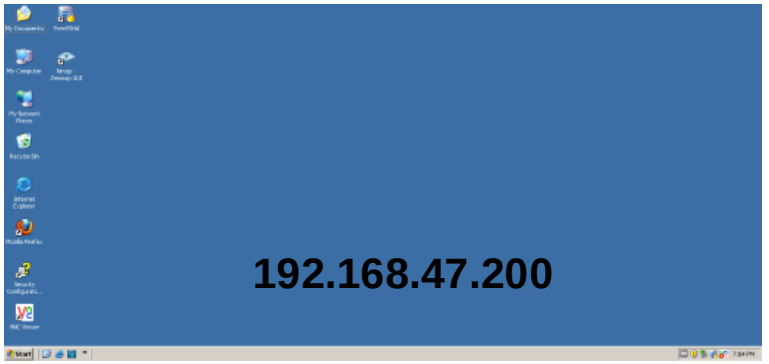
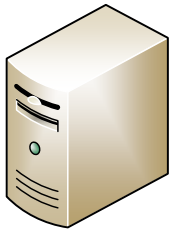
Advanced Network Forensics

- User/Password Crack.
- Port Scan.
- Signature Detection.
- Converted Formats.
- ARP Spoofing.
- DDoS Detection.

Author: Prof Bill Buchanan



hping



Snort -i 1 -c 1.rules

Nmap

WIRESHARK

SNORT

alert.ids

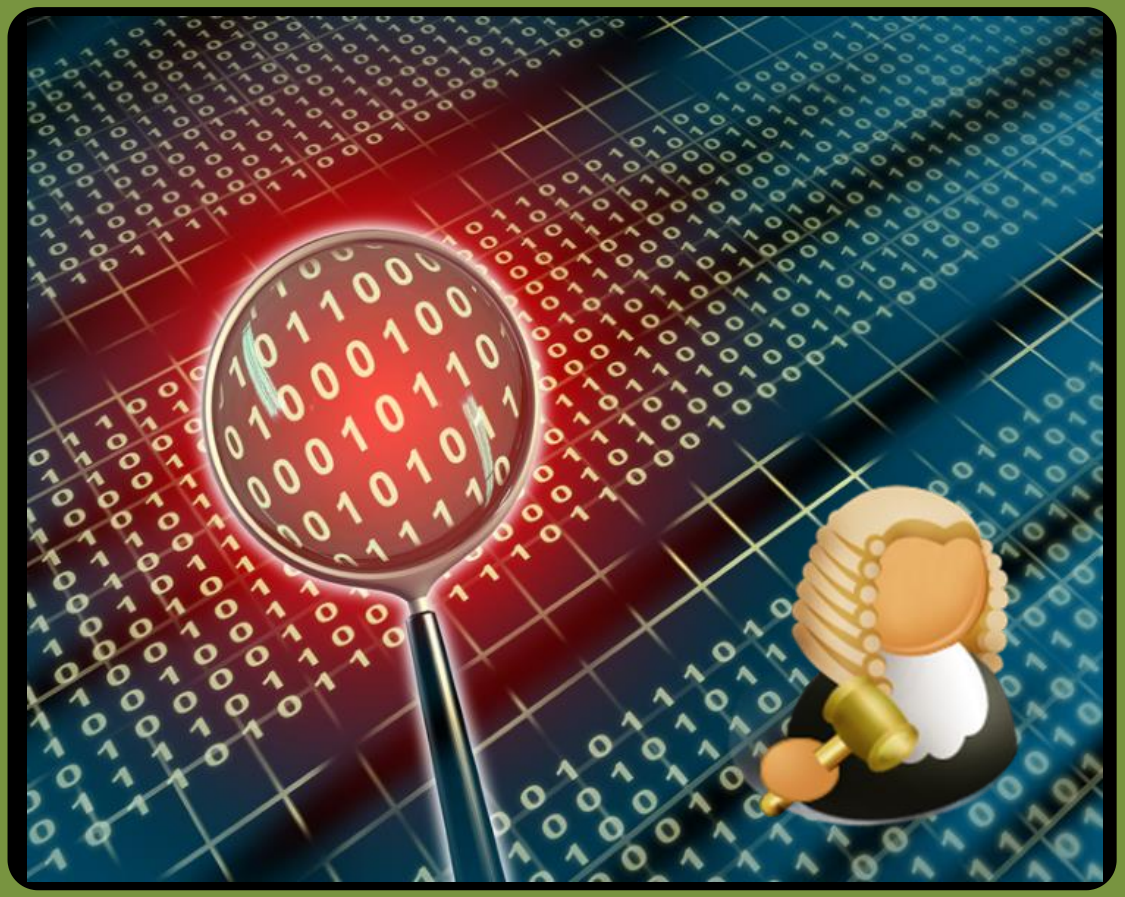
Hydra

1.pcap

Snort -i 1 -r 1.pcap

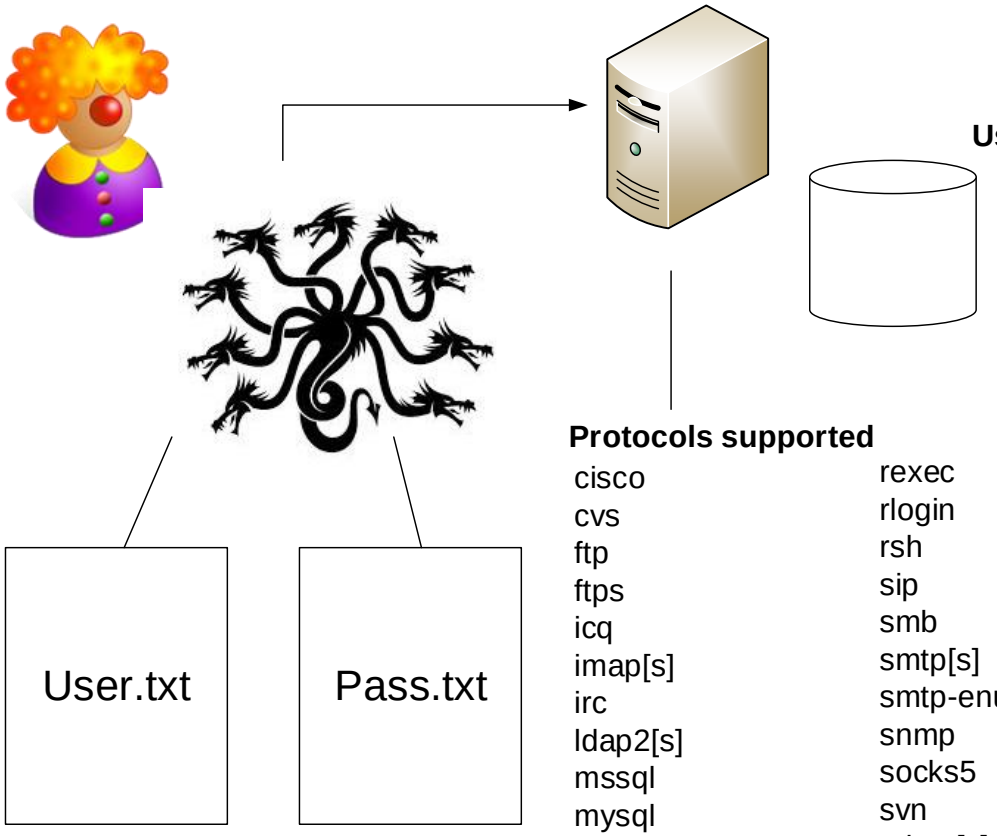
Author: Prof Bill Buchanan

Advanced Network Forensics



User/Password Crack

Author: Prof Bill Buchanan



Protocols supported

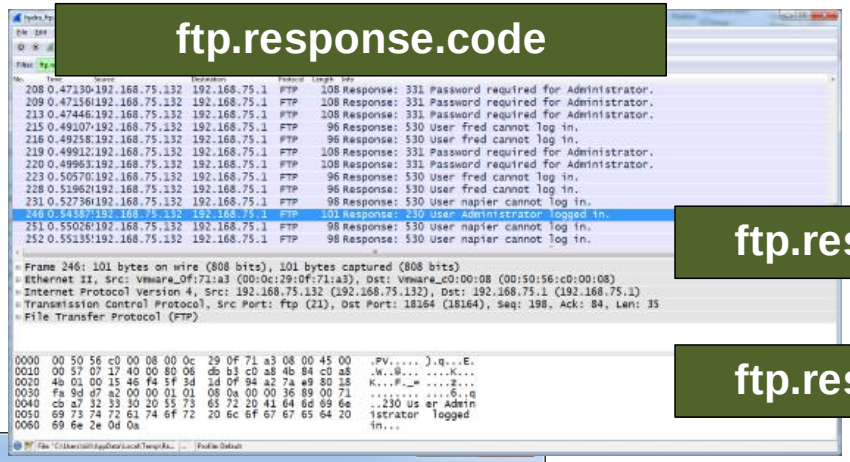
cisco
cvs
ftp
ftps
icq
imap[s]
irc
ldap2[s]
mssql
mysql
nntp
oracle-listener
oracle-sid
pcanywhere
pcnfs
pop3[s]
rdp
rexec
rlogin
rsh
sip
smb
smtp[s]
smtp-enum
snmp
socks5
svn
telnet[s]
vmauthd
vnc
xmpp

Author: Prof Bill Buchanan

Cracking usernames

Adv Net For.

ftp.response.code

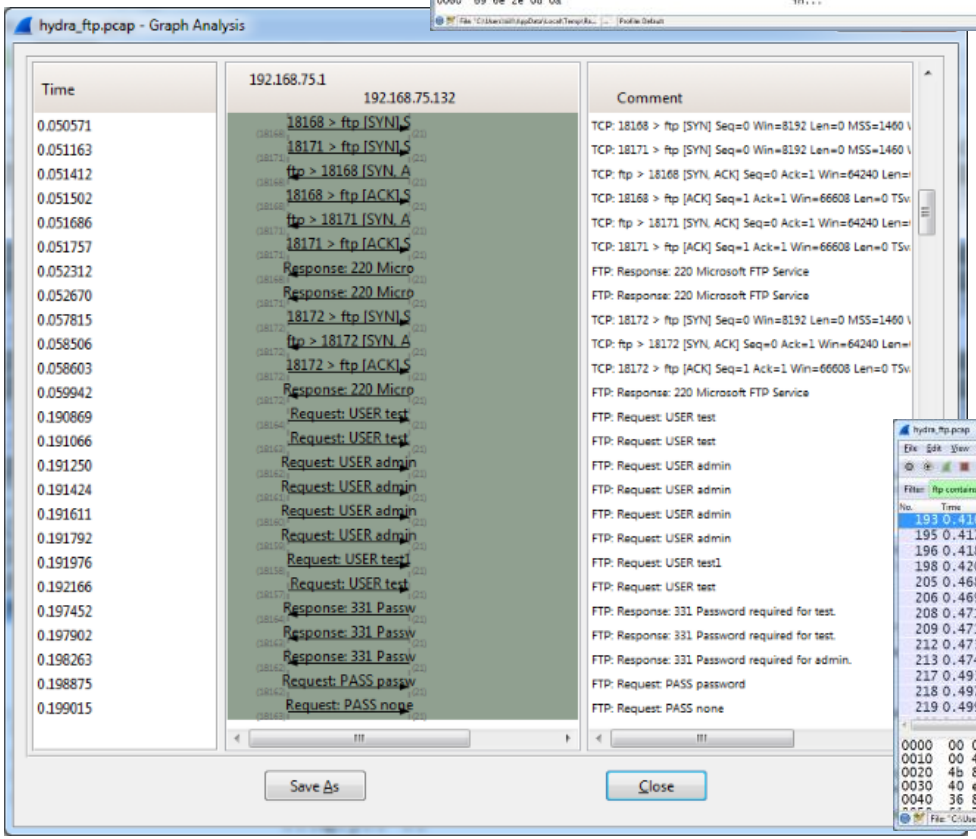


Correct login:

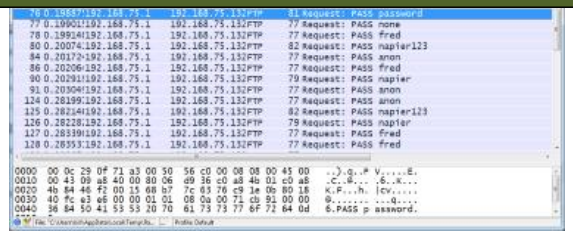
ftp.response.code==230

Incorrect login:

ftp.response.code==530

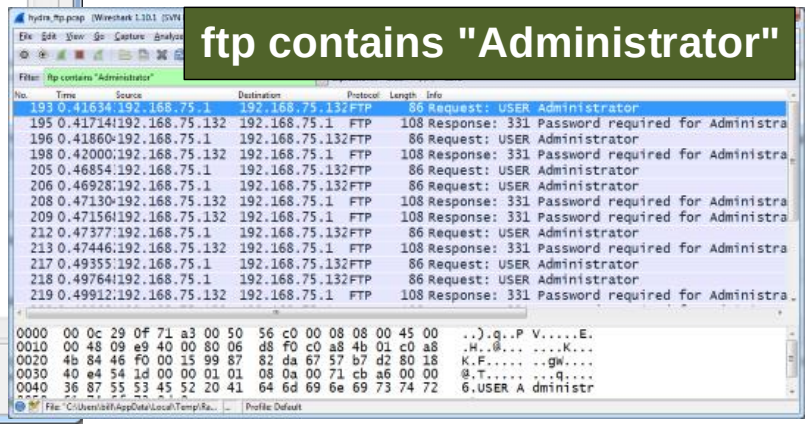


ftp contains "PASS"



"Administrator" search:

ftp contains "Administrator"

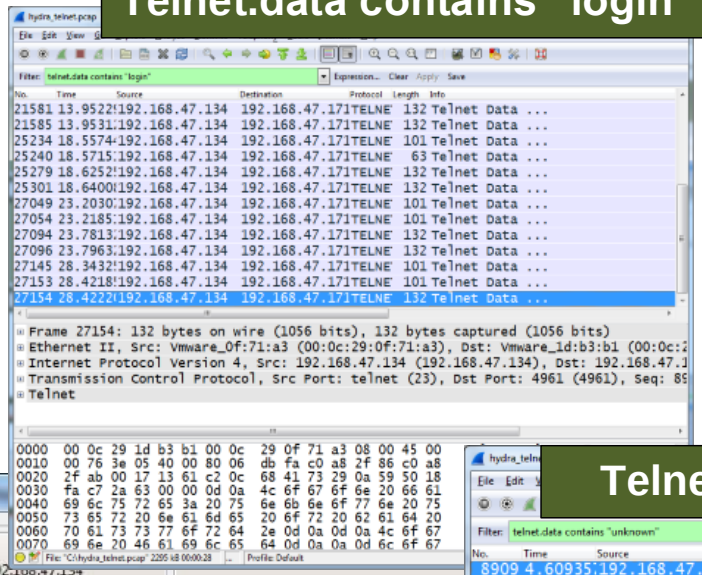


http://asecuritysite.com/log/hydra_ftp.zip

Author: Prof Bill Buchanan

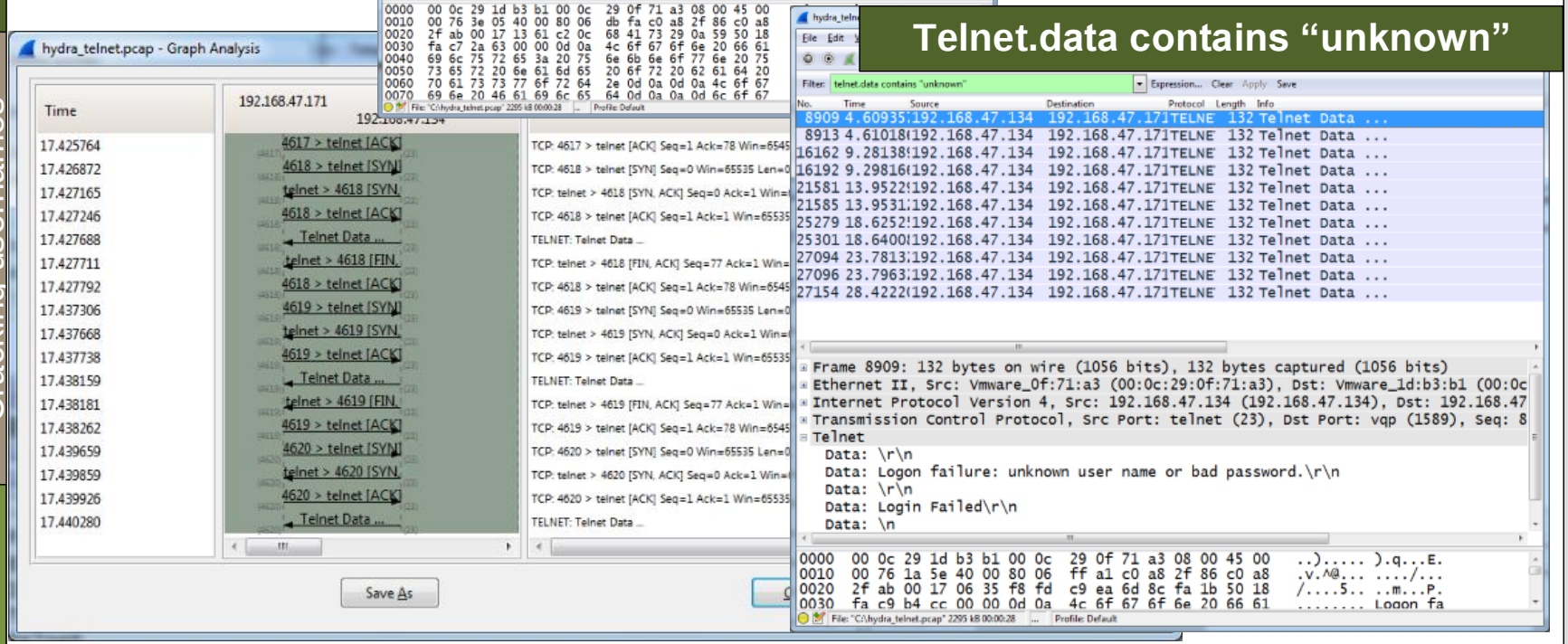
Hydra (FTP)

Telnet.data contains “login”



Bad Login:

Telnet.data contains “unknown”

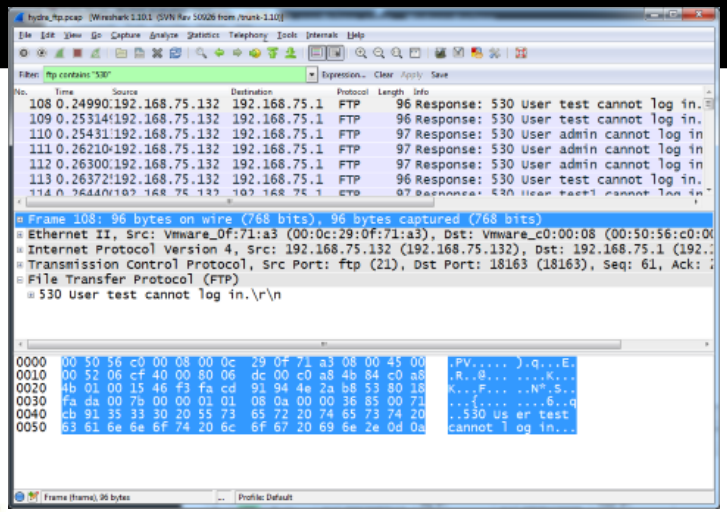


http://asecuritysite.com/log/hydra_telnet.zip

Author: Prof Bill Buchanan

C:\Snort\bin> type 1.rules
alert tcp any 21 -> any any (msg:"FTP Bad login"; content:"530 User "; nocase; flow:from_server,established; sid:491; rev:5;)

C:\Snort\bin> snort -i 1 -c 1.rules -l log



C:\hydra>hydra -L user.txt -P pass.txt 192.168.47.134 ftp
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2014-01-05 16:44:01
[DATA] 12 tasks, 1 server, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking service ftp on port 21
[STATUS] attack finished for 192.168.47.134 (waiting for children to finish)
[21][ftp] host: 192.168.47.134 login: administrator password: napier
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-01-05 16:44:02

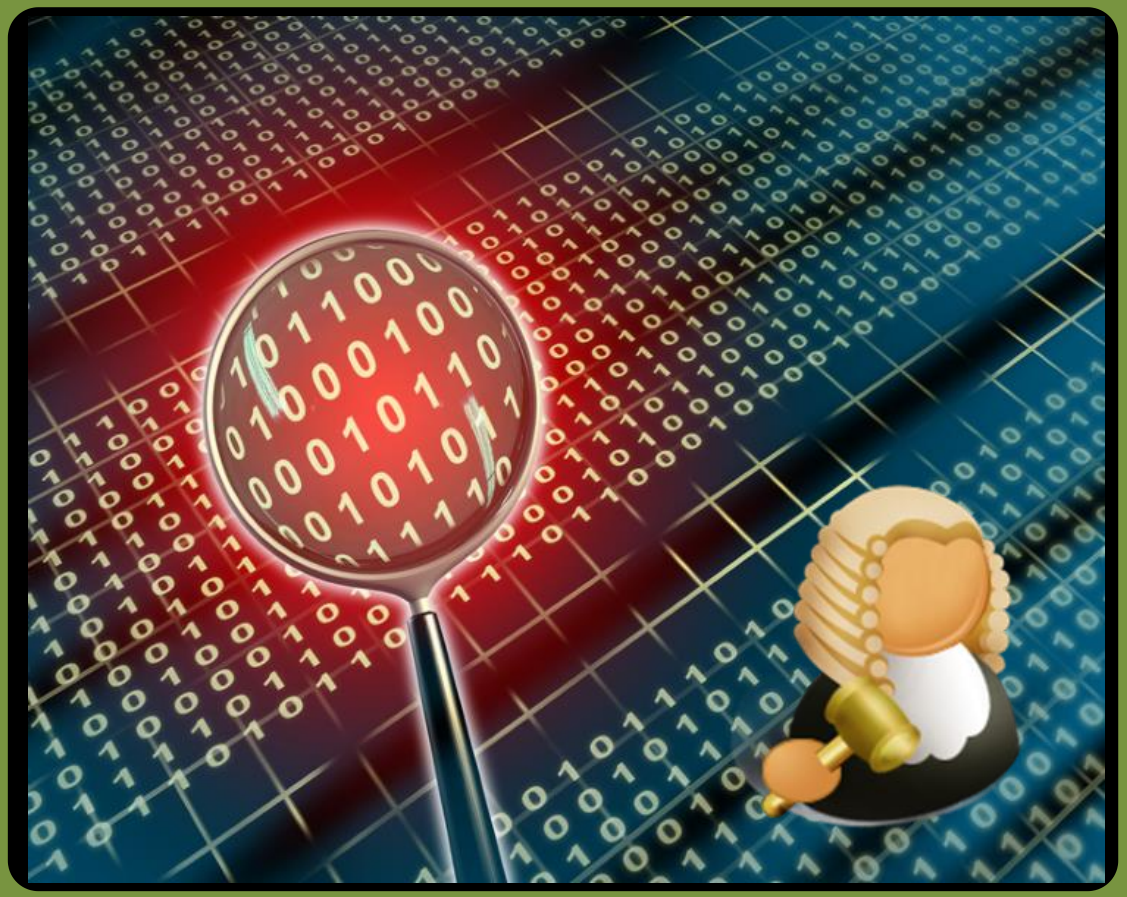
[**] [1:491:5] FTP Bad login [**]
[Priority: 0]
01/05-16:46:25.815069 192.168.47.134:21 -> 192.168.47.171:1230
TCP TTL:128 TOS:0x0 ID:26286 IpLen:20 DgmLen:79 DF
*****AP*** Seq: 0x6852C889 Ack: 0x9F128FC0 Win: 0xFACF TcpLen: 20**

