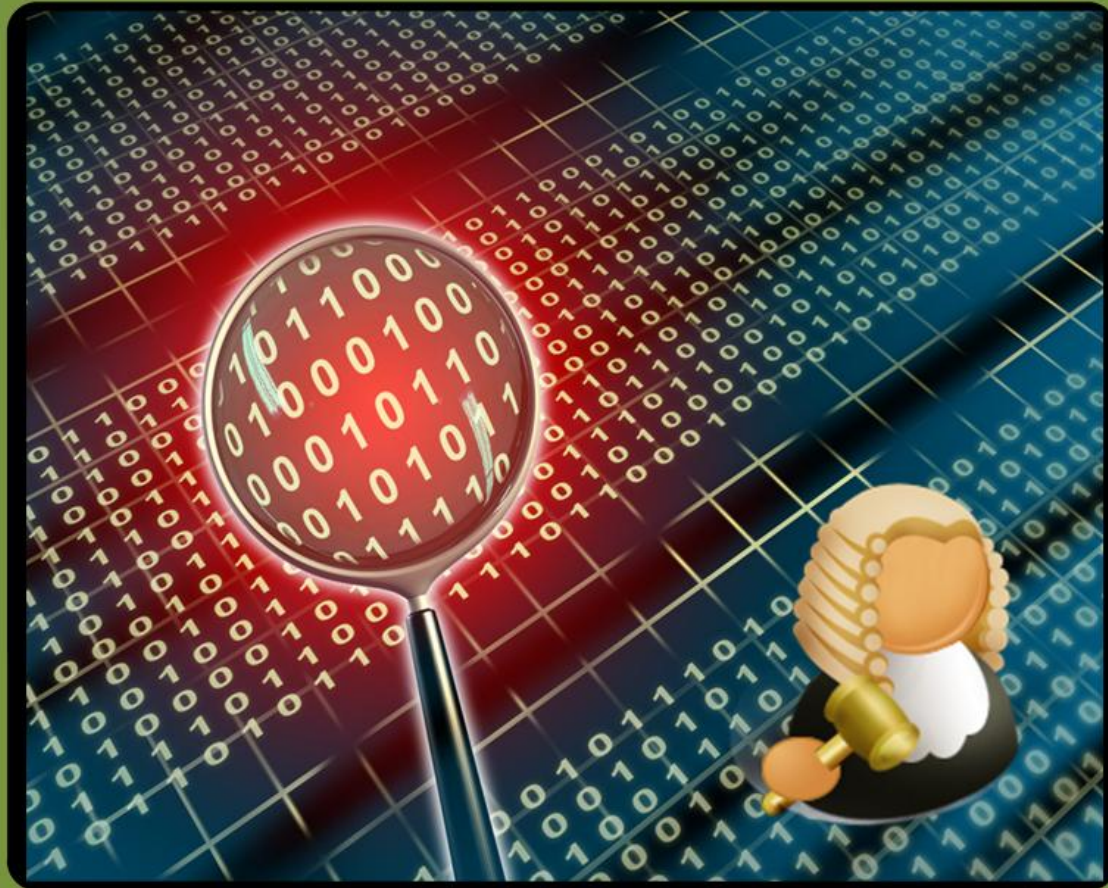
Net Forensics



Author: Prof Bill Buchanan

Port Scan

Net Forensics



SYN FLOOD

No.	Time	Source	Destination	Protocol	Info
2	4.510329	192.168.75.137	192.168.75.1	HTTP	Continuation

or non-HTTP traffic

Frame 2 (58 bytes on wire, 58 bytes captured)

Internet Protocol, Src: 192.168.75.137 (192.168.75.137), Dst: 192.168.75.1 (192.168.75.1)

Transmission Control Protocol, Src Port: smart-lm (1608), Dst Port: http (80), Seq: 0, Len: 4

Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Info
3	5.514164	192.168.75.137	192.168.75.1	HTTP	Continuation

