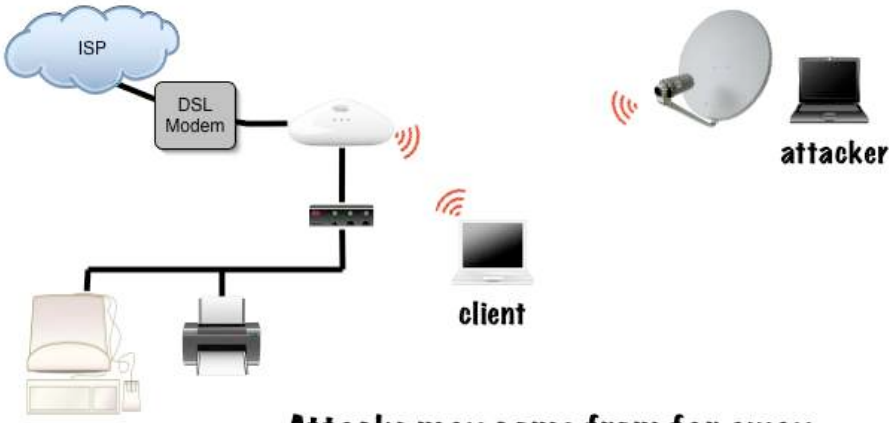
Wireless Security

Rob Flickenger
Metrix Communication LLC

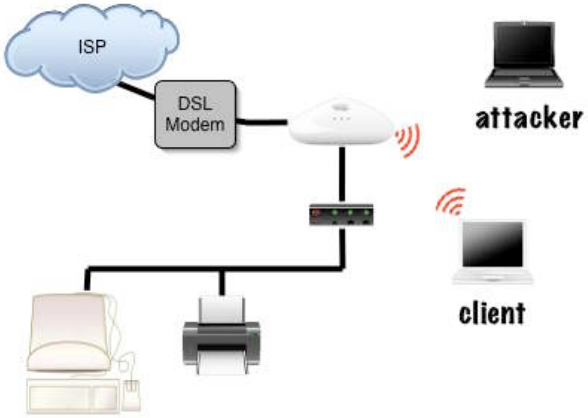
http://nocat.net/talks/security/
rob@nocat.net

Why is wireless security difficult?

* Wireless is a shared medium
* Attackers are relatively anonymous
* End users are poorly educated
* Denial-of-Service is very simple
* Tools are freely available



Attacks may come from far away



...or be completely undetectable

Who creates security problems?

* Unintentional users
* "War Drivers"
* Employees who install "rogue" access points
* Eavesdroppers (personal and corporate spies)
* Malicious users

Basic tools you can use to protect your networks:

* "Closed" networks
* MAC filtering
* WEP encryption
* Firewalls
* Strong Application Layer encryption

Encryption Basics

* Encrypting information is EASY
* Key Distribution is DIFFICULT
* Unique Identification
* Public Key Cryptography
* RSA
  (Rivest, Shamir, Adleman 1978)

Problems with WEP

* Problem is not with RC4, but the WEP implementation
* Incompatible key lengths
* IV reuse (2^24, or 16 million IVs)
* Weak IVs
* Shared key management is difficult
* Offline dictionary attacks

Advanced wireless security features

* 802.1x

  EAP-MD5
  Cisco LEAP
  Microsoft EAP-TLS

* Fast re-keying

* WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access (WPA)

* TKIP + 802.1x == WPA

* 802.1x can provide mutual authentication of client and AP

* EAP-MD5, EAP-TLS, EAP-TTLS, LEAP, PEAP

* Administration is moderately difficult

* AES + 802.1x == 802.1i

Strong (and free) encryption software

Should provide strong **Authentication**, **Encryption**, and **Key Management**.

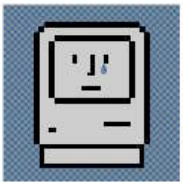
Examples include:

* SSH
* SSL
* IPSec
* OpenVPN
* PPTP

Security Tools

Free tools that will show you *lots* of information about your network

* Network ESSID scanners
* Wireless protocol analyzers
* Port scanners
* Packet sniffers
* Packet creation tools
* WEP crackers



http://www.geekculture.com/joyoftech/joyarchives/368.html

Network SSID Scanners

* Built-in clients
* NetStumbler (Windows)
* MiniStumbler (PocketPC)
* MacStumbler (Mac OS X)
* Wellenreiter (Linux)

Network Stumbler - [20030701091232.ns1]

File Edit View Device Window Help

Channels
SSIDs
Filters

MAC	SSID	Name	Chan	Vendor	Type	Encryption	Signal+	Noise-	SNR+
00022D1CBCCF	NoCat		10	Agere (Lucent) Orinoco	AP		-83	-100	17
00601DF22136	ORA		3	Agere (Lucent) WaveLAN	AP	WEP	-76	-100	24
00022D0C5F07	ORA		3	Agere (Lucent) Orinoco	AP	WEP	-73	-100	27
00022D8D03F7	2WIRE403		6	Agere (Lucent) Orinoco	AP	WEP	-79	-100	21
00306507E49D	dragonfly		1	Apple	AP	WEP	-87	-100	13
000625A33938	linksys		6	Linksys	AP	WEP	-71	-100	29
00022D1D293B	AthenaBC		1	Agere (Lucent) Orinoco	AP	WEP	-88	-100	12
00032F0119CF	FORD707		6	GST (Linksys)	AP		-88	-100	12
00026F03FE64	NoCat-Sebastopol		8, 14	Senao Intl	AP		-59	-100	41