[**] [1:491:5] FTP Bad login [**]
[Priority: 0]
01/05-16:46:25.815104 192.168.47.134:21 -> 192.168.47.171:1231
TCP TTL:128 TOS:0x0 ID:26287 IpLen:20 DgmLen:79 DF
*****AP*** Seq: 0x528728E2 Ack: 0x88B7039E Win: 0xFACD TcpLen: 20**

http://asecuritysite.com/log/hydra_ftp.zip

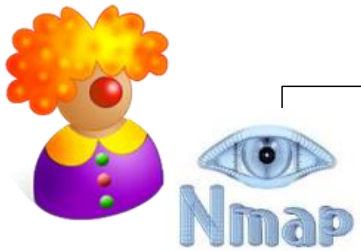
Author: Prof Bill Buchanan

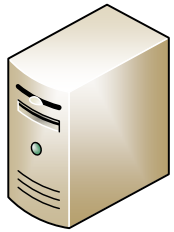
Advanced Network Forensics



Port Scan

Author: Prof Bill Buchanan





```
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given
ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
OS DETECTION:
  -O: Enable OS detection

C:\Documents and Settings\Administrator> nmap -sS 192.168.47.134
Host is up (0.00088s latency).
Not shown: 973 closed ports
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
..
5900/tcp open  vnc
8099/tcp open  unknown
MAC Address: 00:0C:29:0F:71:A3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 8.80 seconds
```

[SYN], Port 1

Port open

[SYN, ACK], Port 1

[ACK], Port 1

[SYN], Port 21

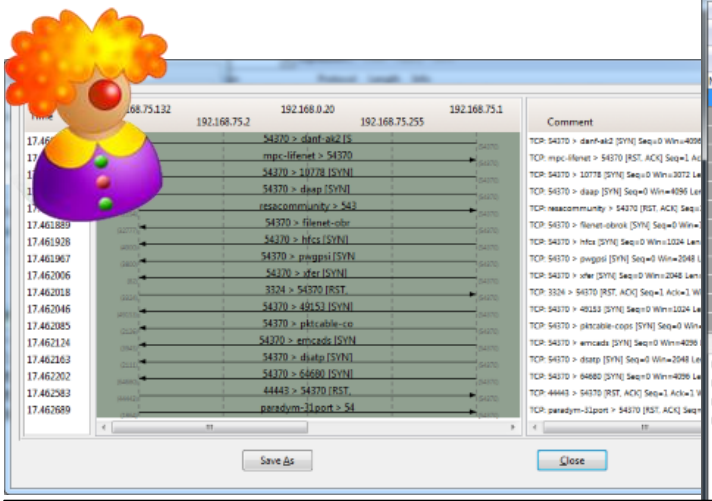
Port closed

[RST, ACK], Port 21

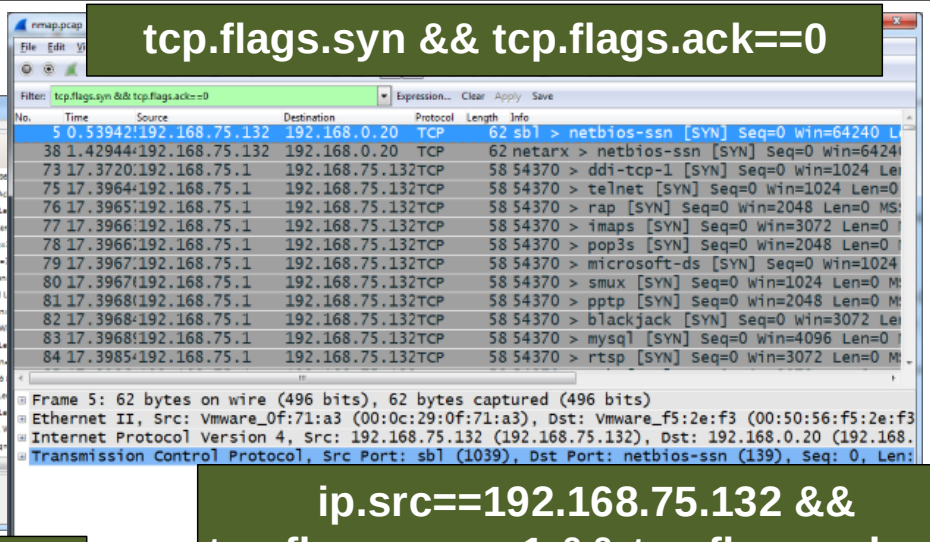
Author: Prof Bill Buchanan

Detecting Scanning

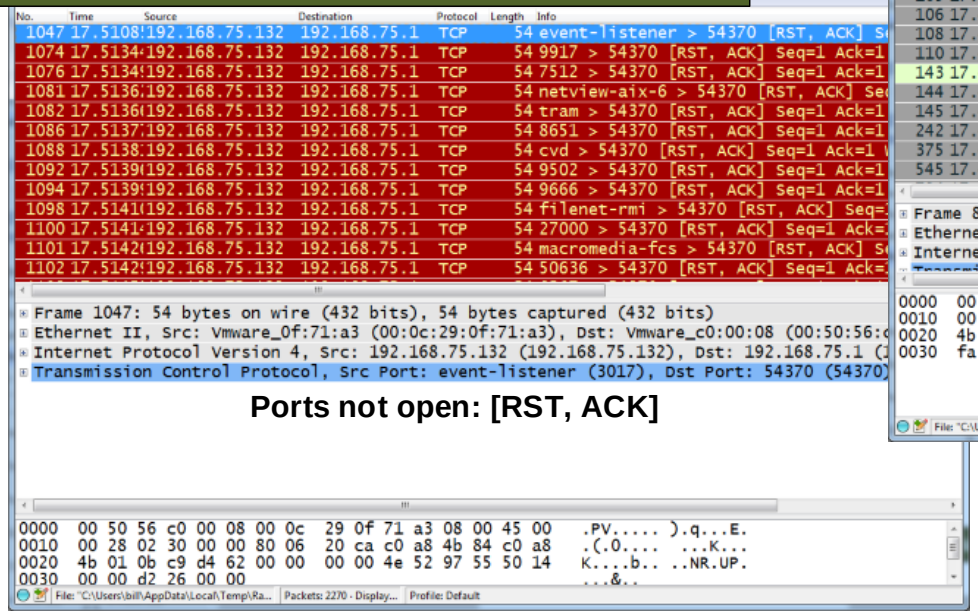
Adv Net For.



tcp.flags.syn && tcp.flags.ack==0

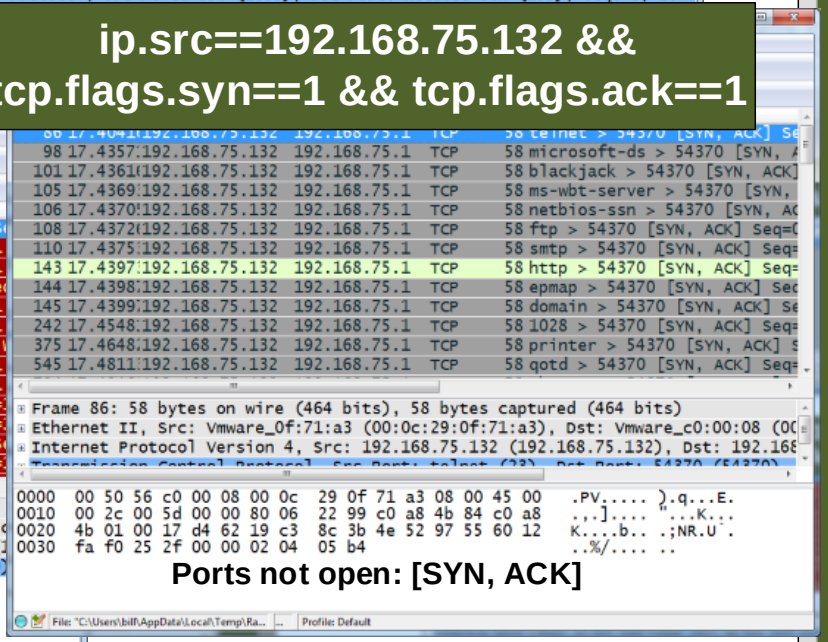


ip.src==192.168.75.132 && tcp.flags.reset && tcp.flags.ack



Ports not open: [RST, ACK]

ip.src==192.168.75.132 && tcp.flags.syn==1 && tcp.flags.ack==1

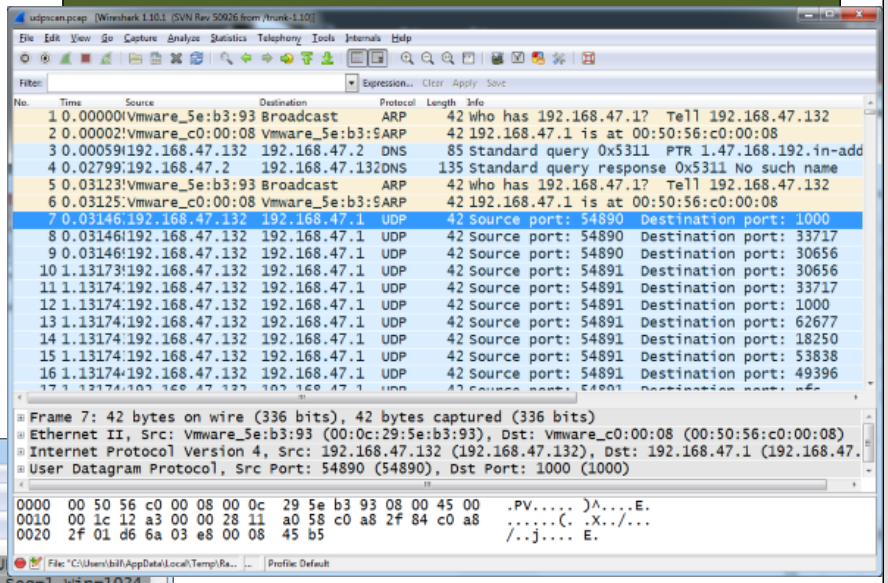


Ports not open: [SYN, ACK]

