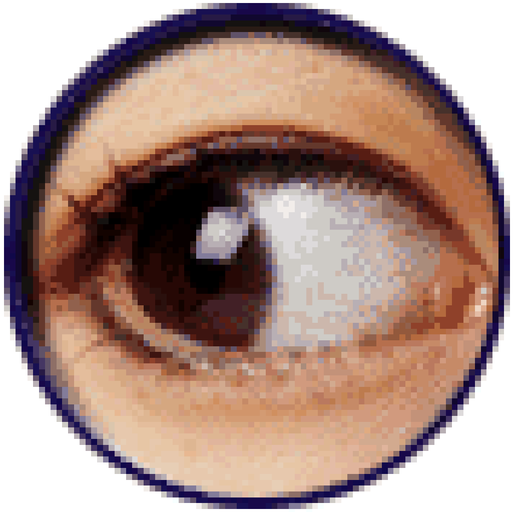
Corporate Network Spying



Andrew Whitaker

Director of Enterprise InfoSec

InfoSec Academy / Training Camp

http://www.infosecacademy.com / http://www.trainingcamp.com

TRAININGCAMP

Accelerated Learning. Education Evolved.

Who is this guy?

- Director of security course offerings for InfoSec Academy (division of Training Camp)
- Teaches ethical hacking / pentesting courses
- Co-author of Penetration Testing and Network Defense (Cisco Press, 2005)
- Author of other books/articles relating to security / networking
- Pentester of numerous financial and healthcare institutions
- M.Sc., Computer Science; CISSP, CEH, CCSP, CCNP, CCNA, CCDA, MCSE, CNE, A+, Network+, Security+, CTP, et al.

Training Camp

- InfoSec Academy division is world leader in teaching information security
  - Authorized CISSP
  - Certified Ethical Hacker
  - Licensed Penetration Tester
  - Sarbanes Oxley
  - HIPAA Compliance Training
  - Certified Information Systems Auditor (CISA)
  - Much, much more…

TRAININGCAMP
Accelerated Learning. Education Evolved.

What this is / What this is not

- What this is
  - Training on corporate network spying
  - Designed for those with beginner to intermediate skills
- What this is not
  - Discussion of hot new exploit (which may only be theoritical or work in a lab environment)
  - An overly technical discussion that only 1% of the techie world can understand

Agenda

- What the heck is this network spying thing?
- Who does it?
- Legal cases (to scare the begeezes out of ya)
- How to get past those darn switches
- General tools of the trade: Windump / TCPdump, Ethereal
- Analyzing common protocols
  - FTP, MSN IM, Web, SMTP/POP
- Demos to make you druel

What is Network Spying?

- Wiretapping
- Targeted packet capturing

Who Spies on Networks?

- Legitimate: Law enforcement
  - FBI
  - NSA
- Legitimate: Corporations with consent
  - Admins
  - Your boss
- Illegitimate: The "bad" guys
  - Hacker hobbyists
  - Corporate espionage

Who Spies on Networks?

- Law Enforcement
  - Patent #5,937,422 "Semantic Forests"
    - NSA solution
    - Captures voice conversation
    - Automatic speech transcription
  - Carnivore
    - Abandoned in 2005
    - Part of DragonWare suite
      - Carnivore – packet capturing
      - Packeteer – reassembles packets
      - Coolminer – searching captured packets

Who Spies on Networks?

- Corporations
  - PC Magazine reported 77% of companies spy on employees
  - Typically e-mail and web surfing
  - Justifications:
    - To ensure employee productivity
    - To ensure company is void of illegal activity
    - To protect trade secrets

Who Spies on Networks?

- Hacker hobbyists
  - Hey, look Ma, a wireless network!
- Corporate espionage
  - Tech companies especially at risk
  - Example: Oracle & Microsoft

Legal and Ethical Considerations

- 4th Amendment
- 1994 Communications Assistance for Law Enforcement
- Federal Electronic Communications Privacy Act (18 U.S.C. § 2511)
- PATRIOT Act

Cases

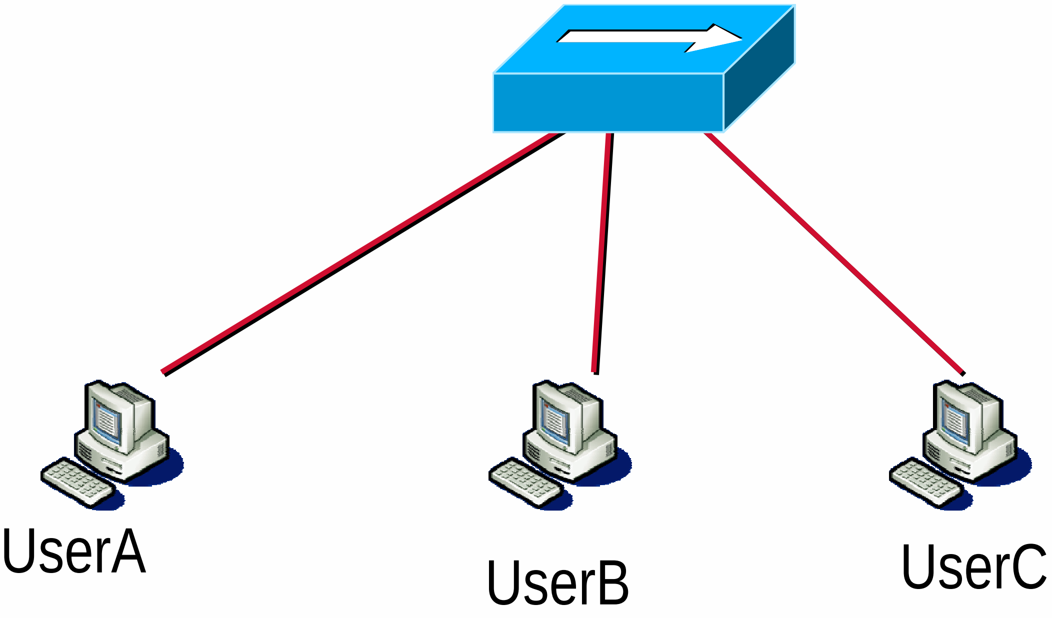
- Katz vs. United States, 1967
- 2004 Nicodemo Scarfo ("Little Nicky")

What You Need To Begin

- Commercial: Network Forensics Analysis Tools (NFAT)
- Packet capturing tool
  - Open-source vs. commercial
  - General vs. targeted
  - remote-vs. local
  - switched vs. shared

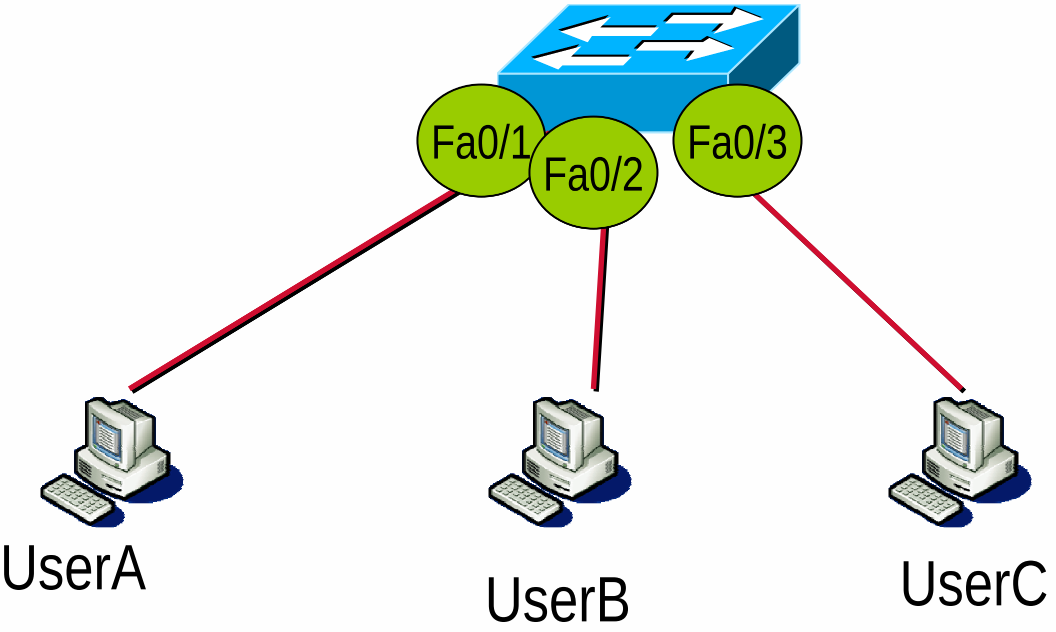
Sniffing on Switched Networks

Hubs…mmm…good

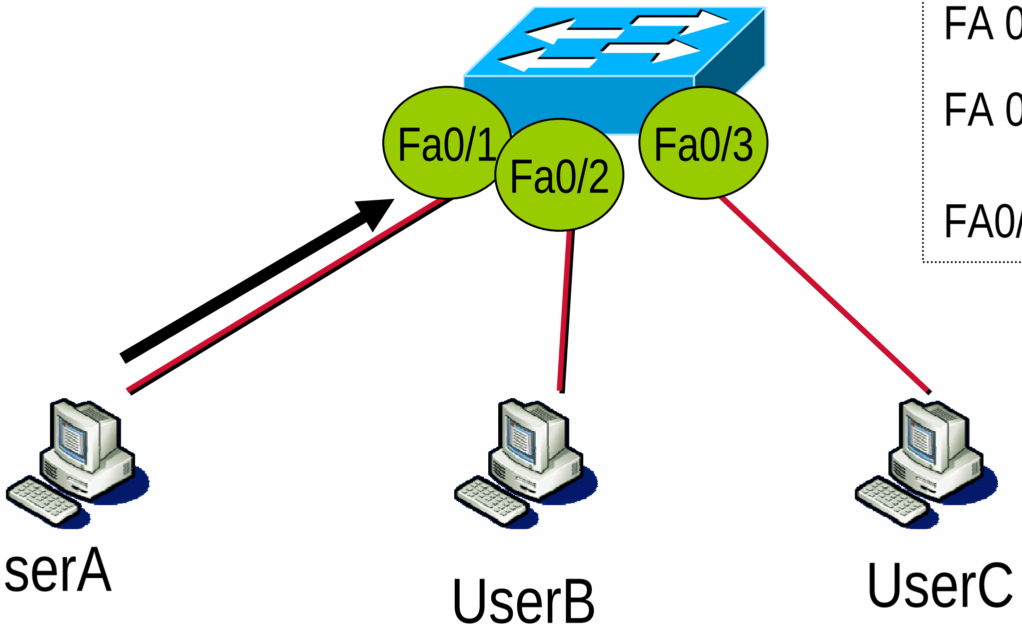


Frame from UserA is always propagated to UserB & UserC

How Switches Work



How Switches Work

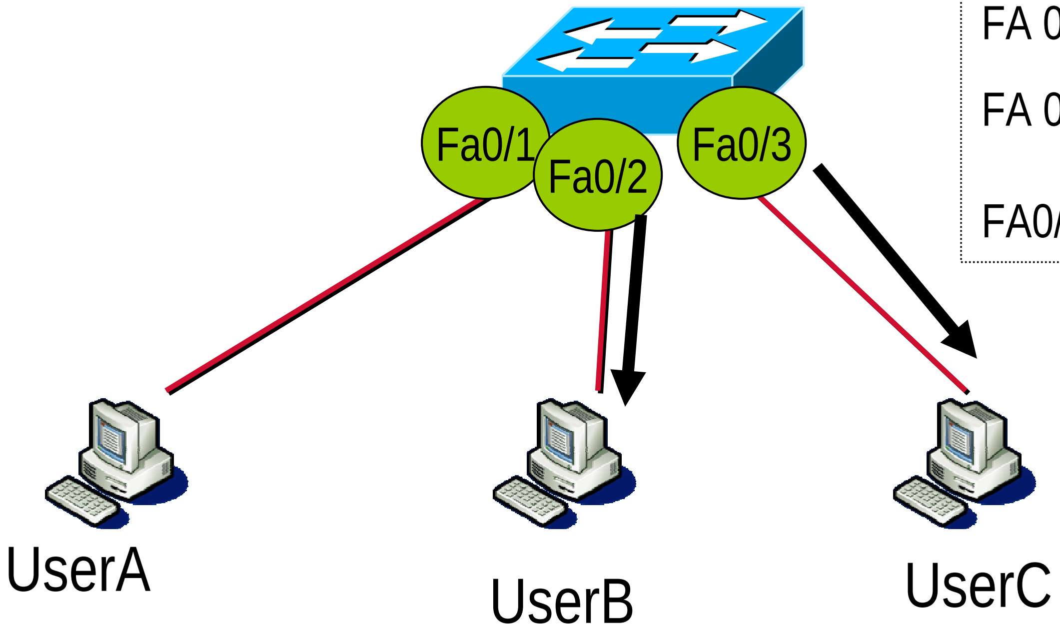


MAC Table

FA 0/1	01C9:44BB:00A1 (USER A)
FA 0/2	???
FA0/3	???

User A sends a frame to user B.

How Switches Work

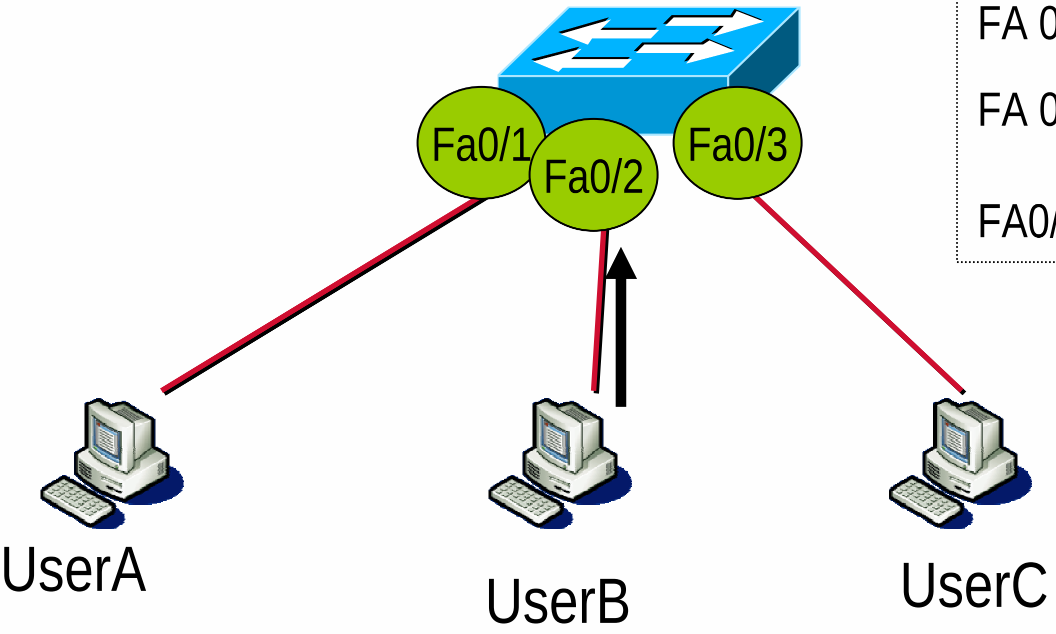


MAC Table

FA 0/1	01C9:44BB:00A1 (USER A)
FA 0/2	???
FA0/3	???

Frame is duplicated out to UserB and UserC.

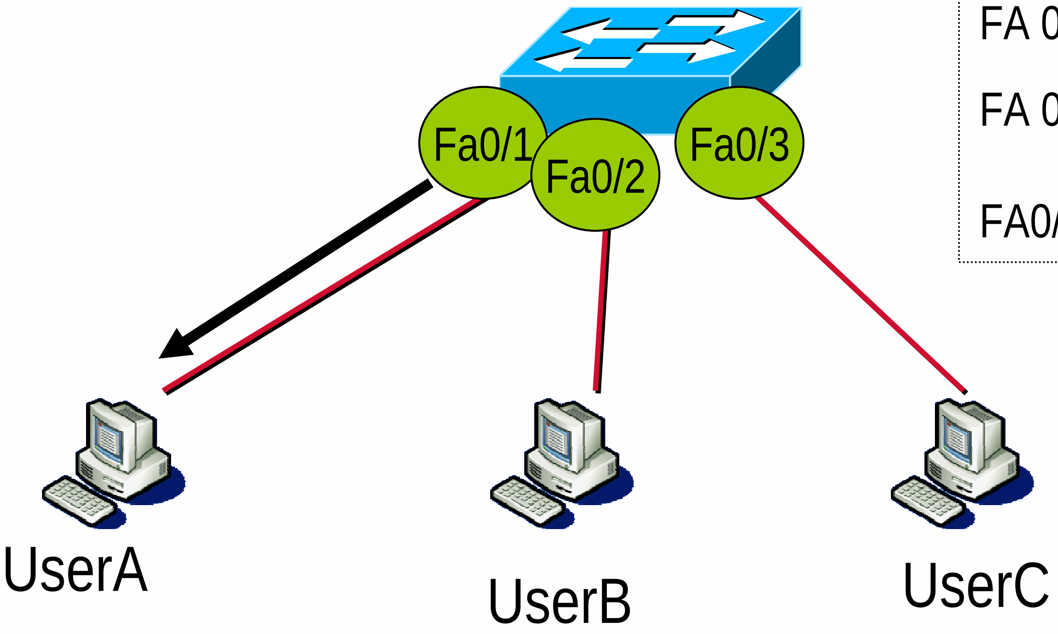
How Switches Work



MAC Table

FA 0/1	01C9:44BB:00A1 (USER A)
FA 0/2	0BB0:0E44:2221 (USER B)
FA0/3	???

How Switches Work



MAC Table

FA 0/1	01C9:44BB:00A1 (USER A)
FA 0/2	0BB0:0E44:2221 (USER B)
FA0/3	???

How To Get Around This Problem

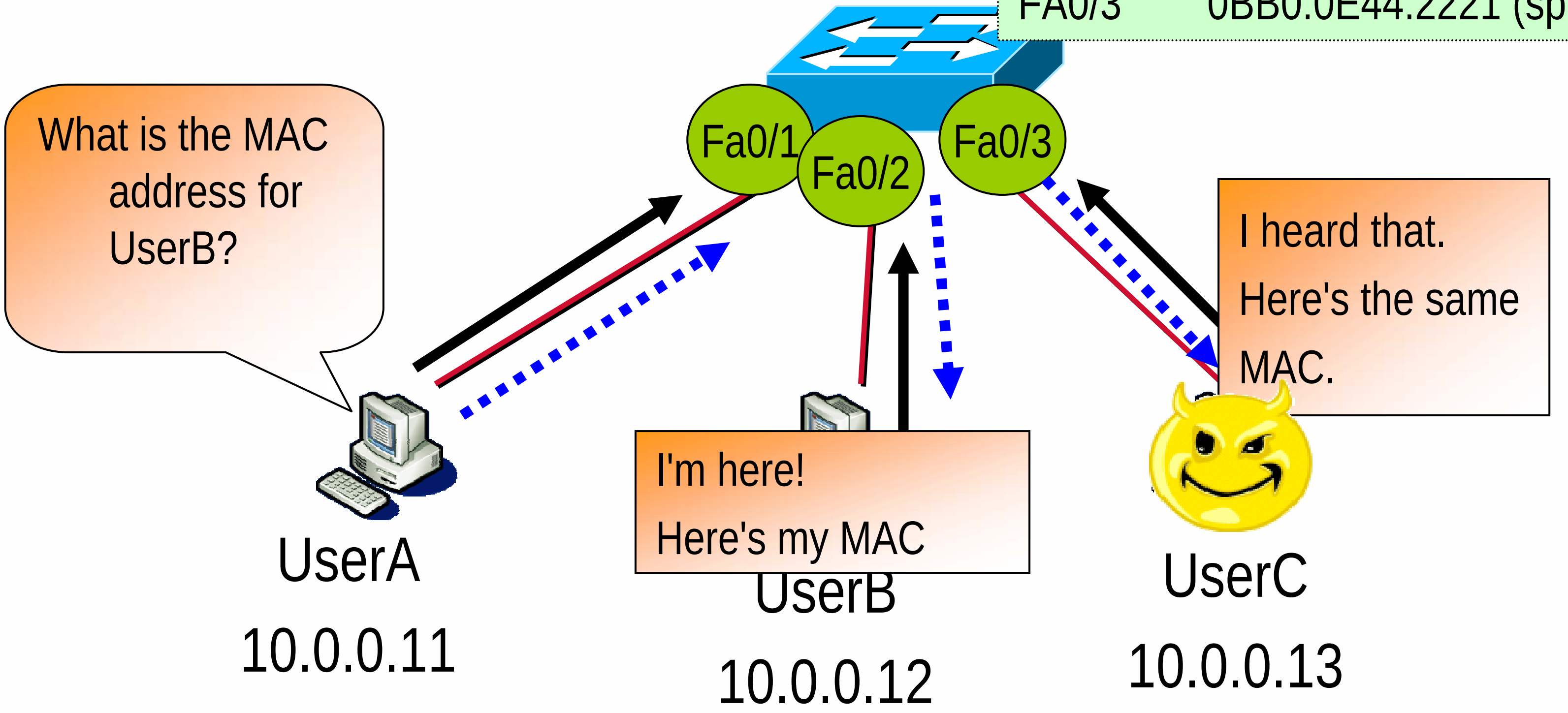
- Five Solutions:
  1. ARP Poisoning method 1
  2. ARP Poisoning method 2
  3. MAC Duplicating
  4. MAC Flooding
  5. Port Mirroring

ARP Poisoning Method 1

- A.K.A. ARP spoofing
- Sending crafted replies to ARP requests

MAC Table

FA 0/1	01C9:44BB:00A1 (USER A)
FA 0/2	0BB0:0E44:2221 (USER B)
FA0/3	0BB0:0E44:2221 (spoofed)



What is the MAC address for UserB?

Fa0/1

Fa0/2

Fa0/3

I heard that.
Here's the same MAC.

