Wireless Network Risks and Controls

Offensive Security Tools, Techniques, and Defenses

22 January 2015 – ISACA Phoenix Chapter – Phoenix, AZ

Presented by:
Ruihai Fang
Dan Petro
Bishop Fox
www.bishopfox.com

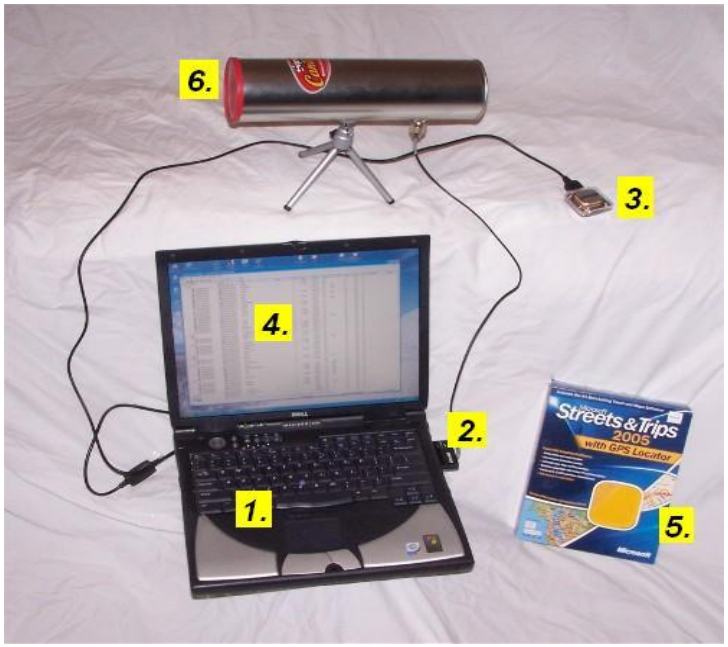
BISHOP FOX

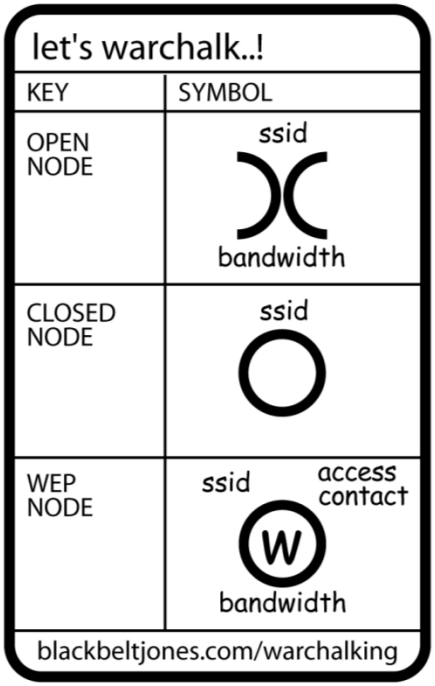
Introduction/Background

GETTING UP TO SPEED

