Wifi Penetration

Wireless Communication and
Computer/Network Forensics

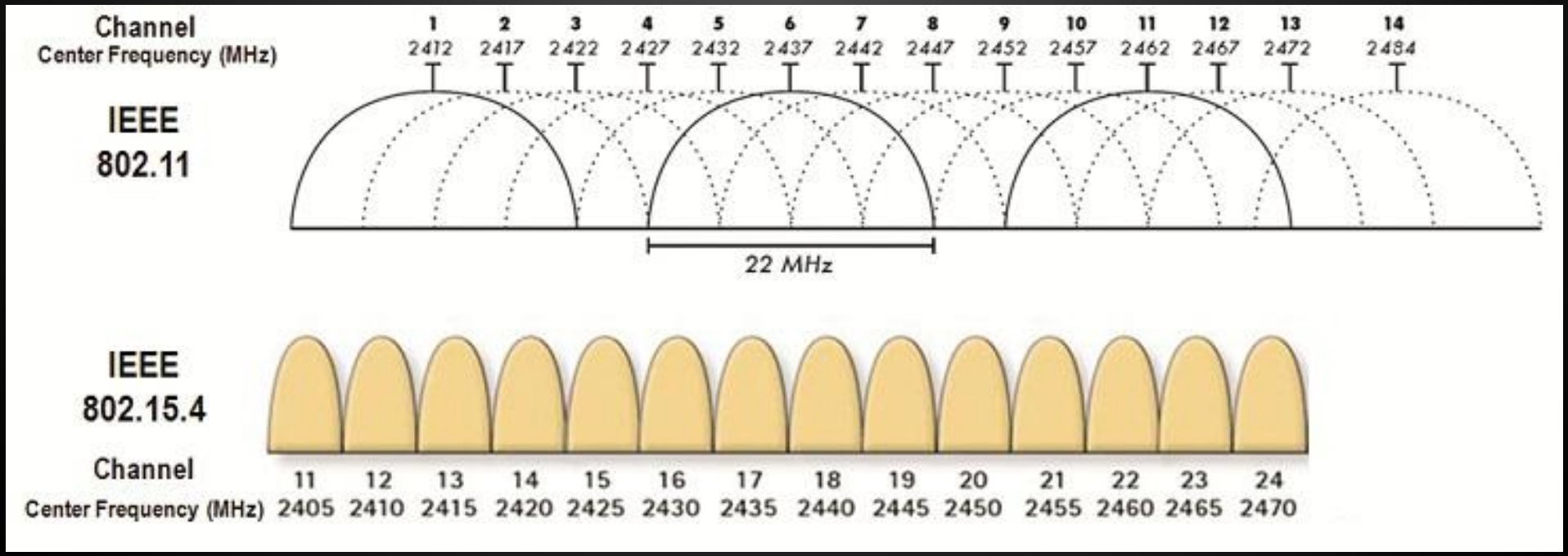
Terms

- Skiddy(Derogatory): Variant of "Script Kiddy".
- Hacker(Derogatory):One who builds something.
- Cracker(Derogatory):One who breaks something.
- Penetration Test: Method of evaluating Computer/Network security by simulating an attack.
- Penetration Tester: One who implements different attack tools to asses Computer/Network vulnerabilities.