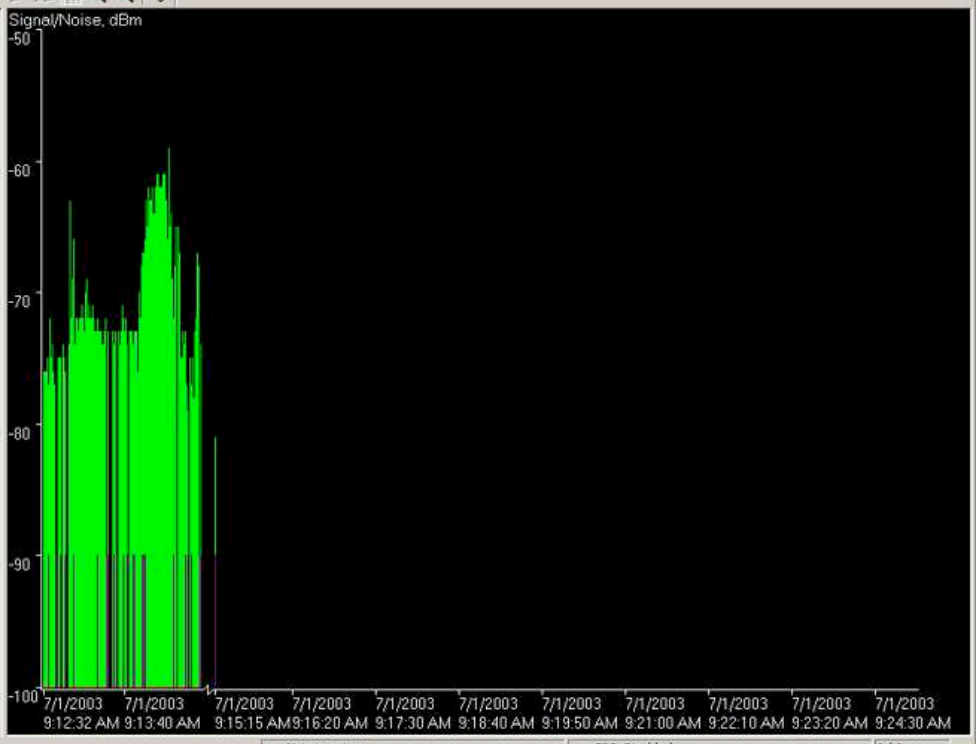
Ready | Not scanning | GPS: Disabled | 9 / 9

Network Stumbler - [20030701091232.ns1]

File Edit View Device Window Help

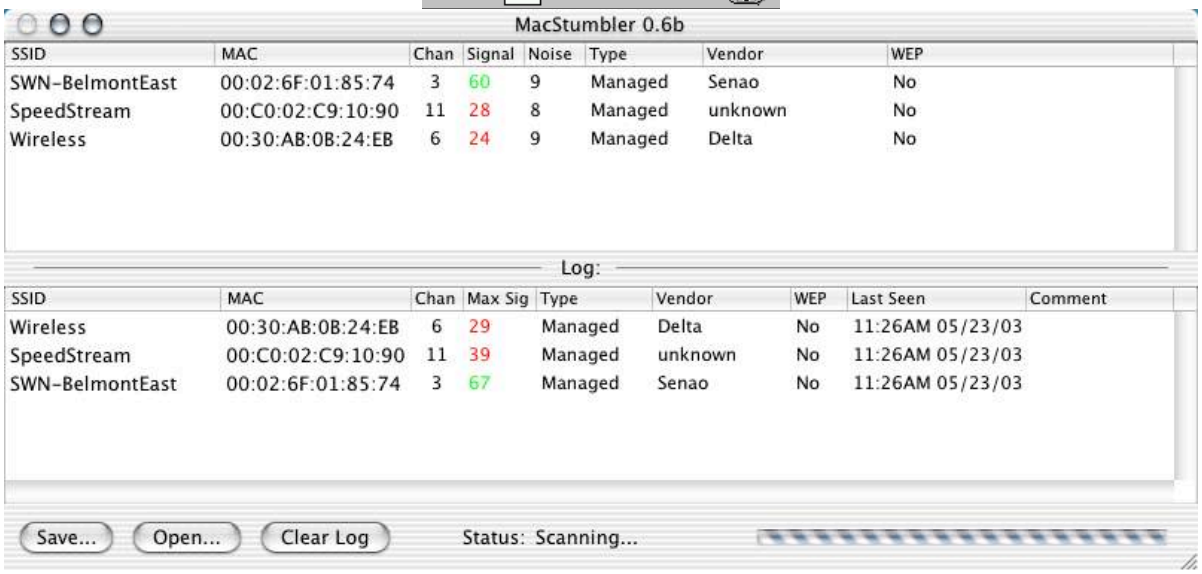
Channels
SSIDs
- 2WIRE403
- AthenaBC
- dragonfly
- FORD707
- linksys
- NoCat
- NoCat-Sebastopol
  - 00026F03FE64
- ORA