Used to be a Pain

Lots to of heavy things to carry





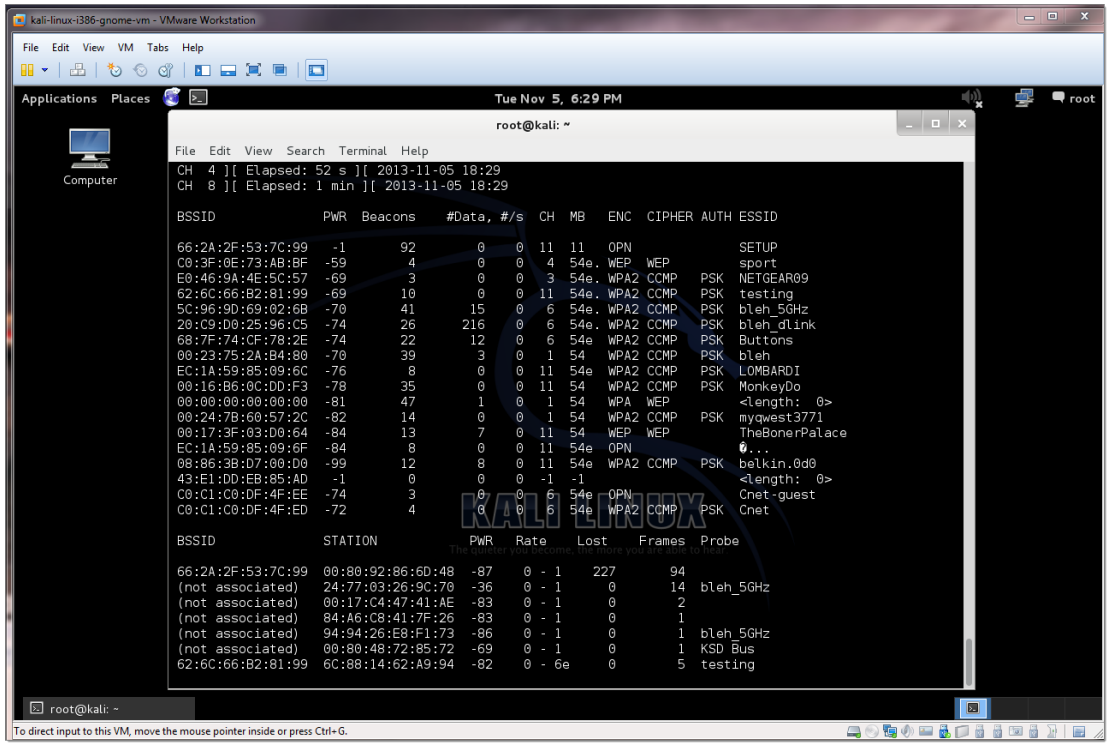
BISHOP FOX

Kali VM and USB Adapter

NOW EASY

- Kali Linux VM + TP-LINK - TL-WN722N (USB)

+



Laptops, Netbooks (easier to conceal), and adapters

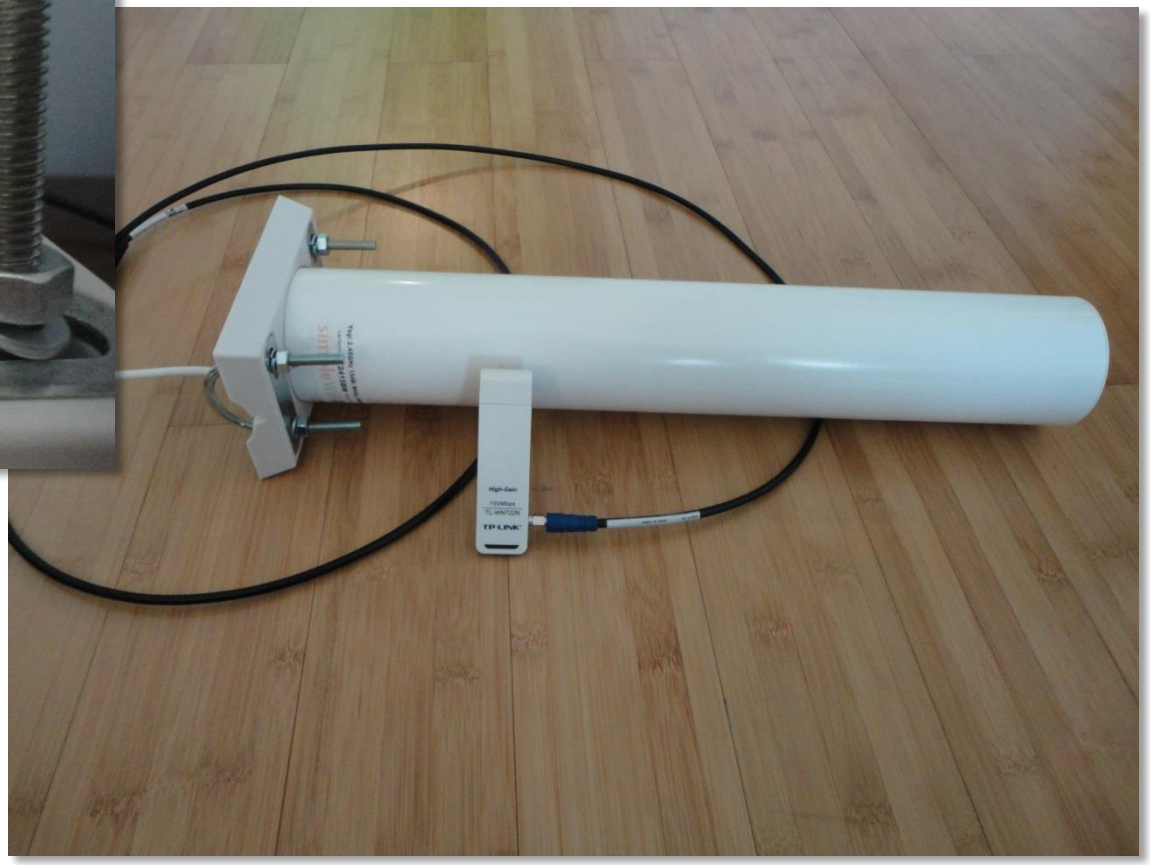
TP-Link Adapter
Capable of attaching a YAGI antenna