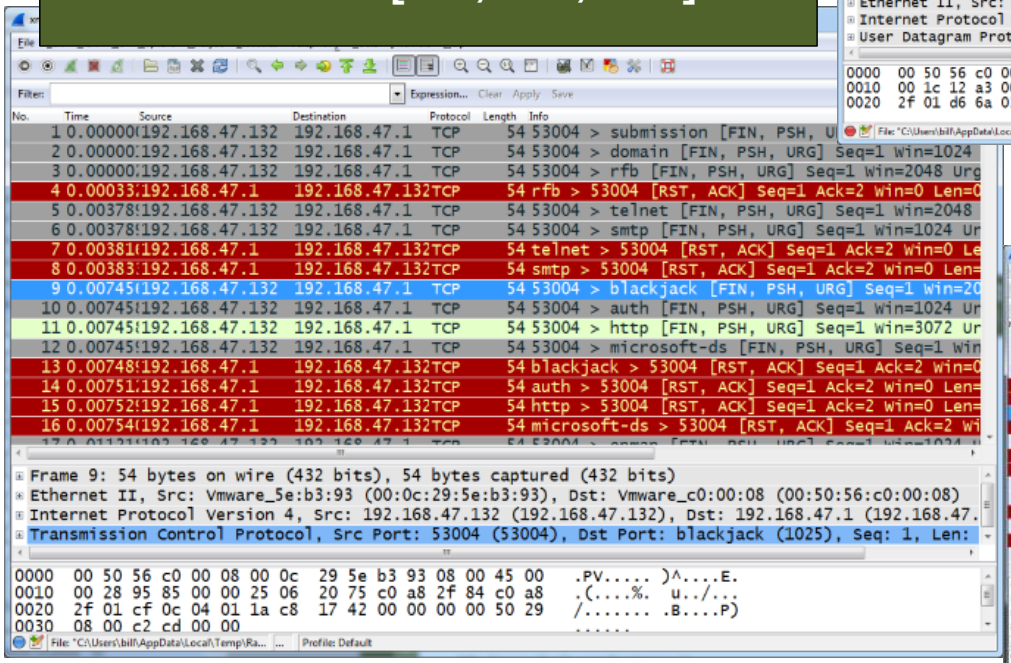
http://asecuritysite.com/log/nmap.zip

Author: Prof Bill Buchanan

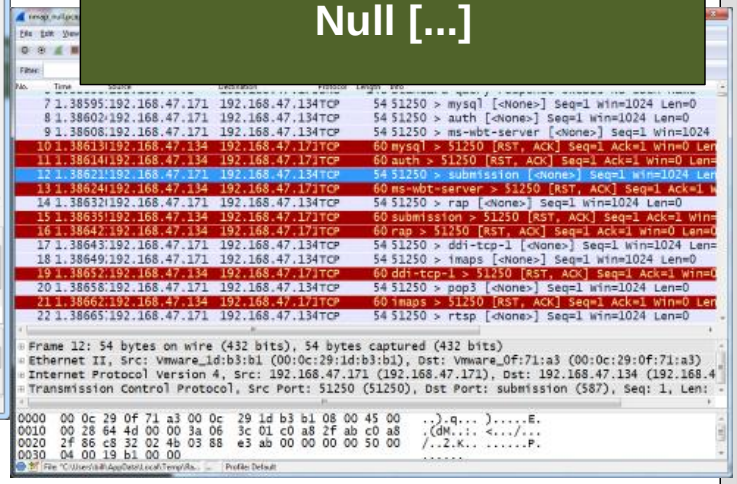
UDP Scan



Xmas Tree [FIN,PSH,URG]



Null [...]



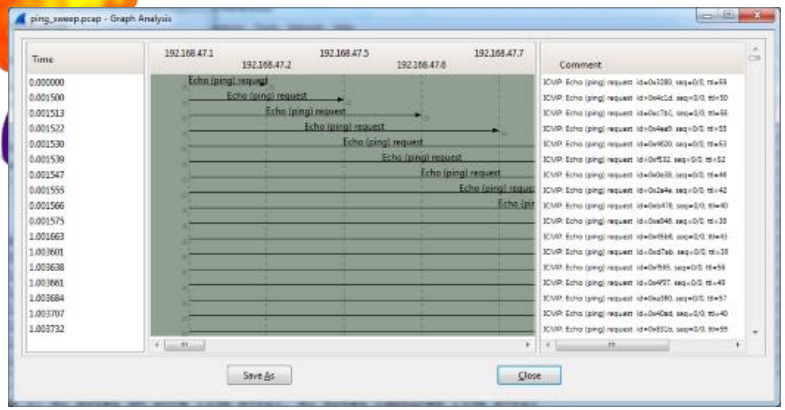
Detecting Scanning

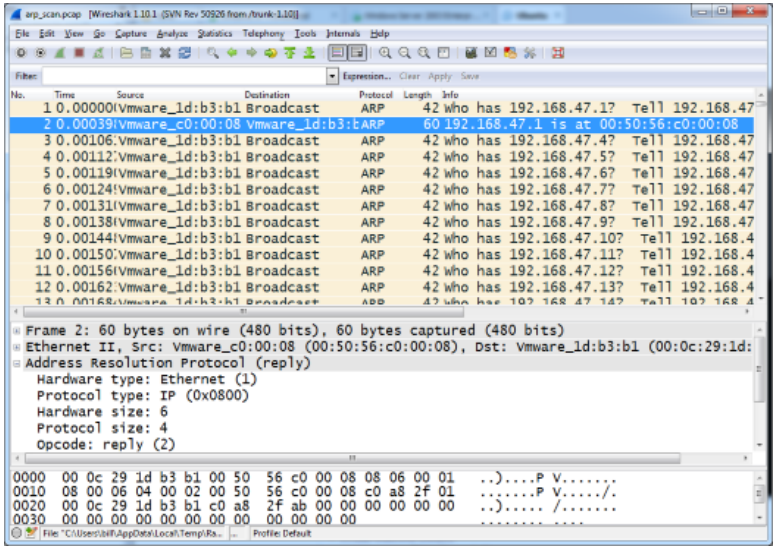
Adv Net For.

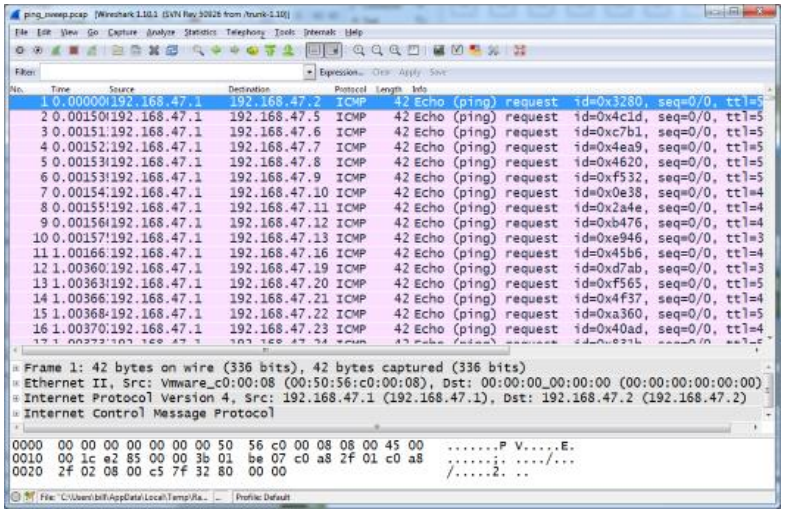
http://asecuritysite.com/log/nmap.zip

Author: Prof Bill Buchanan

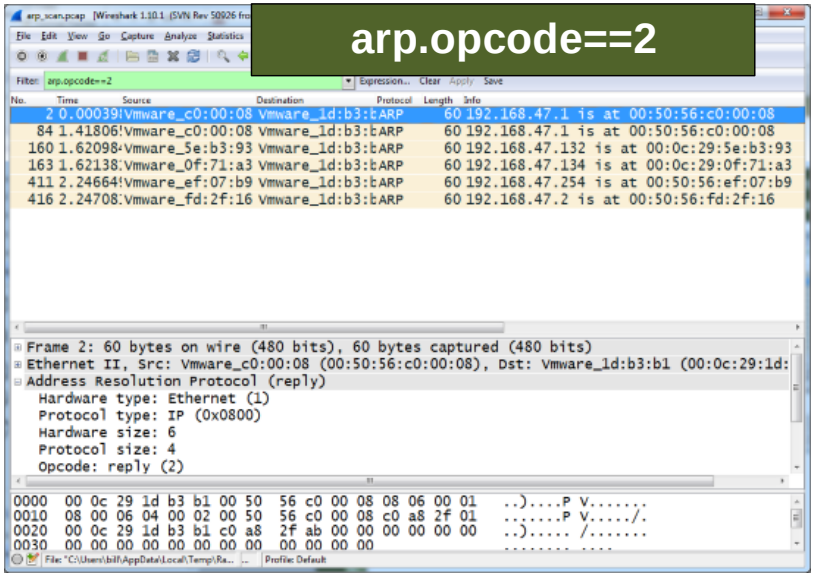
NMAP (Port Scanning)