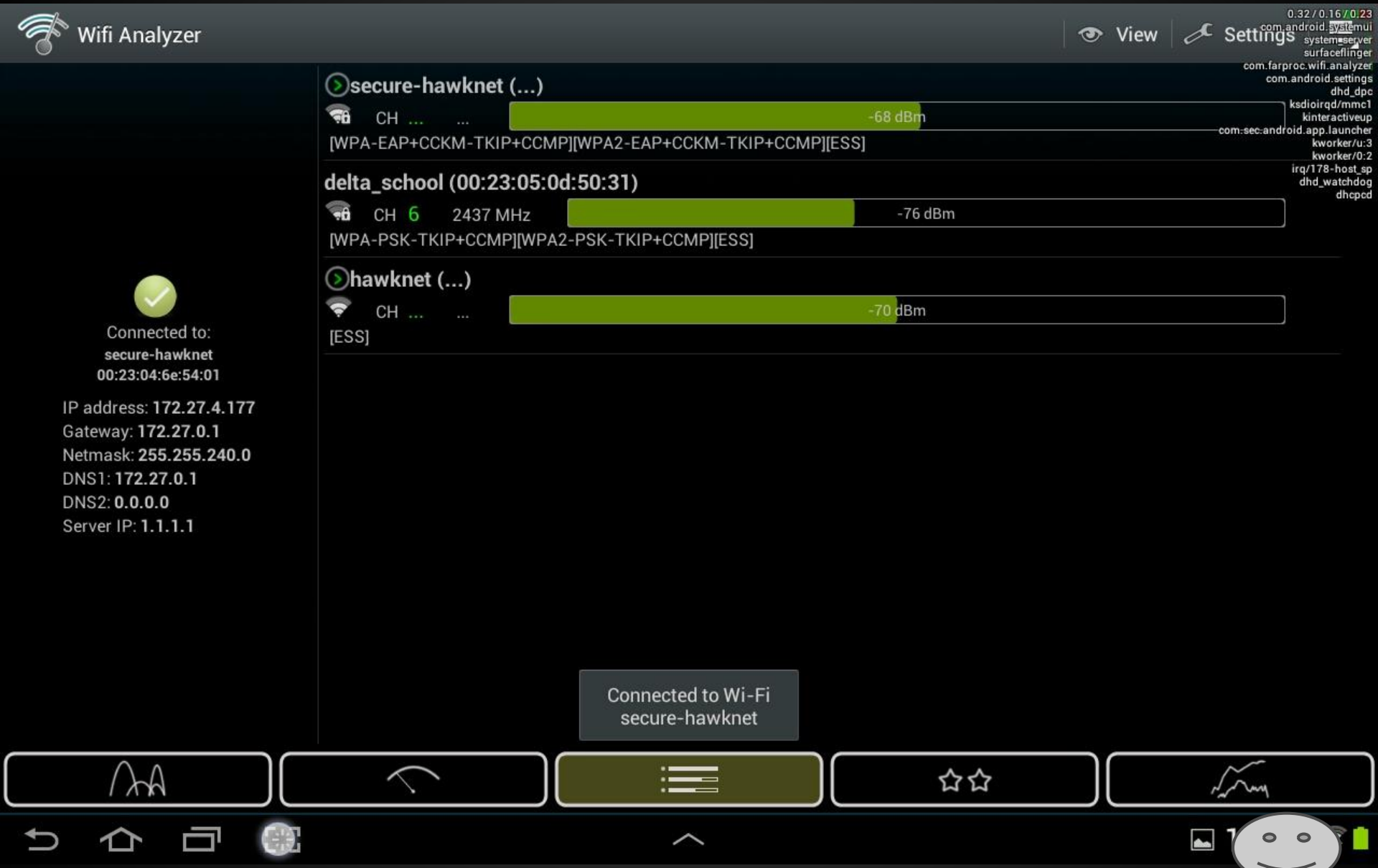
Wifi / WLAN / Wireless

Spectrum depends on what country you're in.

America uses 14 channels designated in 2.4 ghz spaced 5mhz apart.




Wifi Analyzer
View
Settings
0.41 / 0.17 / 0.24
com.android.systemui
surfaceflinger
kinteractiveup
system_server
-30
-40
-50
-60
-70
-80
-90
Signal Strength [dBm]
secure-hawknet
hawknet*
secure-hawknet
hawknet*
1
2
3
4
5
6
7
8
9
10
11
12
13
14
Wifi Channels


Wifi Analyzer
View
Settings
0.32 / 0.16 / 0.23
com.android.systemui
system_server
surfaceflinger
com.farproc.wifi.analyzer
com.android.settings
dhd_dpc
ksdioirqd/mmc1
kinteractiveup
com.sec.android.app.launcher
kworker/u:3
kworker/0:2
irq/178-host_sp
dhd_watchdog
dhcpcd
secure-hawknet (...)
CH ... ...
-68 dBm
[WPA-EAP+CCKM-TKIP+CCMP][WPA2-EAP+CCKM-TKIP+CCMP][ESS]
delta_school (00:23:05:0d:50:31)
CH 6 2437 MHz
-76 dBm
[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]
hawknet (...)
CH ... ...
-70 dBm
[ESS]
Connected to:
secure-hawknet
00:23:04:6e:54:01
IP address: 172.27.4.177
Gateway: 172.27.0.1
Netmask: 255.255.240.0
DNS1: 172.27.0.1
DNS2: 0.0.0.0
Server IP: 1.1.1.1
Connected to Wi-Fi
secure-hawknet