I'm here!
Here's my MAC

UserA
10.0.0.11

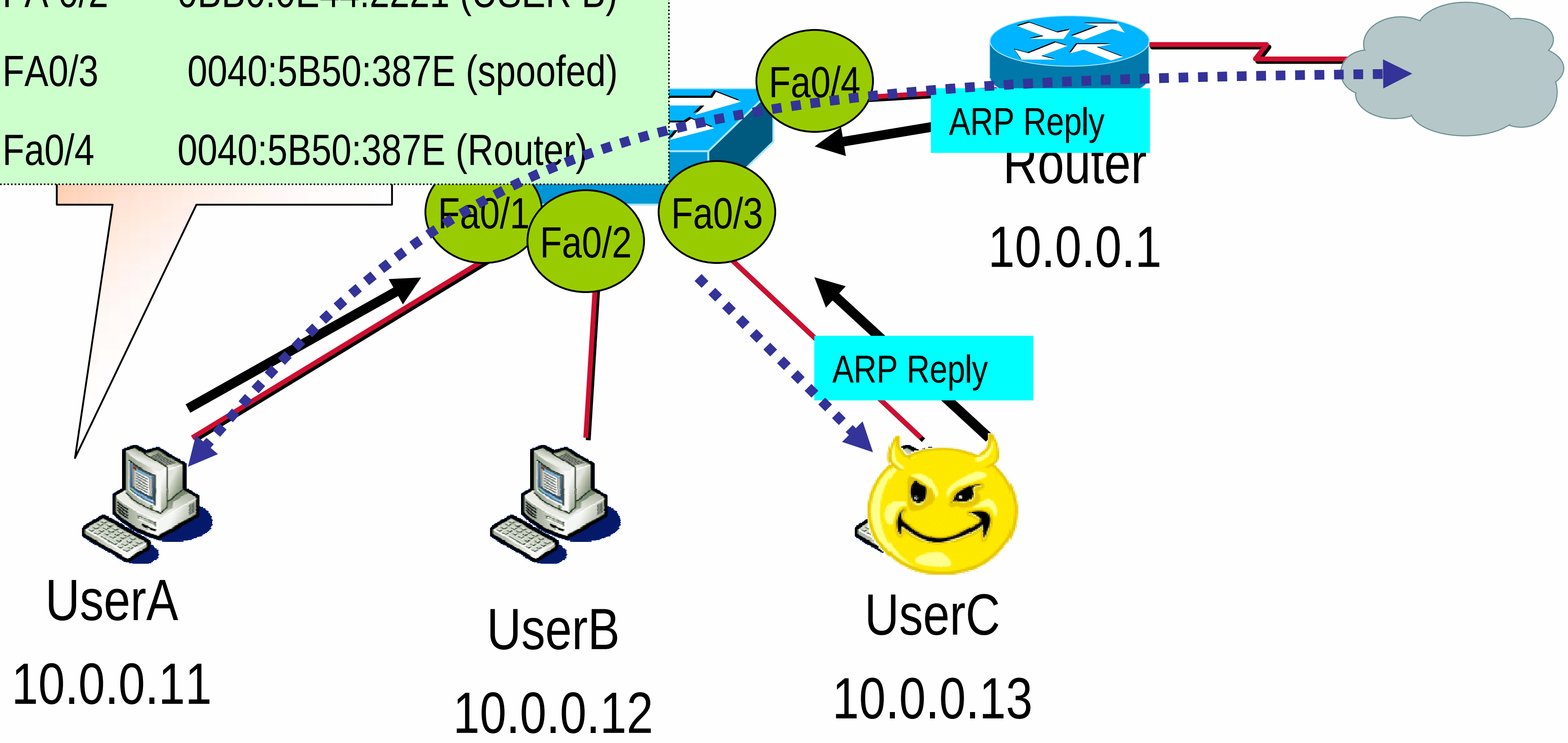
UserB
10.0.0.12

UserC
10.0.0.13

ARP Poisoning Method 2

MAC Table

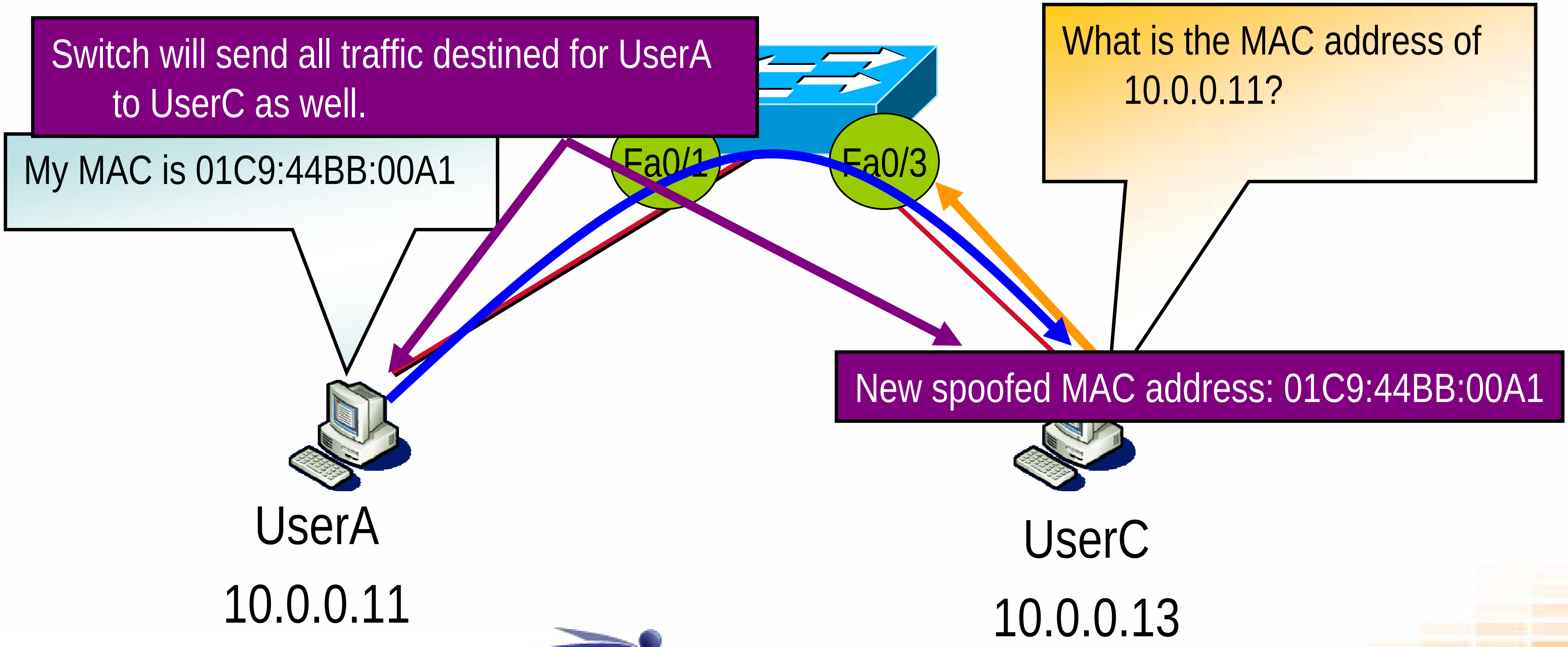
FA 0/1	01C9:44BB:00A1 (USER A)
FA 0/2	0BB0:0E44:2221 (USER B)
FA0/3	0040:5B50:387E (spoofed)
Fa0/4	0040:5B50:387E (Router)



TRAININGCAMP
Accelerated Learning. Education Evolved.

MAC Duplicating

- Used to target traffic sent to a single host (such as a server)
- ARP for a host you want to target to get its MAC address



Switch will send all traffic destined for UserA to UserC as well.

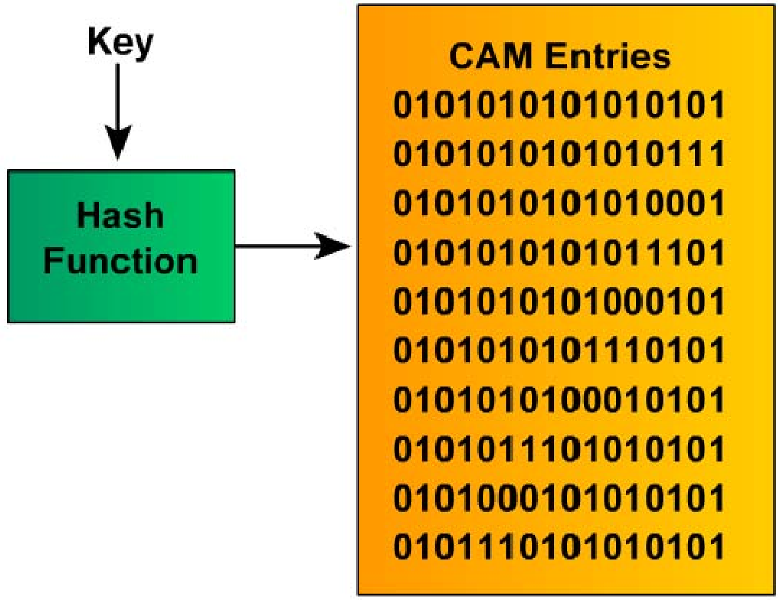
My MAC is 01C9:44BB:00A1

What is the MAC address of 10.0.0.11?

New spoofed MAC address: 01C9:44BB:00A1

MAC Flooding

- MAC addresses are stored in CAM table
- Content Addressable Memory (CAM) table
  - Switch must find an exact binary match
  - Information to do a lookup is called a key
  - Key is fed into a hashing algorithm to produce a pointer into the table



Key

Hash Function

CAM Entries

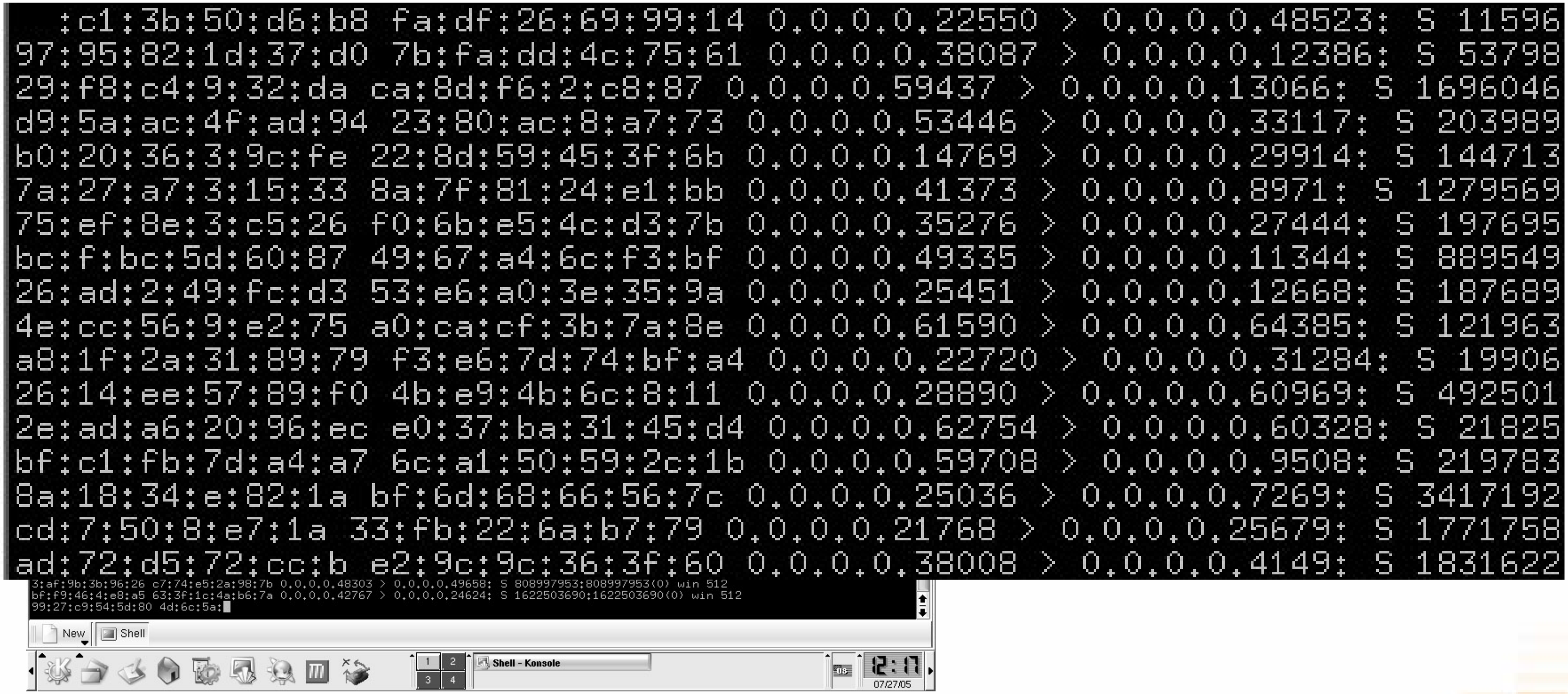
0101010101010101
0101010101010111
0101010101010001
0101010101011101
0101010101000101
0101010101110101
0101010100010101
0101011101010101
0101000101010101
0101110101010101

MAC Flooding

- CAM is limited on switches (typically 64k)
- If filled up, switch can no longer store new addresses
- Switch effectively turns into a hub

MAC Flooding

- MACOF (part of Dsniff)
- http://www.monkey.org/~dugsong/dsniff/



```
  :c1:3b:50:d6:b8 fa:df:26:69:99:14 0.0.0.0.22550 > 0.0.0.0.48523: S 11596
97:95:82:1d:37:d0 7b:fa:dd:4c:75:61 0.0.0.0.38087 > 0.0.0.0.12386: S 53798
29:f8:c4:9:32:da ca:8d:f6:2:c8:87 0.0.0.0.59437 > 0.0.0.0.13066: S 1696046
d9:5a:ac:4f:ad:94 23:80:ac:8:a7:73 0.0.0.0.53446 > 0.0.0.0.33117: S 203989
b0:20:36:3:9c:fe 22:8d:59:45:3f:6b 0.0.0.0.14769 > 0.0.0.0.29914: S 144713
7a:27:a7:3:15:33 8a:7f:81:24:e1:bb 0.0.0.0.41373 > 0.0.0.0.8971: S 1279569
75:ef:8e:3:c5:26 f0:6b:e5:4c:d3:7b 0.0.0.0.35276 > 0.0.0.0.27444: S 197695
bc:f:bc:5d:60:87 49:67:a4:6c:f3:bf 0.0.0.0.49335 > 0.0.0.0.11344: S 889549
26:ad:2:49:fc:d3 53:e6:a0:3e:35:9a 0.0.0.0.25451 > 0.0.0.0.12668: S 187689
4e:cc:56:9:e2:75 a0:ca:cf:3b:7a:8e 0.0.0.0.61590 > 0.0.0.0.64385: S 121963
a8:1f:2a:31:89:79 f3:e6:7d:74:bf:a4 0.0.0.0.22720 > 0.0.0.0.31284: S 19906
26:14:ee:57:89:f0 4b:e9:4b:6c:8:11 0.0.0.0.28890 > 0.0.0.0.60969: S 492501
2e:ad:a6:20:96:ec e0:37:ba:31:45:d4 0.0.0.0.62754 > 0.0.0.0.60328: S 21825
bf:c1:fb:7d:a4:a7 6c:a1:50:59:2c:1b 0.0.0.0.59708 > 0.0.0.0.9508: S 219783
8a:18:34:e:82:1a bf:6d:68:66:56:7c 0.0.0.0.25036 > 0.0.0.0.7269: S 3417192
cd:7:50:8:e7:1a 33:fb:22:6a:b7:79 0.0.0.0.21768 > 0.0.0.0.25679: S 1771758
ad:72:d5:72:cc:b e2:9c:9c:36:3f:60 0.0.0.0.38008 > 0.0.0.0.4149: S 1831622
3:af:9b:3b:96:26 c7:74:e5:2a:98:7b 0.0.0.0.48303 > 0.0.0.0.49658: S 808997953:808997953(0) win 512
bf:f9:46:4:e8:a5 63:3f:1c:4a:b6:7a 0.0.0.0.42767 > 0.0.0.0.24624: S 1622503690:1622503690(0) win 512
99:27:c9:54:5d:80 4d:6c:5a:
```

TRAININGCAMP
Accelerated Learning. Education Evolved.

Port Mirroring

- Port mirroring is a legitimate method of mirroring one port to another port
- Cisco calls this *switched port analyzer* (SPAN)
  - Remote SPAN (RSPAN) can send traffic from one or more ports or an entire VLAN to another port on a different switch
  - There can be more than one source and more than one destination (up to 64 destination ports!)
- SPAN can copy traffic in one of three ways:
  - Rx SPAN
  - Tx SPAN
  - Rx/Tx SPAN

Port Mirroring

1) Specify source

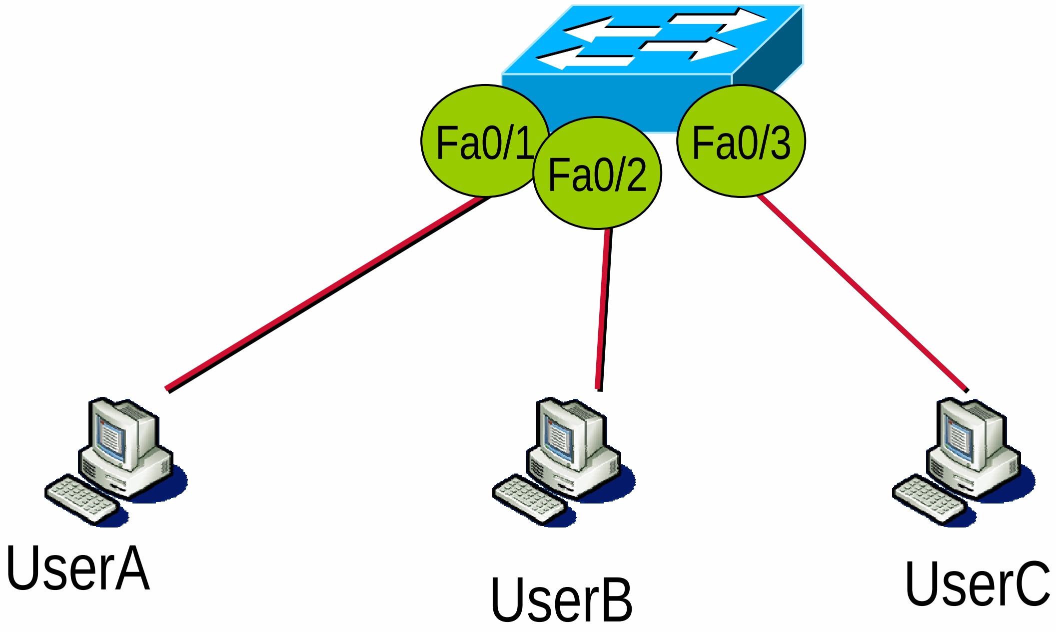
```
monitor session session_number source
   {interface interface-id | vlan vlan-id} [, |
   -] [both | rx | tx]
```

2) Specify destination

```
monitor session session_number destination
   {interface interface-id [, | -]
   [encapsulation replicate]
```

Port Mirroring

```
Switch(config)#monitor session 1 source interface
   fastethernet 0/1 , 0/2 both
Switch(config)#monitor session 1 destination fastethernet
   0/3
```



Packet Capturing Software

- Tons!!!
- PacketStorm Security (http://packetstormsecurity.org/sniffers/) has almost 200 different sniffers
- Most popular freeware utilities:
  - Windump / Tcpdump
  - Ethereal (Now Wireshark)

Windump / TCPDump

- Developed by Loris Degioanni, Gianluca Varenni, Fulvio Risso, John Bruno, Piero Viano
- Http://www.tcpdump.org & http://www.winpcap.org/windump/default.htm
- Requires winpcap / libpcap library

Using WinDump / TCPDump

```
• tcpdump [ -ABdDeflLnNOpqRStuUvxX ] [ -c count ]

        [ -C file_size ] [ -F file ]

        [ -i interface ] [ -m module ] [ -M secret ]

        [ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]

        [ -W filecount ]

        [ -E spi@ipaddr algo:secret,... ]

        [ -y datalinktype ] [ -Z user ]
        [ expression ]
```

Using WinDump / tcpdump

- **Display interfaces:** windump –D
- **Use interface:** windump –i <interface # or identifier>
- **Print out in Ascii:** windump –A
- **Log to file**: windump –w *file.log*
- **Read from log:** windump –r *file.log*
- **Verbose output:** windump –vvv

Windump Example

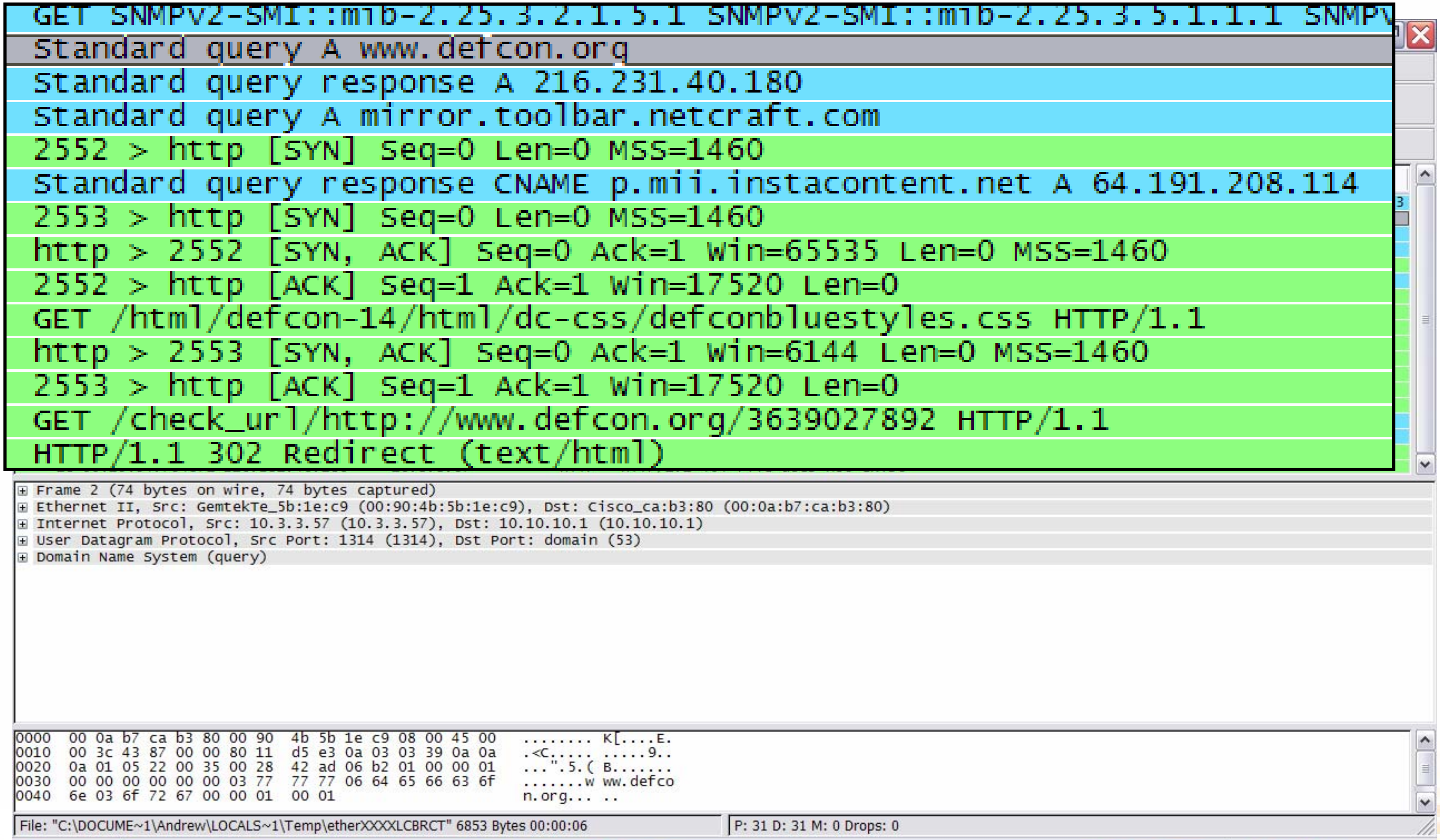
```
23:23:52.991879 IP (tos 0x0, ttl 128, id 11231, offset 0, flags [DF], proto: TCP (6), length: 48)
    A152B.2436 > www.defcon.org.80: S, cksum 0x86d6 (correct), 916679930:916679930(0) win
    16384 <mss 1460,nop,nop,sackOK>
E..0+.@.....
..9..(.         ..P6.l.....p.@............
23:23:53.116681 IP (tos 0x0, ttl  47, id 35735, offset 0, flags [none], proto: TCP (6), length: 44)
    www.defcon.org.80 > A152B.2436: S, cksum 0x2304 (correct), 451321314:451321314(0) ack
    916679931 win 65535 <mss 1460>
E..,..../..]..(.
..9.P           .....6.l.`...#.........
23:23:53.116738 IP (tos 0x0, ttl 128, id 11232, offset 0, flags [DF], proto: TCP (6), length: 40)
    A152B.2436 > www.defcon.org.80: ., cksum 0xf650 (correct), 1:1(0) ack 1 win 17520
E..(+.@.....
..9..(.         ..P6.l.....P.Dp.P..
23:23:53.117616 IP (tos 0x0, ttl 128, id 11233, offset 0, flags [DF], proto: TCP (6), length: 495)
    A152B.2436 > www.defcon.org.80: P 1:456(455) ack 1 win 17520
E...+.@....P
..9..(.         ..P6.l.....P.Dp1/..GET /html/defcon-14/html/dc-css/defconblue
```