http://asecuritysite.com/log/ping_sweep.zip



http://asecuritysite.com/log/arp_scan.zip

Author: Prof Bill Buchanan

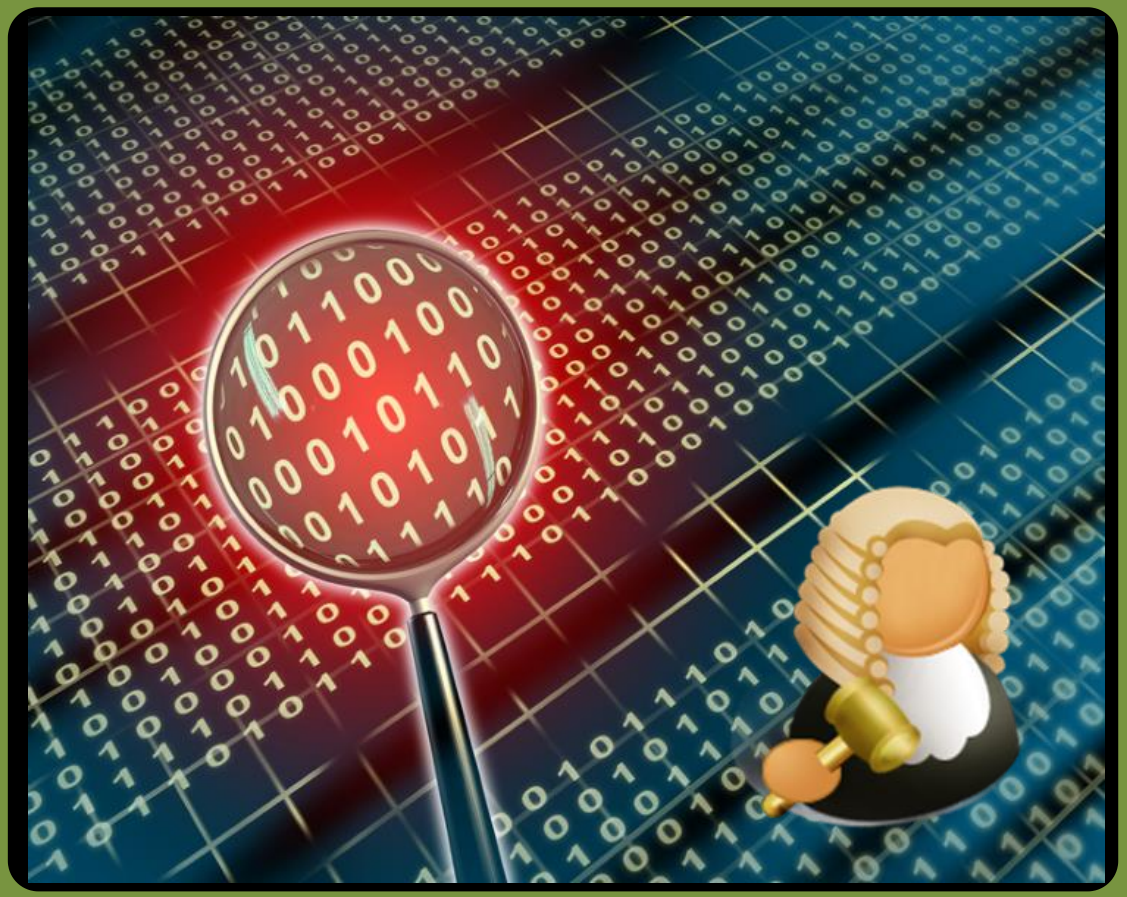
```
C:\Snort\bin>nmap 192.168.47.134

Starting Nmap 6.40 ( http://nmap.org ) at
2014-01-05 16:22 GMT Standard Time
Nmap scan report for 192.168.47.134
Host is up (0.000028s latency).
Not shown: 972 closed ports
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
...
5900/tcp open  vnc
8099/tcp open  unknown
MAC Address: 00:0C:29:0F:71:A3
(VMware)

Nmap done: 1 IP address (1 host up)
scanned in 1.78 seconds
```

```
C:\snort\bin> type 1.rules
preprocessor sfportscan:\
        proto { all } \
        scan_type { all } \
        sense_level { high } \
         logfile { portscan.log }

C:\Snort\bin>snort -W

Index   Physical Address        IP Address      Device Name
Description
-----   ----------------        ----------      -----------     -----------
    1   00:0C:29:0F:71:A3       192.168.47.134  \Device\
NPF_{BEB6E6E9-8D1A-463E-
B650-4C388AEE925D}      Intel(R) PRO/1000 MT Network Connection

C:\Snort\bin>snort -i 1 -c 1.rules -l log
```


```
Time: 01/05-16:22:35.960159
event_ref: 0
192.168.47.171 -> 192.168.47.134 (portscan) TCP Filtered Portscan
Priority Count: 0
Connection Count: 200
IP Count: 1
Scanner IP Range: 192.168.47.171:192.168.47.171
Port/Proto Count: 200
Port/Proto Range: 6:60443
```

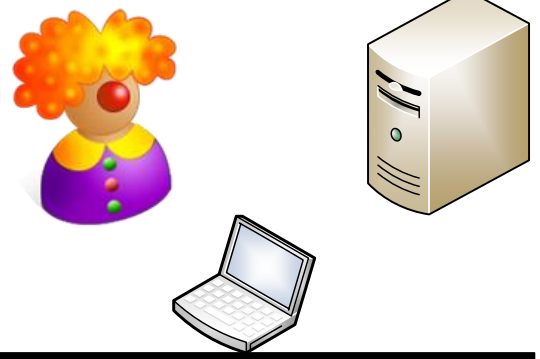
Author: Prof Bill Buchanan

Advanced Network Forensics

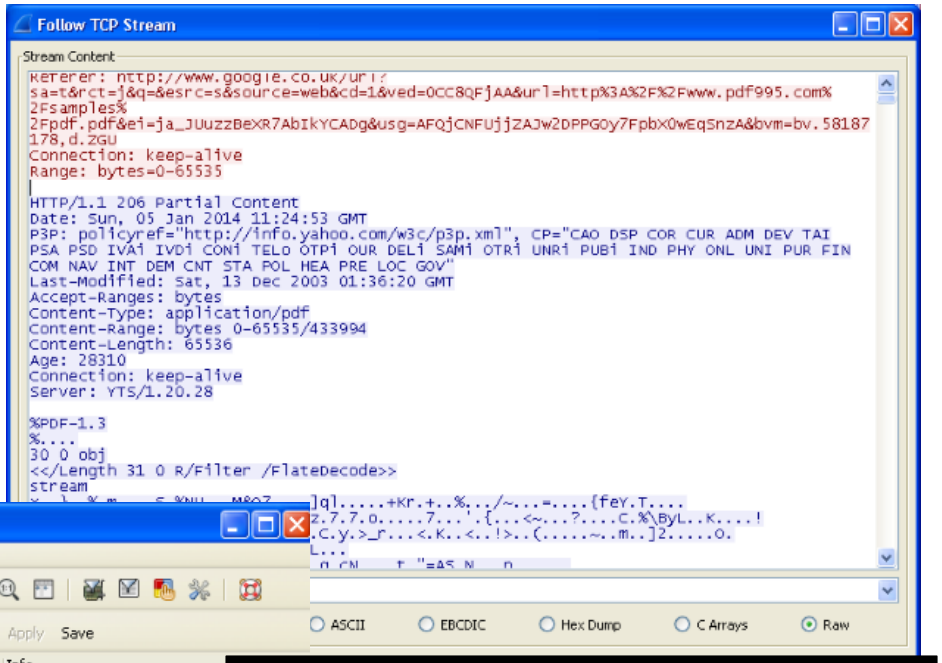


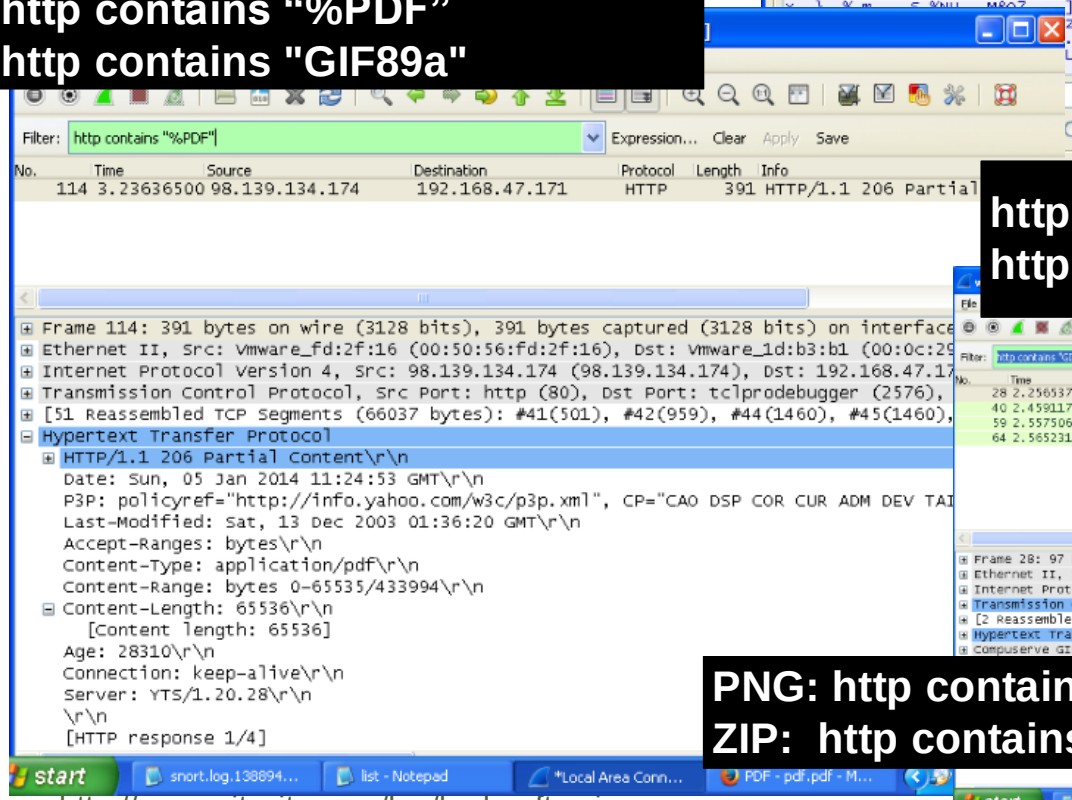
Signature Detection

Author: Prof Bill Buchanan

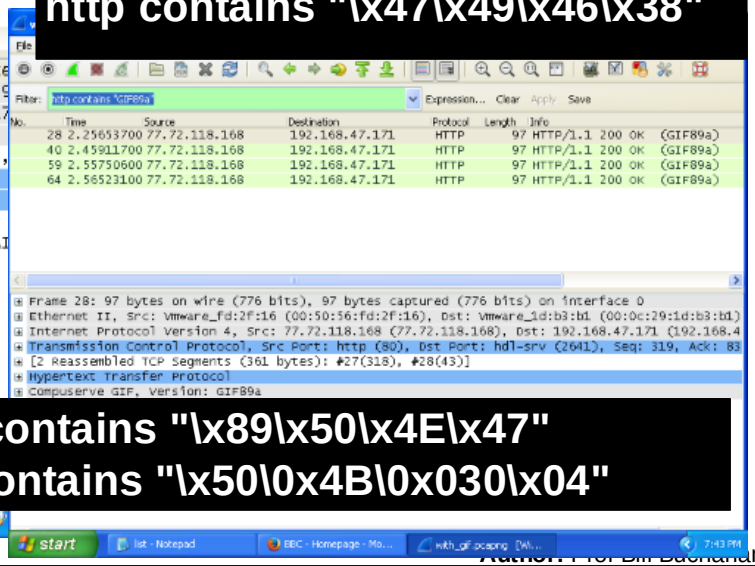


http contains "\x25\x50\x44\x46"
http contains "%PDF"
http contains "GIF89a"



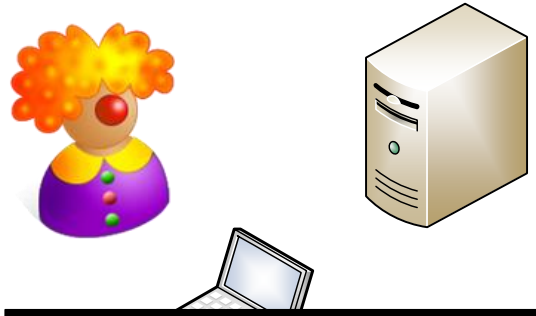


http contains "GIF89a"
http contains "\x47\x49\x46\x38"