Wifi Analyzer
View
Settings
0.41 / 0.17 / 0.24
com.android.systemui
surfaceflinger
kinteractiveup
system_server
-30
-40
-50
-60
-70
-80
-90
Signal Strength [dBm]
secure-hawknet
hawknet*
secure-hawknet
hawknet*
1
2
3
4
5
6
7
8
9
10
11
12
13
14
Wifi Channels

Wireless Encryption

- Wired Equivalent Privacy(WEP): The least form of security. FBI Demonstrated 3 minute hack in 2005. 40 bit or 104 bit encryption Key.

- Wifi Protected Acces(WPA): Replace WEP, and use of Temporal Key Integrity Protocol (TKIP). Implements 128 bit encryption.

- (WPA2): Successor to WPA, replaces TKIP with Counter Cypher Mode Protocol (CCMP). Also Implements different algorithm Advanced Encryption Standard (AES), 256 bit encryption.

Wireless Antennas

Omnidirectional: Common "Rubber Ducky" antenna.

Directional: Common "Flat-Panel" or a variant of "Pringles-Can" antenna.

Sniper Directional: Common "Yagi" antenna, resembles antennas commonly found on house roofs.

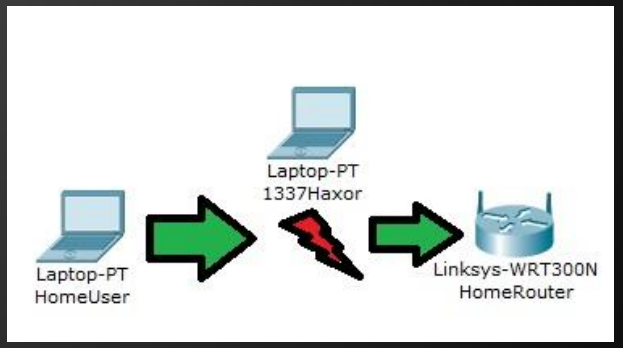
http://vimeo.com/8826952

Wiretapping/Eavesdropping laws

- CA Eavesdropping and Wiretapping law: PENAL CODE SECTION 630-638
- CA PENAL CODE SECTION 484-502.9
- Google was fined $7 million because a rogue engineer was using a penetration tool called "Kismet". Kismet is similar to aircrack, but is scripted to automatically break into networks when a password is found. It also provides a google maps view.
- It is perfectly legal to perform penetration testing techniques on your own equipment. It is also perfectly legal to be in promiscuous mode, i.e. "Listening to wireless". Once you perform an attack or cause a redirect of the traffic, it starts to become a gray area and could potentially be illegal. SNIFF RESPONSIBLY

Man-In-The-Middle

The man-in-the-middle attack often abbreviated as (MITM) is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims, and inject new ones.



Common Programs:

Cain and Abel - Windows

Ettercap - LAN based attacks

SSLStrip - Tool for SSL based MITM attacks

Karma - Tool that uses Evil twin attack

Aircrack - A toolset of Wireless Penetration scripts, GNU/Linux based

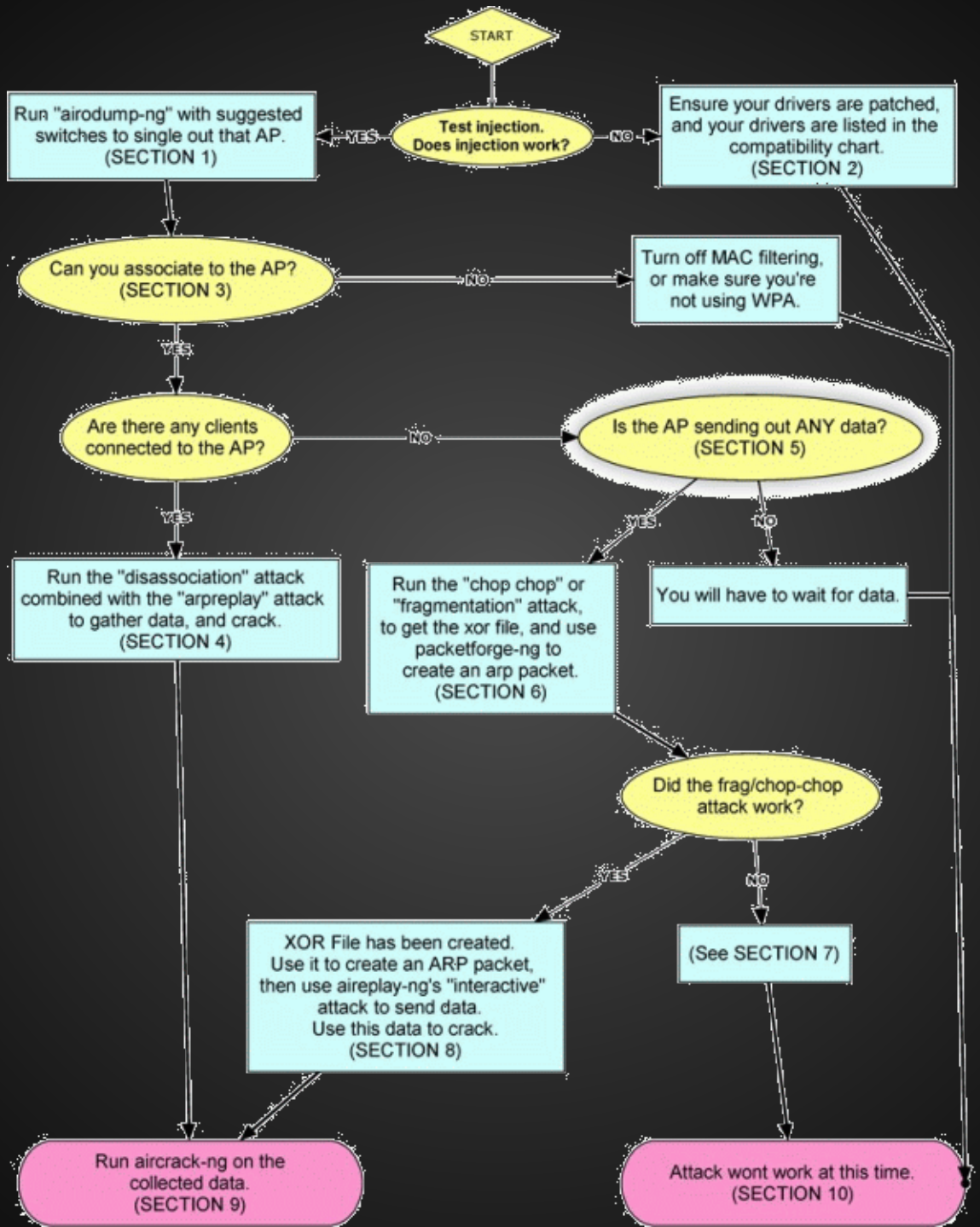
http://en.wikipedia.org/wiki/Man-in-the-middle_attack

Aircrack Suite

- "Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack. Aircrack-ng is a set of tools for auditing wireless networks."
- Version 1.0 released on 2004-07-29
- More information at: http://www.aircrack-ng.org/doku.php?id=Main

Aircrack-ng suite

airbase-ng
aircrack-ng
airdecap-ng
airdecloak-ng
airdriver-ng
airdrop-ng
aireplay-ng
airgraph-ng
airmon-ng
airodump-ng
airolib-ng
airserv-ng
airtun-ng
besside-ng
easside-ng
packetforge-ng
tkiptun-ng
wesside-ng


START
Test injection. Does injection work?
YES
NO
Run "airodump-ng" with suggested switches to single out that AP. (SECTION 1)
Ensure your drivers are patched, and your drivers are listed in the compatibility chart. (SECTION 2)
Can you associate to the AP? (SECTION 3)
NO
Turn off MAC filtering, or make sure you're not using WPA.
YES
Are there any clients connected to the AP?
NO
Is the AP sending out ANY data? (SECTION 5)
YES
Run the "disassociation" attack combined with the "arpreplay" attack to gather data, and crack. (SECTION 4)
YES
Run the "chop chop" or "fragmentation" attack, to get the xor file, and use packetforge-ng to create an arp packet. (SECTION 6)
NO
You will have to wait for data.
Did the frag/chop-chop attack work?
YES
NO
XOR File has been created. Use it to create an ARP packet, then use aireplay-ng's "interactive" attack to send data. Use this data to crack. (SECTION 8)
(See SECTION 7)
Run aircrack-ng on the collected data. (SECTION 9)
Attack wont work at this time. (SECTION 10)

Fun Part!