Ethereal / Wireshark

- Packet analyzer
- Original author was Gerald Combs
- Now supported by over 100 programmers
- Can 'dissect' 759 protocols
- Linux & Windows friendly
- Now licensed through CACE Technologies

  http://www.wireshark.org/

Ethereal / Wirehsark



```
GET SNMPv2-SMI::mib-2.25.3.2.1.5.1 SNMPv2-SMI::mib-2.25.3.5.1.1.1 SNMPv
Standard query A www.defcon.org
Standard query response A 216.231.40.180
Standard query A mirror.toolbar.netcraft.com
2552 > http [SYN] Seq=0 Len=0 MSS=1460
Standard query response CNAME p.mii.instacontent.net A 64.191.208.114
2553 > http [SYN] Seq=0 Len=0 MSS=1460
http > 2552 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
2552 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
GET /html/defcon-14/html/dc-css/defconbluestyles.css HTTP/1.1
http > 2553 [SYN, ACK] Seq=0 Ack=1 Win=6144 Len=0 MSS=1460
2553 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
GET /check_url/http://www.defcon.org/3639027892 HTTP/1.1
HTTP/1.1 302 Redirect (text/html)
```

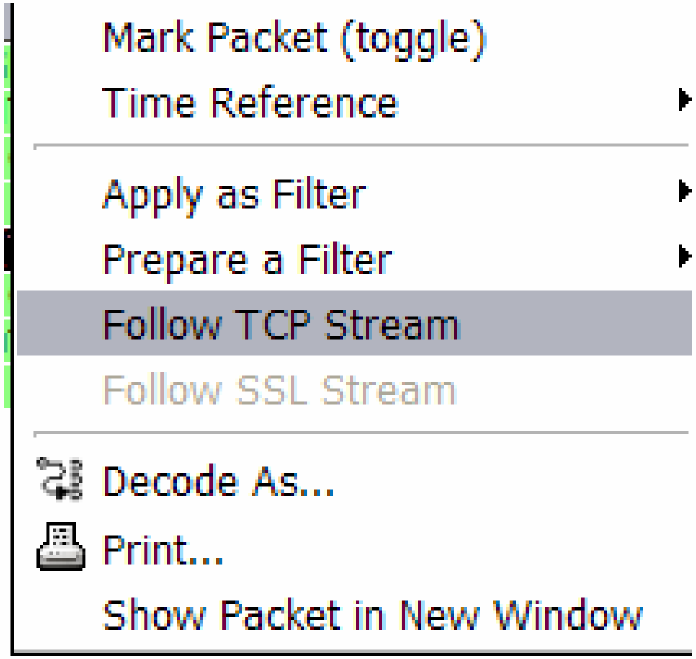
```
⊞ Frame 2 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: GemtekTe_5b:1e:c9 (00:90:4b:5b:1e:c9), Dst: Cisco_ca:b3:80 (00:0a:b7:ca:b3:80)
⊞ Internet Protocol, Src: 10.3.3.57 (10.3.3.57), Dst: 10.10.10.1 (10.10.10.1)
⊞ User Datagram Protocol, Src Port: 1314 (1314), Dst Port: domain (53)
⊞ Domain Name System (query)
```

```
0000  00 0a b7 ca b3 80 00 90  4b 5b 1e c9 08 00 45 00   ........ K[....E.
0010  00 3c 43 87 00 00 80 11  d5 e3 0a 03 03 39 0a 0a   .<C..... .....9..
0020  0a 01 05 22 00 35 00 28  42 ad 06 b2 01 00 00 01   ...".5.( B.......
0030  00 00 00 00 00 00 03 77  77 77 06 64 65 66 63 6f   .......w ww.defco
0040  6e 03 6f 72 67 00 00 01  00 01                     n.org... ..
```

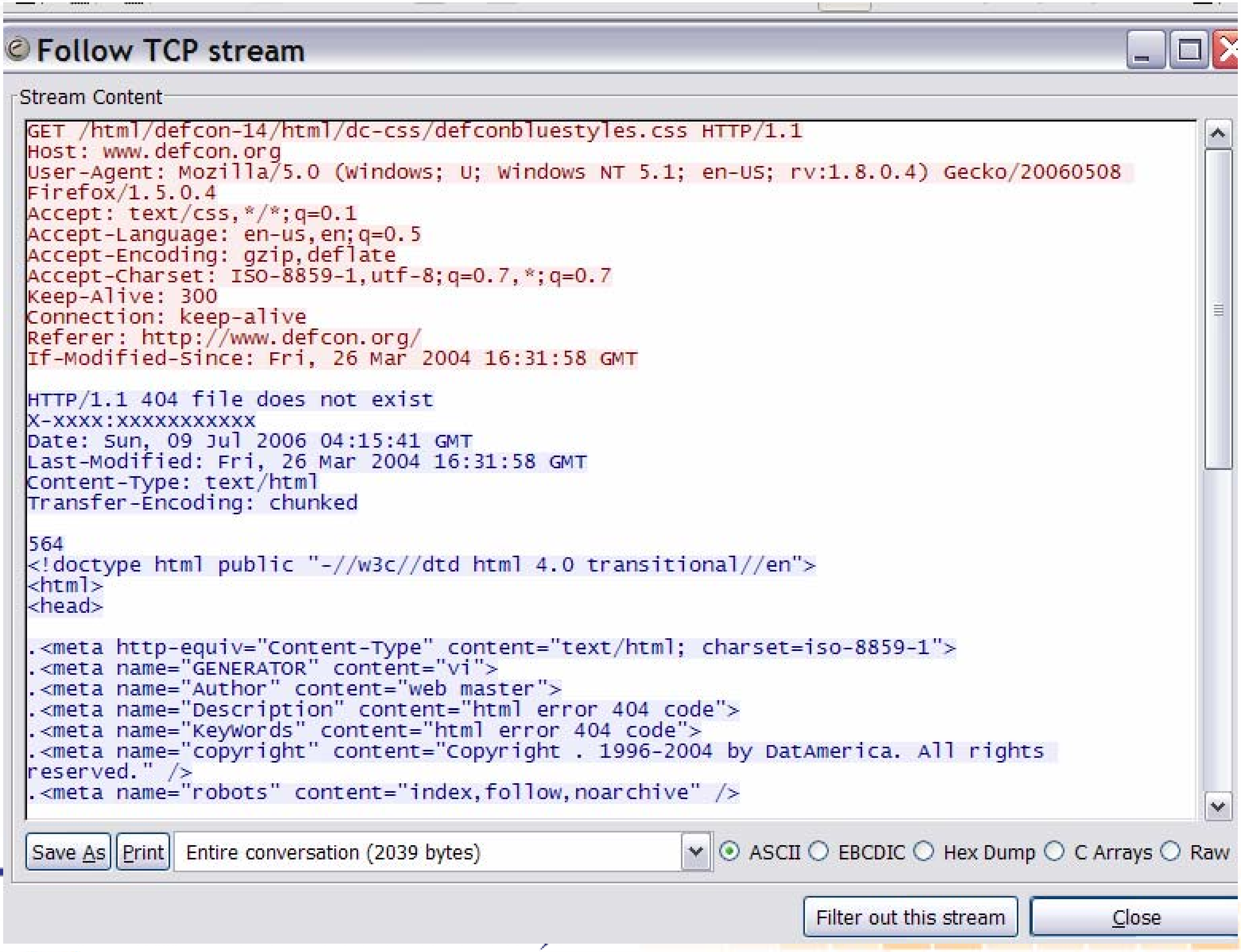
```
File: "C:\DOCUME~1\Andrew\LOCALS~1\Temp\etherXXXXLCBRCT" 6853 Bytes 00:00:06    P: 31 D: 31 M: 0 Drops: 0
```

Ethereal / Wireshark

- To view entire conversation, right-click and choose Follow TCP Stream



Ethereal / Wireshark



```
GET /html/defcon-14/html/dc-css/defconbluestyles.css HTTP/1.1
Host: www.defcon.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.4) Gecko/20060508
Firefox/1.5.0.4
Accept: text/css,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.defcon.org/
If-Modified-Since: Fri, 26 Mar 2004 16:31:58 GMT

HTTP/1.1 404 file does not exist
X-xxxx:xxxxxxxxxxx
Date: Sun, 09 Jul 2006 04:15:41 GMT
Last-Modified: Fri, 26 Mar 2004 16:31:58 GMT
Content-Type: text/html
Transfer-Encoding: chunked

564
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html>
<head>

.<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
.<meta name="GENERATOR" content="vi">
.<meta name="Author" content="web master">
.<meta name="Description" content="html error 404 code">
.<meta name="Keywords" content="html error 404 code">
.<meta name="copyright" content="Copyright . 1996-2004 by DatAmerica. All rights
reserved." />
.<meta name="robots" content="index,follow,noarchive" />
```

Entire conversation (2039 bytes)

● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw

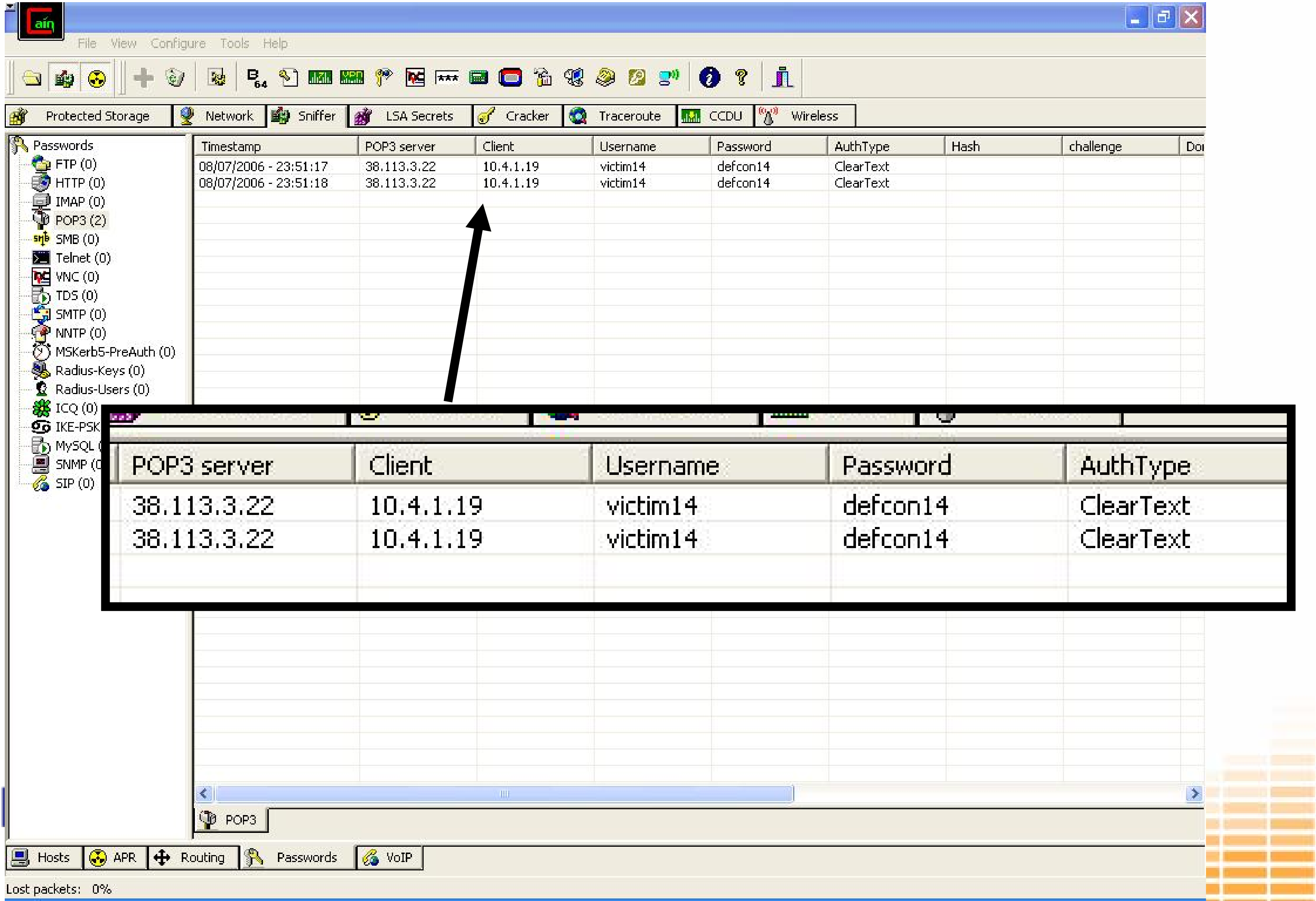
Password Capturing

- The following protocols send passwords in plain text
  - Telnet
  - FTP
  - POP
  - SMTP
  - Just to name a few!
- Even if password is not in plain text, it is often easily cracked

Tool: Cain and Abel

- Developed by Massimiliano Montoro
- http://www.oxid.it/index.html
- Password recovery tool that supports packet capturing
- Can even capture & replay voice conversations

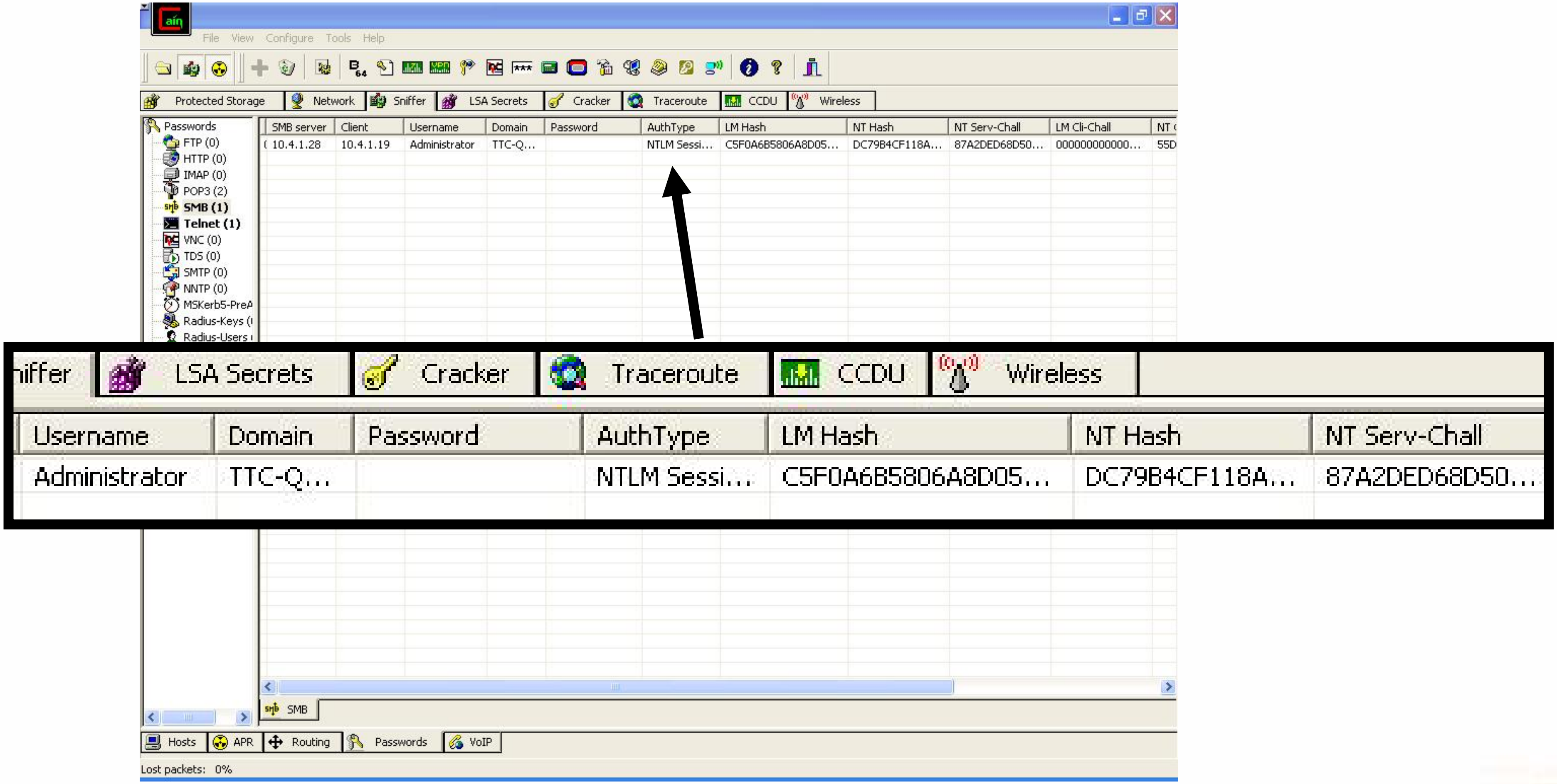
Cain and Abel



Timestamp	POP3 server	Client	Username	Password	AuthType	Hash	challenge	Do
08/07/2006 - 23:51:17	38.113.3.22	10.4.1.19	victim14	defcon14	ClearText			
08/07/2006 - 23:51:18	38.113.3.22	10.4.1.19	victim14	defcon14	ClearText			

POP3 server	Client	Username	Password	AuthType
38.113.3.22	10.4.1.19	victim14	defcon14	ClearText
38.113.3.22	10.4.1.19	victim14	defcon14	ClearText

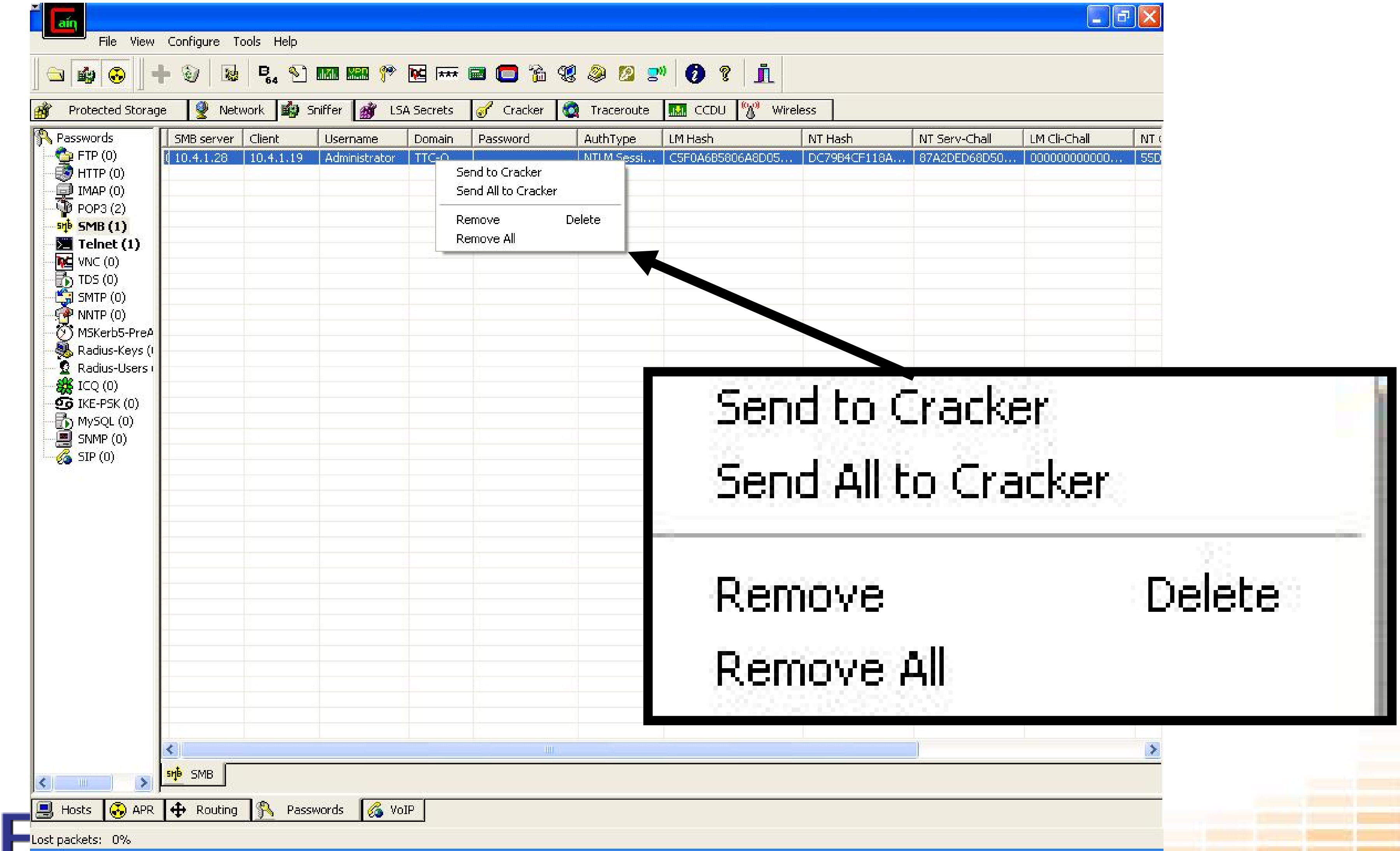
Cain and Abel



SMB server	Client	Username	Domain	Password	AuthType	LM Hash	NT Hash	NT Serv-Chall	LM Cli-Chall	NT c
(10.4.1.28	10.4.1.19	Administrator	TTC-Q...		NTLM Sessi...	C5F0A6B5806A8D05...	DC79B4CF118A...	87A2DED68D50...	000000000000...	55D

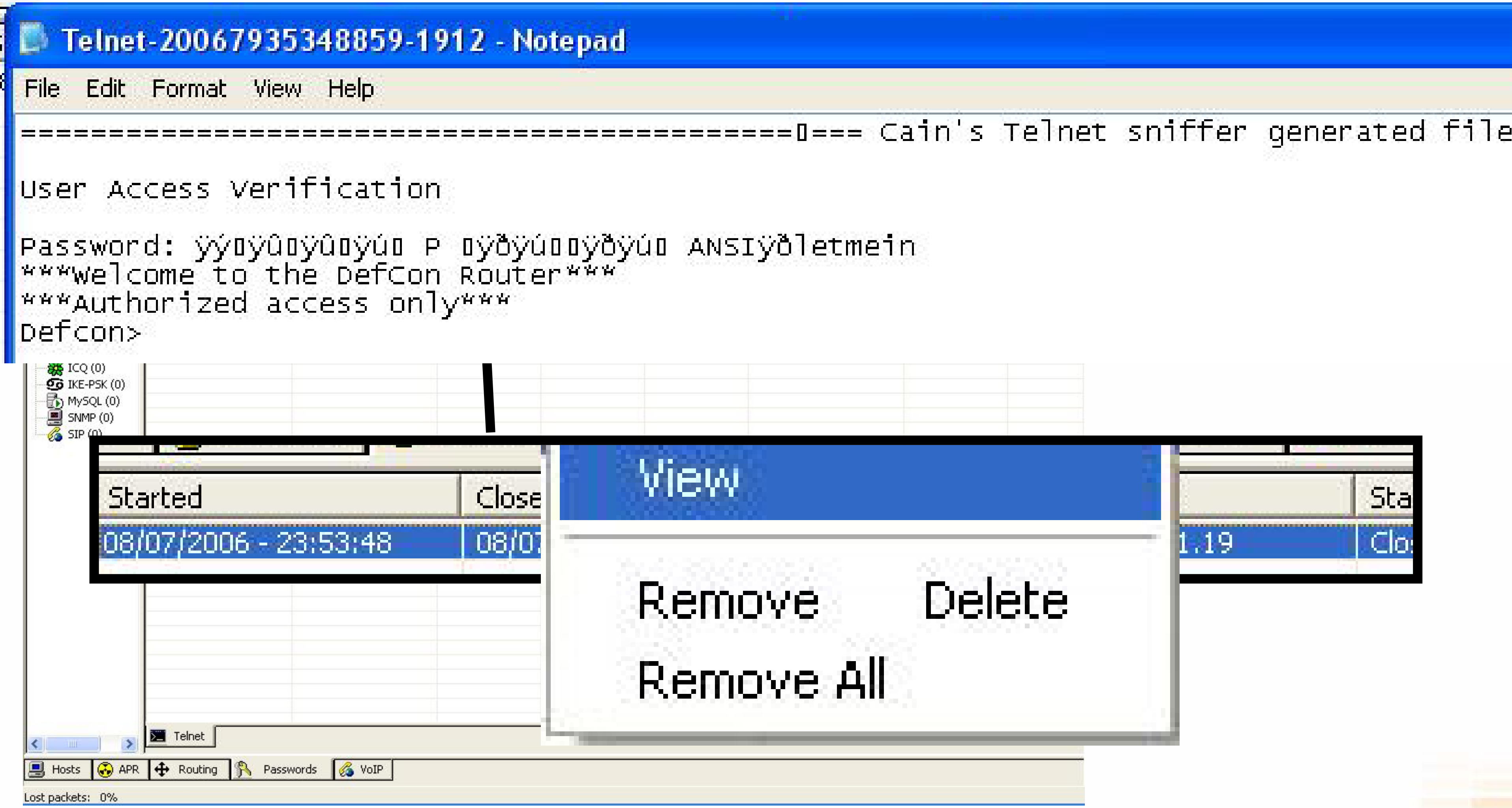
Username	Domain	Password	AuthType	LM Hash	NT Hash	NT Serv-Chall
Administrator	TTC-Q...		NTLM Sessi...	C5F0A6B5806A8D05...	DC79B4CF118A...	87A2DED68D50...