PNG: http contains "\x89\x50\x4E\x47"
ZIP: http contains "\x50\0x4B\0x030\x04"

http://asecuritysite.com/log/hydra_ftp.zip

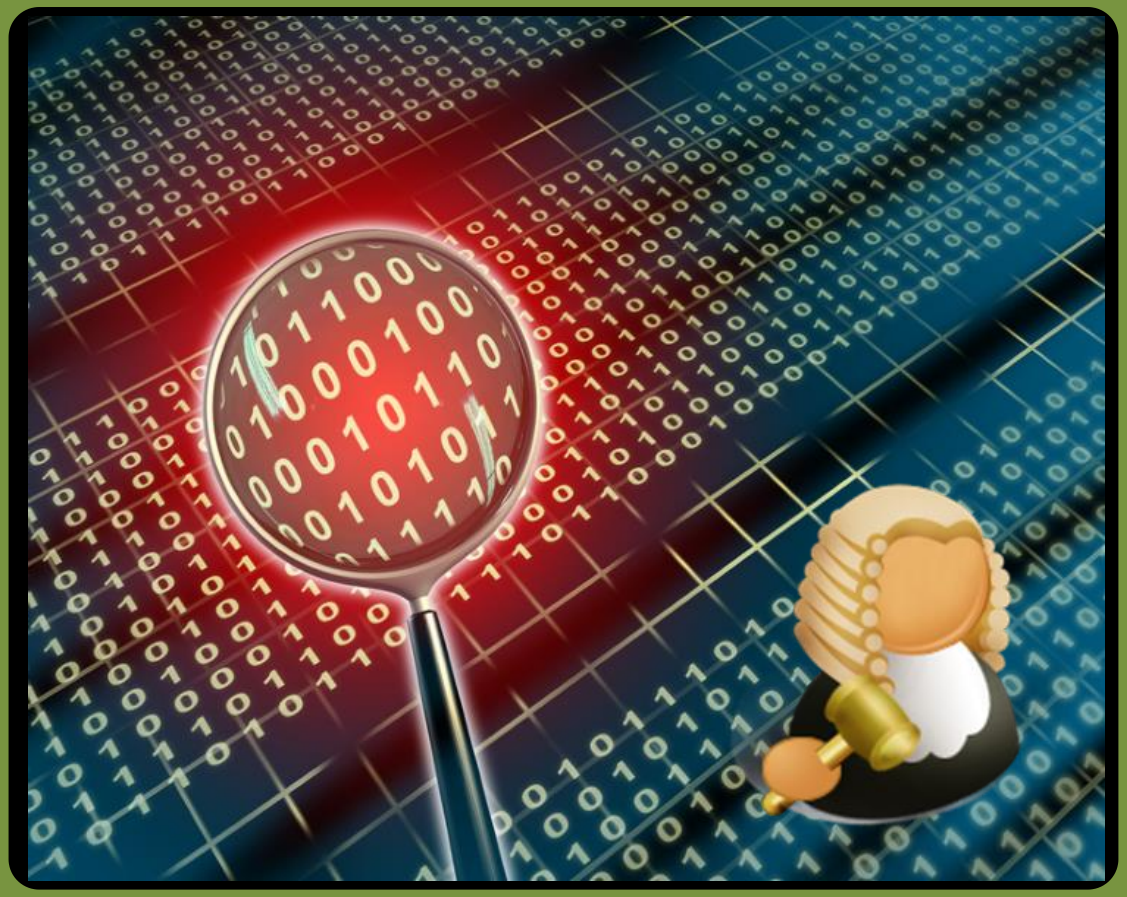


```
alert tcp any any -> any any (content:"GIF89a"; msg:"GIF";sid:10000)
alert tcp any any -> any any (content:"%PDF"; msg:"PDF";sid:10001)
alert tcp any any -> any any (content:"|89 50 4E 47|"; msg:"PNG";sid:10002)
alert tcp any any -> any any (content:"|50 4B 03 04|"; msg:"ZIP";sid:10003)
```

```
[**] [1:10001:0] PDF [**]
[Priority: 0]
01/05-20:08:06.177354 61.67.219.91:80 -> 192.168.47.171:2700
TCP TTL:128 TOS:0x0 ID:62294 IpLen:20 DgmLen:1238
***AP*** Seq: 0x6BFA2147  Ack: 0xC3534C66  Win: 0xFAF0  TcpLen: 20
```

Author: Prof Bill Buchanan

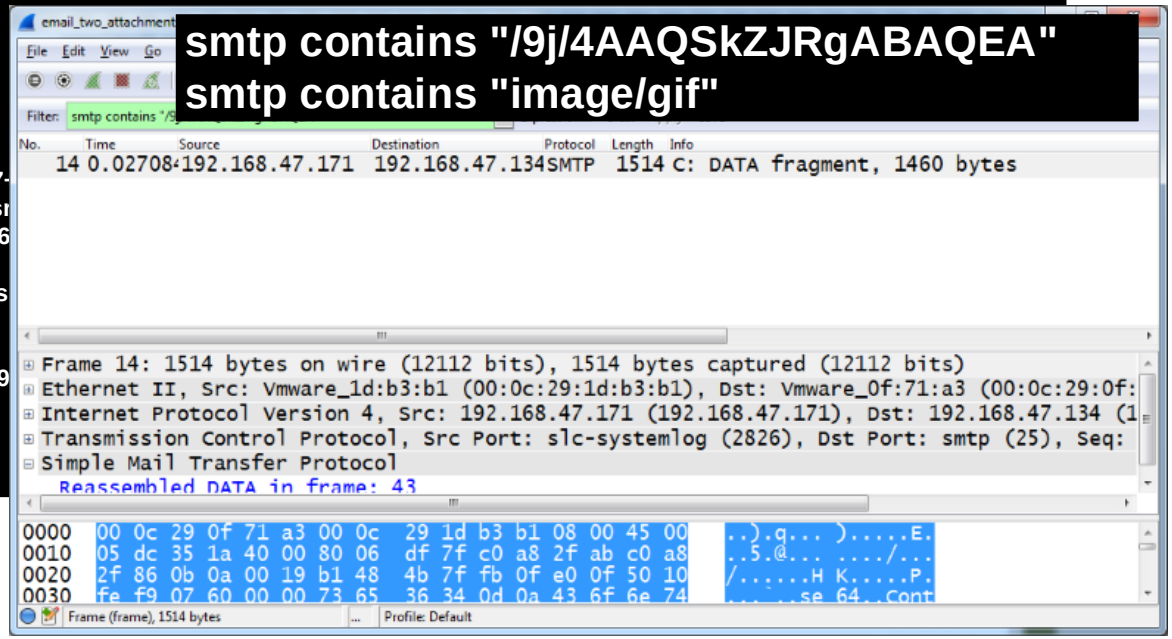
Advanced Network Forensics



Converted Formats

Author: Prof Bill Buchanan

```
... Email message

------=_NextPart_001_0005_01CF0A5E.E9FFC210--

------=_NextPart_000_0004_01CF0A5E.E9FFC210
Content-Type: image/jpeg;
.name="ehealth.jpg"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
.filename="ehealth.jpg"

/9j/4AAQSkZJRgABAQEASABIAAD/2wBDAAICAgICAgICAgICAwMDAgIDAwQDAwMDAwQFBAQE
BAQEBQUGBgcGBgUHBwgIBwcKCgoKCgoKCgoKCgr/2wBDAQMDAwQDBAcFBQcLCQcJCwwLCwsL
DAwKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgr/wAARCABeALQDAREA
..
kI0dL8lyLFHb6Xkc9uW9YNVUGsjDPW0WNX1DboMiUr2Fby/3ypsrKrsiKTjhKpdIRLnSEHSEHSEH
SEHSEHSEHSEHSEHSEHSEf//Z

------=_NextPart_000_0004_01CF0A5E.E9FFC210
Content-Type: image/gif;
.name="cat01_with_hidden_text.gif"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
.filename="cat01_with_hidden_text.gif"

R0lGODlhZABVAOYAAP////f39vH08u7u7-
bGxvwNHGhMC/vb27uLi2tbWzrqqxtqusr
lpiLZpCHgoODg3qEisteXvtlSIJ8c3x6flV6
...
AMb5Ca3QER7Rn/75nwDqn8bZGwFAEs
oR66CIEAADs=

------=_NextPart_000_0004_01CF0A5E.E9

.
```



Author: Prof Bill Buchanan

```
... Email message

------=_NextPart_000_0004_01CF0A5E.E9FFC210
Content-Type: image/jpeg;
.name="ehealth.jpg"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
.filename="ehealth.jpg"

/9j/4AAQSkZJRgABAQEASABIAAD/2wBDAAICAgICAgICAgICAwMDAgIDAwQDAwMDAwQFBAQE
BAQEBQUGBgcGBgUHBwgIBwcKCgoKCgoKCgoKCgoKCgr/2wBDAQMDAwQDBAcFBQcLCQcJCwwLCwsL
DAwKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgoKCgr/wAARCABeALQDAREA
..
kl0dL8lyLFHb6Xkc9uW9YNVUGsjDPW0WNX1DboMiUr2Fby/3ypsrKrsiKTjhKpdIRLnSEHSEHSEH
SEHSEHSEHSEHSEHSEHSEf//Z

------=_NextPart_000_0004_01CF0A5E.E9FFC210--

.
```

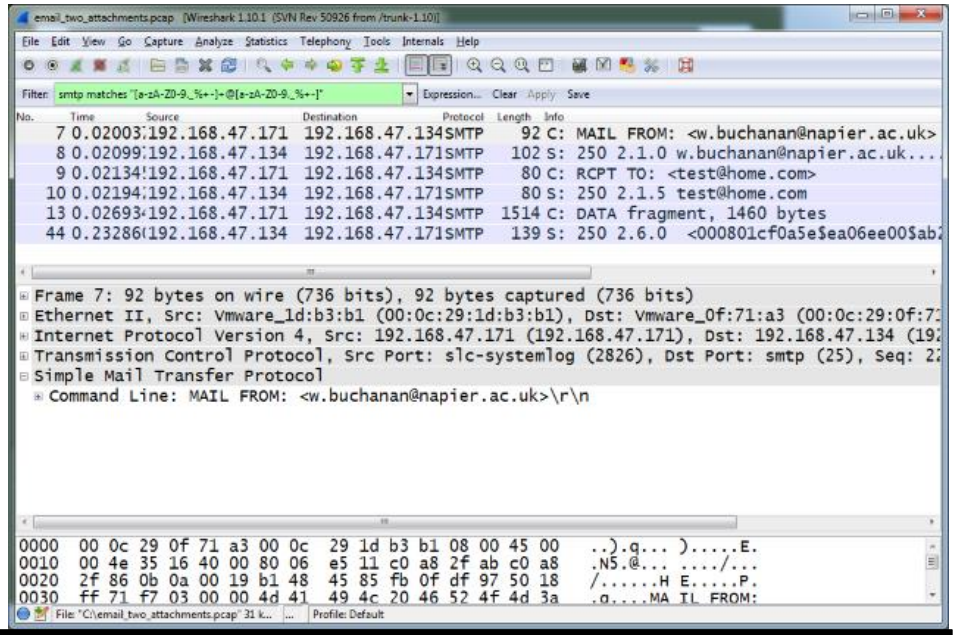
```
alert tcp any any -> any 25 (content:"/9j/4AAQSkZJRgABAQEA"; msg:"Cat in
email";sid:10005)
alert tcp any any -> any 25 (content:"image/gif"; msg:"GIF in
email";sid:10006)
```


```
[**] [1:10006:0] GIF in email [**]
[Priority: 0]
01/05-22:04:00.115020 192.168.47.171:2832 -> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:13973 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x56ECBE11  Ack: 0xBB60A76D  Win: 0xFEF9  TcpLen: 20

[**] [1:10005:0] Cat in email [**]
[Priority: 0]
01/05-22:04:00.115371 192.168.47.171:2832 -> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:13977 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x56ECD4E1  Ack: 0xBB60A76D  Win: 0xFEF9  TcpLen: 2
```