#Recognize Interface
ifconfig
#Bring Interface Down
ifconfig wlan0 down
#Spoof Mac Random
macchanger -A wlan0
#Bring Interface Back Up
ifconfig wlan0 up
#Discover USB Ports
lsusb
#Dongleing Intensifies
iw reg set BO
iwconfig wlan0 txpower 30dBm

#Start Usb Dongle wlan1
airmon-ng start wlan1
#Bring down Monitoring interface
ifconfig mon0 down
#Spoof Mac Random - Preferably 10 times
macchanger -A mon0
#Bring Monitoring Interface Up
ifconfig mon0 up
#Walk to a folder where I intend to save
cd Desktop/Swoosh
#Kill Wicd/Networkmanager because ICS
killall wicd/networkmanager
#Recon
airodump-ng

Karma

"KARMA is a set of tools for assessing the security of wireless clients at multiple layers. Wireless sniffing tools discover clients and their preferred/trusted networks by passively listening for 802.11 Probe Request frames. From there, individual clients can be targeted by creating a Rogue AP for one of their probed networks (which they may join automatically) or using a custom driver that responds to probes and association requests for any SSID. Higher-level fake services can then capture credentials or exploit client-side vulnerabilities on the host.

KARMA includes patches for the Linux MADWifi driver to allow the creation of an 802.11 Access Point that responds to any probed SSID. So if a client looks for 'linksys', it is 'linksys' to them (even while it may be 'tmobile' to someone else). Operating in this fashion has revealed vulnerabilities in how Windows and Mac look for networks, so clients may join even if their preferred networks list is empty."