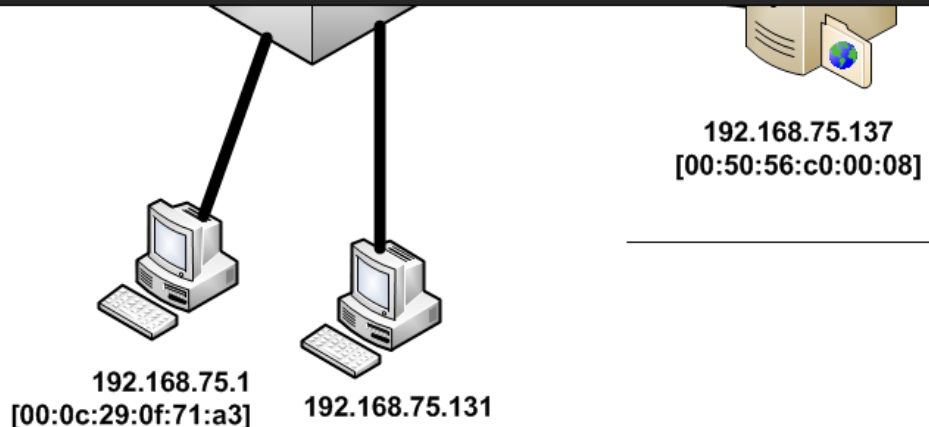
or non-HTTP traffic

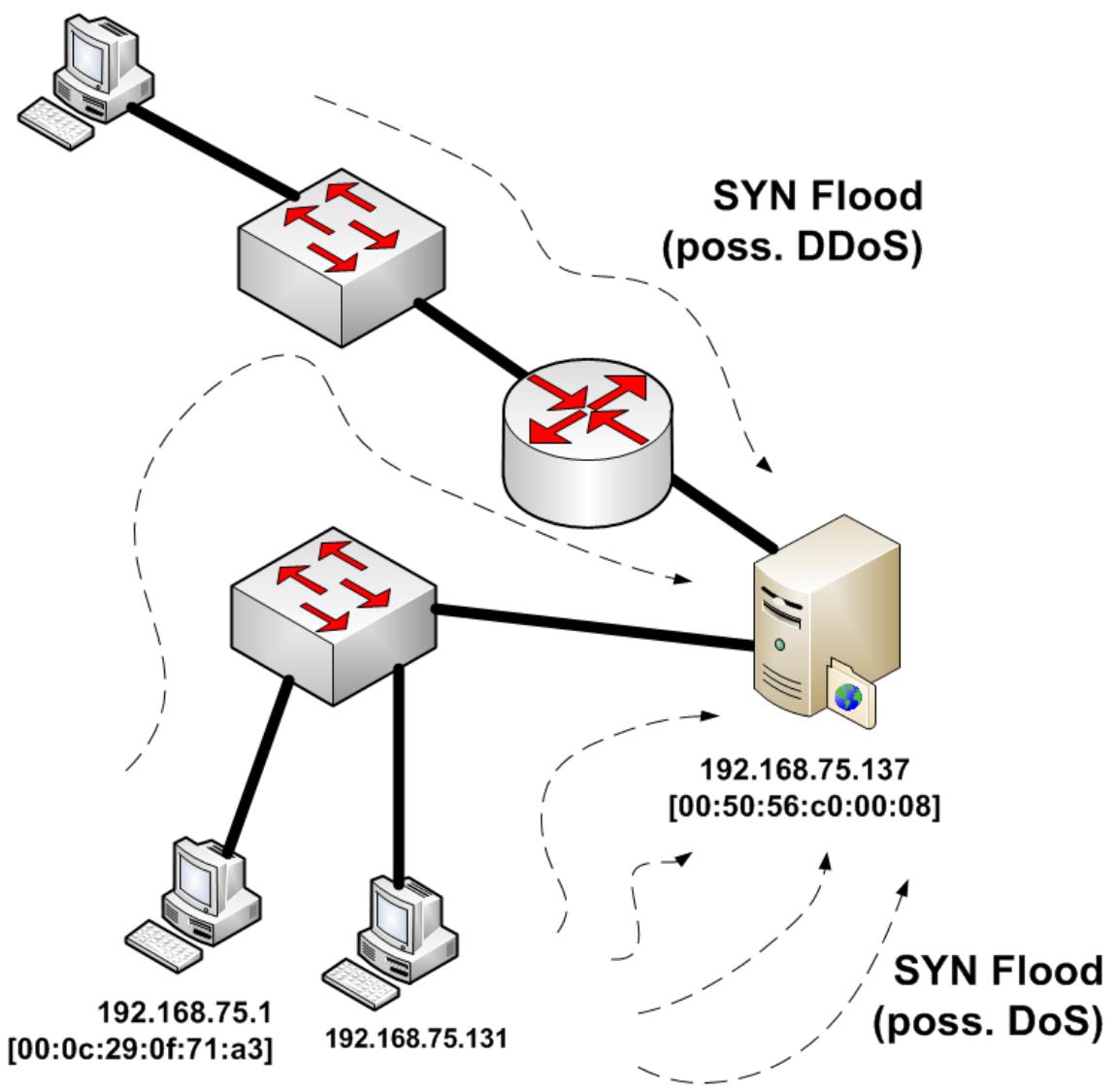
Frame 3 (58 bytes on wire, 58 bytes captured)