Cain and Abel



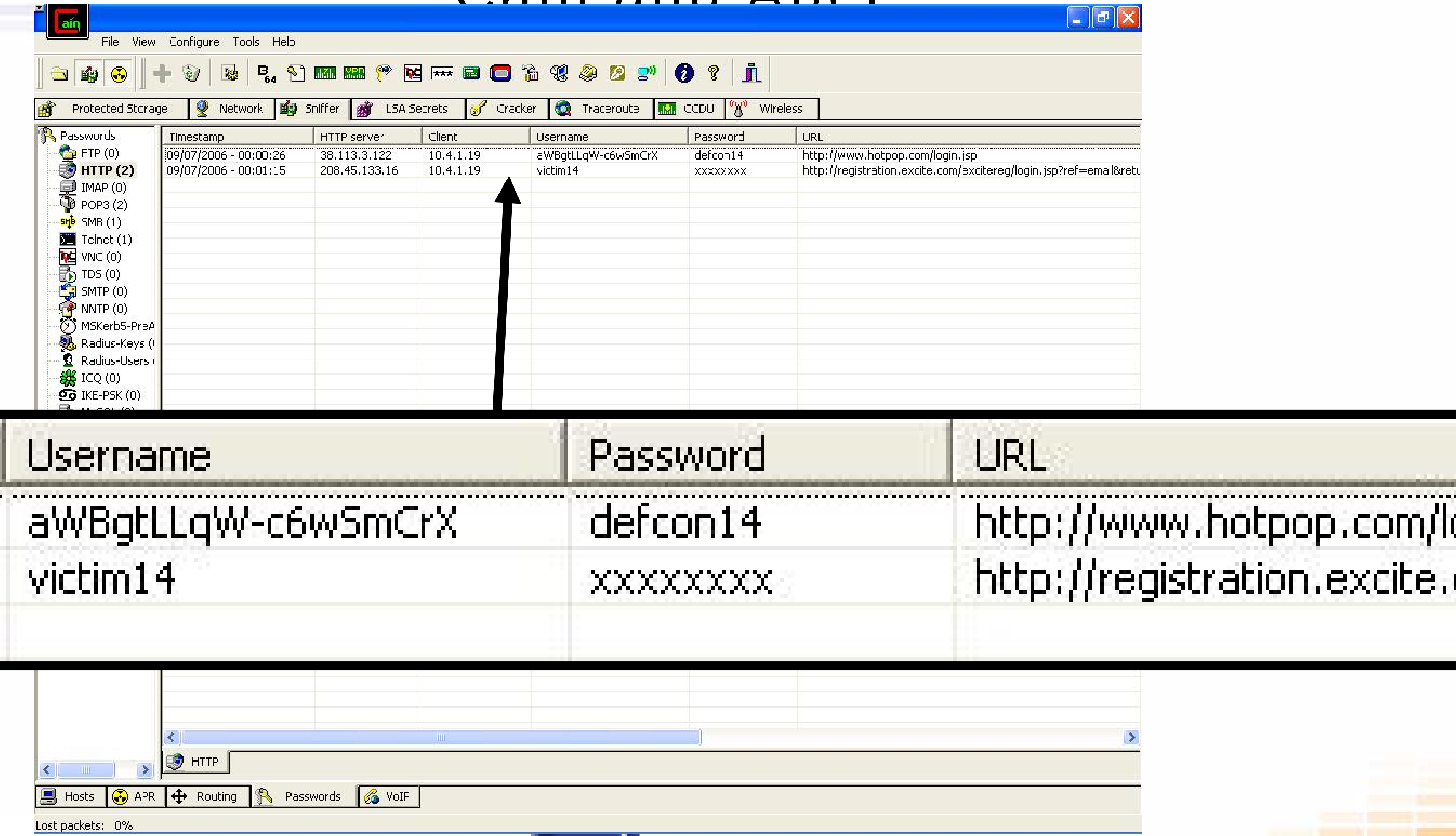
SMB server	Client	Username	Domain	Password	AuthType	LM Hash	NT Hash	NT Serv-Chall	LM Cli-Chall	NT
10.4.1.28	10.4.1.19	Administrator	TTC-O		NTLM Sessi...	C5F0A6B5806A8D05...	DC79B4CF118A...	87A2DED68D50...	000000000000...	55D

Cain and Abel



```
========================================□=== Cain's Telnet sniffer generated file

User Access Verification

Password: ÿý□ÿû□ÿû□ÿú□ P □ÿðÿú□□ÿðÿú□ ANSIÿðletmein
***Welcome to the DefCon Router***
***Authorized access only***
Defcon>
```

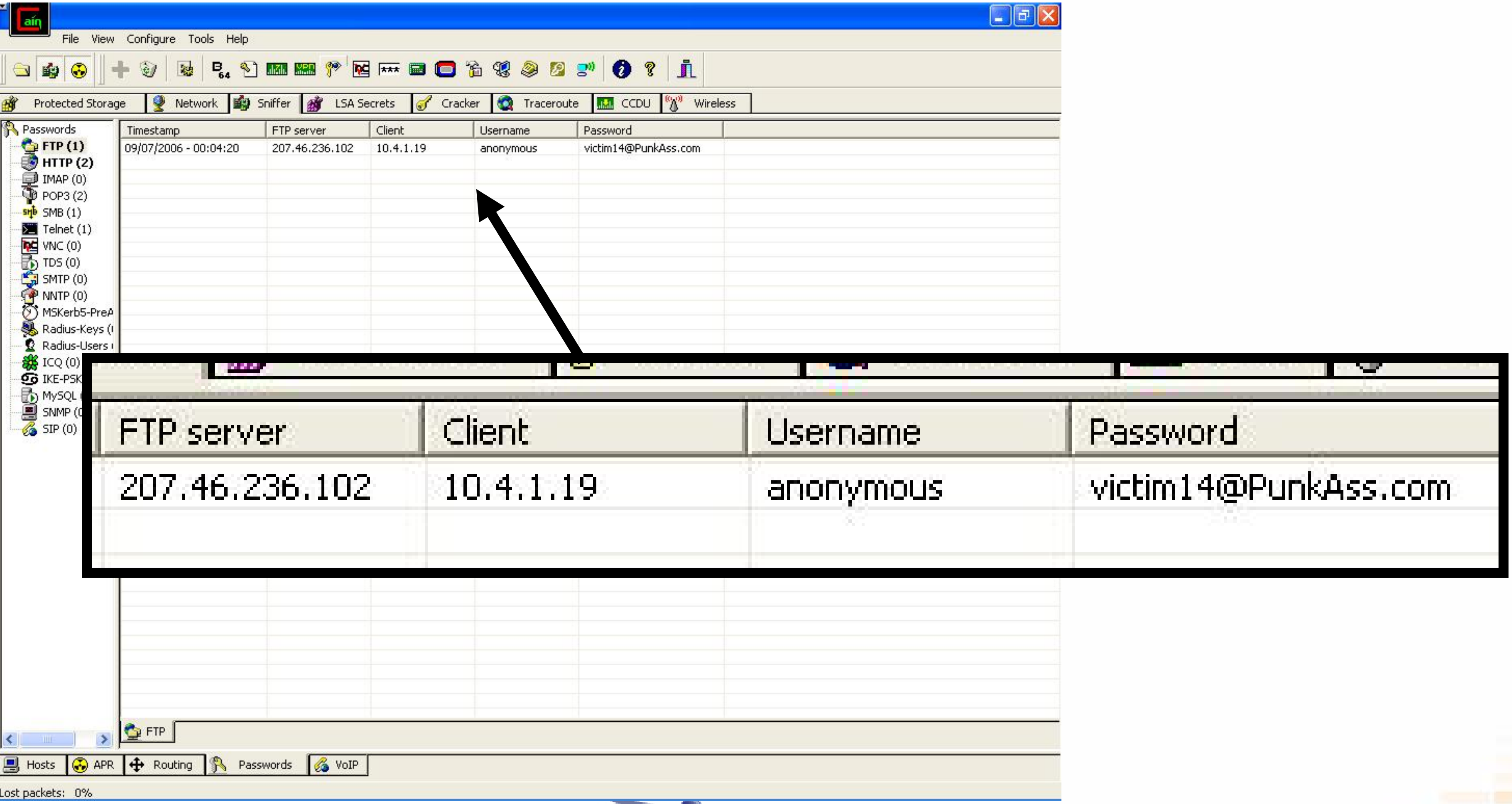
Cain and Abel



Timestamp	HTTP server	Client	Username	Password	URL
09/07/2006 - 00:00:26	38.113.3.122	10.4.1.19	aWBgtLLqW-c6wSmCrX	defcon14	http://www.hotpop.com/login.jsp
09/07/2006 - 00:01:15	208.45.133.16	10.4.1.19	victim14	xxxxxxxx	http://registration.excite.com/excitereg/login.jsp?ref=email&retu

Username	Password	URL
aWBgtLLqW-c6wSmCrX	defcon14	http://www.hotpop.com/l
victim14	xxxxxxxx	http://registration.excite.

Cain and Abel

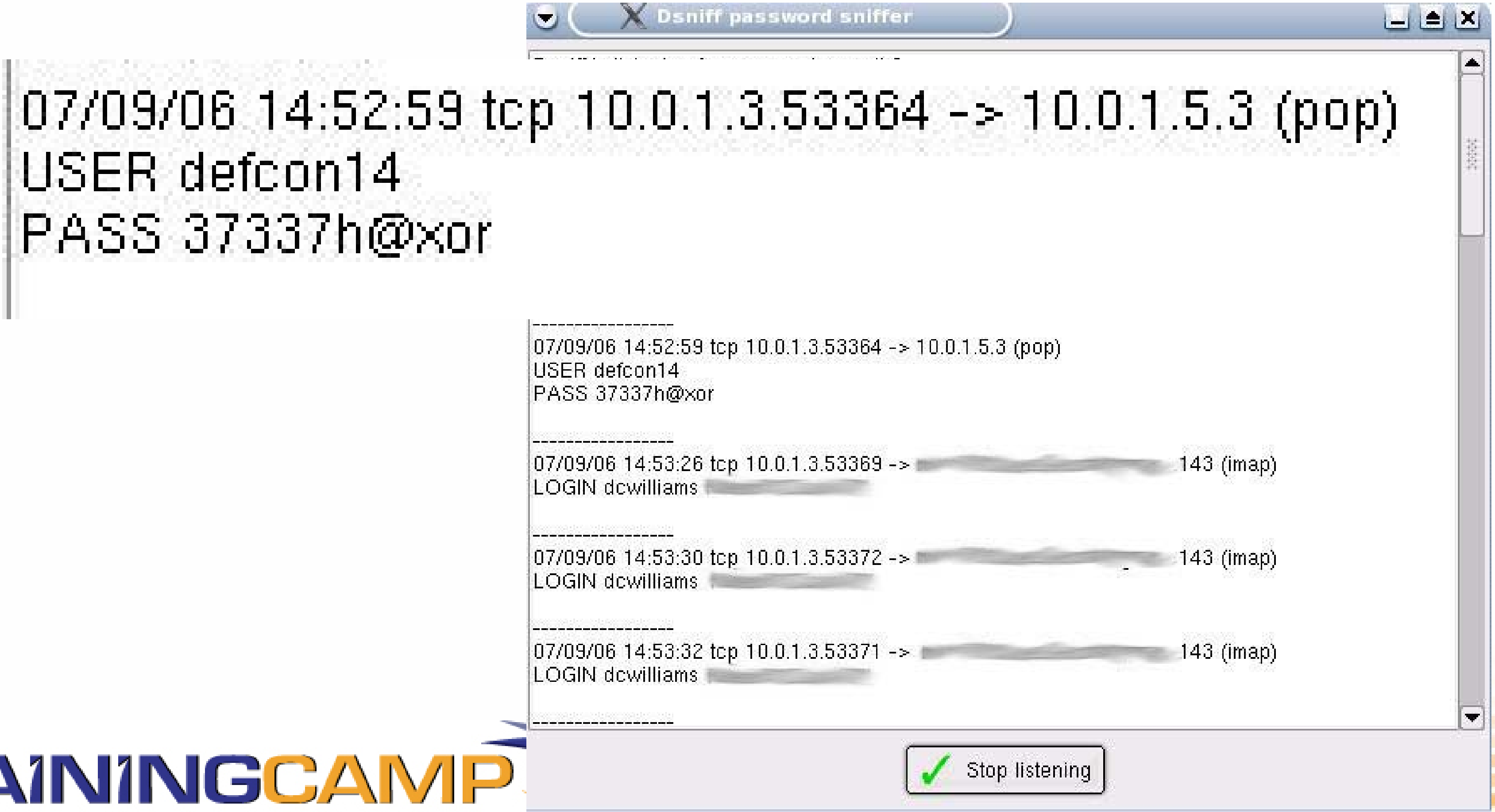


Timestamp	FTP server	Client	Username	Password
09/07/2006 - 00:04:20	207.46.236.102	10.4.1.19	anonymous	victim14@PunkAss.com

FTP server	Client	Username	Password
207.46.236.102	10.4.1.19	anonymous	victim14@PunkAss.com

Tool: Dsniff

- http://www.monkey.org/~dugsong/dsniff/
- Dsniff can be used to listen only for passwords



```
07/09/06 14:52:59 tcp 10.0.1.3.53364 -> 10.0.1.5.3 (pop)
USER defcon14
PASS 37337h@xor
```

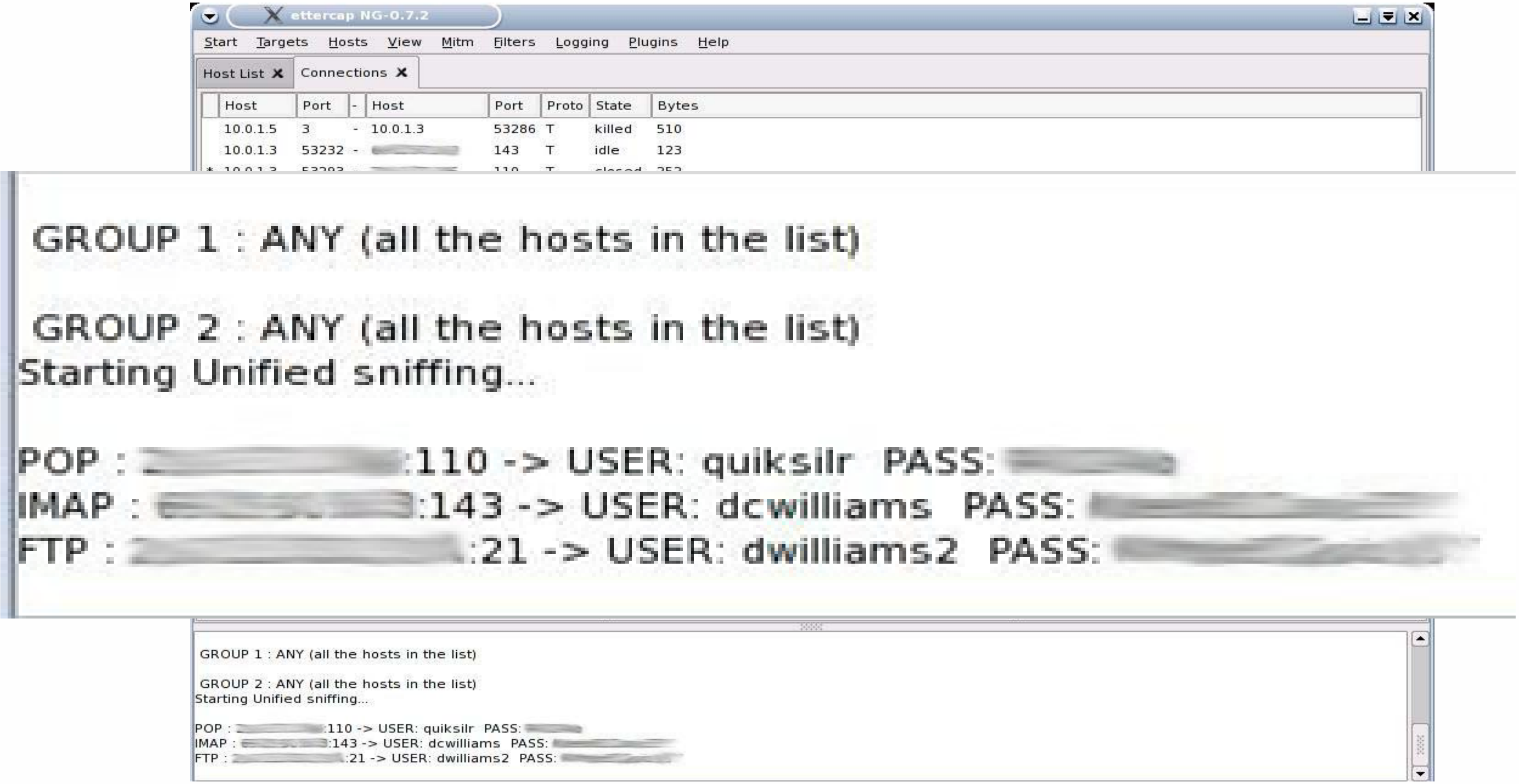
```
-----------------
07/09/06 14:52:59 tcp 10.0.1.3.53364 -> 10.0.1.5.3 (pop)
USER defcon14
PASS 37337h@xor
```

```
-----------------
07/09/06 14:53:26 tcp 10.0.1.3.53369 -> [redacted] 143 (imap)
LOGIN dcwilliams [redacted]

-----------------
07/09/06 14:53:30 tcp 10.0.1.3.53372 -> [redacted] 143 (imap)
LOGIN dcwilliams [redacted]

-----------------
07/09/06 14:53:32 tcp 10.0.1.3.53371 -> [redacted] 143 (imap)
LOGIN dcwilliams [redacted]

-----------------
```

Tool: Ettercap

- http://ettercap.sourceforge.net/
- Can be used to sniff passwords
- Active and passive capturing capabilities
- Content filtering

Tool: Ettercap



Host	Port	-	Host	Port	Proto	State	Bytes
10.0.1.5	3	-	10.0.1.3	53286	T	killed	510
10.0.1.3	53232	-	[redacted]	143	T	idle	123

```
 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...

POP : [redacted]:110 -> USER: quiksilr  PASS: [redacted]
IMAP : [redacted]:143 -> USER: dcwilliams  PASS: [redacted]
FTP : [redacted]:21 -> USER: dwilliams2  PASS: [redacted]
```

```
 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...

POP : [redacted]:110 -> USER: quiksilr  PASS: [redacted]
IMAP : [redacted]:143 -> USER: dcwilliams  PASS: [redacted]
FTP : [redacted]:21 -> USER: dwilliams2  PASS: [redacted]
```

Analysis of E-mail Traffic

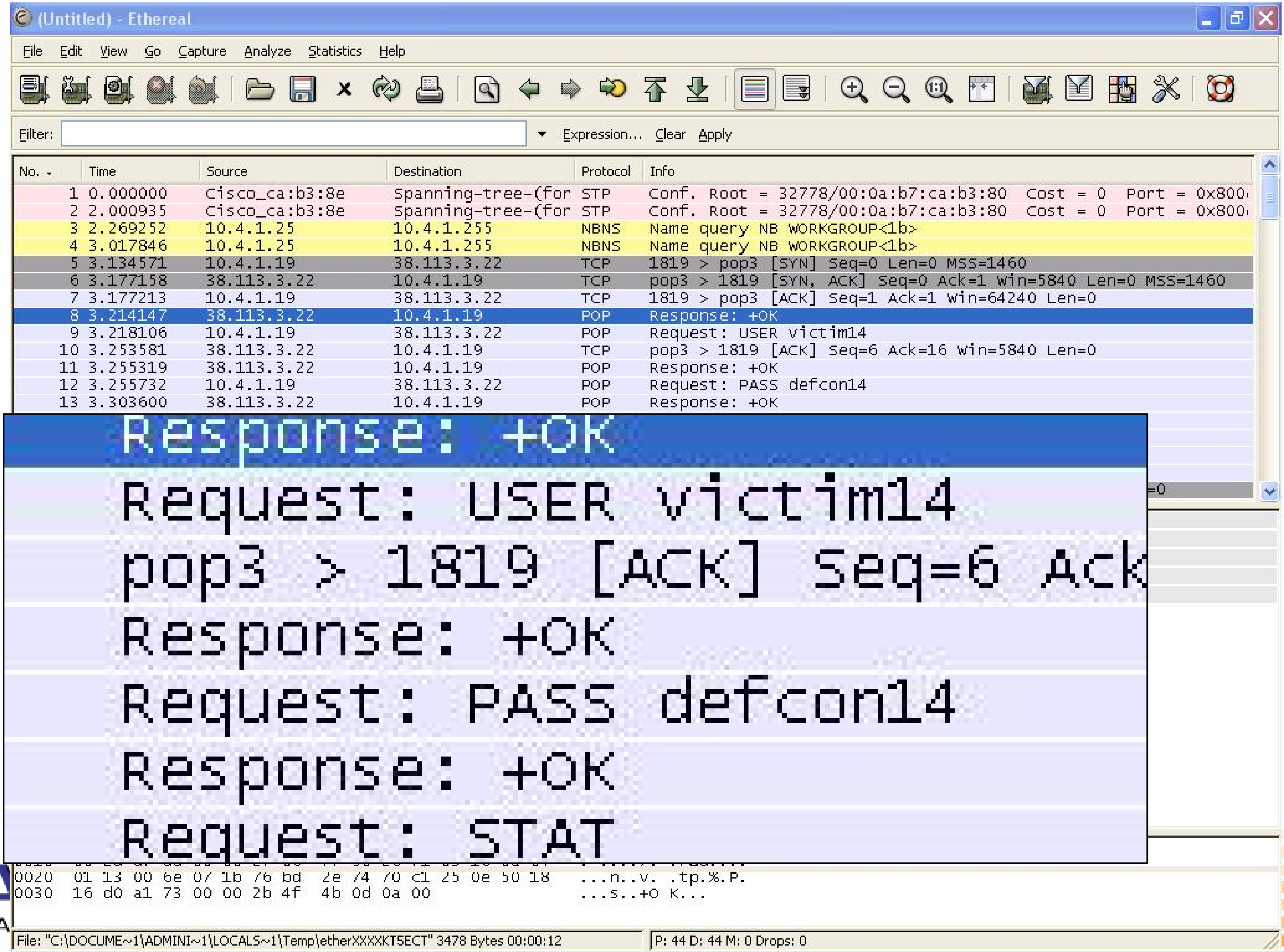
SMTP Commands

HELO	Used to initiate communication to an SMTP server
EHLO	Same as HELO
MAIL FROM:	Address you are sending e-mail from (easy to spoof!)
RCPT TO:	Destination of e-mail
SIZE=# *of bytes*	Not necessary. Specifies size of e-mail in bytes.
DATA	The message body. Terminated with a single period (.) on a line by itself.
QUIT	Terminates the SMTP session
VRFY *username*	Verify that a username is valid. Excellent way to enumerate users.
EXPN *name*	Like VRFY, can verify a username. EXPN can also list out all usernames in a distribution list.