Asus EEPc

BISHOP FOX

YAGI Antennas – Directional

Very good for attacking from a distance, like from the comfort of your hotel room.



BISHOP FOX

Antenna Connector Cables are Necessary

BISHOP FOX

WiFi Hacking Using Android Phones

StarTech Micro USB
On-the-go Adapter

Samsung Galaxy S3

Alfa 1000mW 1W 802.11b/g USB
WiFi Adapter. Uses RTL8187 Chipset.

BISHOP FOX

Wireless Hacking Tools

ACROSS VARIOUS OS'S

Wireless Tools

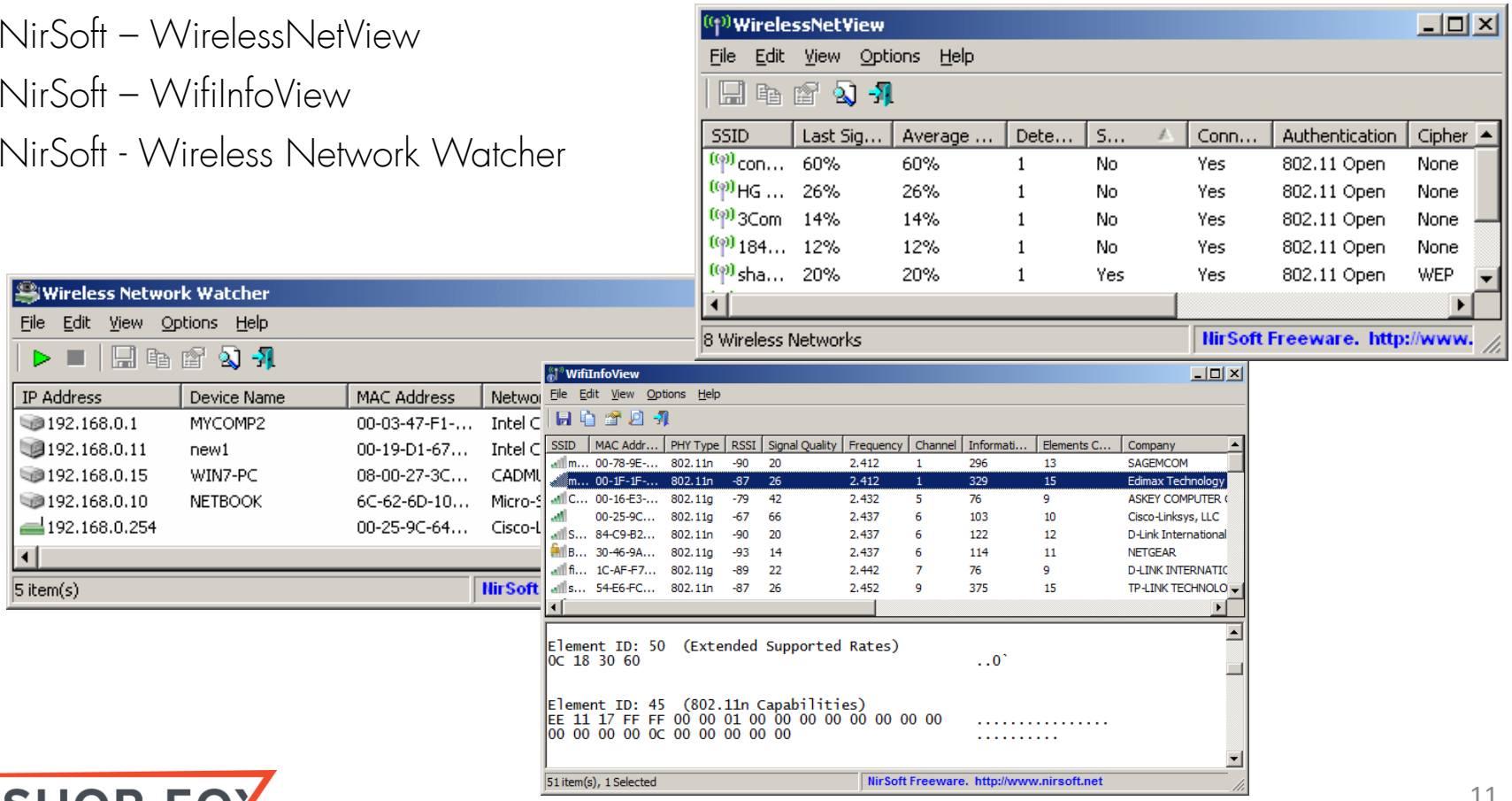
Discovery

- Supported operating systems
- Supported wireless protocols
- Active vs. passive scanning
- Packet capturing and decoding
- Distinguishes between AP, ad hoc, and client devices
- Statistics and reporting capabilities
- User interface
- Price