Internet Protocol, Src: 192.168.75.137 (192.168.75.137), Dst: 192.168.75.1 (192.168.75.1)

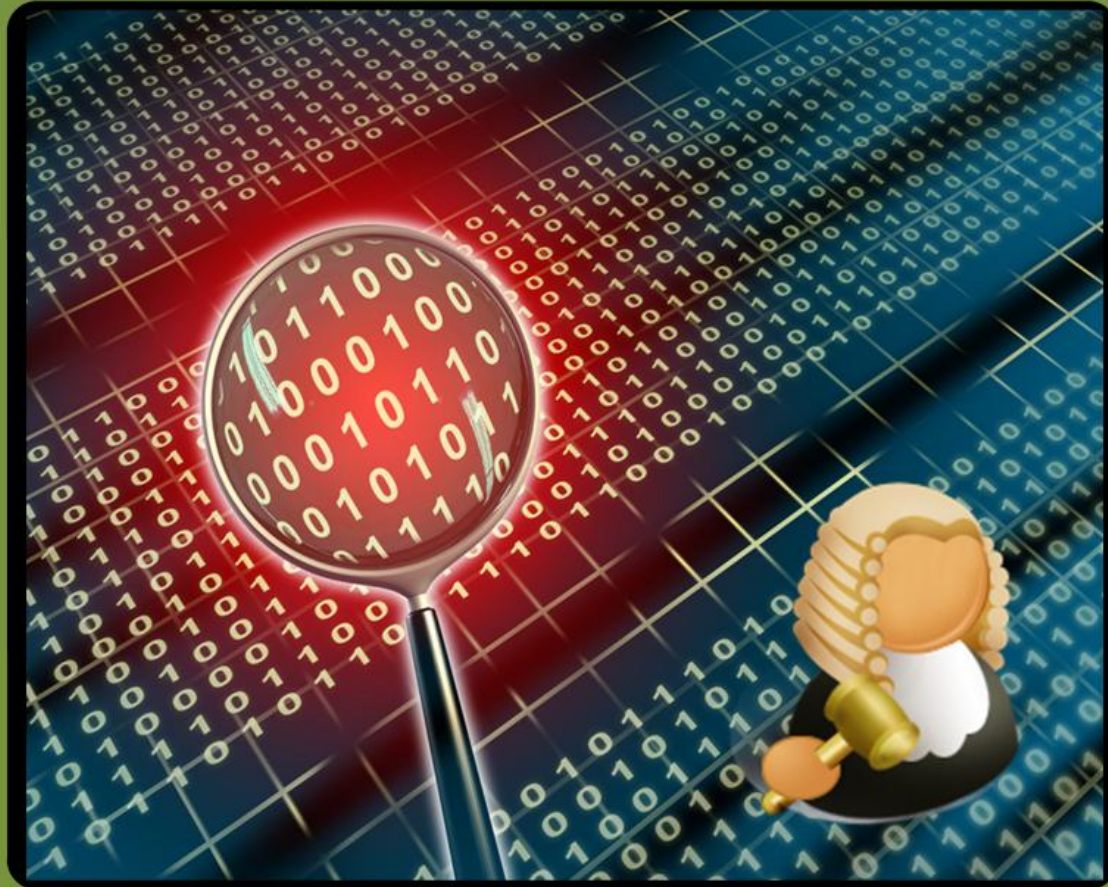
Transmission Control Protocol, Src Port: isysg-lm (1609), Dst Port: http (80), Seq: 0, Len: 4