Author: Prof Bill Buchanan

```
alert tcp any any <> any 25 (pcre:"/[a-zA-Z0-9._%+-]+@[a-zA-Z0-9._%+-]/"; \
msg:"Email in message";sid:9000000;rev:1;)
```

```
[**] [1:9000000:1] Email in message [**]
[Priority: 0]
01/05-21:41:38.648260 192.168.47.171:2826 -> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:13590 IpLen:20 DgmLen:78 DF
***AP*** Seq: 0xB1484585  Ack: 0xFB0FDF97  Win: 0xFF71  TcpLen: 20

[**] [1:9000000:1] Email in message [**]
[Priority: 0]
01/05-21:41:38.649220 192.168.47.134:25 -> 192.168.47.171:2826
TCP TTL:128 TOS:0x0 ID:2017 IpLen:20 DgmLen:88 DF
***AP*** Seq: 0xFB0FDF97  Ack: 0xB14845AB  Win: 0xFAB5  TcpLen: 20

[**] [1:9000000:1] Email in message [**]
[Priority: 0]
01/05-21:41:38.649568 192.168.47.171:2826 -> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:13591 IpLen:20 DgmLen:66 DF
***AP*** Seq: 0xB14845AB  Ack: 0xFB0FDFC7  Win: 0xFF41  TcpLen: 20

[**] [1:9000000:1] Email in message [**]
[Priority: 0]
01/05-21:41:38.650165 192.168.47.134:25 -> 192.168.47.171:2826
TCP TTL:128 TOS:0x0 ID:2018 IpLen:20 DgmLen:66 DF
***AP*** Seq: 0xFB0FDFC7  Ack: 0xB14845C5  Win: 0xFA9B  TcpLen: 20

[**] [1:9000000:1] Email in message [**]
[Priority: 0]
01/05-21:41:38.655157 192.168.47.171:2826 -> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:13593 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xB14845CB  Ack: 0xFB0FE00F  Win: 0xFEF9  TcpLen: 20

[**] [1:9000000:1] Email in message [**]
[Priority: 0]
01/05-21:41:38.861083 192.168.47.134:25 -> 192.168.47.171:2826
TCP TTL:128 TOS:0x0 ID:2030 IpLen:20 DgmLen:125 DF
***AP*** Seq: 0xFB0FE00F  Ack: 0xB148AE2E  Win: 0xFAEB  TcpLen: 20
```

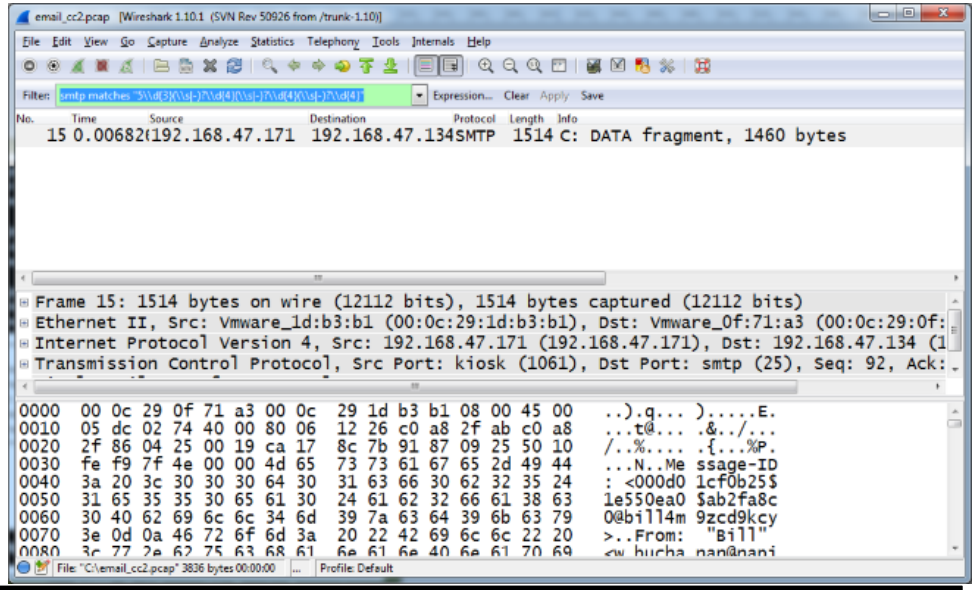



```
smtp matches "[a-zA-Z0-9._%+-]+@[a-zA-Z0-9._%+-]"
```

Author: Prof Bill Buchanan

```
alert tcp any any <> any any (pcre:"/5\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/"; \
      msg:"MasterCard number detected in clear
text";content:"number";nocase;sid:9000003;rev:1;)

alert tcp any any <> any any (pcre:"/3\d{3}(\s|-)?\d{6}(\s|-)?\d{5}/"; \
      msg:"American Express number detected in clear
text";content:"number";nocase;sid:9000004;rev:1;)

alert tcp any any <> any any (pcre:"/4\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/"; \
      msg:"Visa number detected in clear
text";content:"number";nocase;sid:9000005;rev:1;)
```

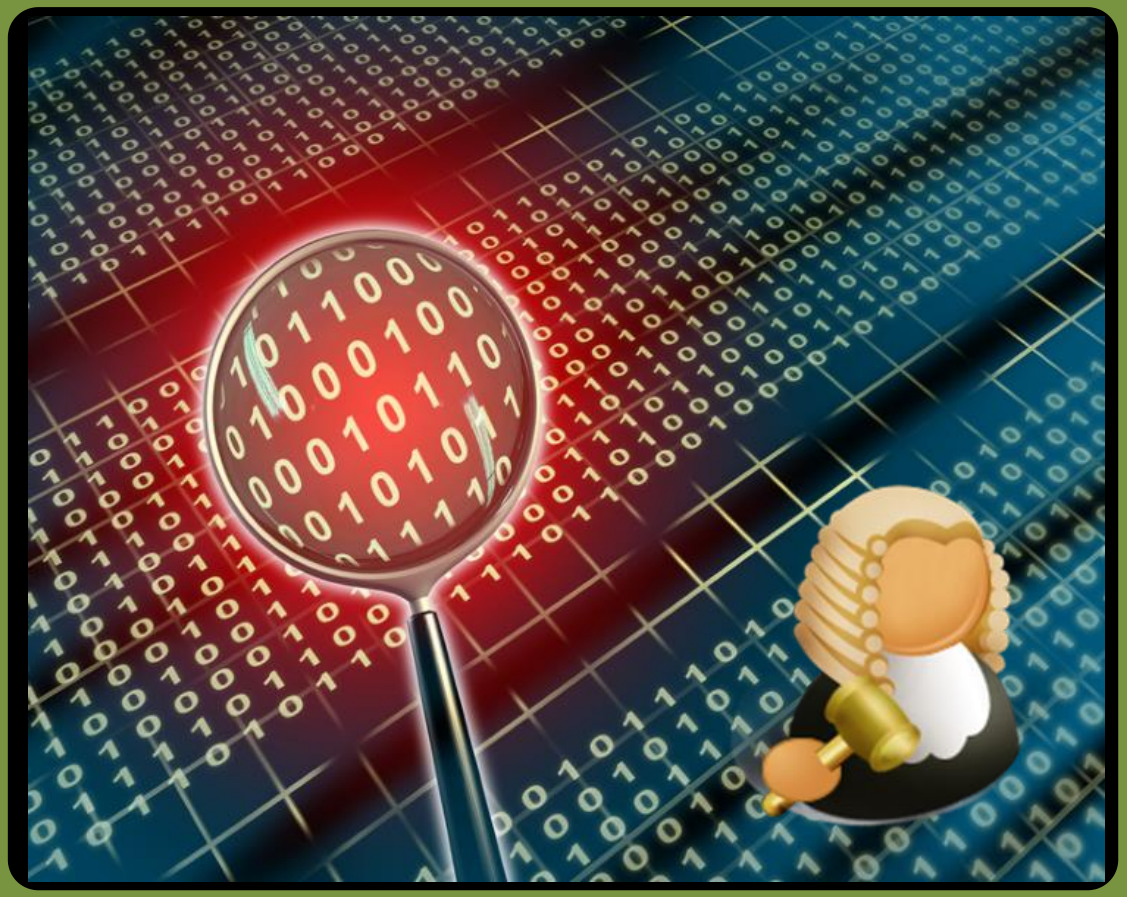
```
[**] [1:9000005:1] Visa number detected in clear text [**]
[Priority: 0]
01/06-21:20:26.755456 192.168.47.171:1061 -> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:628 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xCA178C7B  Ack: 0x91870925  Win: 0xFEF9  TcpLen: 20

[**] [1:9000003:1] MasterCard number detected in clear text [**]
[Priority: 0]
01/06-21:20:26.755456 192.168.47.171:1061 -> 192.168.47.134:25
TCP TTL:128 TOS:0x0 ID:628 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xCA178C7B  Ack: 0x91870925  Win: 0xFEF9  TcpLen: 20
```




```
smtp matches "5\\d{3}(\\s|-)?\\d{4}(\\s|-)?\\d{4}(\\s|-)?\\d{4}"
```