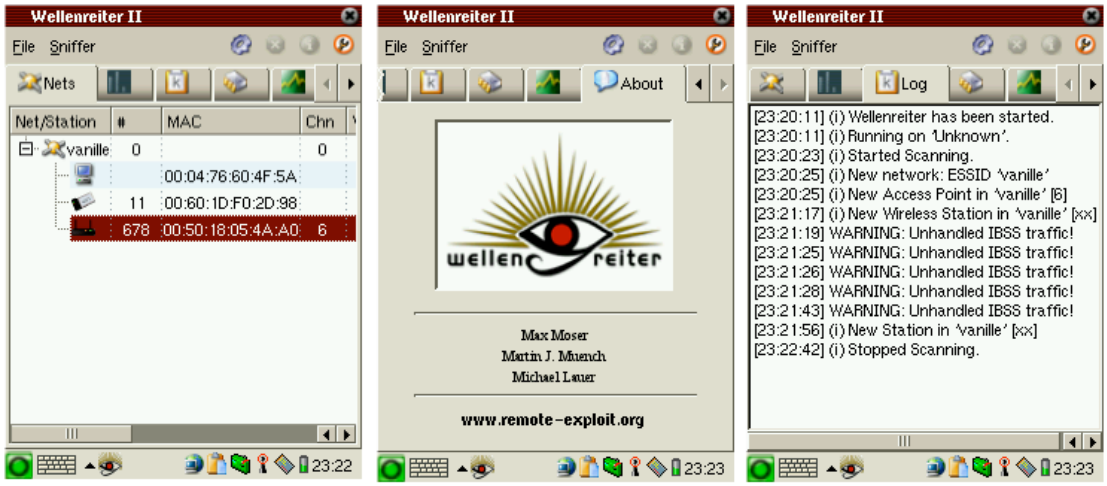
Filters



Ready | Not scanning | GPS: Disabled | 9 / 9

MiniStumbler 9:59a
MAC SSID
00032F0119CF FORD707
00026F03FE64 NoCat-Sebastopol
00022D1D293B AthenaBC
00062560130F linksys
00022D8D03F7 2WIRE403
00601DF2211F ORA
00022D0C11F4 ORA
00022D0C5F07 ORA
00601DF22136 ORA
004005B1F5E3 victree
New document starts scan
Reconfigure card automatically
Get AP Names
Auto Save
File View Opt Spd GPS


MacStumbler 0.6b
SSID MAC Chan Signal Noise Type Vendor WEP
SWN-BelmontEast 00:02:6F:01:85:74 3 60 9 Managed Senao No
SpeedStream 00:C0:02:C9:10:90 11 28 8 Managed unknown No
Wireless 00:30:AB:0B:24:EB 6 24 9 Managed Delta No
Log:
SSID MAC Chan Max Sig Type Vendor WEP Last Seen Comment
Wireless 00:30:AB:0B:24:EB 6 29 Managed Delta No 11:26AM 05/23/03
SpeedStream 00:C0:02:C9:10:90 11 39 Managed unknown No 11:26AM 05/23/03
SWN-BelmontEast 00:02:6F:01:85:74 3 67 Managed Senao No 11:26AM 05/23/03
Save... Open... Clear Log
Status: Scanning...