Hypertext Transfer Protocol

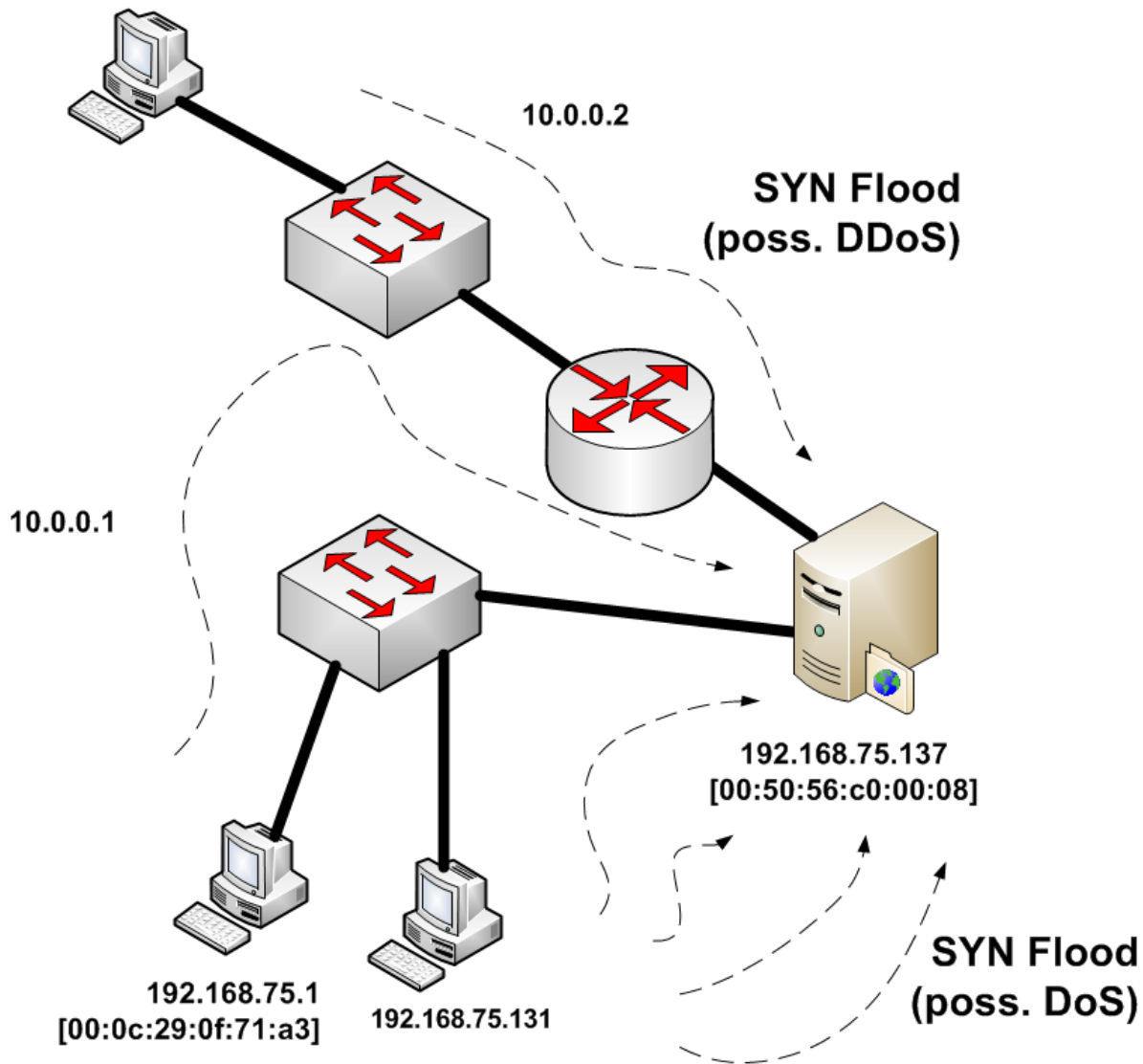




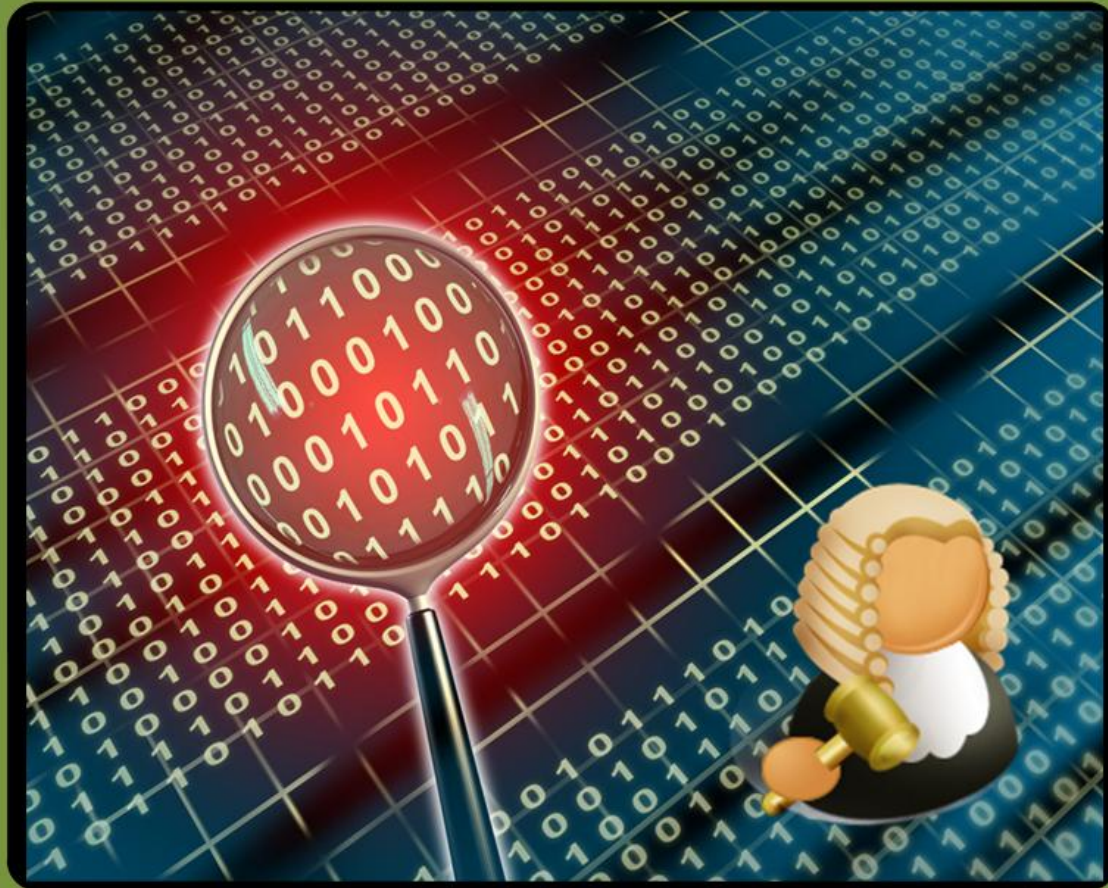
Net Forensics



SPOOFED ADDRESSES



Net Forensics



Application Protocol

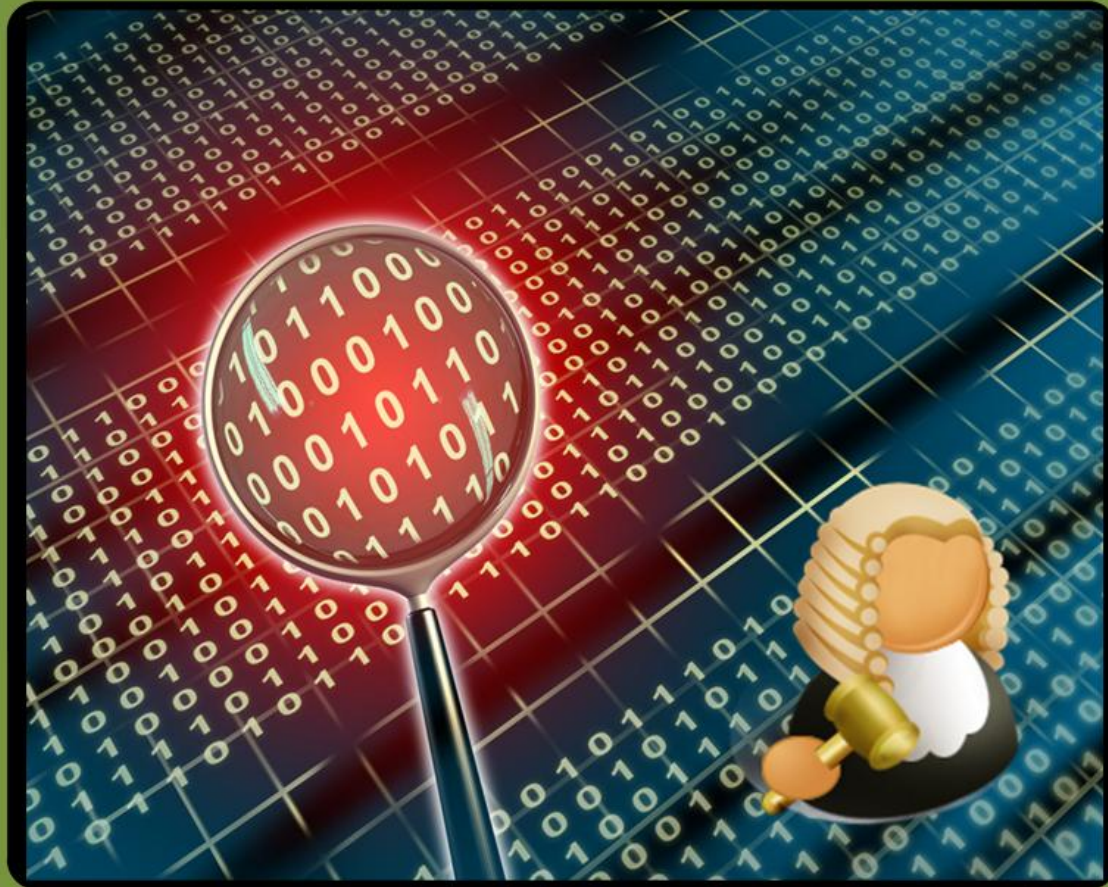
```
GET / HTTP/1.1
User-Agent: Opera/9.80 (Windows NT 6.0; U; en) Presto/
2.2.15 Version/10.01
Host: 192.168.75.132
Accept: text/html, application/xml;q=0.9, application/
xhtml+xml, image/png, image/jpeg, image/gif, image/x-
bitmap, */*;q=0.1 Accept-Language: en-GB,en;q=0.9
Accept-Charset: iso-8859-1, 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: "fc31243677ccal: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"> ...
```