Author: Prof Bill Buchanan

Advanced Network Forensics

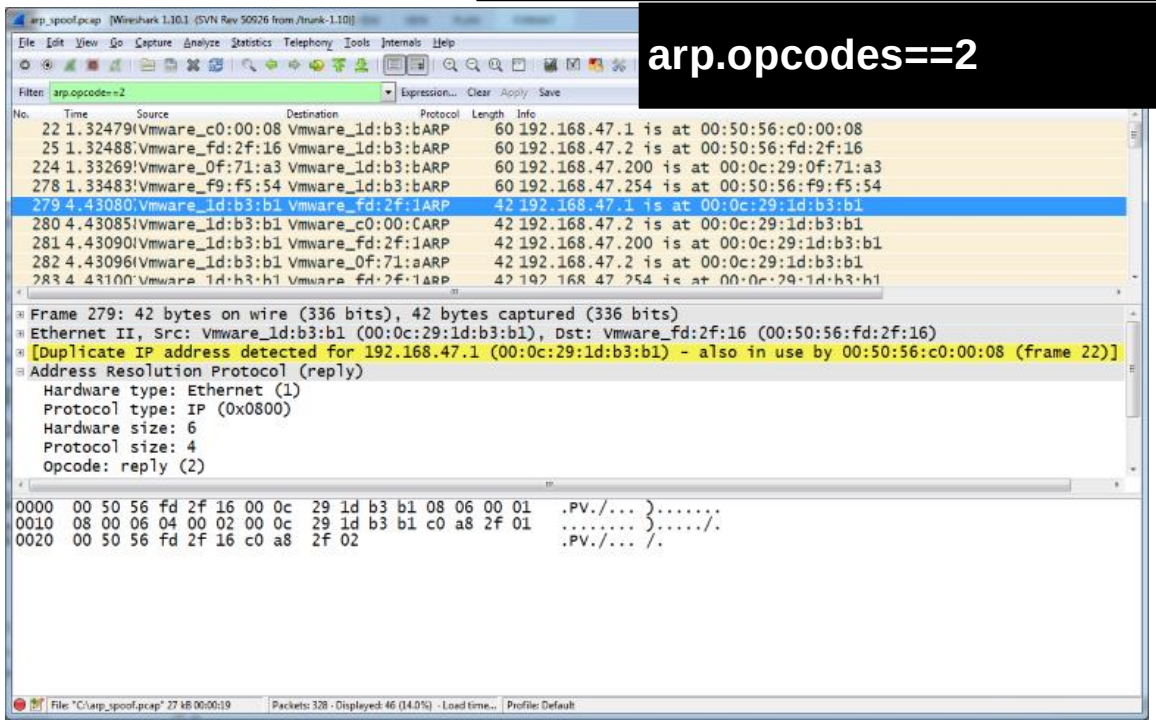


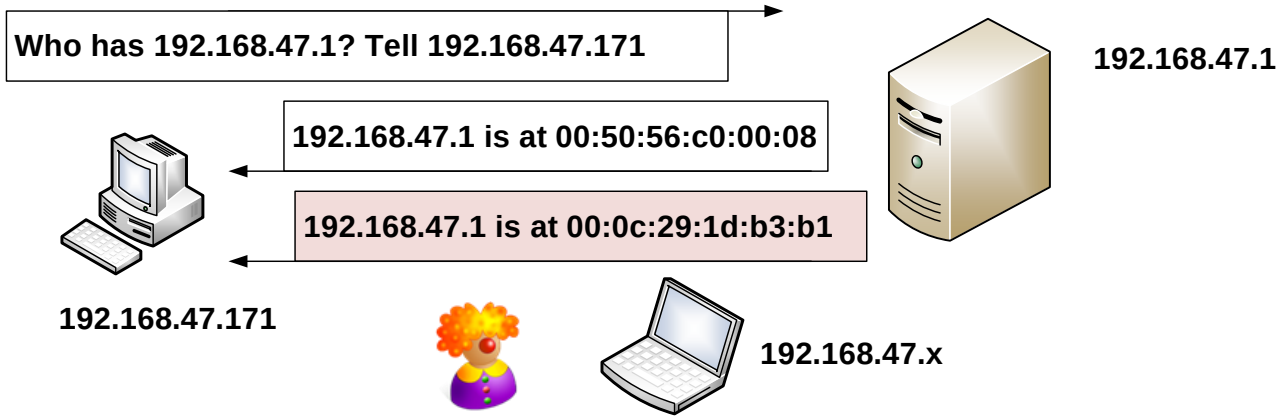
ARP Spoofing

Author: Prof Bill Buchanan

```
preprocessor arpspoof
preprocessor arpspoof_detect_host: 192.168.47.200 00:0C:29:0F:71:A3
```

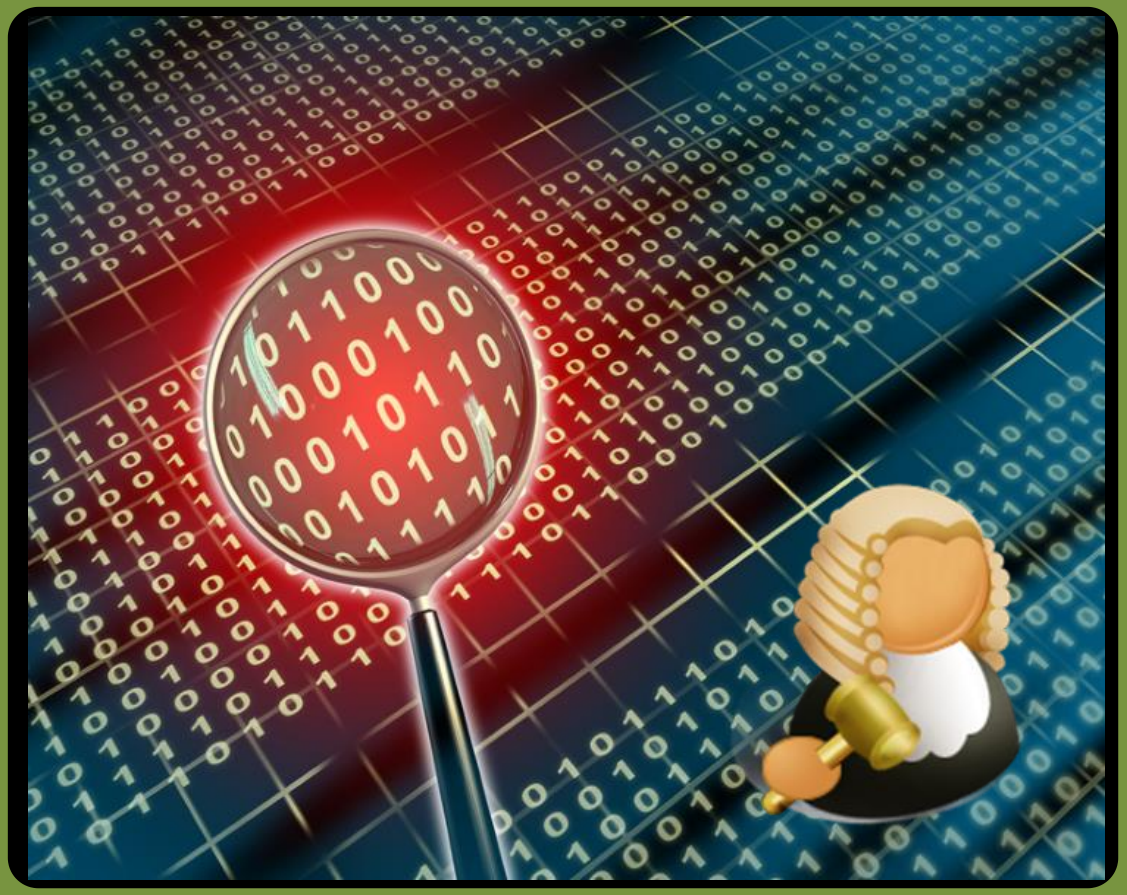
arp.opcodes==2





Author: Prof Bill Buchanan

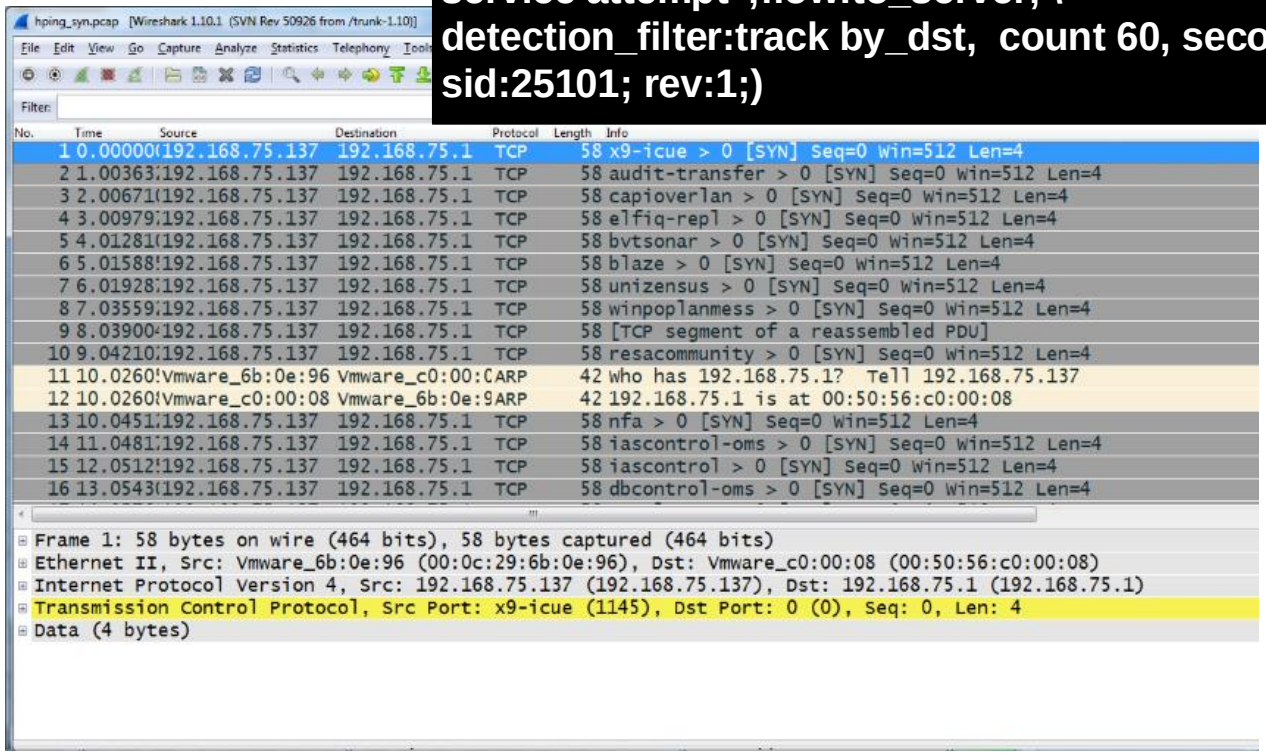
Advanced Network Forensics

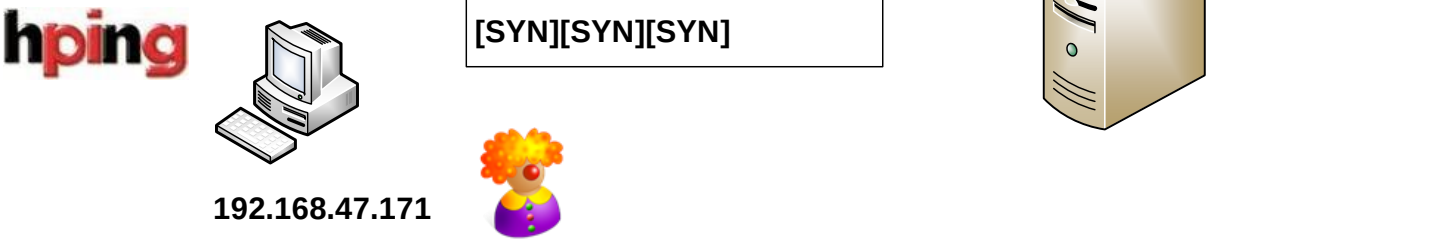


DDoS Detection

Author: Prof Bill Buchanan

```
alert tcp any any -> any 80 (msg:"DOS flood denial of
service attempt";flow:to_server; \
detection_filter:track by_dst,  count 60, seconds 60; \
sid:25101; rev:1;)
```





Author: Prof Bill Buchanan

Advanced Network Forensics

- User/Password Crack.
- Port Scan.
- Signature Detection.
- Converted Formats.
- ARP Spoofing.
- DDoS Detection.

Author: Prof Bill Buchanan