Analysis of E-mail Traffic

- POP Commands (RFC 1225)
  - USER
  - PASS
  - QUIT
  - STAT
  - LIST
  - RETR
  - DELE
  - LAST
  - RSET

Analysis of E-mail Traffic



```
No. -  Time       Source             Destination         Protocol Info
     1 0.000000   Cisco_ca:b3:8e     Spanning-tree-(for  STP      Conf. Root = 32778/00:0a:b7:ca:b3:80  Cost = 0  Port = 0x800
     2 2.000935   Cisco_ca:b3:8e     Spanning-tree-(for  STP      Conf. Root = 32778/00:0a:b7:ca:b3:80  Cost = 0  Port = 0x800
     3 2.269252   10.4.1.25          10.4.1.255          NBNS     Name query NB WORKGROUP<1b>
     4 3.017846   10.4.1.25          10.4.1.255          NBNS     Name query NB WORKGROUP<1b>
     5 3.134571   10.4.1.19          38.113.3.22         TCP      1819 > pop3 [SYN] Seq=0 Len=0 MSS=1460
     6 3.177158   38.113.3.22        10.4.1.19           TCP      pop3 > 1819 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
     7 3.177213   10.4.1.19          38.113.3.22         TCP      1819 > pop3 [ACK] Seq=1 Ack=1 Win=64240 Len=0
     8 3.214147   38.113.3.22        10.4.1.19           POP      Response: +OK
     9 3.218106   10.4.1.19          38.113.3.22         POP      Request: USER victim14
    10 3.253581   38.113.3.22        10.4.1.19           TCP      pop3 > 1819 [ACK] Seq=6 Ack=16 Win=5840 Len=0
    11 3.255319   38.113.3.22        10.4.1.19           POP      Response: +OK
    12 3.255732   10.4.1.19          38.113.3.22         POP      Request: PASS defcon14
    13 3.303600   38.113.3.22        10.4.1.19           POP      Response: +OK
```

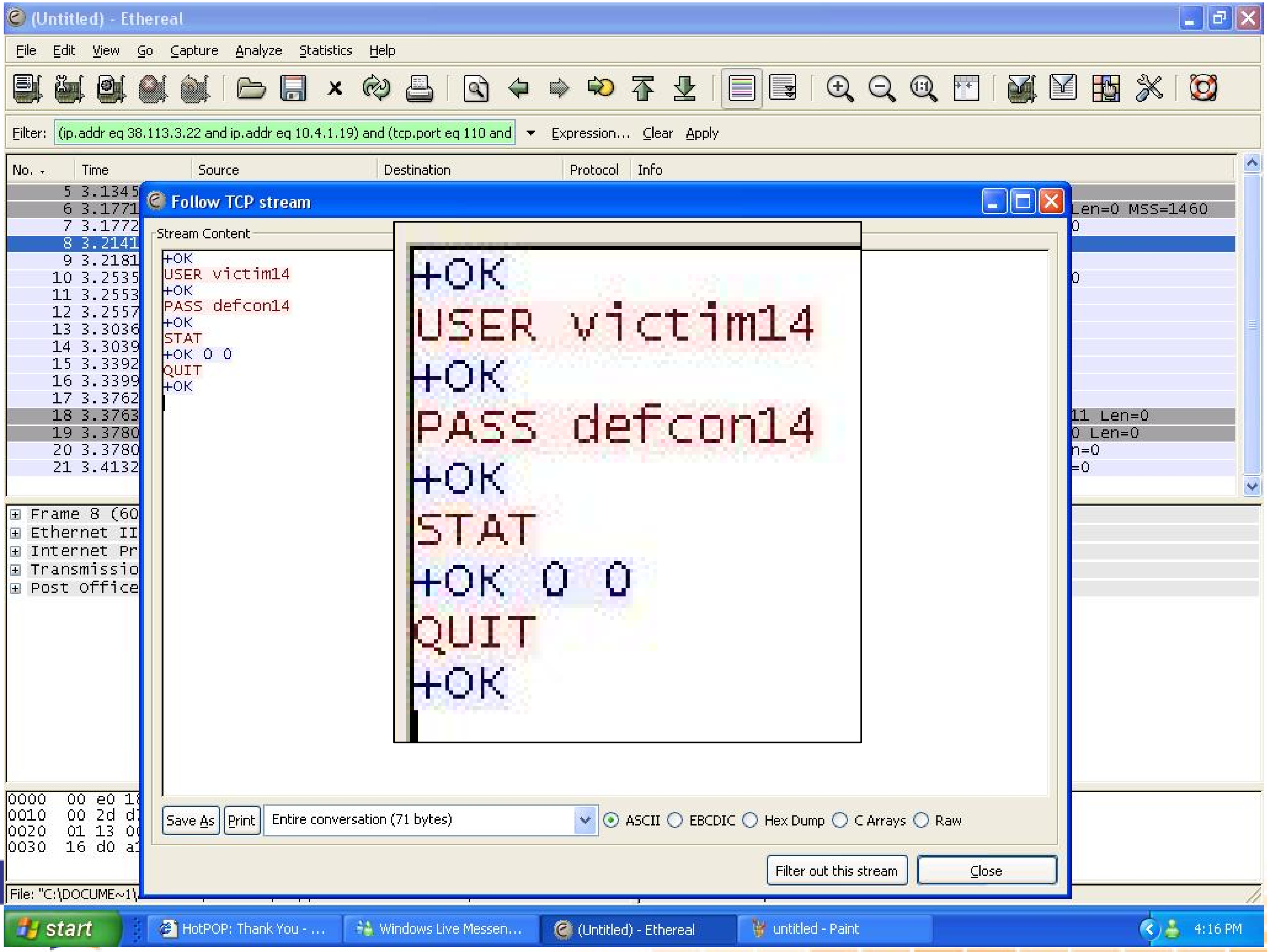
```
Response: +OK
Request: USER victim14
pop3 > 1819 [ACK] Seq=6 Ack
Response: +OK
Request: PASS defcon14
Response: +OK
Request: STAT
```

```
0020  01 13 00 6e 07 1b 76 bd  2e 74 70 c1 25 0e 50 18   ...n..v. .tp.%.P.
0030  16 d0 a1 73 00 00 2b 4f  4b 0d 0a 00               ...s..+O K...
```

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXXKT5ECT" 3478 Bytes 00:00:12

P: 44 D: 44 M: 0 Drops: 0

Analysis of E-mail Traffic



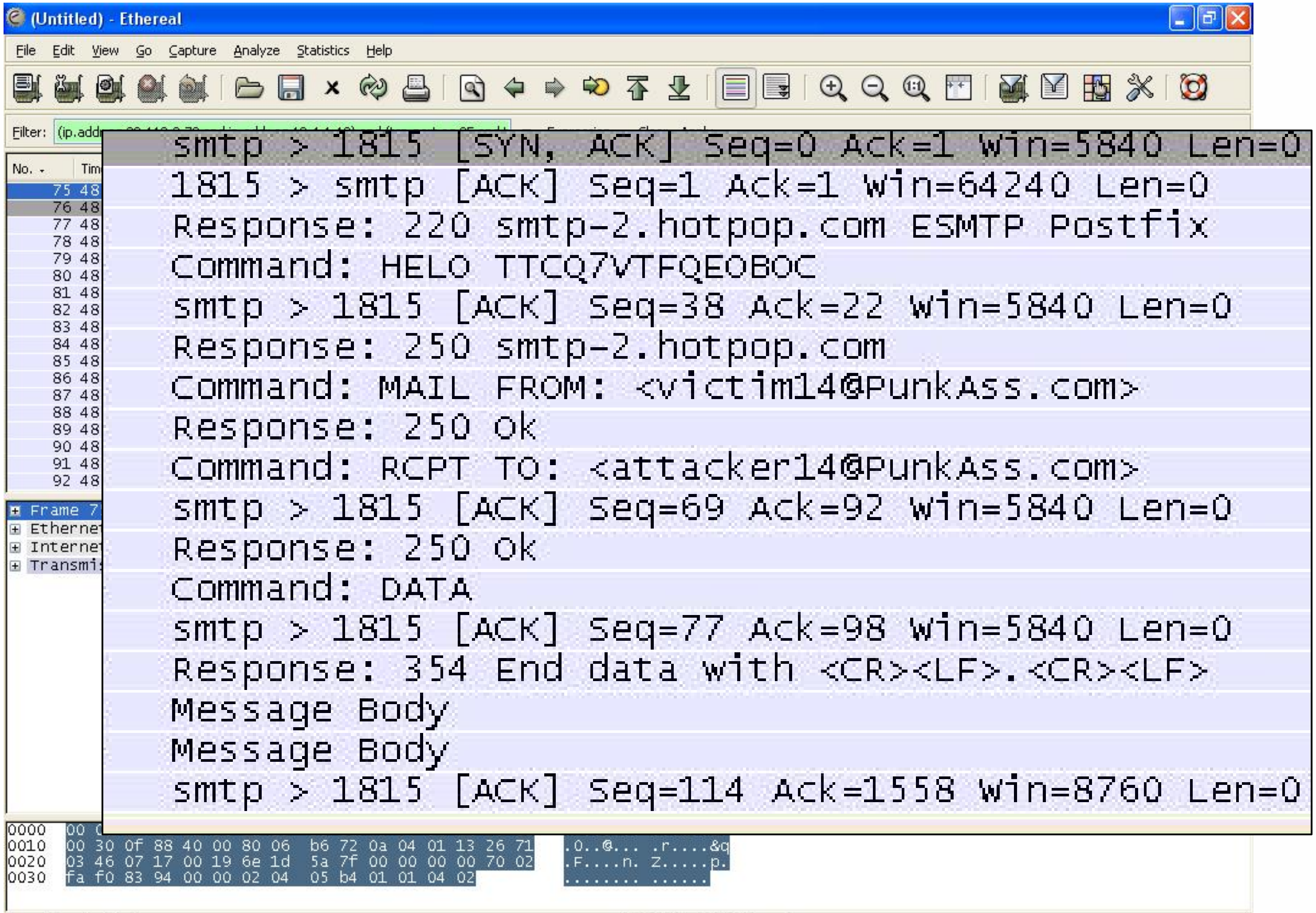
Filter: (ip.addr eq 38.113.3.22 and ip.addr eq 10.4.1.19) and (tcp.port eq 110 and

```
+OK
USER victim14
+OK
PASS defcon14
+OK
STAT
+OK 0 0
QUIT
+OK
```

Entire conversation (71 bytes)

● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw

Analysis of E-mail Traffic



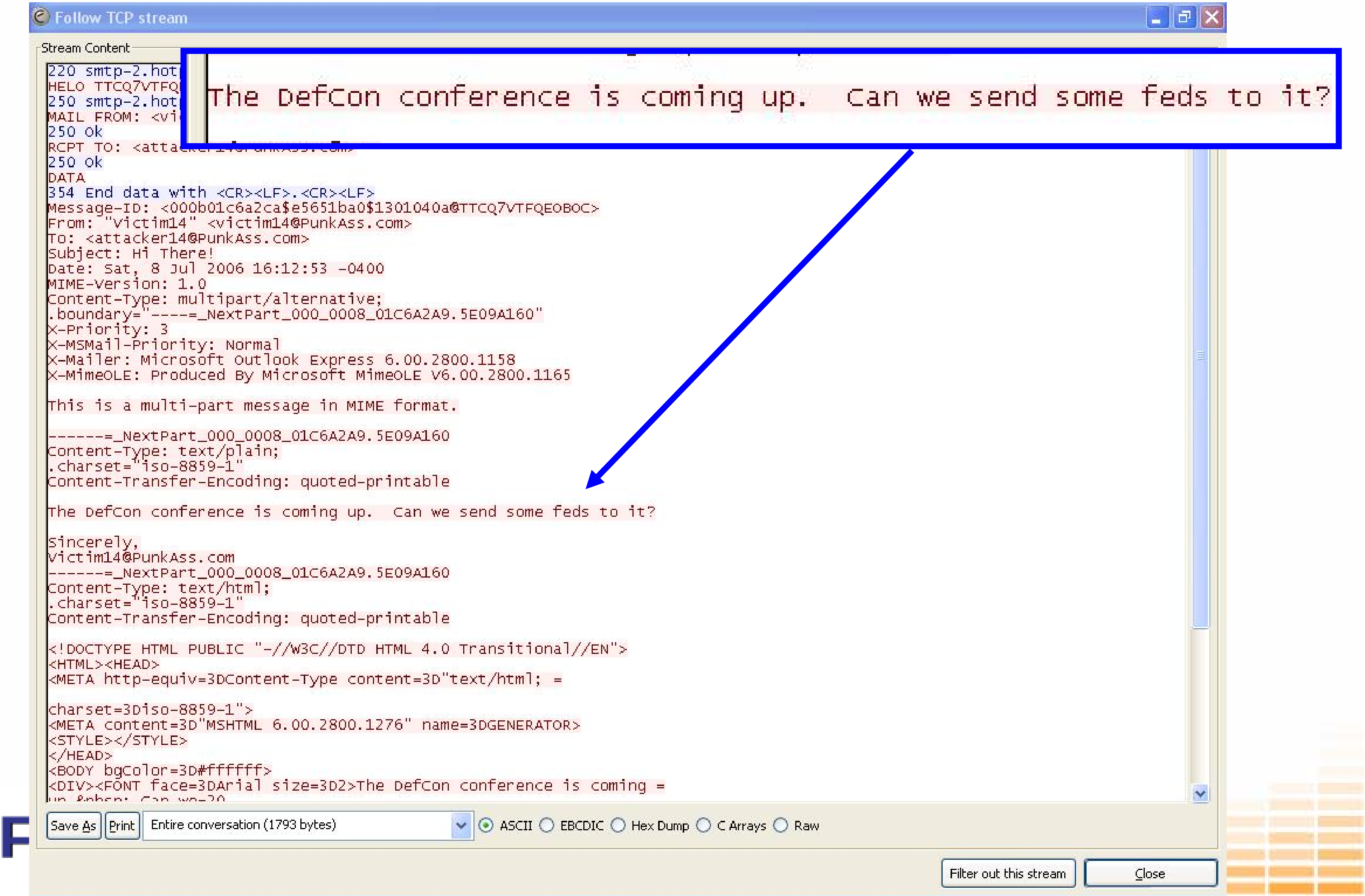
```
smtp > 1815 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
1815 > smtp [ACK] Seq=1 Ack=1 Win=64240 Len=0
Response: 220 smtp-2.hotpop.com ESMTP Postfix
Command: HELO TTCQ7VTFQEOBOC
smtp > 1815 [ACK] Seq=38 Ack=22 Win=5840 Len=0
Response: 250 smtp-2.hotpop.com
Command: MAIL FROM: <victim14@PunkAss.com>
Response: 250 Ok
Command: RCPT TO: <attacker14@PunkAss.com>
smtp > 1815 [ACK] Seq=69 Ack=92 Win=5840 Len=0
Response: 250 Ok
Command: DATA
smtp > 1815 [ACK] Seq=77 Ack=98 Win=5840 Len=0
Response: 354 End data with <CR><LF>.<CR><LF>
Message Body
Message Body
smtp > 1815 [ACK] Seq=114 Ack=1558 Win=8760 Len=0
```

```
0000   00 0
0010   00 30 0f 88 40 00 80 06  b6 72 0a 04 01 13 26 71   .0..@... .r....&q
0020   03 46 07 17 00 19 6e 1d  5a 7f 00 00 00 00 70 02   .F....n. Z.....p.
0030   fa f0 83 94 00 00 02 04  05 b4 01 01 04 02         ........ ......
```

Frame (frame), 62 bytes

P: 121 D: 28 M: 0 Drops: 0

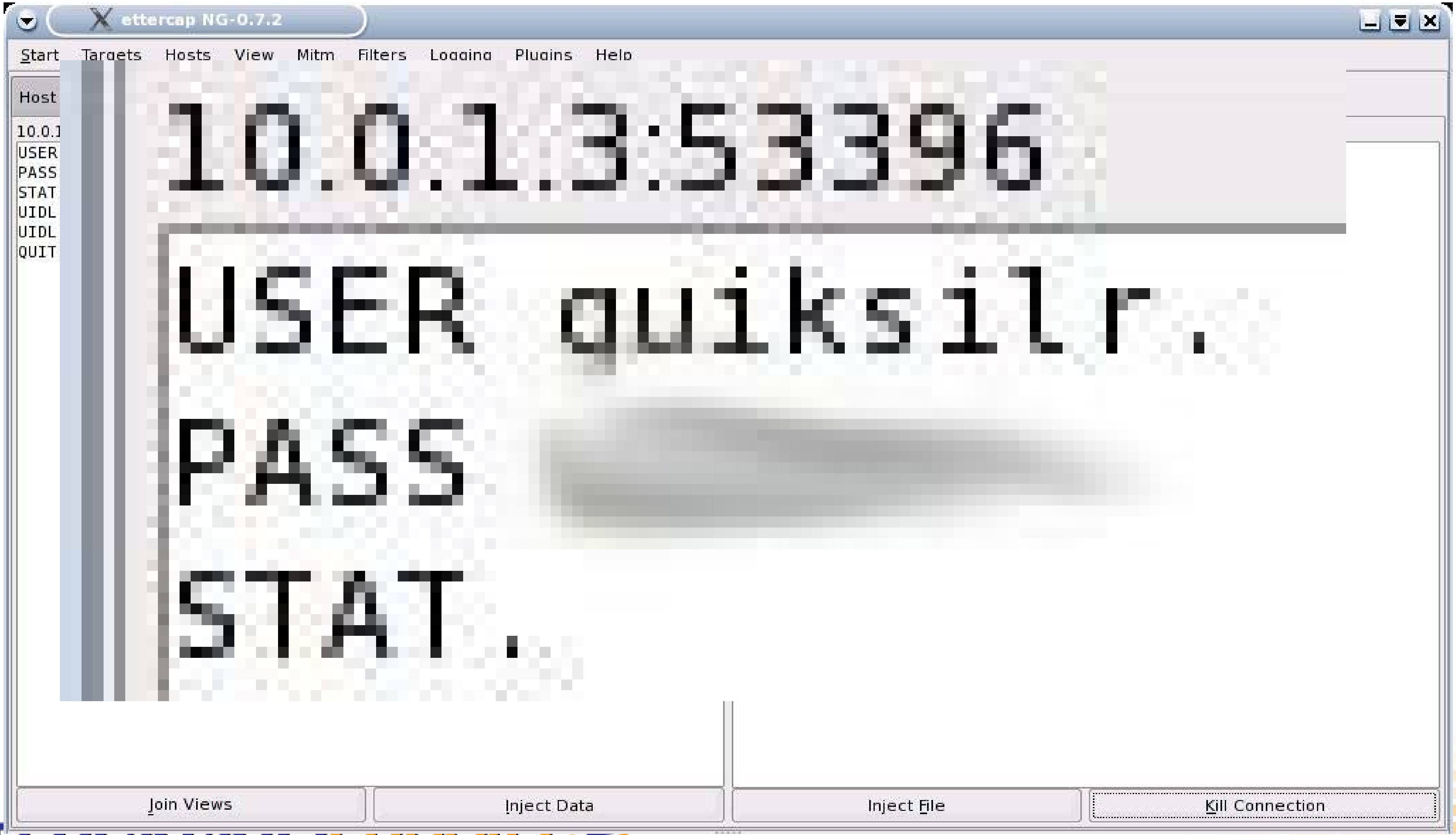
Analysis of E-mail Traffic



The DefCon conference is coming up. Can we send some feds to it?

```
220 smtp-2.hot
HELO TTCQ7VTFQ
250 smtp-2.hot
MAIL FROM: <vi
250 ok
RCPT TO: <atta
250 ok
DATA
354 End data with <CR><LF>.<CR><LF>
Message-ID: <000b01c6a2ca$e5651ba0$1301040a@TTCQ7VTFQEOBOC>
From: "victim14" <victim14@PunkAss.com>
To: <attacker14@PunkAss.com>
Subject: Hi There!
Date: Sat, 8 Jul 2006 16:12:53 -0400
MIME-Version: 1.0
Content-Type: multipart/alternative;
.boundary="----=_NextPart_000_0008_01C6A2A9.5E09A160"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1158
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165

This is a multi-part message in MIME format.

------=_NextPart_000_0008_01C6A2A9.5E09A160
Content-Type: text/plain;
.charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

The DefCon conference is coming up.  Can we send some feds to it?

Sincerely,
Victim14@PunkAss.com
------=_NextPart_000_0008_01C6A2A9.5E09A160
Content-Type: text/html;
.charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; =

charset=3Diso-8859-1">
<META content=3D"MSHTML 6.00.2800.1276" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV><FONT face=3DArial size=3D2>The DefCon conference is coming =
```

Analysis of E-mail Traffic:Ettercap



```
10.0.1
USER
PASS
STAT
UIDL
UIDL
QUIT
```

```
10.0.1.3:53396
USER quiksilr.
PASS [redacted]
STAT.
```

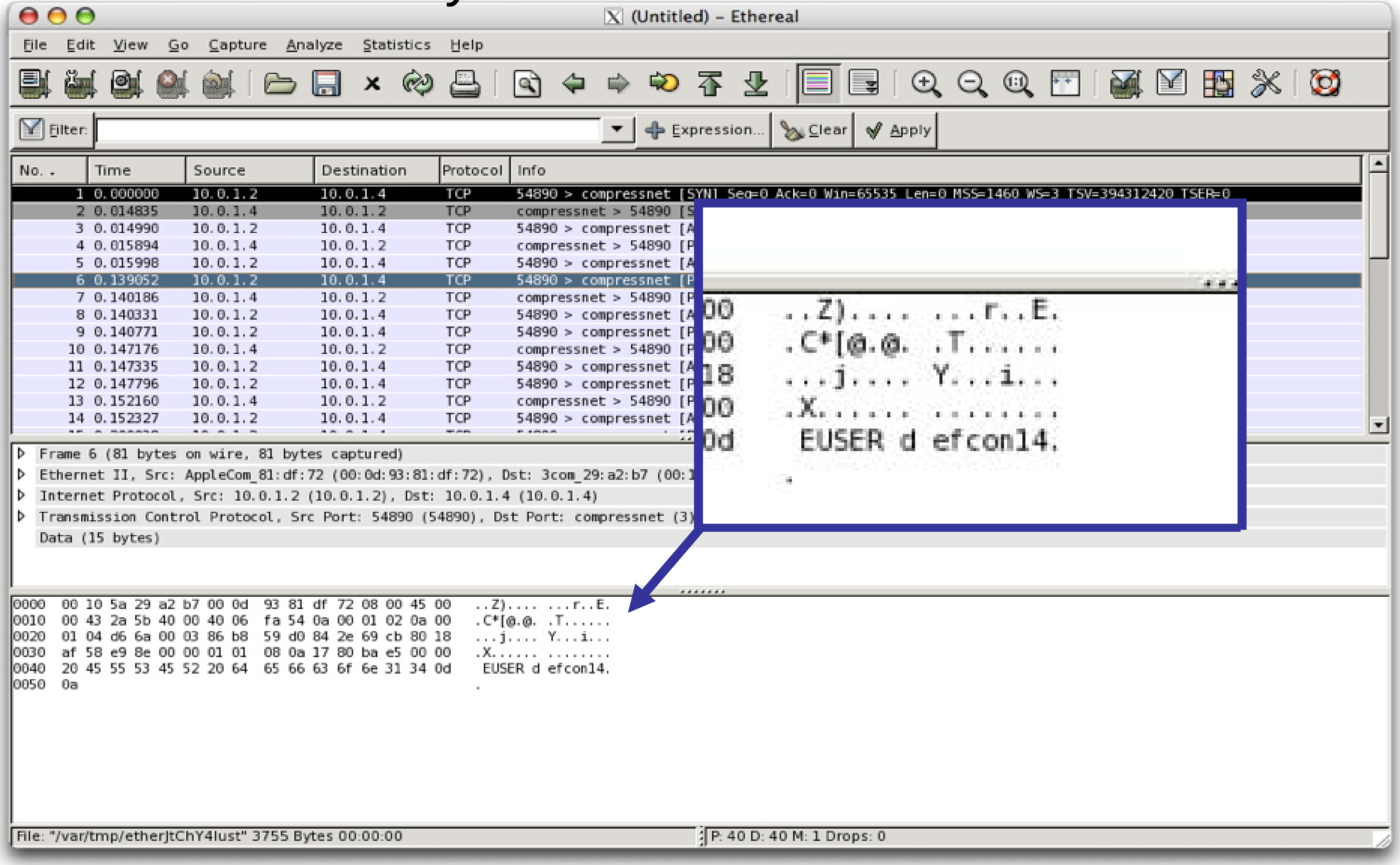
Tool: Mailsnarf

- Part of Dsniff: http://www.monkey.org/~dugsong/dsniff/
- Dug Song
- Listens only for e-mail