NirSoft Wireless Tools

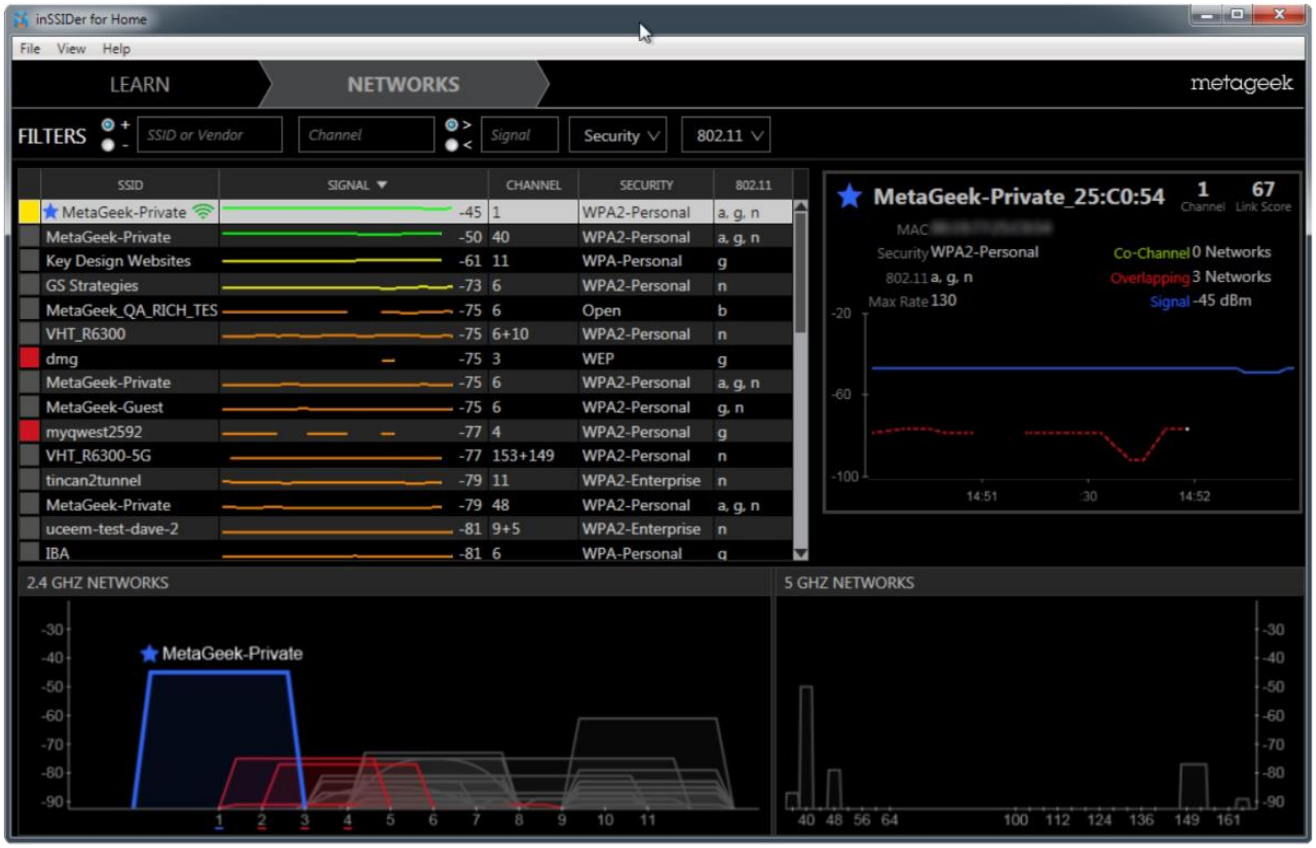
WINDOWS HACKING TOOLS

- NirSoft – WirelessNetView
- NirSoft – WifiInfoView
- NirSoft - Wireless Network Watcher