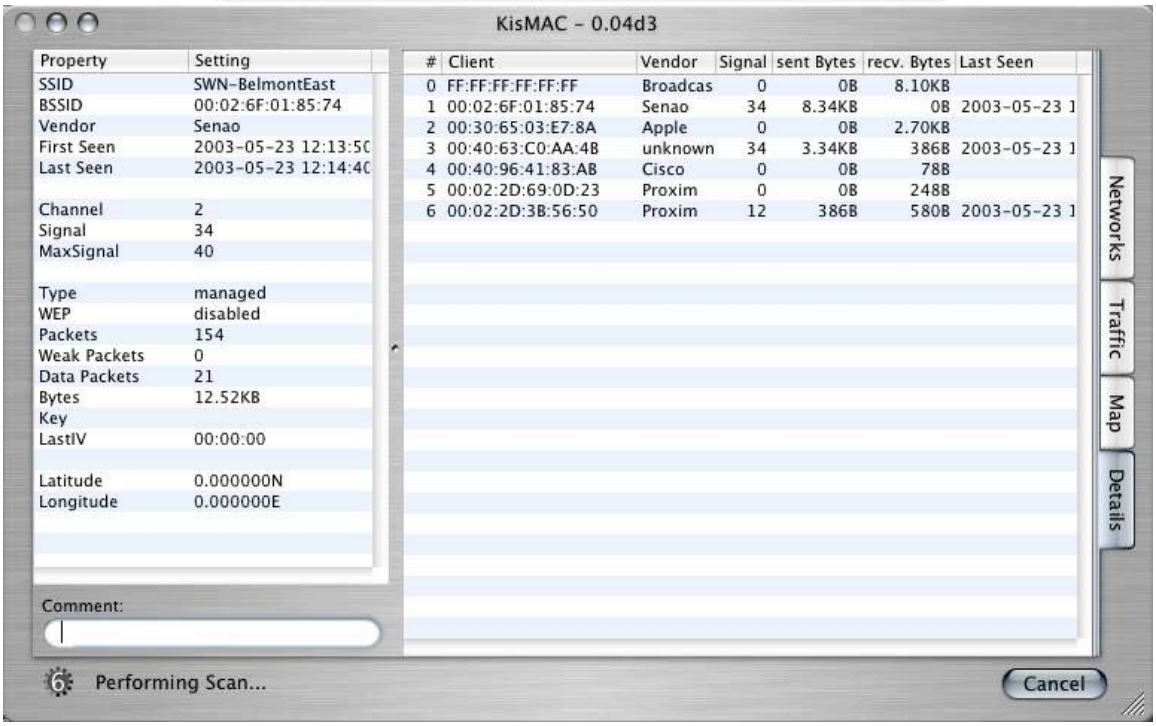


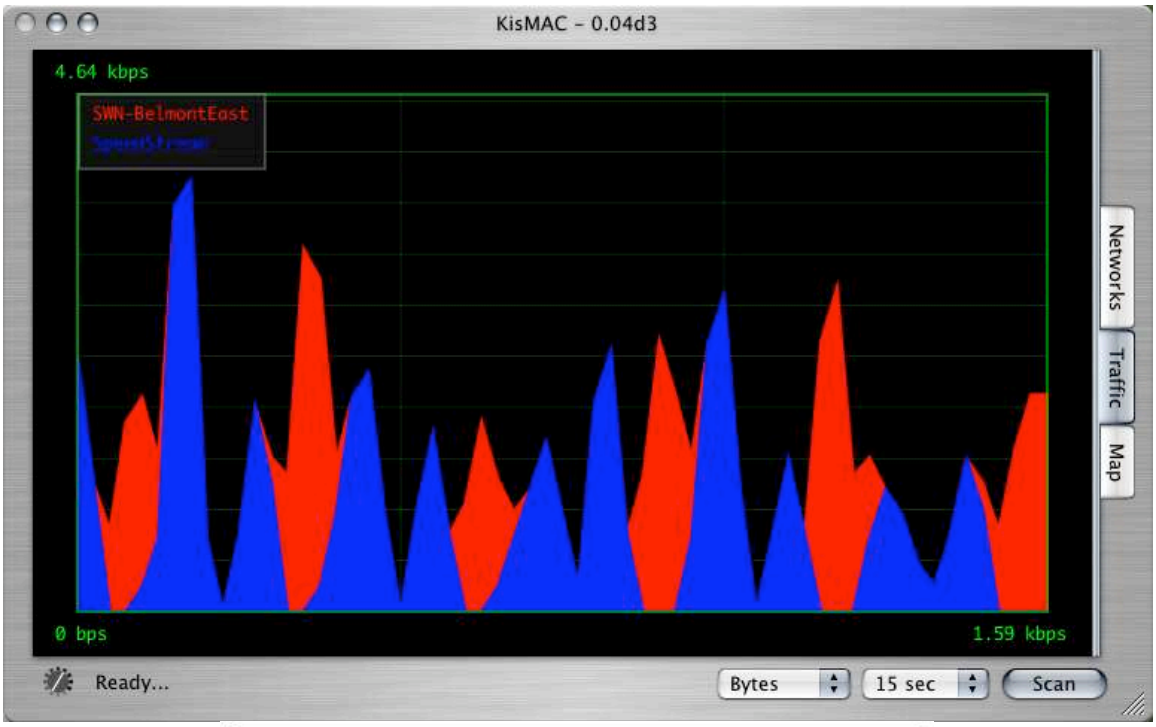
Wireless Protocol Analyzers

* Airopeek (Windows)
* KisMAC (Mac OS X)
* Kismet + Ethereal (Linux + Mac OS X)

Airopeek NX

* $3500 US
* Windows Only
* Free Demo available





Kismet

http://www.kismetwireless.net/

Raw 802.11 frame logger + packet capture

Requirements:

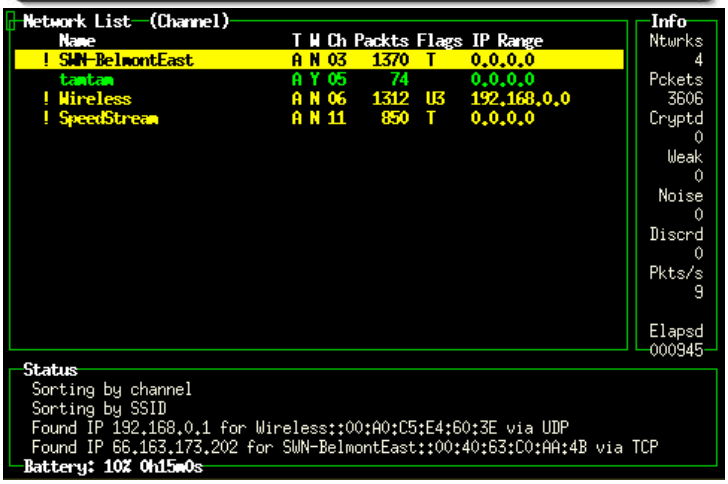
Linux, OpenBSD, or OS X

Cisco Aironet, Orinoco, or Prism 2

No AirPort (yet...)

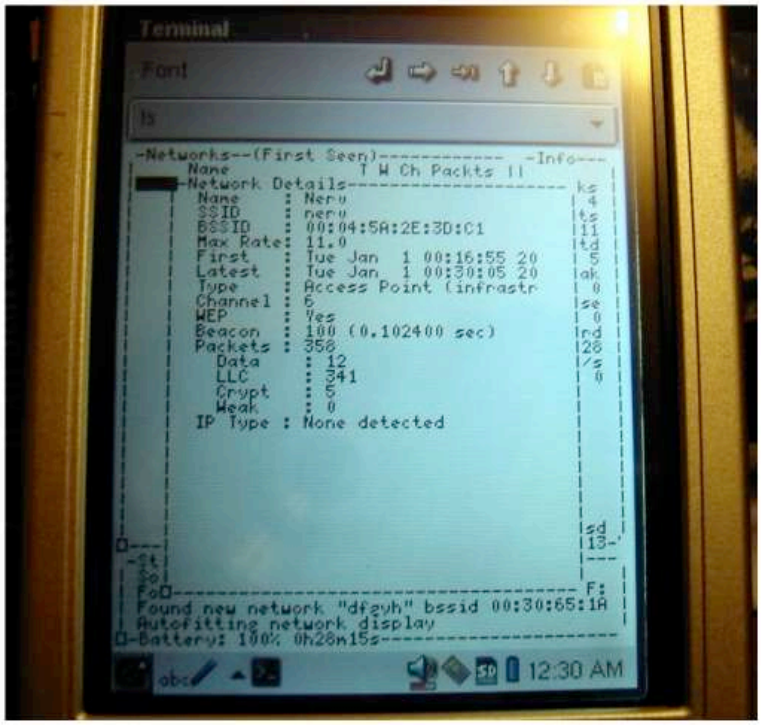
Kismet Features:

* AP Hardware fingerprinting
* NetStumbler detection
* Will speak detected networks and stats
* GPS support
* Tons of details, logging, statistics



```
Network List (Channel)                                          Info
  Name                    T W Ch Packts Flags IP Range          Ntwrks
Network Details
  Name    : SWN-BelmontEast

  SSID    : SWN-BelmontEast
  Server  : localhost:2501
  BSSID   : 00:02:6F:01:85:74
  Carrier : IEEE 802.11b
  Manuf   : Senao
  Model   : Unknown
  Matched : 00:02:6F:00:00:00
  Max Rate: 11.0
  First   : Thu Jun  5 22:08:13 2003
  Latest  : Thu Jun  5 22:18:01 2003
  Clients : 3
  Type    : Access Point (infrastructure)
  Info    :
  Channel : 3
  WEP     : No
  Beacon  : 100 (0.102400 sec)
  Packets : 1501
                                                            (+) Down
Battery: 10% 0h14m0s
Network List (Channel)                                          Info
  Name                    T W Ch Packts Flags IP Range          Ntwrks
Client List (Autofit)
  T MAC               Manuf      Data Crypt  Size IP Range        Sgn
  F 00:40:63:C0:AA:4B Unknown     156     0  127k 66.163.173.202    0
  F 00:06:25:AB:79:F6 Linksys       6     0  748B 10.15.6.84        0
  F 00:30:65:29:2E:B0 Apple         9     0  264B 0.0.0.0           0
Battery: 10% 0h15m0s
```