Tool: Mailsnarf

```
root@1[ettercap]# mailsnarf
mailsnarf: listening on eth0
Mime-Version: 1.0 (Apple Message framework v752.2)
To: David Williams [redacted]
Message-Id: <E7819150-0632-42A5-B70B-F447CF313500@trainingcamp.net>
Content-Type: multipart/alternative; boundary=Apple-Mail-4-218664851
From: David Williams [redacted]
Subject: Defcon 14  Mailsnarf
Date: Sun, 9 Jul 2006 15:07:20 -0400
X-Mailer: Apple Mail (2.752.2)

Testing Mail Snarf


David Williams
Information Systems Support Specialist

Tech Train | The Training Camp | Infosec Academy
Visit our website at http://www.trainingcamp.net
```

Analysis of FTP Traffic



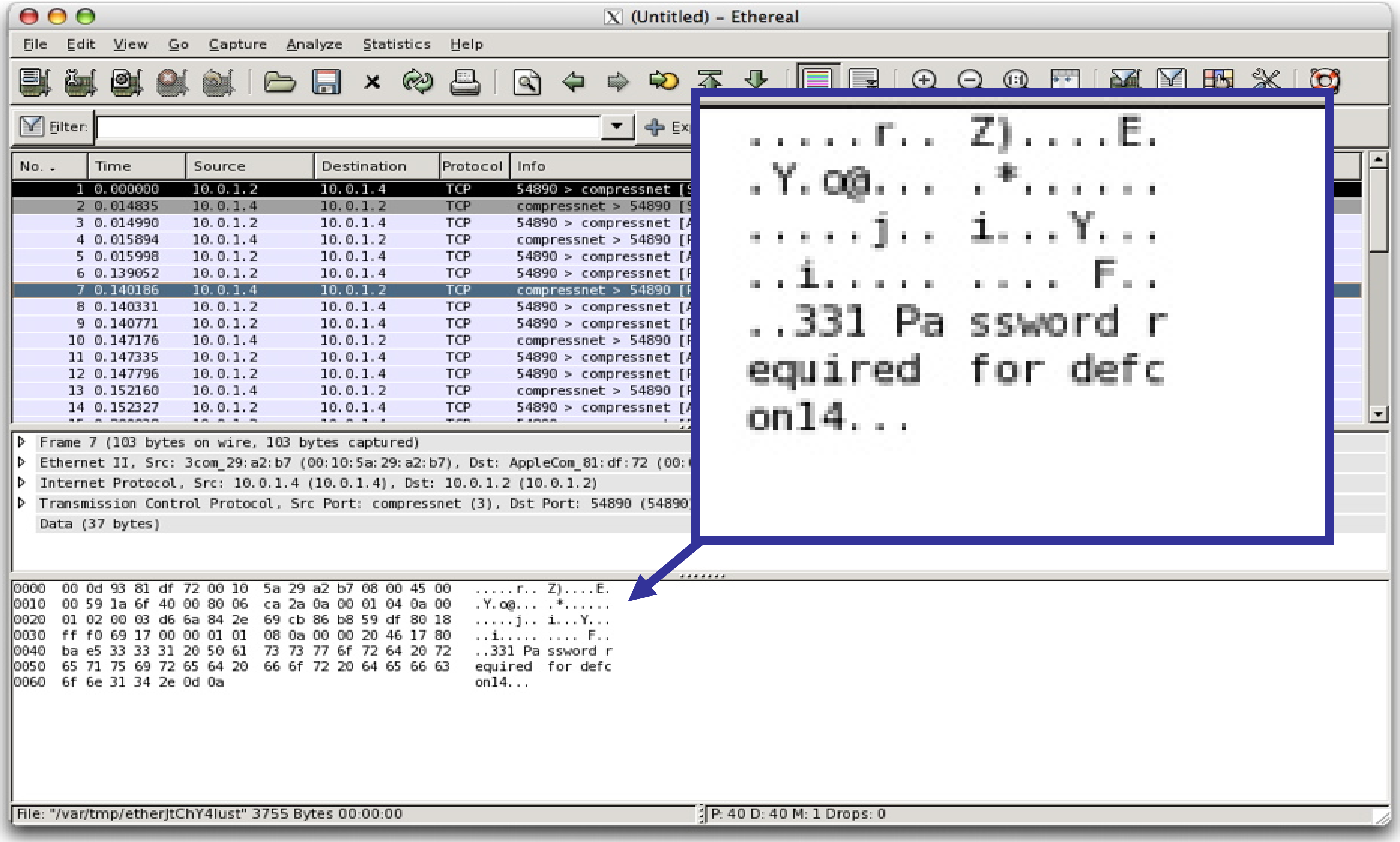
```
No. .  Time       Source      Destination  Protocol  Info
    1  0.000000   10.0.1.2    10.0.1.4     TCP       54890 > compressnet [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460 WS=3 TSV=394312420 TSER=0
    2  0.014835   10.0.1.4    10.0.1.2     TCP       compressnet > 54890 [S
    3  0.014990   10.0.1.2    10.0.1.4     TCP       54890 > compressnet [A
    4  0.015894   10.0.1.4    10.0.1.2     TCP       compressnet > 54890 [P
    5  0.015998   10.0.1.2    10.0.1.4     TCP       54890 > compressnet [A
    6  0.139052   10.0.1.2    10.0.1.4     TCP       54890 > compressnet [P
    7  0.140186   10.0.1.4    10.0.1.2     TCP       compressnet > 54890 [P
    8  0.140331   10.0.1.2    10.0.1.4     TCP       54890 > compressnet [A
    9  0.140771   10.0.1.2    10.0.1.4     TCP       54890 > compressnet [P
   10  0.147176   10.0.1.4    10.0.1.2     TCP       compressnet > 54890 [P
   11  0.147335   10.0.1.2    10.0.1.4     TCP       54890 > compressnet [A
   12  0.147796   10.0.1.2    10.0.1.4     TCP       54890 > compressnet [P
   13  0.152160   10.0.1.4    10.0.1.2     TCP       compressnet > 54890 [P
   14  0.152327   10.0.1.2    10.0.1.4     TCP       54890 > compressnet [A
```

```
▷ Frame 6 (81 bytes on wire, 81 bytes captured)
▷ Ethernet II, Src: AppleCom_81:df:72 (00:0d:93:81:df:72), Dst: 3com_29:a2:b7 (00:1
▷ Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.1.4 (10.0.1.4)
▷ Transmission Control Protocol, Src Port: 54890 (54890), Dst Port: compressnet (3)
  Data (15 bytes)
```

```
0000  00 10 5a 29 a2 b7 00 0d  93 81 df 72 08 00 45 00   ..Z).... ...r..E.
0010  00 43 2a 5b 40 00 40 06  fa 54 0a 00 01 02 0a 00   .C*[@.@. .T......
0020  01 04 d6 6a 00 03 86 b8  59 d0 84 2e 69 cb 80 18   ...j.... Y...i...
0030  af 58 e9 8e 00 00 01 01  08 0a 17 80 ba e5 00 00   .X...... ........
0040  20 45 55 53 45 52 20 64  65 66 63 6f 6e 31 34 0d    EUSER d efcon14.
0050  0a                                                 .
```

```
File: "/var/tmp/etherJtChY4lust" 3755 Bytes 00:00:00    P: 40 D: 40 M: 1 Drops: 0
```

Analysis of FTP Traffic



```
No. .   Time      Source     Destination  Protocol  Info
    1 0.000000   10.0.1.2   10.0.1.4     TCP       54890 > compressnet [
    2 0.014835   10.0.1.4   10.0.1.2     TCP       compressnet > 54890 [
    3 0.014990   10.0.1.2   10.0.1.4     TCP       54890 > compressnet [
    4 0.015894   10.0.1.4   10.0.1.2     TCP       compressnet > 54890 [
    5 0.015998   10.0.1.2   10.0.1.4     TCP       54890 > compressnet [
    6 0.139052   10.0.1.2   10.0.1.4     TCP       54890 > compressnet [
    7 0.140186   10.0.1.4   10.0.1.2     TCP       compressnet > 54890 [
    8 0.140331   10.0.1.2   10.0.1.4     TCP       54890 > compressnet [
    9 0.140771   10.0.1.2   10.0.1.4     TCP       54890 > compressnet [
   10 0.147176   10.0.1.4   10.0.1.2     TCP       compressnet > 54890 [
   11 0.147335   10.0.1.2   10.0.1.4     TCP       54890 > compressnet [
   12 0.147796   10.0.1.2   10.0.1.4     TCP       54890 > compressnet [
   13 0.152160   10.0.1.4   10.0.1.2     TCP       compressnet > 54890 [
   14 0.152327   10.0.1.2   10.0.1.4     TCP       54890 > compressnet [
```

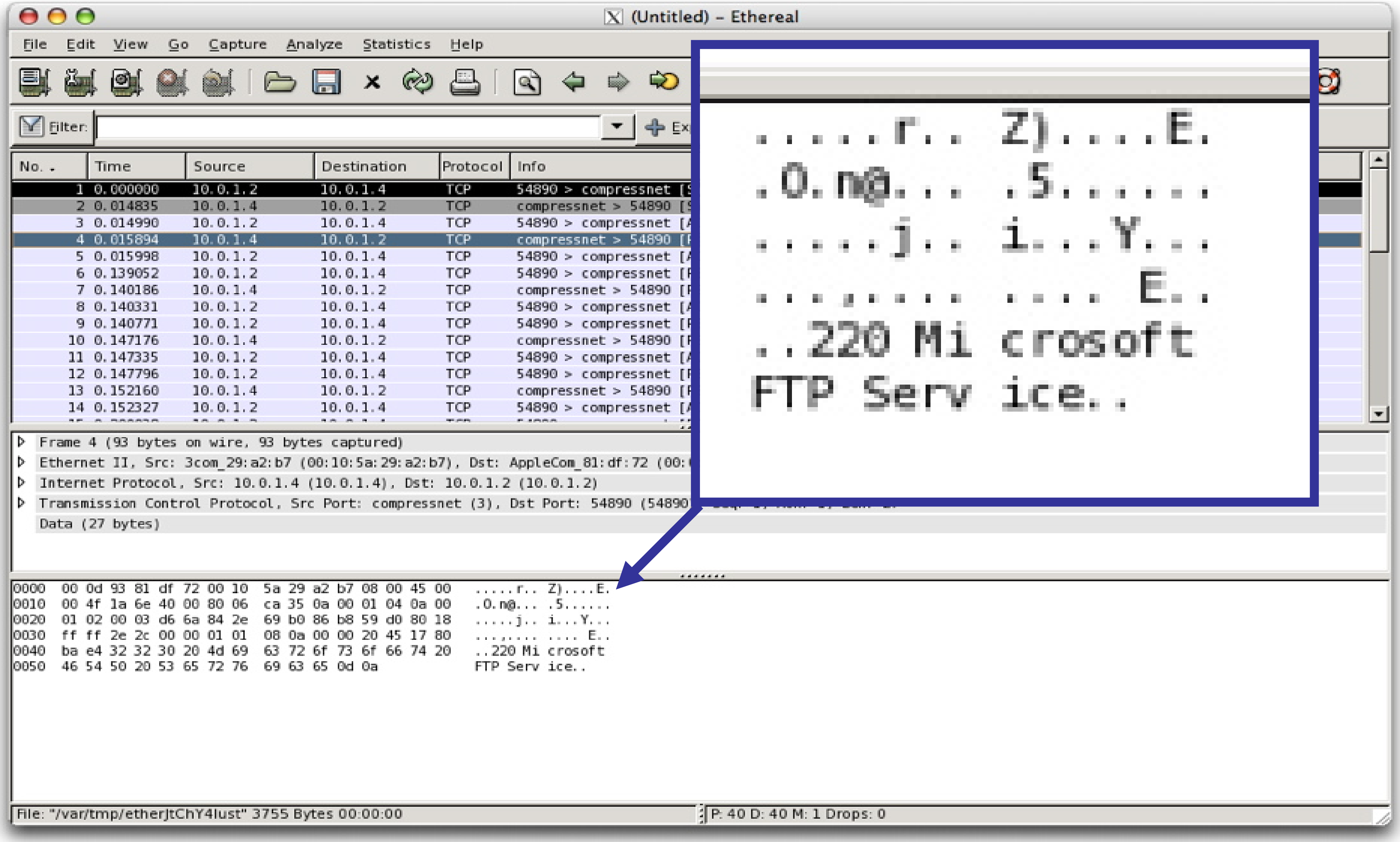
```
▷ Frame 7 (103 bytes on wire, 103 bytes captured)
▷ Ethernet II, Src: 3com_29:a2:b7 (00:10:5a:29:a2:b7), Dst: AppleCom_81:df:72 (00:
▷ Internet Protocol, Src: 10.0.1.4 (10.0.1.4), Dst: 10.0.1.2 (10.0.1.2)
▷ Transmission Control Protocol, Src Port: compressnet (3), Dst Port: 54890 (54890)
  Data (37 bytes)
```

```
0000  00 0d 93 81 df 72 00 10  5a 29 a2 b7 08 00 45 00   .....r.. Z)....E.
0010  00 59 1a 6f 40 00 80 06  ca 2a 0a 00 01 04 0a 00   .Y.o@... .*......
0020  01 02 00 03 d6 6a 84 2e  69 cb 86 b8 59 df 80 18   .....j.. i...Y...
0030  ff f0 69 17 00 00 01 01  08 0a 00 00 20 46 17 80   ..i..... .... F..
0040  ba e5 33 33 31 20 50 61  73 73 77 6f 72 64 20 72   ..331 Pa ssword r
0050  65 71 75 69 72 65 64 20  66 6f 72 20 64 65 66 63   equired  for defc
0060  6f 6e 31 34 2e 0d 0a                              on14...
```

```
.....r.. Z)....E.
.Y.o@... .*......
.....j.. i...Y...
..i..... .... F..
..331 Pa ssword r
equired  for defc
on14...
```

```
File: "/var/tmp/etherJtChY4lust" 3755 Bytes 00:00:00    P: 40 D: 40 M: 1 Drops: 0
```

Analysis of FTP Traffic



No. .	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.1.2	10.0.1.4	TCP	54890 > compressnet [
2	0.014835	10.0.1.4	10.0.1.2	TCP	compressnet > 54890 [
3	0.014990	10.0.1.2	10.0.1.4	TCP	54890 > compressnet [
4	0.015894	10.0.1.4	10.0.1.2	TCP	compressnet > 54890 [
5	0.015998	10.0.1.2	10.0.1.4	TCP	54890 > compressnet [
6	0.139052	10.0.1.2	10.0.1.4	TCP	54890 > compressnet [
7	0.140186	10.0.1.4	10.0.1.2	TCP	compressnet > 54890 [
8	0.140331	10.0.1.2	10.0.1.4	TCP	54890 > compressnet [
9	0.140771	10.0.1.2	10.0.1.4	TCP	54890 > compressnet [
10	0.147176	10.0.1.4	10.0.1.2	TCP	compressnet > 54890 [
11	0.147335	10.0.1.2	10.0.1.4	TCP	54890 > compressnet [
12	0.147796	10.0.1.2	10.0.1.4	TCP	54890 > compressnet [
13	0.152160	10.0.1.4	10.0.1.2	TCP	compressnet > 54890 [
14	0.152327	10.0.1.2	10.0.1.4	TCP	54890 > compressnet [

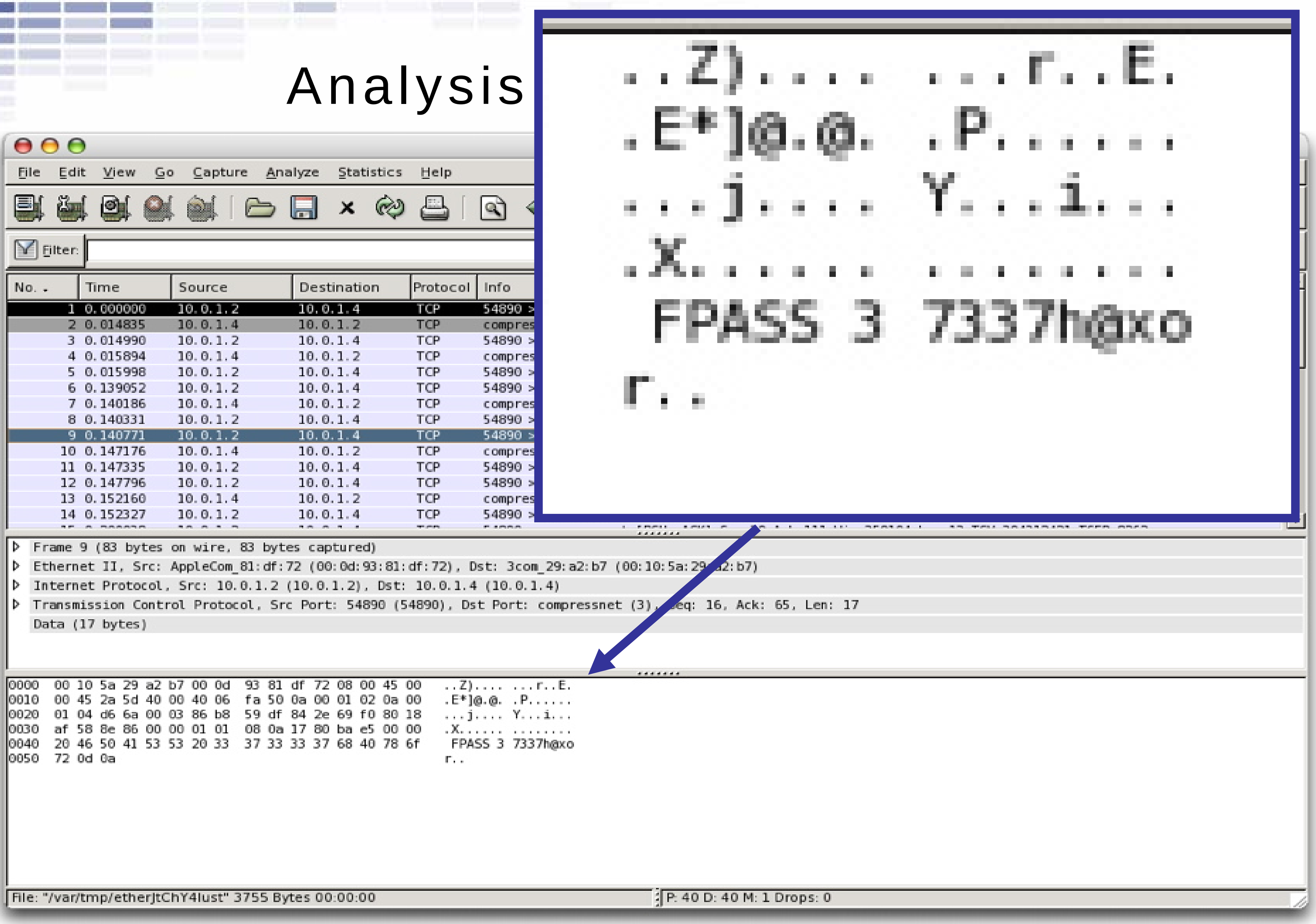
```
Frame 4 (93 bytes on wire, 93 bytes captured)
Ethernet II, Src: 3com_29:a2:b7 (00:10:5a:29:a2:b7), Dst: AppleCom_81:df:72 (00:
Internet Protocol, Src: 10.0.1.4 (10.0.1.4), Dst: 10.0.1.2 (10.0.1.2)
Transmission Control Protocol, Src Port: compressnet (3), Dst Port: 54890 (54890
  Data (27 bytes)
```

```
0000  00 0d 93 81 df 72 00 10  5a 29 a2 b7 08 00 45 00   .....r.. Z)....E.
0010  00 4f 1a 6e 40 00 80 06  ca 35 0a 00 01 04 0a 00   .O.n@... .5......
0020  01 02 00 03 d6 6a 84 2e  69 b0 86 b8 59 d0 80 18   .....j.. i...Y...
0030  ff ff 2e 2c 00 00 01 01  08 0a 00 00 20 45 17 80   ...,.... .... E..
0040  ba e4 32 32 30 20 4d 69  63 72 6f 73 6f 66 74 20   ..220 Mi crosoft 
0050  46 54 50 20 53 65 72 76  69 63 65 0d 0a            FTP Serv ice..
```

```
......r.. Z)....E.
.O.n@... .5......
.....j.. i...Y...
...,.... .... E..
..220 Mi crosoft
FTP Serv ice..
```

File: "/var/tmp/etherJtChY4lust" 3755 Bytes 00:00:00 | P: 40 D: 40 M: 1 Drops: 0

Analysis



```
No. .  Time      Source    Destination Protocol Info
    1  0.000000  10.0.1.2  10.0.1.4    TCP      54890 >
    2  0.014835  10.0.1.4  10.0.1.2    TCP      compres
    3  0.014990  10.0.1.2  10.0.1.4    TCP      54890 >
    4  0.015894  10.0.1.4  10.0.1.2    TCP      compres
    5  0.015998  10.0.1.2  10.0.1.4    TCP      54890 >
    6  0.139052  10.0.1.2  10.0.1.4    TCP      54890 >
    7  0.140186  10.0.1.4  10.0.1.2    TCP      compres
    8  0.140331  10.0.1.2  10.0.1.4    TCP      54890 >
    9  0.140771  10.0.1.2  10.0.1.4    TCP      54890 >
   10  0.147176  10.0.1.4  10.0.1.2    TCP      compres
   11  0.147335  10.0.1.2  10.0.1.4    TCP      54890 >
   12  0.147796  10.0.1.2  10.0.1.4    TCP      54890 >
   13  0.152160  10.0.1.4  10.0.1.2    TCP      compres
   14  0.152327  10.0.1.2  10.0.1.4    TCP      54890 >
```