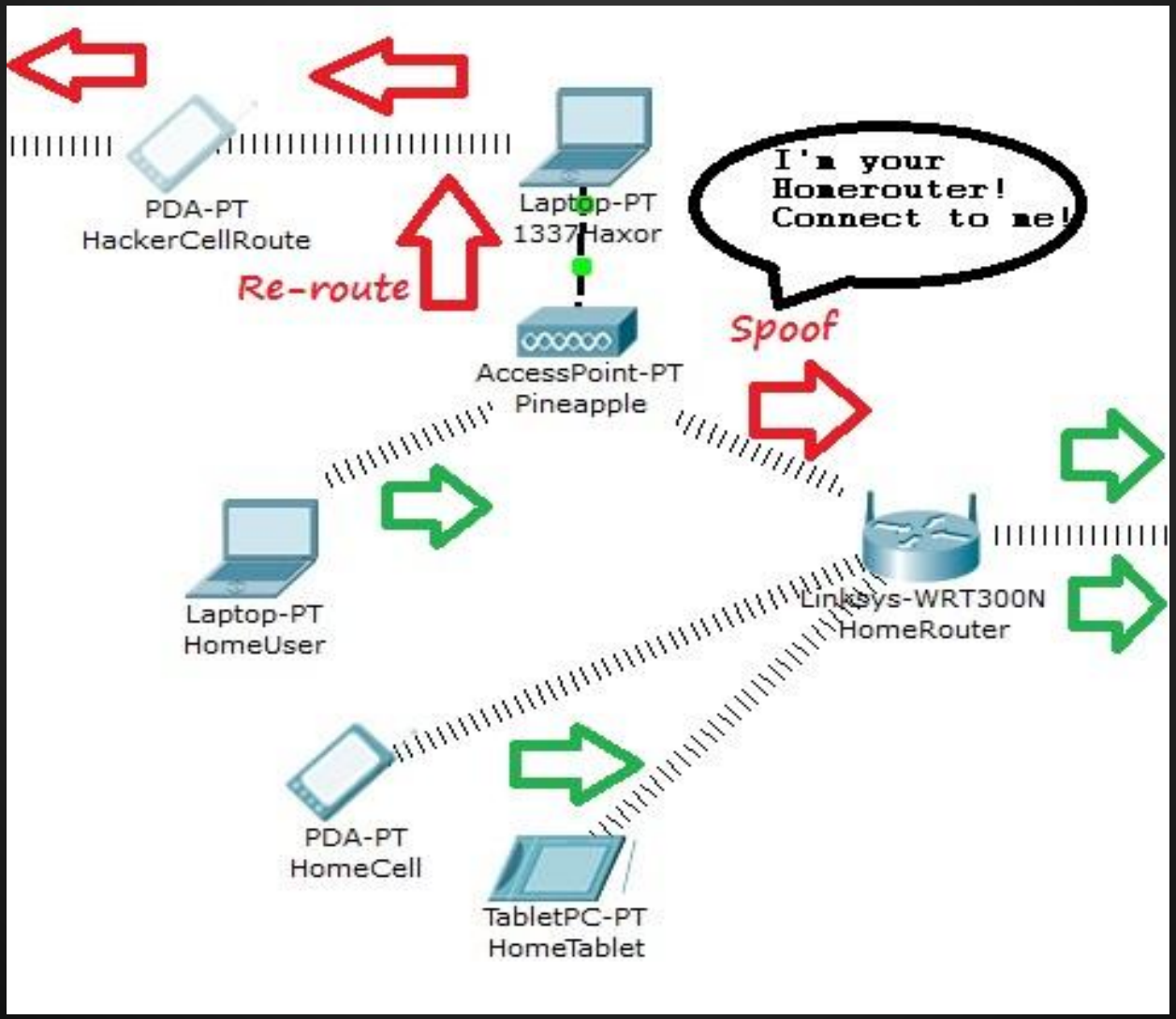
http://www.theta44.org/karma/

Wifi Pineapple Mark IV

Jasager firmware, based on openwrt with the latest Linux 3.2 kernel, implements a highly efficient kernel mode wireless "Karma" driver and support for loads of packages.

- Six common stealth deployment scenarios for secure remote target monitoring.
- MITM attack tools: Karma, DNS Spoof, SSL Strip, URL Snarf, Ngrep.
- Schedule tasks with editable user-scripts.
- Community built modules add functionality with web interfaces for additional tools: nmap, tcpdump, java attacks, WiFi Jammer, bandwidth monitor, dynamic dns, site survey and many more.
- Wireless cracking and deauth attacks with the Aircrack-NG suite.
- Autostart service like karma and reverse ssh for instant attack on power-up.
- Simple Mobile Broadband, Android Tethering, and Reverse SSH setups
- Hands-off deployment of locally hosted payloads in standalone mode
- http://wifipineapple.com/

Pineapple Reroute setup



Pineapple

- Demo Occupineapple/MK4
- Demo Karma/Deauth-Mk3/Jammer
- Demo Dns/Spoof Rickroll
- Demo Dual Attack Interfaces Via Backtrack

Demo Firestorm

Things to do prior:

1. Whitelist/Blacklist MAC Vulnerable AP
2. Confirm Cronjobs/Clean-up Scripts
3. Add auto-connection/Antenna directional
4. Killall Wicd/Networkmanager for ICS Demo

Deauthentication

Aireplay-ng is used to inject frames.

It currently implements multiple different attacks:

Attack 0: Deauthentication

Attack 1: Fake authentication

Attack 2: Interactive packet replay

Attack 3: ARP request replay attack

Attack 4: KoreK chopchop attack

Attack 5: Fragmentation attack

Attack 6: Cafe-latte attack

Attack 7: Client-oriented fragmentation attack

Attack 8: WPA Migration Mode

Attack 9: Injection test

aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 mon0

Where:

-0 means deauthentication

1 is the number of deauths to send (you can send multiple if you wish); 0 means send them continuously

-a 00:14:6C:7E:40:80 is the MAC address of the access point

-c 00:0F:B5:34:30:30 is the MAC address of the client to deauthenticate; if this is omitted then all clients are deauthenticated

mon0 is the Dongle interface name

http://www.aircrack-ng.org/doku.php?id=deauthentication

Maltego / Casefile

" CaseFile is the little brother to Maltego. It targets a unique market of 'offline' analysts whose primary sources of information are not gained from the open-source intelligence side or can be programmatically queried. We see these people as investigators and analysts who are working 'on the ground', getting intelligence from other people in the team and building up an information map of their investigation.