Kismet on a Sharp Zaurus running Linux

DumpLog 03-06-21 14:50.dump - Ethereal

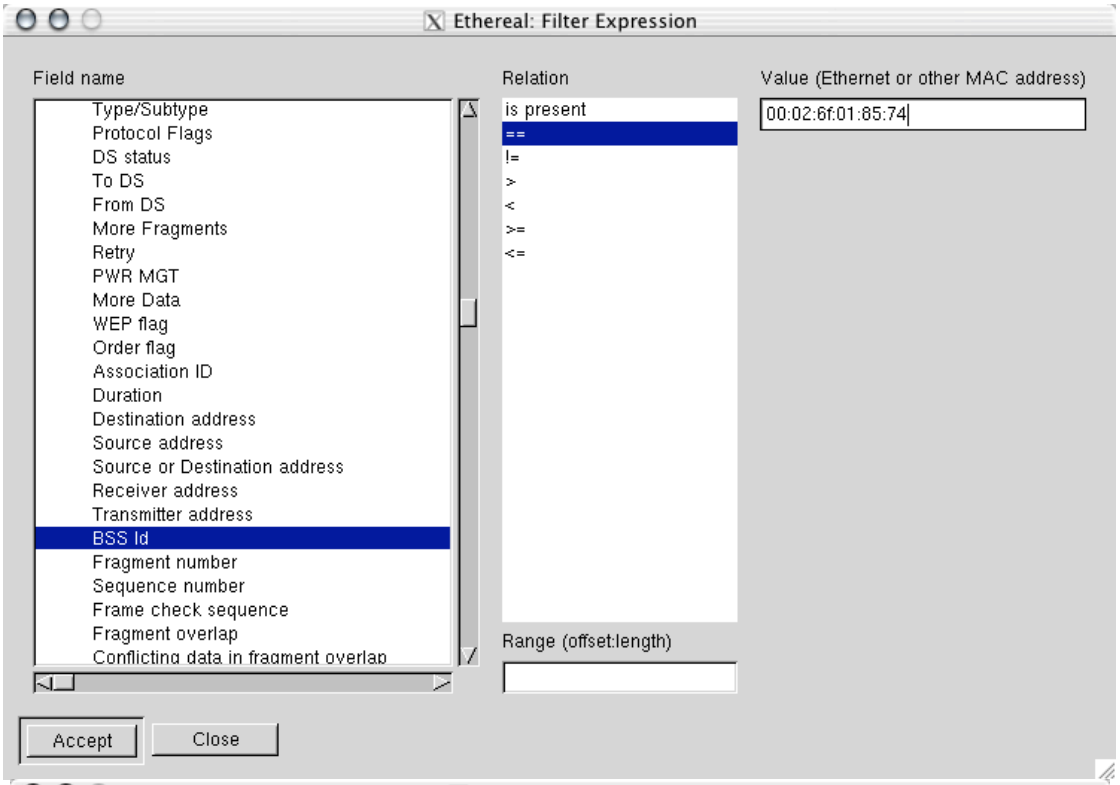
File Edit Capture Display Tools Help

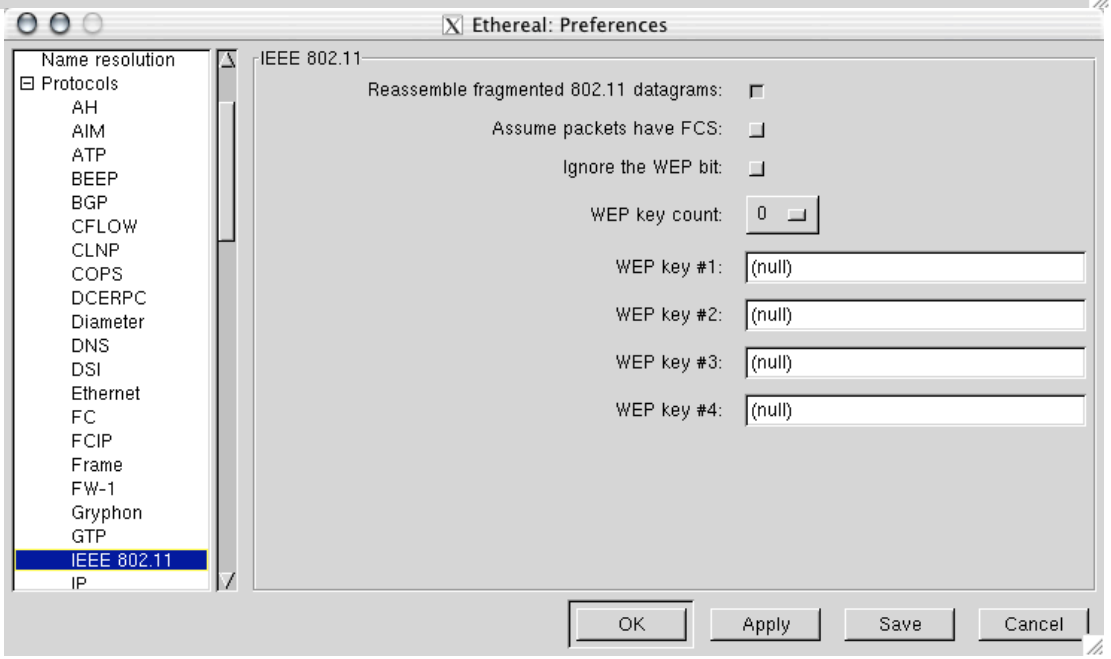
No.	Time	Source	Destination	Protocol	Info
344	19.099107	00:02:6f:01:85:74	00:06:25:12:cf:c6	IEEE 802.11	Probe Response
345	19.100770	00:02:6f:01:85:74	00:06:25:12:cf:c6	IEEE 802.11	Probe Response
346	19.129647	00:02:6f:01:85:74	00:06:25:12:cf:c6	IEEE 802.11	Probe Response
347	19.130652	00:02:6f:01:85:74	00:06:25:12:cf:c6	IEEE 802.11	Probe Response
348	19.132844	00:02:6f:01:85:74	00:06:25:12:cf:c6	IEEE 802.11	Probe Response
351	19.149973	00:02:6f:01:85:74	ff:ff:ff:ff:ff:ff	IEEE 802.11	Beacon frame
352	19.252298	00:02:6f:01:85:74	ff:ff:ff:ff:ff:ff	IEEE 802.11	Beacon frame
357	20.174012	00:02:6f:01:85:74	ff:ff:ff:ff:ff:ff	IEEE 802.11	Beacon frame
358	20.276660	00:02:6f:01:85:74	ff:ff:ff:ff:ff:ff	IEEE 802.11	Beacon frame
428	21.198078	00:02:6f:01:85:74	ff:ff:ff:ff:ff:ff	IEEE 802.11	Beacon frame
429	21.300603	00:02:6f:01:85:74	ff:ff:ff:ff:ff:ff	IEEE 802.11	Beacon frame
430	21.403110	00:02:6f:01:85:74	ff:ff:ff:ff:ff:ff	IEEE 802.11	Beacon frame

```
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters (12 bytes)
      Timestamp: 0x00000012FB3A8219
      Beacon Interval: 0.102400 [Seconds]
    ⊞ Capability Information: 0x0001
  ⊟ Tagged parameters (32 bytes)
      Tag Number: 0 (SSID parameter set)
      Tag length: 15
      Tag interpretation: SWN-BelmontEast
      Tag Number: 1 (Supported Rates)
      Tag length: 4
      Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5 11.0 [Mbit/sec]
      Tag Number: 3 (DS Parameter set)
      Tag length: 1
```

```
0000  80 00 00 00 ff ff ff ff  ff ff 00 02 6f 01 85 74   ........ ....o..t
0010  00 02 6f 01 85 74 d0 66  19 82 3a fb 12 00 00 00   ..o..t.f ..:.....
0020  64 00 01 00 00 0f 53 57  4e 2d 42 65 6c 6d 6f 6e   d.....SW N-Belmon
0030  74 45 61 73 74 01 04 82  84 0b 16 03 01 03 05 04   tEast... ........
0040  00 01 00 04                                        ....
```

Filter: wlan.bssid == 00:02:6f:01:85:74 Reset Apply File: DumpLog 03-06-21 14:50.dump


Ethereal: Filter Expression
Field name
Type/Subtype
Protocol Flags
DS status
To DS
From DS
More Fragments
Retry
PWR MGT
More Data
WEP flag
Order flag
Association ID
Duration
Destination address
Source address
Source or Destination address
Receiver address
Transmitter address
BSS Id
Fragment number
Sequence number
Frame check sequence
Fragment overlap
Conflicting data in fragment overlap
Relation
is present
==
!=
>
<
>=
<=
Value (Ethernet or other MAC address)
00:02:6f:01:85:74
Range (offset:length)
Accept
Close