inSSIDer Wi-Fi Scanner

WINDOWS HACKING TOOLS



BISHOP FOX

Aircrack-ng Suite

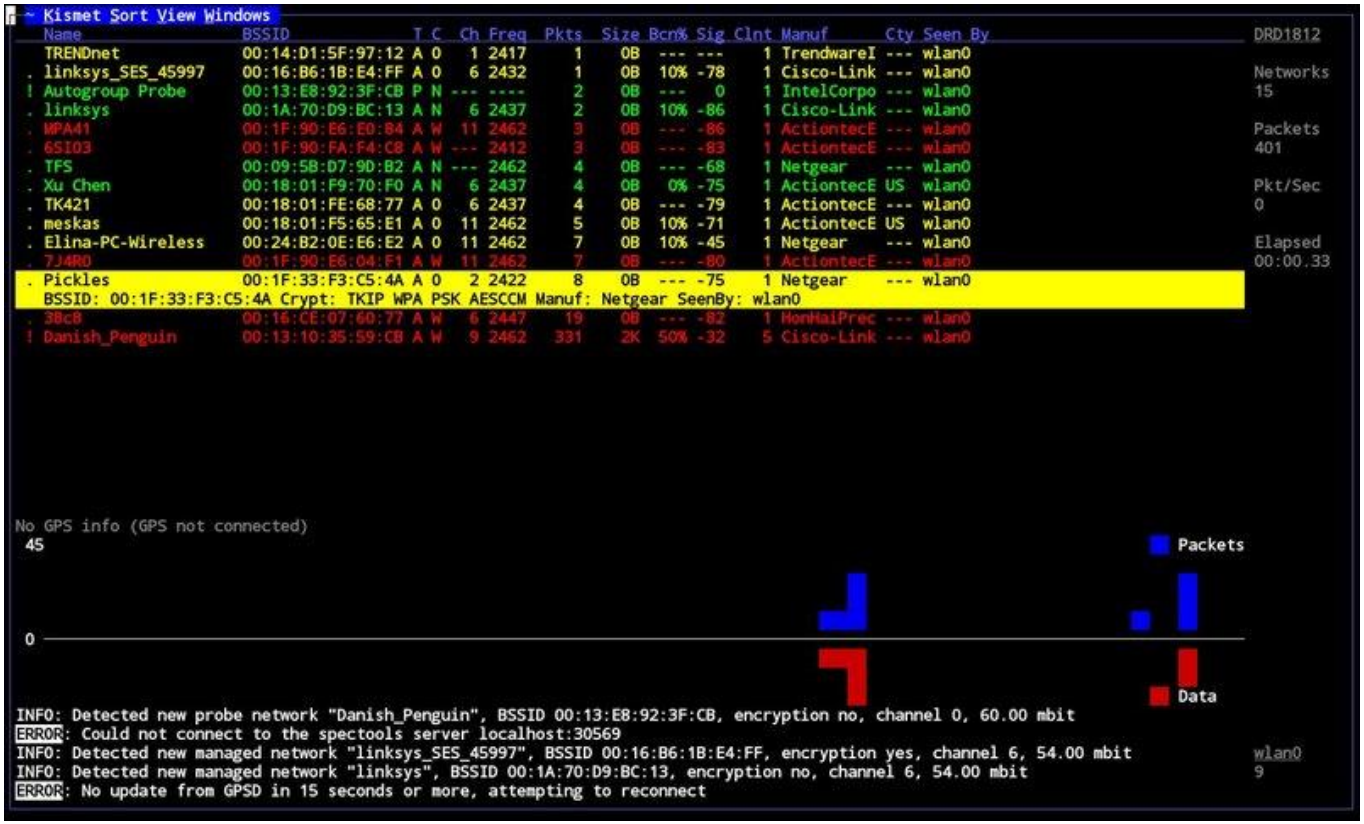
LINUX HACKING TOOLS

The aircrack-ng software suite includes:

Name	Description
aircrack-ng	Cracks WEP and WPA (Dictionary attack) keys.
airdecap-ng	Decrypts WEP or WPA encrypted capture files with known key.
airmon-ng	Placing different cards in monitor mode.
aireplay-ng	Packet injector (Linux, and Windows with CommView drivers).
airodump-ng	Packet sniffer: Places air traffic into PCAP or IVS files and shows information about networks.
airtun-ng	Virtual tunnel interface creator.
packetforge-ng	Create encrypted packets for injection.
ivstools	Tools to merge and convert.
airbase-ng	Incorporates techniques for attacking client, as opposed to Access Points
airdecloak-ng	removes WEP cloaking from pcap files
airdriver-ng	Tools for managing wireless drivers
airolib-ng	stores and manages ESSID and password lists and compute Pairwise Master Keys
airserv-ng	allows you to access the wireless card from other computers.
buddy-ng	the helper server for easside-ng, run on a remote computer
easside-ng	a tool for communicating to an access point, without the WEP key
tkiptun-ng	WPA/TKIP attack
wesside-ng	automatic tool for recovering wep key.