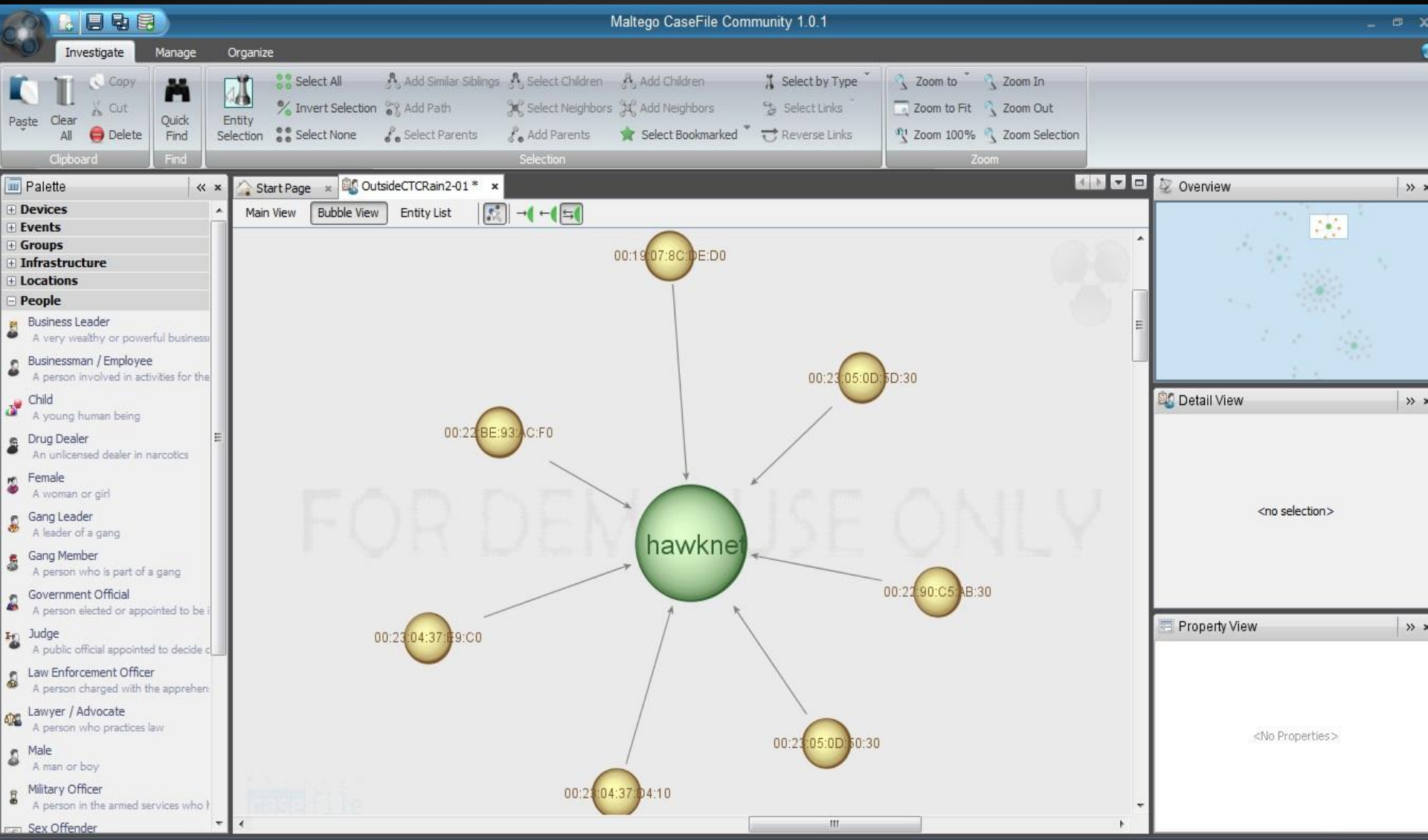
CaseFile gives you the ability to quickly add, link and analyze data having the same graphing flexibility and performance as Maltego without the use of transforms. CaseFile is roughly a third of the price of Maltego."

- http://www.paterva.com/web6/products/casefile.php

"Open-source intelligence (**OSINT**) is intelligence collected from publicly available sources. In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources); it is not related to open-source software or public intelligence."

- http://en.wikipedia.org/wiki/Open_source_intelligence

Maltego / Casefile



References

http://vimeo.com/8826952 - **Antennas 101 - Polarization, Diversity & Gain Patterns**

http://www.aircrack-ng.org/doku.php?id=Main **- Aircrack-ng**

http://www.theta44.org/karma/ **- Karma**

http://wifipineapple.com/ - **Wifi Pineapple**

http://www.paterva.com/web6/products/casefile.php - **Casefile**