Ethereal: Preferences
Name resolution
Protocols
AH
AIM
ATP
BEEP
BGP
CFLOW
CLNP
COPS
DCERPC
Diameter
DNS
DSI
Ethernet
FC
FCIP
Frame
FW-1
Gryphon
GTP
IEEE 802.11
IP
IEEE 802.11
Reassemble fragmented 802.11 datagrams:
Assume packets have FCS:
Ignore the WEP bit:
WEP key count:
0
WEP key #1:
(null)
WEP key #2:
(null)
WEP key #3:
(null)
WEP key #4:
(null)
OK
Apply
Save
Cancel

nmap

http://www.nmap.org/nmap/

Network and port scanner

Scans any number of ports on any number of hosts

Remote OS detection

Sophisticated stealth scanning

Idle, undetectable service "scanning"

OS X, Linux, *BSD, Solaris

Ethereal

http://www.ethereal.com/

"Sniffing the glue that holds the Internet together"

Network protocol analyzer

Layer 2+ (Layer 1 agnostic)

libpcap packet capture

OS X (on X), Linux, *BSD, Solaris, Win*

tcpdump compatible file format

<capture> - Ethereal
File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
1 0.000000 10.15.6.1 10.15.6.33 HTTP HTTP/1.1 200 OK
2 0.002895 10.15.6.1 10.15.6.33 HTTP Continuation
3 0.003344 10.15.6.33 10.15.6.1 TCP 52824 > http [ACK] Seq=966073767 Ack=107601726 Win=33304
5 0.007514 10.15.6.1 10.15.6.33 HTTP Continuation
10 0.061774 10.15.6.33 10.15.6.1 HTTP GET /style.css HTTP/1.1
11 0.067010 10.15.6.1 10.15.6.33 TCP http > 52824 [ACK] Seq=107601857 Ack=966074200 Win=7504
12 0.073638 10.15.6.1 10.15.6.33 HTTP HTTP/1.1 200 OK
13 0.073861 10.15.6.1 10.15.6.33 HTTP Continuation
14 0.097565 216.254.17.166 10.15.6.33 SSH Encrypted response packet len=1448
15 0.100457 216.254.17.166 10.15.6.33 SSH Encrypted response packet len=1448
Frame 10 (499 bytes on wire, 499 bytes captured)
Ethernet II, Src: 00:30:65:03:e7:8a, Dst: 00:40:63:c0:aa:4b
Internet Protocol, Src Addr: 10.15.6.33 (10.15.6.33), Dst Addr: 10.15.6.1 (10.15.6.1)
Transmission Control Protocol, Src Port: 52824 (52824), Dst Port: http (80), Seq: 966073767, Ack: 107601857, Len: 433
Hypertext Transfer Protocol
GET /style.css HTTP/1.1\r\n
Host: muzik.rob.swn\r\n
Connection: keep-alive\r\n
Referer: http://muzik.rob.swn/cgi/playing?channel=Muzik\r\n
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en-us) AppleWebKit/74 (KHTML, like Gecko) Safari/74\r\n
Accept: */*\r\n
Accept-Language: en-us, ja;q=0.21, de-de;q=0.86, de;q=0.79, fr-fr;q=0.71, fr;q=0.64, nl-nl;q=0.57, nl;q=0.50, it-it;q=0.43
\r\n
0000 00 40 63 c0 aa 4b 00 30 65 03 e7 8a 08 00 45 00 .@c..K.0 e.....E.
0010 01 e5 5e 54 40 00 40 06 ba 7f 0a 0f 06 21 0a 0f ..^T@.@. .....!..
0020 06 01 ce 58 00 50 39 95 1d a7 06 69 df c1 80 18 ...X.P9. ...i....
0030 82 18 5d cf 00 00 01 01 08 0a b1 15 f1 44 21 63 ..]..... .....D!c
0040 8e ed 47 45 54 20 2f 73 74 79 6c 65 2e 63 73 73 ..GET /s tyle.css
0050 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1. 1..Host:
0060 20 6d 75 7a 69 6b 2e 72 6f 62 2e 73 77 6e 0d 0a muzik.r ob.swn..
Filter: ip.addr == 10.15.6.33
Reset Apply
File: <capture> Drops: 0
Contents of TCP stream
GET /style.css HTTP/1.1
Host: muzik.rob.swn
Connection: keep-alive
Referer: http://muzik.rob.swn/cgi/playing?channel=Muzik
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en-us) AppleWebKit/74 (KHTML, like Gecko) Safari/74
Accept: */*
Accept-Language: en-us, ja;q=0.21, de-de;q=0.86, de;q=0.79, fr-fr;q=0.71, fr;q=0.64, nl-nl;q=0.57, nl;q=0.50, it-it;q=0.43, it;q=0.36, ja-jp;q=0.29, en;q=0.93, es-es;q=0.14, es;q=0.07
HTTP/1.1 200 OK
Date: Sat, 21 Jun 2003 21:35:03 GMT
Server: Apache/1.3.27 (Unix) PHP/4.3.1 DAV/1.0.3
Last-Modified: Mon, 02 Jun 2003 20:52:41 GMT
ETag: "5556cf-478-3edbb919"
Accept-Ranges: bytes
Content-Length: 1144
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: text/css
body {
background-color: #b0b0b0;
color: #000000;
font-family: "Trebuchet MS","Lydian BT";
}
A:link {color: #790079;}
A:visited {color: #400040;}
A:active {color: #FF00FF;}
A:hover {color: #B000B0;}
.squeallink {
font-size: 9pt;
}
.title {
font-size: 18pt;
}
Entire conversation (17461 bytes)
ASCII EBCDIC Hex Dump C Arrays
Print Save As Close