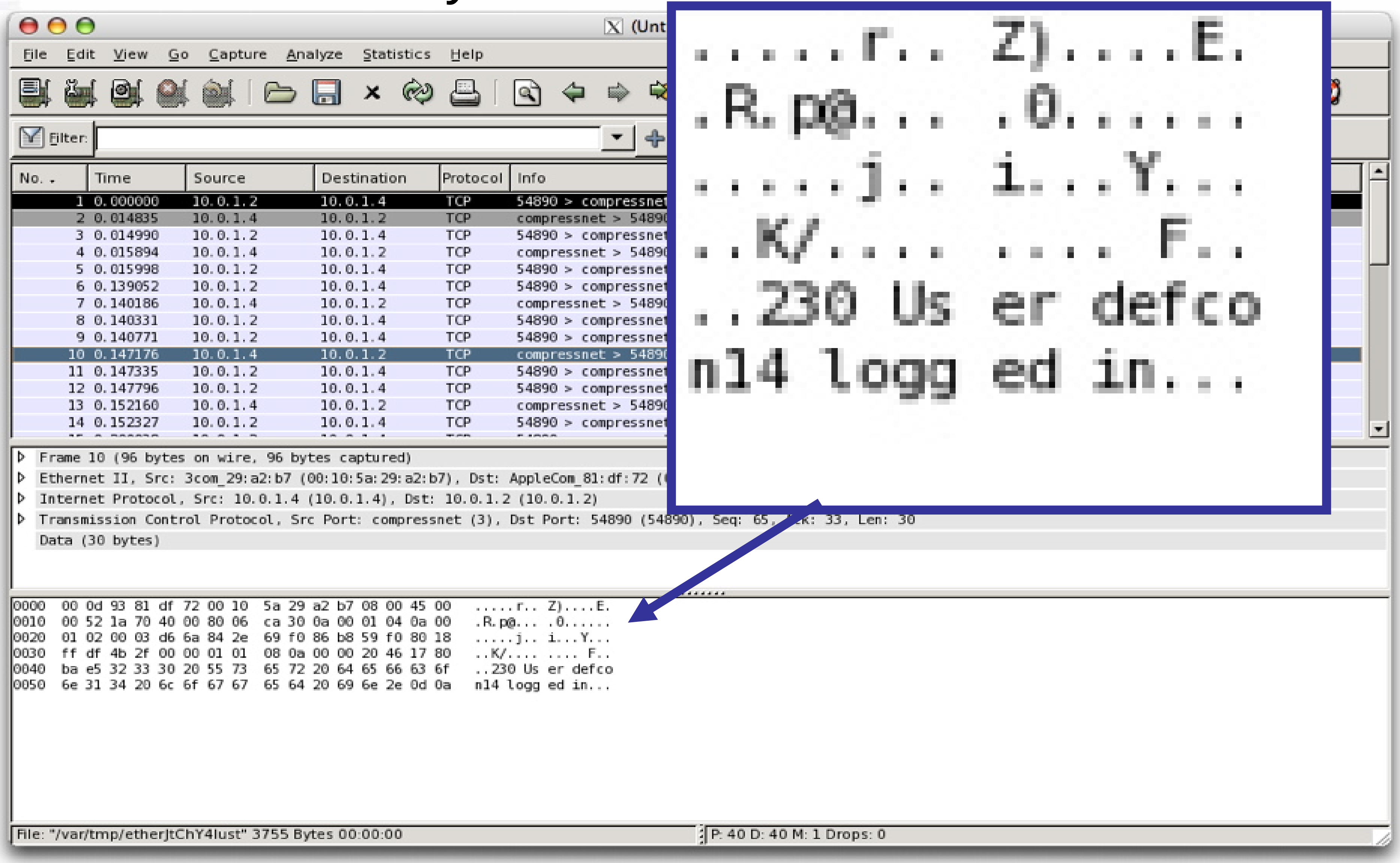
```
▷ Frame 9 (83 bytes on wire, 83 bytes captured)
▷ Ethernet II, Src: AppleCom_81:df:72 (00:0d:93:81:df:72), Dst: 3com_29:a2:b7 (00:10:5a:29:a2:b7)
▷ Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.1.4 (10.0.1.4)
▷ Transmission Control Protocol, Src Port: 54890 (54890), Dst Port: compressnet (3), Seq: 16, Ack: 65, Len: 17
  Data (17 bytes)
```

```
0000  00 10 5a 29 a2 b7 00 0d  93 81 df 72 08 00 45 00   ..Z).... ...r..E.
0010  00 45 2a 5d 40 00 40 06  fa 50 0a 00 01 02 0a 00   .E*]@.@. .P......
0020  01 04 d6 6a 00 03 86 b8  59 df 84 2e 69 f0 80 18   ...j.... Y...i...
0030  af 58 8e 86 00 00 01 01  08 0a 17 80 ba e5 00 00   .X...... ........
0040  20 46 50 41 53 53 20 33  37 33 33 37 68 40 78 6f    FPASS 3 7337h@xo
0050  72 0d 0a                                           r..
```

File: "/var/tmp/etherJtChY4lust" 3755 Bytes 00:00:00 | P: 40 D: 40 M: 1 Drops: 0

```
..Z).... ...r..E.
.E*]@.@. .P......
...j.... Y...i...
.X...... ........
 FPASS 3 7337h@xo
r..
```

Analysis of FTP Traffic



```
No. .  Time      Source    Destination Protocol Info
     1 0.000000  10.0.1.2  10.0.1.4    TCP      54890 > compressnet
     2 0.014835  10.0.1.4  10.0.1.2    TCP      compressnet > 5489
     3 0.014990  10.0.1.2  10.0.1.4    TCP      54890 > compressnet
     4 0.015894  10.0.1.4  10.0.1.2    TCP      compressnet > 5489
     5 0.015998  10.0.1.2  10.0.1.4    TCP      54890 > compressnet
     6 0.139052  10.0.1.2  10.0.1.4    TCP      54890 > compressnet
     7 0.140186  10.0.1.4  10.0.1.2    TCP      compressnet > 5489
     8 0.140331  10.0.1.2  10.0.1.4    TCP      54890 > compressnet
     9 0.140771  10.0.1.2  10.0.1.4    TCP      54890 > compressnet
    10 0.147176  10.0.1.4  10.0.1.2    TCP      compressnet > 5489
    11 0.147335  10.0.1.2  10.0.1.4    TCP      54890 > compressnet
    12 0.147796  10.0.1.2  10.0.1.4    TCP      54890 > compressnet
    13 0.152160  10.0.1.4  10.0.1.2    TCP      compressnet > 5489
    14 0.152327  10.0.1.2  10.0.1.4    TCP      54890 > compressnet
```

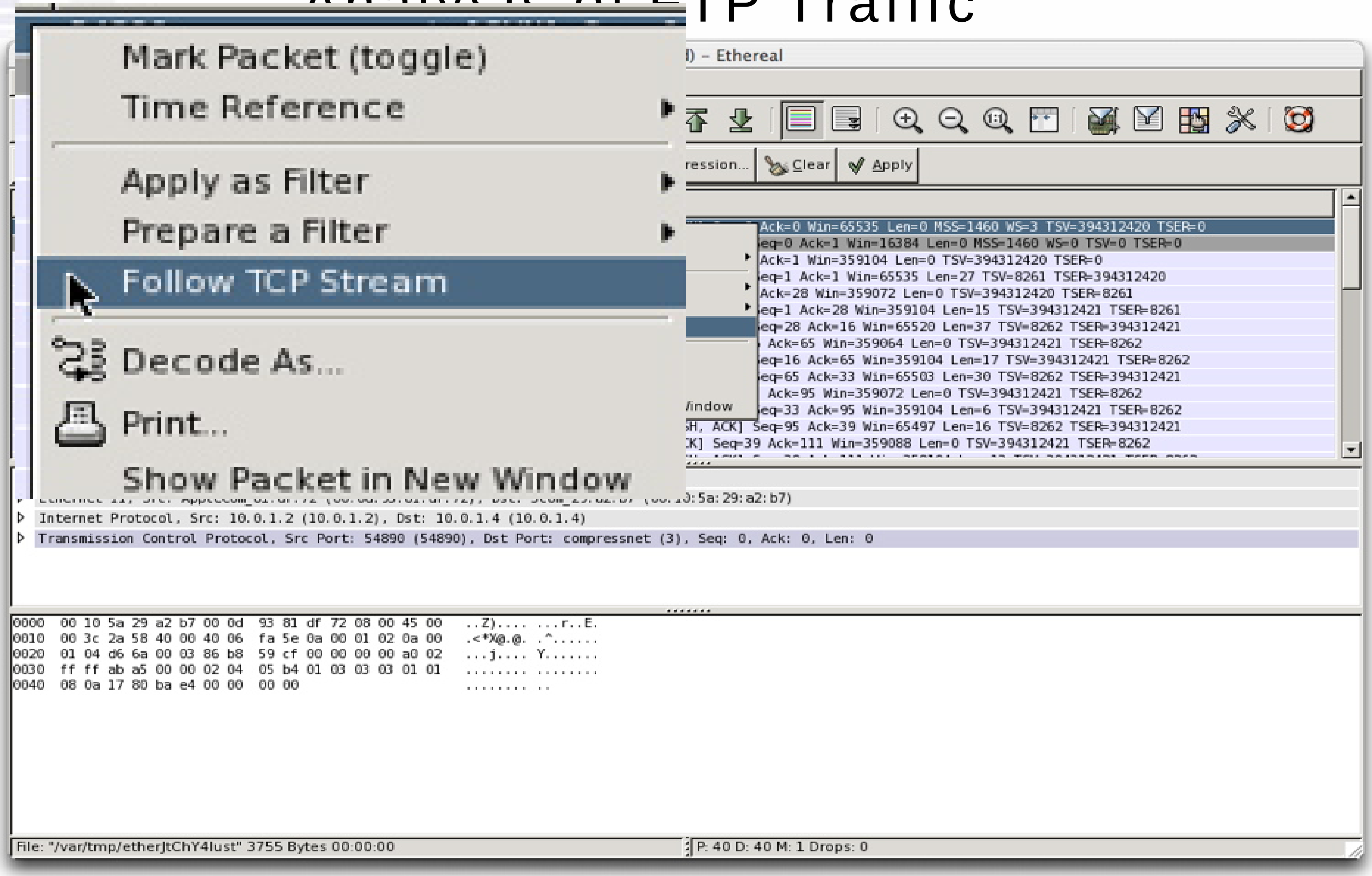
```
▷ Frame 10 (96 bytes on wire, 96 bytes captured)
▷ Ethernet II, Src: 3com_29:a2:b7 (00:10:5a:29:a2:b7), Dst: AppleCom_81:df:72 (
▷ Internet Protocol, Src: 10.0.1.4 (10.0.1.4), Dst: 10.0.1.2 (10.0.1.2)
▷ Transmission Control Protocol, Src Port: compressnet (3), Dst Port: 54890 (54890), Seq: 65, Ack: 33, Len: 30
  Data (30 bytes)
```

```
0000  00 0d 93 81 df 72 00 10  5a 29 a2 b7 08 00 45 00   .....r.. Z)....E.
0010  00 52 1a 70 40 00 80 06  ca 30 0a 00 01 04 0a 00   .R.p@... .0......
0020  01 02 00 03 d6 6a 84 2e  69 f0 86 b8 59 f0 80 18   .....j.. i...Y...
0030  ff df 4b 2f 00 00 01 01  08 0a 00 00 20 46 17 80   ..K/.... .... F..
0040  ba e5 32 33 30 20 55 73  65 72 20 64 65 66 63 6f   ..230 Us er defco
0050  6e 31 34 20 6c 6f 67 67  65 64 20 69 6e 2e 0d 0a   n14 logg ed in...
```

```
.....r.. Z)....E.
.R.p@... .0......
.....j.. i...Y...
..K/.... .... F..
..230 Us er defco
n14 logg ed in...
```

```
File: "/var/tmp/etherJtChY4lust" 3755 Bytes 00:00:00
P: 40 D: 40 M: 1 Drops: 0
```

Analysis of FTP Traffic



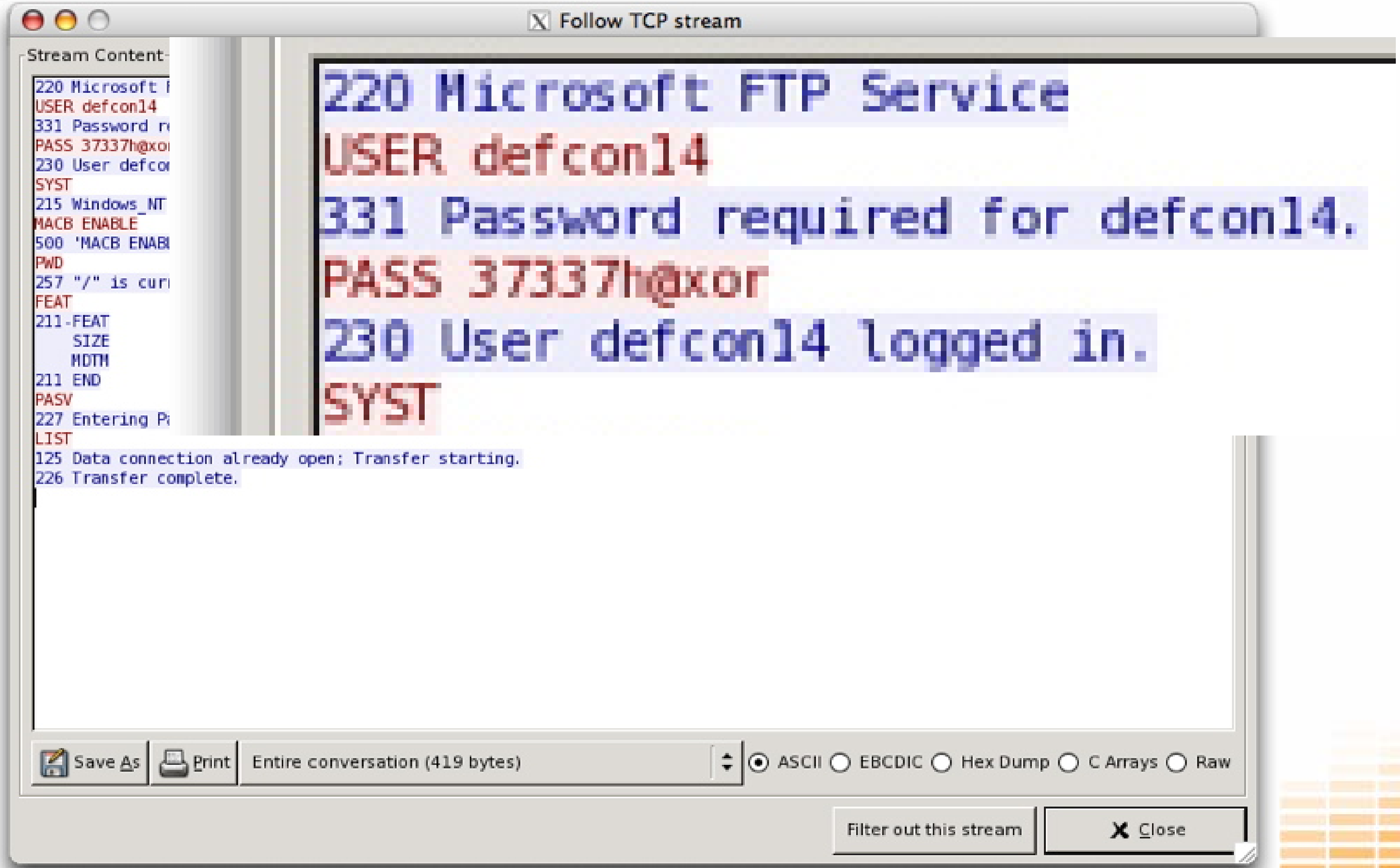
```
 Ack=0 Win=65535 Len=0 MSS=1460 WS=3 TSV=394312420 TSER=0
eq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
 Ack=1 Win=359104 Len=0 TSV=394312420 TSER=0
eq=1 Ack=1 Win=65535 Len=27 TSV=8261 TSER=394312420
 Ack=28 Win=359072 Len=0 TSV=394312420 TSER=8261
eq=1 Ack=28 Win=359104 Len=15 TSV=394312421 TSER=8261
eq=28 Ack=16 Win=65520 Len=37 TSV=8262 TSER=394312421
 Ack=65 Win=359064 Len=0 TSV=394312421 TSER=8262
eq=16 Ack=65 Win=359104 Len=17 TSV=394312421 TSER=8262
eq=65 Ack=33 Win=65503 Len=30 TSV=8262 TSER=394312421
 Ack=95 Win=359072 Len=0 TSV=394312421 TSER=8262
eq=33 Ack=95 Win=359104 Len=6 TSV=394312421 TSER=8262
H, ACK] Seq=95 Ack=39 Win=65497 Len=16 TSV=8262 TSER=394312421
K] Seq=39 Ack=111 Win=359088 Len=0 TSV=394312421 TSER=8262
```

```
:5a:29:a2:b7)
Internet Protocol, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.1.4 (10.0.1.4)
Transmission Control Protocol, Src Port: 54890 (54890), Dst Port: compressnet (3), Seq: 0, Ack: 0, Len: 0
```

```
0000  00 10 5a 29 a2 b7 00 0d  93 81 df 72 08 00 45 00   ..Z).... ...r..E.
0010  00 3c 2a 58 40 00 40 06  fa 5e 0a 00 01 02 0a 00   .<*X@.@. .^......
0020  01 04 d6 6a 00 03 86 b8  59 cf 00 00 00 00 a0 02   ...j.... Y.......
0030  ff ff ab a5 00 00 02 04  05 b4 01 03 03 03 01 01   ........ ........
0040  08 0a 17 80 ba e4 00 00  00 00                     ........ ..
```

```
File: "/var/tmp/etherJtChY4lust" 3755 Bytes 00:00:00
P: 40 D: 40 M: 1 Drops: 0
```

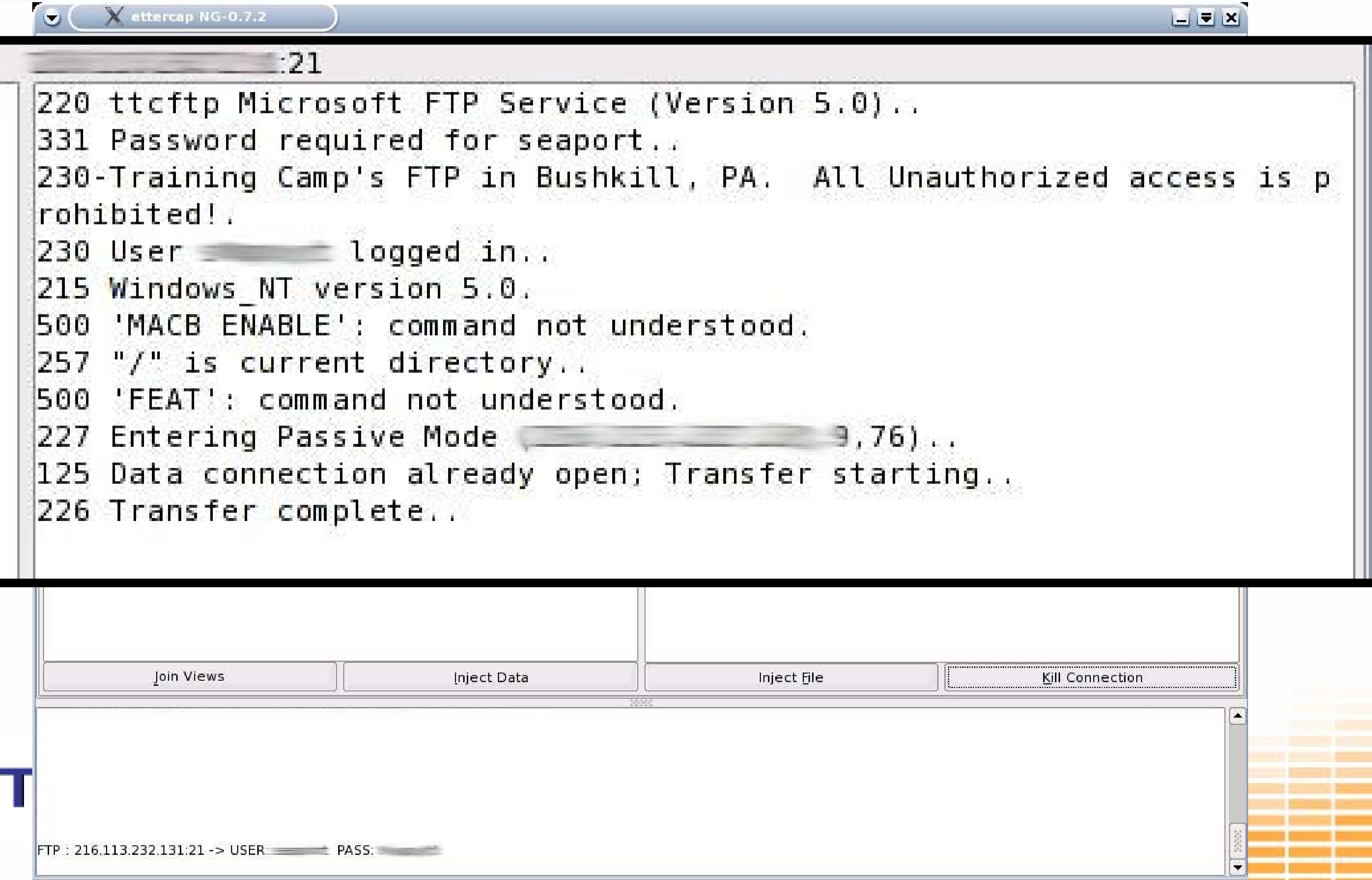
Analysis of FTP Traffic



```
220 Microsoft FTP Service
USER defcon14
331 Password required for defcon14.
PASS 37337h@xor
230 User defcon14 logged in.
SYST
```

```
220 Microsoft F
USER defcon14
331 Password re
PASS 37337h@xor
230 User defcon
SYST
215 Windows_NT
MACB ENABLE
500 'MACB ENABL
PWD
257 "/" is curr
FEAT
211-FEAT
    SIZE
    MDTM
211 END
PASV
227 Entering Pa
LIST
125 Data connection already open; Transfer starting.
226 Transfer complete.
```

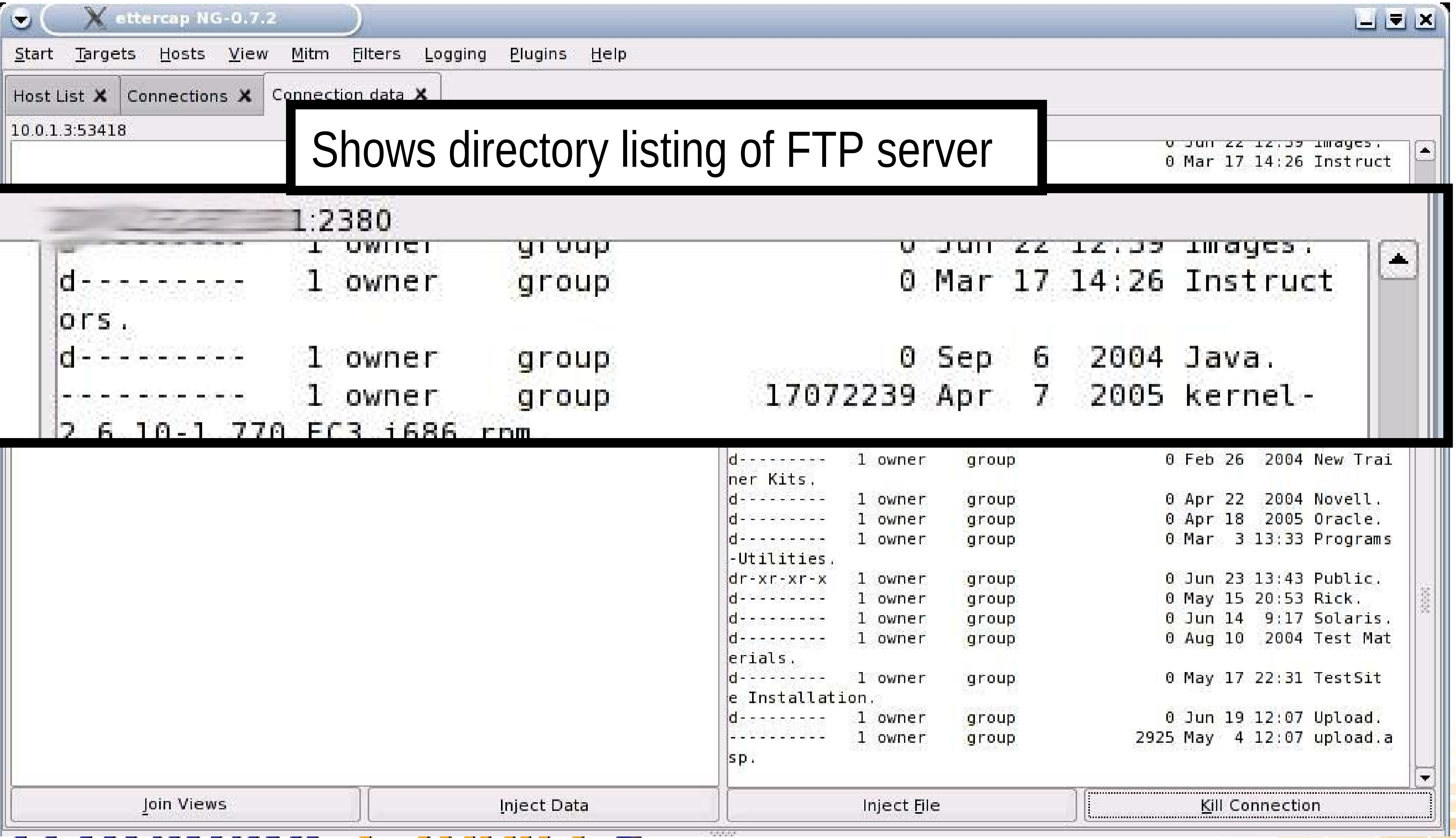
Analysis Of FTP Traffic: Ettercap



```
[redacted]:21
220 ttcftp Microsoft FTP Service (Version 5.0)..
331 Password required for seaport..
230-Training Camp's FTP in Bushkill, PA.  All Unauthorized access is p
rohibited!.
230 User [redacted] logged in..
215 Windows_NT version 5.0.
500 'MACB ENABLE': command not understood.
257 "/" is current directory..
500 'FEAT': command not understood.
227 Entering Passive Mode [redacted]9,76)..
125 Data connection already open; Transfer starting..
226 Transfer complete..
```

```
FTP : 216.113.232.131:21 -> USER: [redacted]  PASS: [redacted]
```