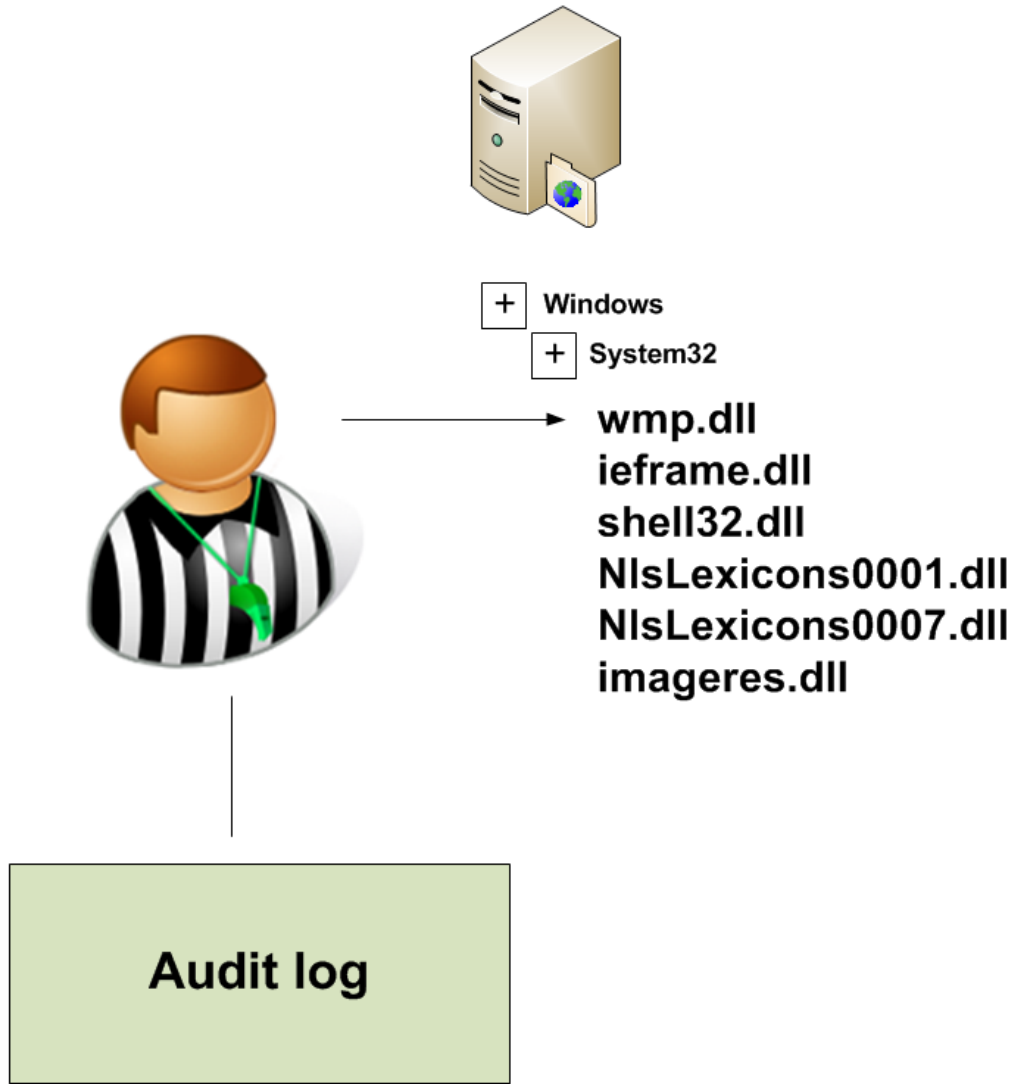
Bob

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

Net Forensics



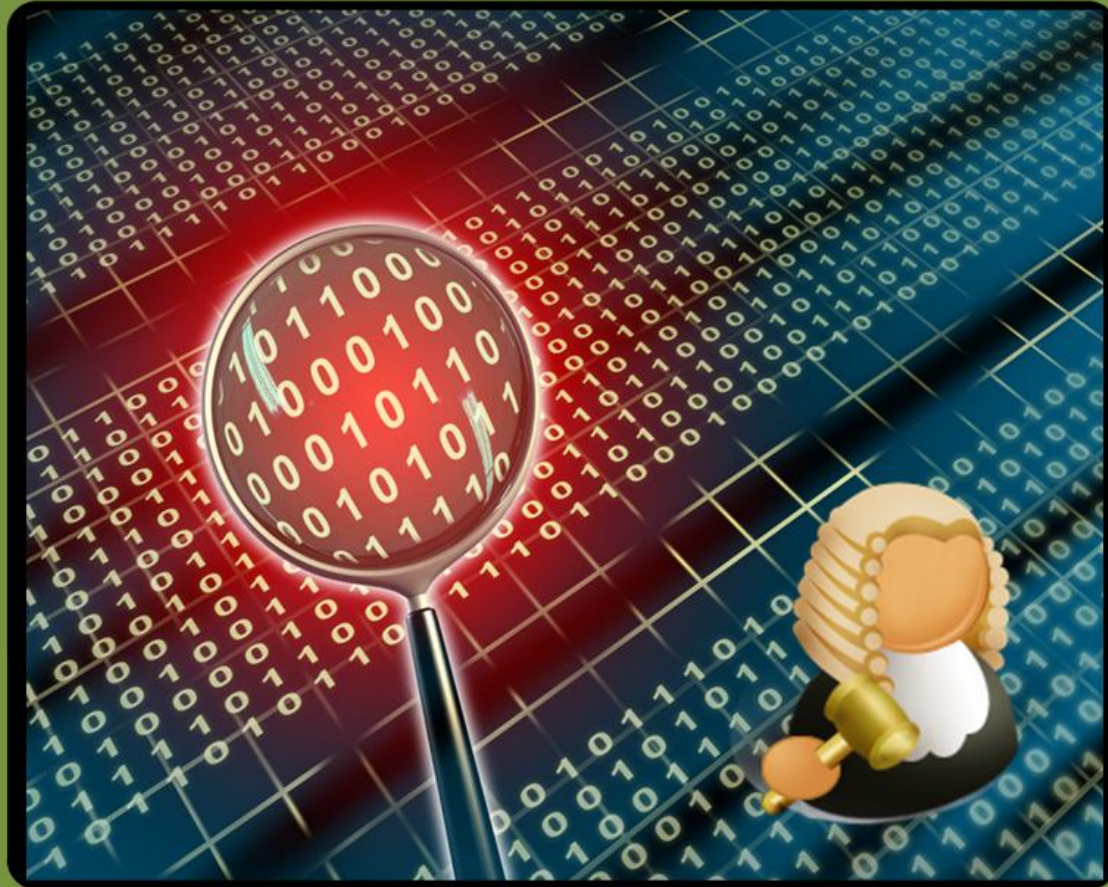
Tripwire



Start of demo

End of demo

Net Forensics



Host trace

Recent Files

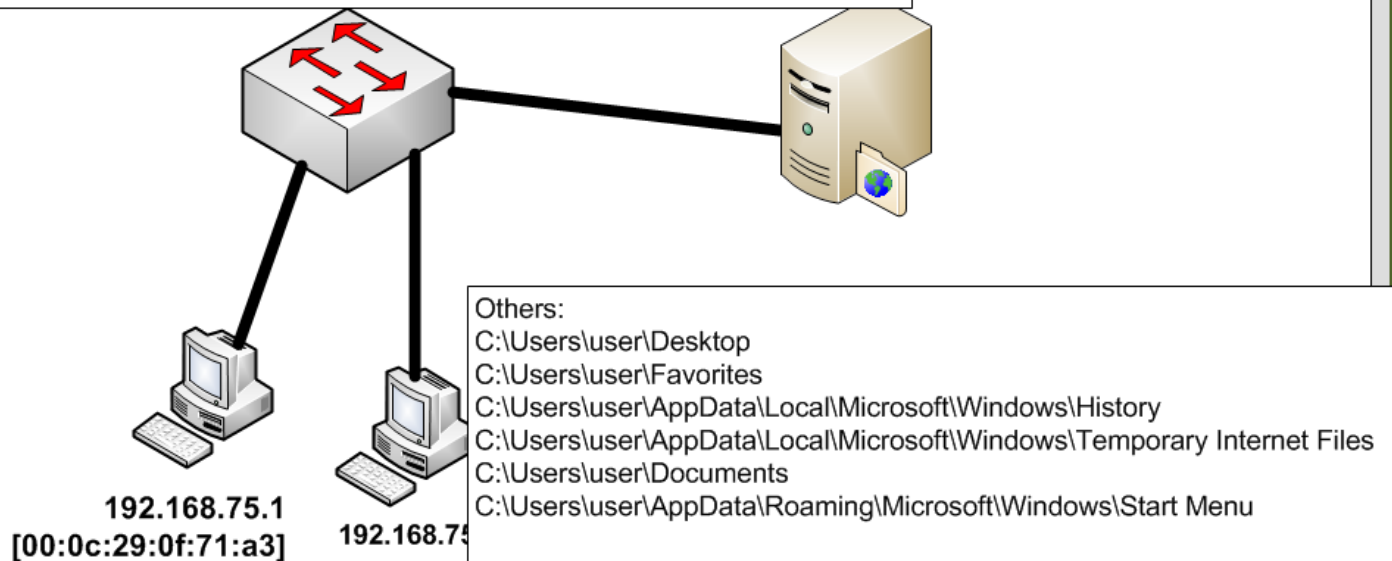
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent

Cookies

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies

Explorer History

C:\Users\user\AppData\Local\Microsoft\Windows\History
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files



Author: Prof Bill Buchanan

Network Forensics

- Understand some of the methodologies used in network forensics.
- Provide an in-depth understanding of the key network protocols, including IP, TCP, ARP, ICMP, DNS, Application Layer protocols, and so on.
- Define a range of audit sources for network activity.