EtherPEG

http://www.etherpeg.org/

Packet capture and graphics renderer

OS X / OS 9 only

Cool hack, little monitoring or debugging value

Leaves a surprisingly big impression

ngrep

http://www.packetfactory.net/Projects/ngrep/

"Network Grep"

GNU grep switch syntax and regex match

Hex or ASCII output

Runs on OS X, *BSD, Linux, Solaris, Win*

Prints data to STDOUT

ettercap

http://ettercap.sourceforge.net/

Aggressive Packet capture and crack tool
SSH1 MITM attack tool
Data injection
Password collector
HTTP File capture
ARP Poisoning...

Runs only on Linux

http://airsnort.shmoo.com/

WEP cracking tool (IV collector and analyzer)

Completely passive monitoring (pre-assoc.)

Linux only

Cisco Aironet, Orinoco, or Prism 2 card

Some success with iBook + AirPort + Linux:

http://www.swieskowski.net/code/wifi.php

ntop

http://www.ntop.org/ntop.html

"If you obey all the rules, you'll miss all the fun"

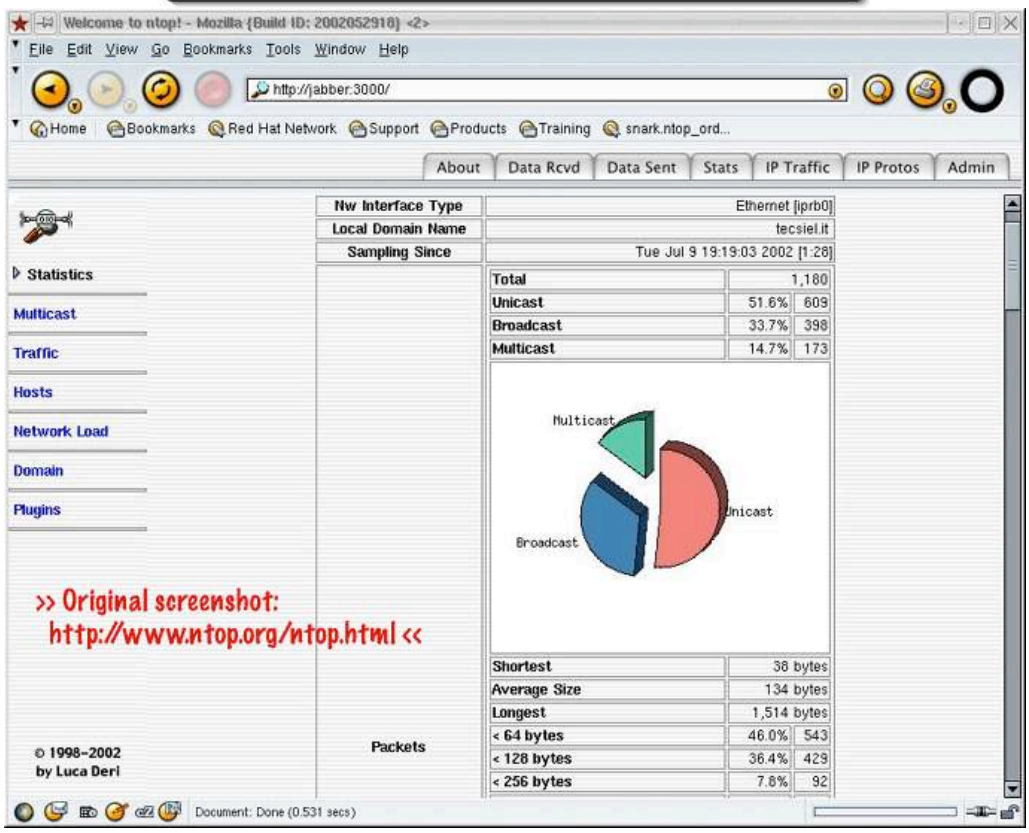
Network statistics logging and analysis

Charts & Graphs of network traffic

Mostly for tracking flows, can show client detail

OS X, Linux, FreeBSD, Solaris, Win*

http or https web interface and configuration

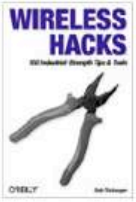


>> Original screenshot:
http://www.ntop.org/ntop.html <<

References:

This talk:

http://nocat.net/talk/security/



NetStumbler: http://stumbler.net/
MacStumbler: http://www.macstumbler.com/
AirSnort: http://airsnort.shmoo.com/
Kismet: http://www.kismetwireless.net/
KisMAC: http://www.binaervarianz.de/projekte/programmieren/kismac/
Wellenreiter: http://www.wellenreiter.net/
Airopeek: http://www.wildpackets.com/
ettercap: http://ettercap.sourceforge.net/
ngrep: http://www.packetfactory.net/Projects/ngrep/
ntop: http://www.ntop.org/ntop.html
nmap: http://www.nmap.org/nmap/
EtherPEG: http://www.etherpeg.org/
Driftnet: http://www.ex-parrot.com/~chris/driftnet/
Ethereal: http://www.ethereal.com/