Kismet

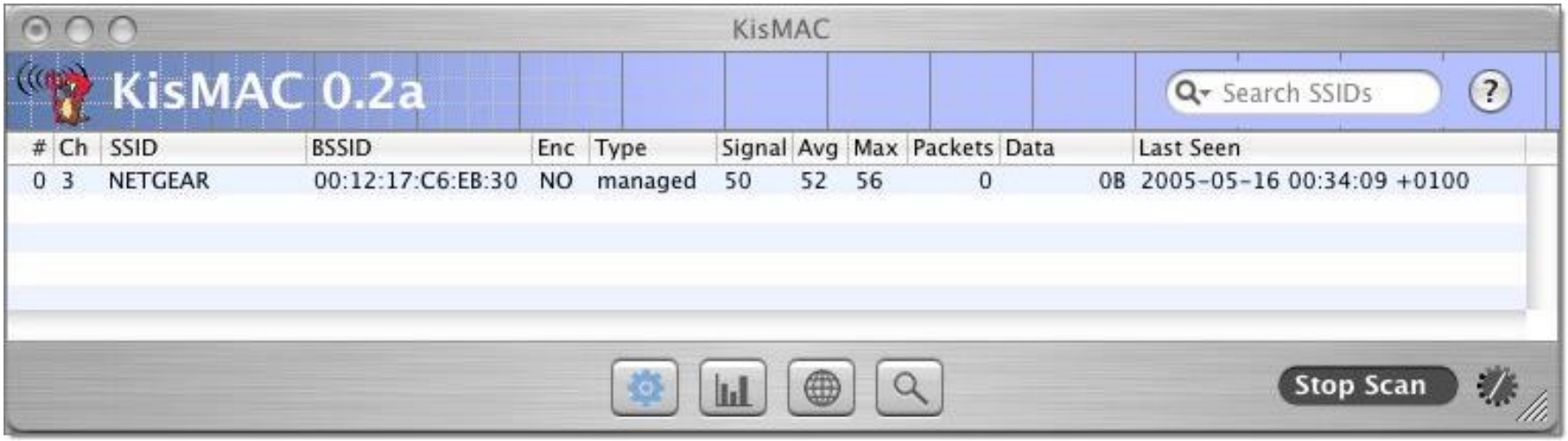
LINUX HACKING TOOLS



BISHOP FOX

Kismac

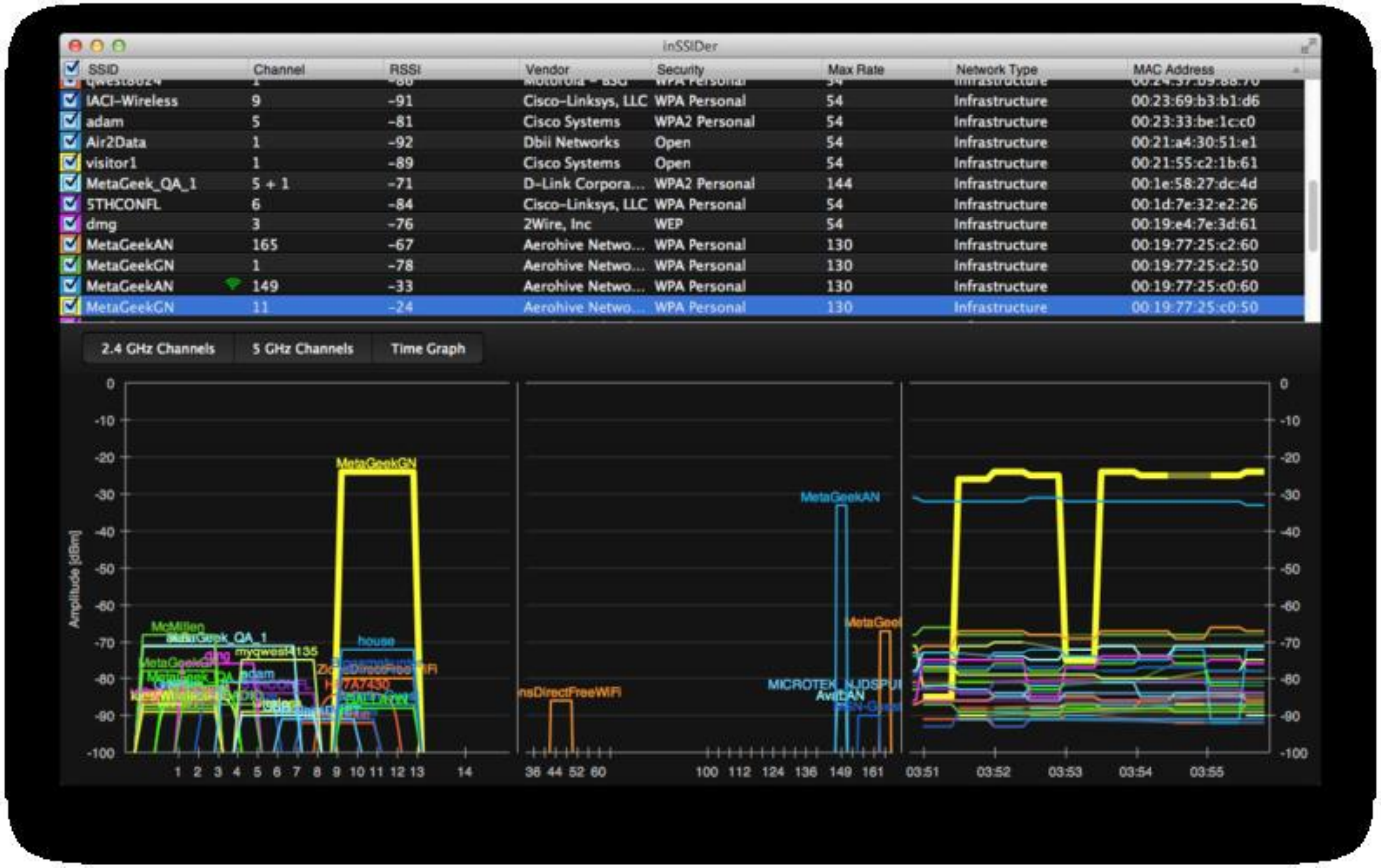
MAC OS X HACKING TOOLS



BISHOP FOX

inSSIDer for Mac

MAC OS X HACKING TOOLS



Wi-Fi Pineapple

WIRELESS PENETRATION TESTING ROUTER

Features

WHAT CAN IT DO?

- Wireless Jamming (De-auth Attack)
- Man-in-the-Middle attack
- DNS Spoof on lure client
- Web base management
- Tether via Mobile Broadband
- Battery power and portable

BISHOP FOX

Specs

THE HARDWARE

- Atheros AR9331 SoC at 400MHz
- 802.11 b/g/n 150 Mbps wireless