Analysis of FTP Traffic: Ettercap



Shows directory listing of FTP server

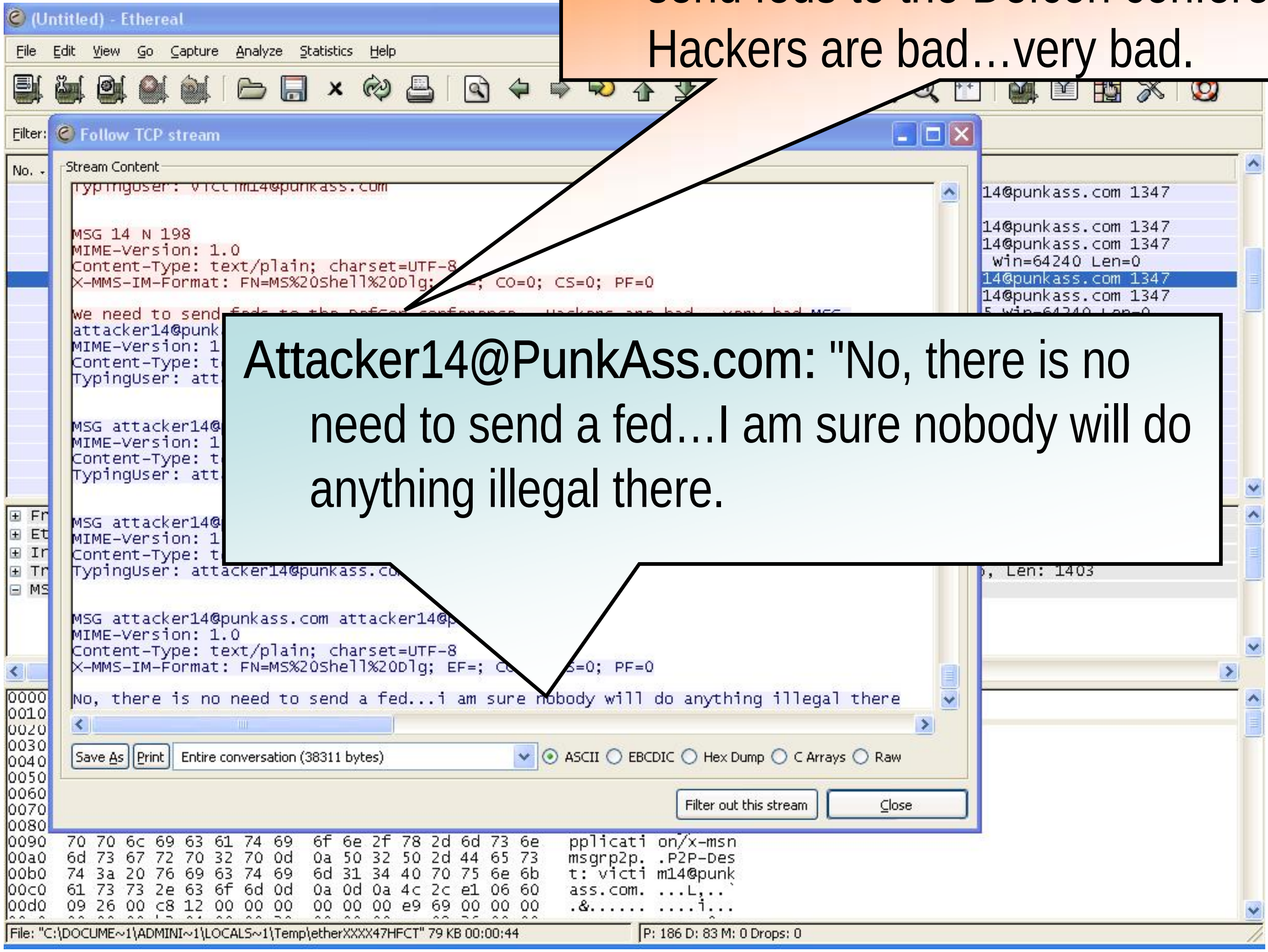
10.0.1.3:53418

[redacted]1:2380

```
d---------   1 owner    group              0 Jun 22 12:39 Images.
d---------   1 owner    group              0 Mar 17 14:26 Instruct
ors.
d---------   1 owner    group              0 Sep  6  2004 Java.
----------   1 owner    group       17072239 Apr  7  2005 kernel-
2.6.10-1.770_FC3.i686.rpm
d---------   1 owner    group              0 Feb 26  2004 New Trai
ner Kits.
d---------   1 owner    group              0 Apr 22  2004 Novell.
d---------   1 owner    group              0 Apr 18  2005 Oracle.
d---------   1 owner    group              0 Mar  3 13:33 Programs
-Utilities.
dr-xr-xr-x   1 owner    group              0 Jun 23 13:43 Public.
d---------   1 owner    group              0 May 15 20:53 Rick.
d---------   1 owner    group              0 Jun 14  9:17 Solaris.
d---------   1 owner    group              0 Aug 10  2004 Test Mat
erials.
d---------   1 owner    group              0 May 17 22:31 TestSit
e Installation.
d---------   1 owner    group              0 Jun 19 12:07 Upload.
----------   1 owner    group           2925 May  4 12:07 upload.a
sp.
```

Analysis of MS

Victim14@PunkAss.com: "We need to send feds to the Defcon conference. Hackers are bad…very bad.



```
TypingUser: victim14@punkass.com


MSG 14 N 198
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=MS%20Shell%20Dlg; E  ; CO=0; CS=0; PF=0

We need to send
attacker14@punk
MIME-Version: 1
Content-Type: t
TypingUser: att


MSG attacker14@
MIME-Version: 1
Content-Type: t
TypingUser: att


MSG attacker14@
MIME-Version: 1
Content-Type: t
TypingUser: attacker14@punkass.co


MSG attacker14@punkass.com attacker14@p
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
X-MMS-IM-Format: FN=MS%20Shell%20Dlg; EF=; C     S=0; PF=0

No, there is no need to send a fed...i am sure nobody will do anything illegal there
```

Entire conversation (38311 bytes)

● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw

```
14@punkass.com 1347

14@punkass.com 1347
14@punkass.com 1347
 Win=64240 Len=0
14@punkass.com 1347
14@punkass.com 1347
```

```
0090  70 70 6c 69 63 61 74 69  6f 6e 2f 78 2d 6d 73 6e   pplicati on/x-msn
00a0  6d 73 67 72 70 32 70 0d  0a 50 32 50 2d 44 65 73   msgrp2p. .P2P-Des
00b0  74 3a 20 76 69 63 74 69  6d 31 34 40 70 75 6e 6b   t: victi m14@punk
00c0  61 73 73 2e 63 6f 6d 0d  0a 0d 0a 4c 2c e1 06 60   ass.com. ...L,..`
00d0  09 26 00 c8 12 00 00 00  00 00 00 e9 69 00 00 00   .&...... ....i...
```

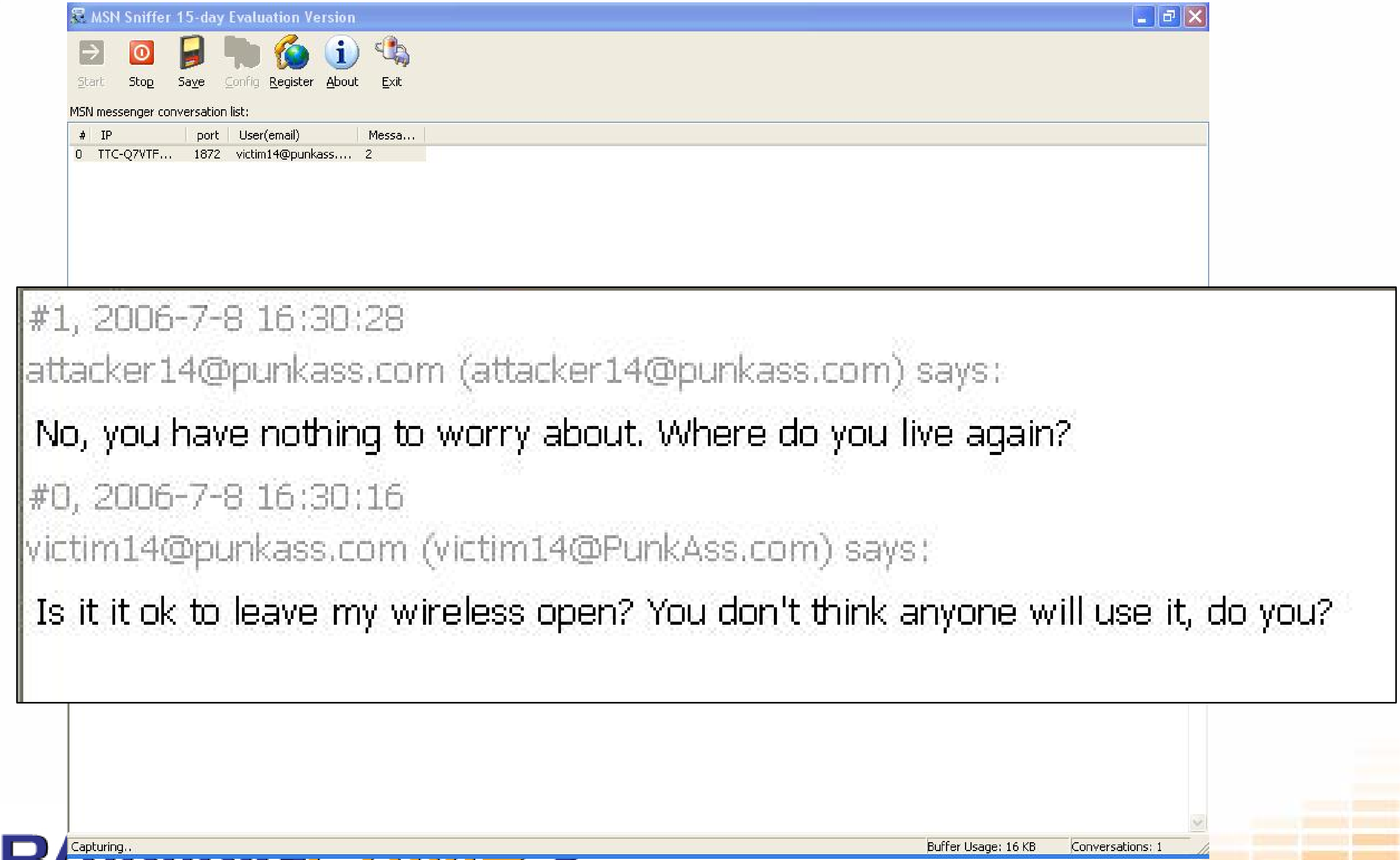
File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXX47HFCT" 79 KB 00:00:44 | P: 186 D: 83 M: 0 Drops: 0

Attacker14@PunkAss.com: "No, there is no need to send a fed…I am sure nobody will do anything illegal there.

Analysis of MSN Messenger Traffic

- MSN Sniffer
- www.effetech.com
- Also have ICQ Sniffer, AIM Sniffer, HTTP Sniffer, ACE Password Sniffer, and much more

Analysis of MSN Messenger Traffic



MSN messenger conversation list:

#	IP	port	User(email)	Messa...
0	TTC-Q7VTF...	1872	victim14@punkass....	2

#1, 2006-7-8 16:30:28

attacker14@punkass.com (attacker14@punkass.com) says:

No, you have nothing to worry about. Where do you live again?

#0, 2006-7-8 16:30:16

victim14@punkass.com (victim14@PunkAss.com) says:

Is it it ok to leave my wireless open? You don't think anyone will use it, do you?

Capturing..

Buffer Usage: 16 KB

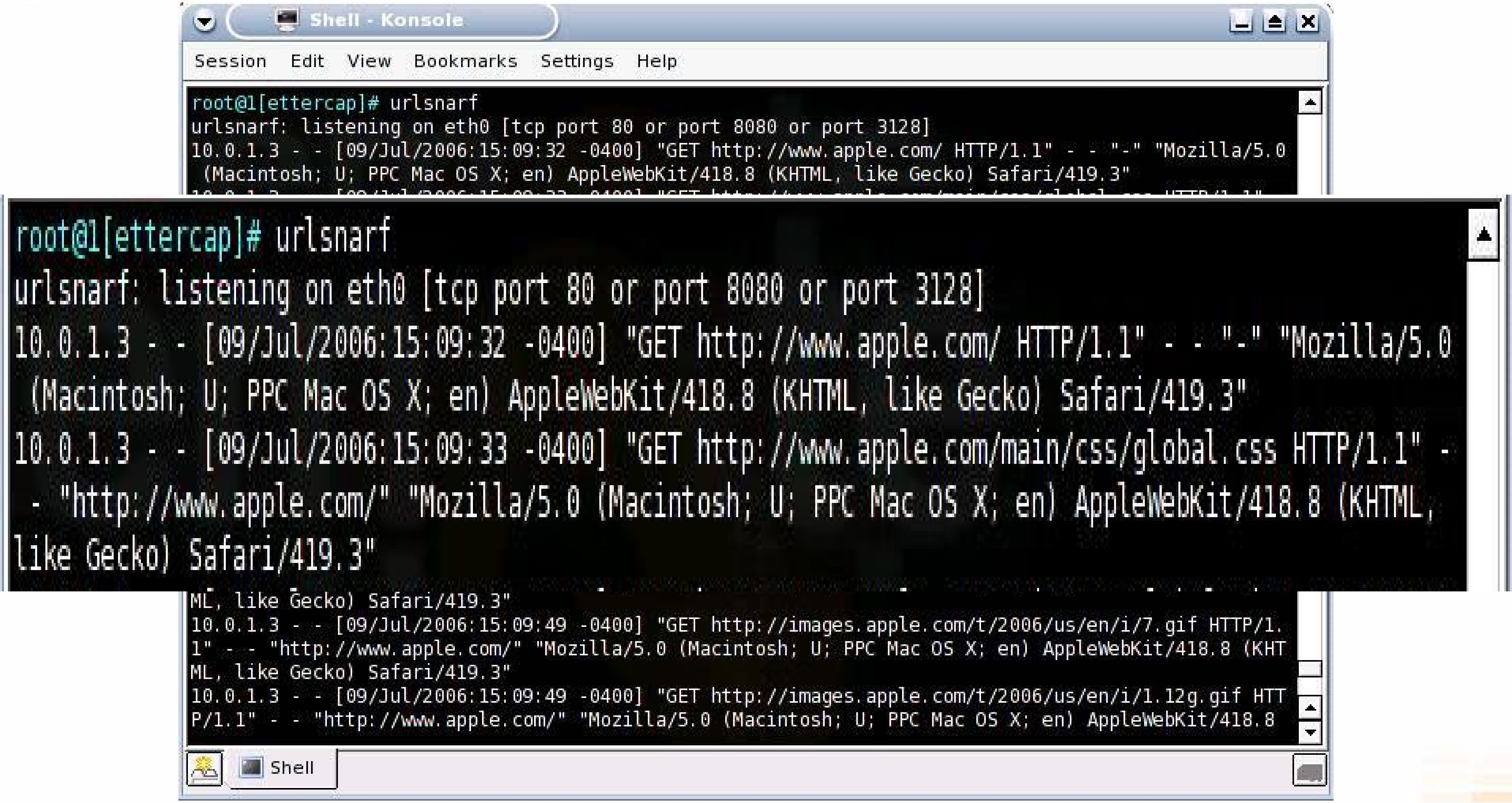
Conversations: 1

Web Traffic:URLSnarf

- Part of dsniff, written by Dug Song
- http://www.monkey.org/~dugsong/dsniff/
- urlsnarf [-n] [-i interface] [[-v] pattern [expression]]

-n	Do not resolve IP to hostname
-i	Interface
-v	"versus mode" Invert the pattern you are matching
pattern	Specify regular expression to match
Expression	Specify a tcpdump filter expression to select traffic to dump

Web Traffic: URLSnarf

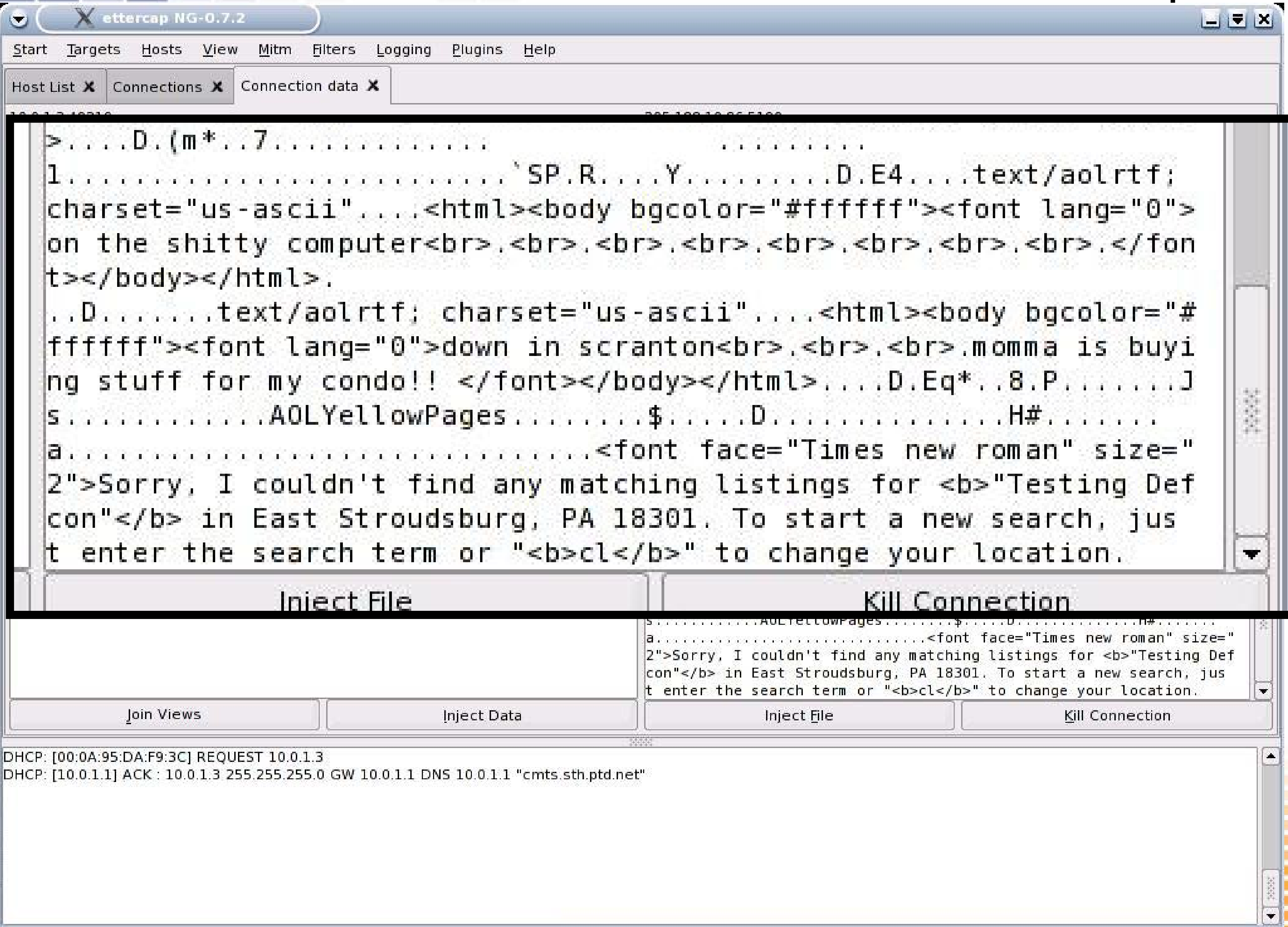


```
root@1[ettercap]# urlsnarf
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
10.0.1.3 - - [09/Jul/2006:15:09:32 -0400] "GET http://www.apple.com/ HTTP/1.1" - - "-" "Mozilla/5.0
 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/418.8 (KHTML, like Gecko) Safari/419.3"
```

```
root@1[ettercap]# urlsnarf
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
10.0.1.3 - - [09/Jul/2006:15:09:32 -0400] "GET http://www.apple.com/ HTTP/1.1" - - "-" "Mozilla/5.0
 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/418.8 (KHTML, like Gecko) Safari/419.3"
10.0.1.3 - - [09/Jul/2006:15:09:33 -0400] "GET http://www.apple.com/main/css/global.css HTTP/1.1" -
 - "http://www.apple.com/" "Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/418.8 (KHTML,
like Gecko) Safari/419.3"
```

```
ML, like Gecko) Safari/419.3"
10.0.1.3 - - [09/Jul/2006:15:09:49 -0400] "GET http://images.apple.com/t/2006/us/en/i/7.gif HTTP/1.
1" - - "http://www.apple.com/" "Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/418.8 (KHT
ML, like Gecko) Safari/419.3"
10.0.1.3 - - [09/Jul/2006:15:09:49 -0400] "GET http://images.apple.com/t/2006/us/en/i/1.12g.gif HTT
P/1.1" - - "http://www.apple.com/" "Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/418.8
```

Tool: Ettercap



```
>....D.(m*..7..............            .........
l..........................`SP.R....Y.........D.E4....text/aolrtf;
charset="us-ascii"....<html><body bgcolor="#ffffff"><font lang="0">
on the shitty computer<br>.<br>.<br>.<br>.<br>.<br>.<br>.<br>.</fon
t></body></html>.
..D.......text/aolrtf; charset="us-ascii"....<html><body bgcolor="#
ffffff"><font lang="0">down in scranton<br>.<br>.<br>.momma is buyi
ng stuff for my condo!! </font></body></html>....D.Eq*..8.P.......J
s............AOLYellowPages........$....D.............H#.......
a............................<font face="Times new roman" size="
2">Sorry, I couldn't find any matching listings for <b>"Testing Def
con"</b> in East Stroudsburg, PA 18301. To start a new search, jus
t enter the search term or "<b>cl</b>" to change your location.
```

```
a............................<font face="Times new roman" size="
2">Sorry, I couldn't find any matching listings for <b>"Testing Def
con"</b> in East Stroudsburg, PA 18301. To start a new search, jus
t enter the search term or "<b>cl</b>" to change your location.
```

```
DHCP: [00:0A:95:DA:F9:3C] REQUEST 10.0.1.3
DHCP: [10.0.1.1] ACK : 10.0.1.3 255.255.255.0 GW 10.0.1.1 DNS 10.0.1.1 "cmts.sth.ptd.net"
```

Countermeasures

- Port Security
- IPSec

Demo Time

TRAININGCAMP
Accelerated Learning. Education Evolved.