- 2x Ethernet, one PoE (Power-Over-Ethernet) capable
- USB 2.0 for expanded storage, WiFi Interface and Mobile Broadband
- Fast Linux Kernel 3.2 based Jasager Firmware

Methodology

Social Engineering

1. **Karma (Rogue AP)**

2. **DNS Spoof & MITM**

3. **Phishing**

Auto-Association

PROBLEM TO EXPLOIT

BISHOP FOX

Karma

HOW DOES IT WORK?

- Listen to wireless probes from nearby wireless devices
- Impersonate as the requested wireless AP

Karma

ROGUE AP

DNS Spoof

POISONING YOUR DNS

- Modify DNS records and point to a malicious site
- Man-in-the-middle between the victim and Internet

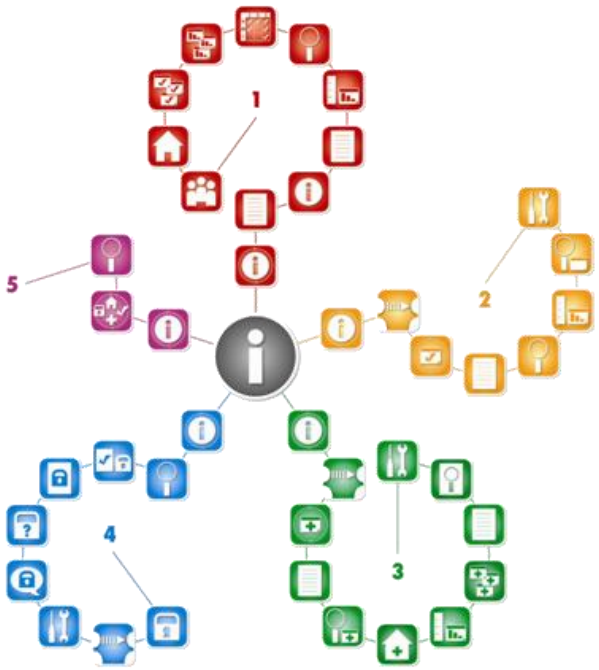
BISHOP FOX

Phishing

PHISHING ATTACK

- Clone the official website (reddit.com)
- Implement key logger
- Deploy malware or backdoor on the forged website
- Compromise the victim

DEMO



Mitigation

Things that you should be doing

1. Disable the "Connect Automatically" setting on all unsecured wireless networks.

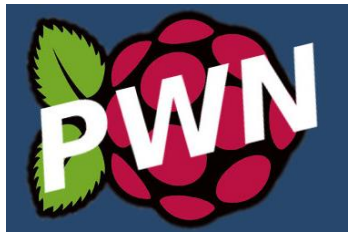
2. Use DNS Crypt or Google DNS

3. Don't connect to any unsecured or unknown wireless network

4. Use a trusted VPN tunnel to encrypt the traffic on public network

Raspberry Pi

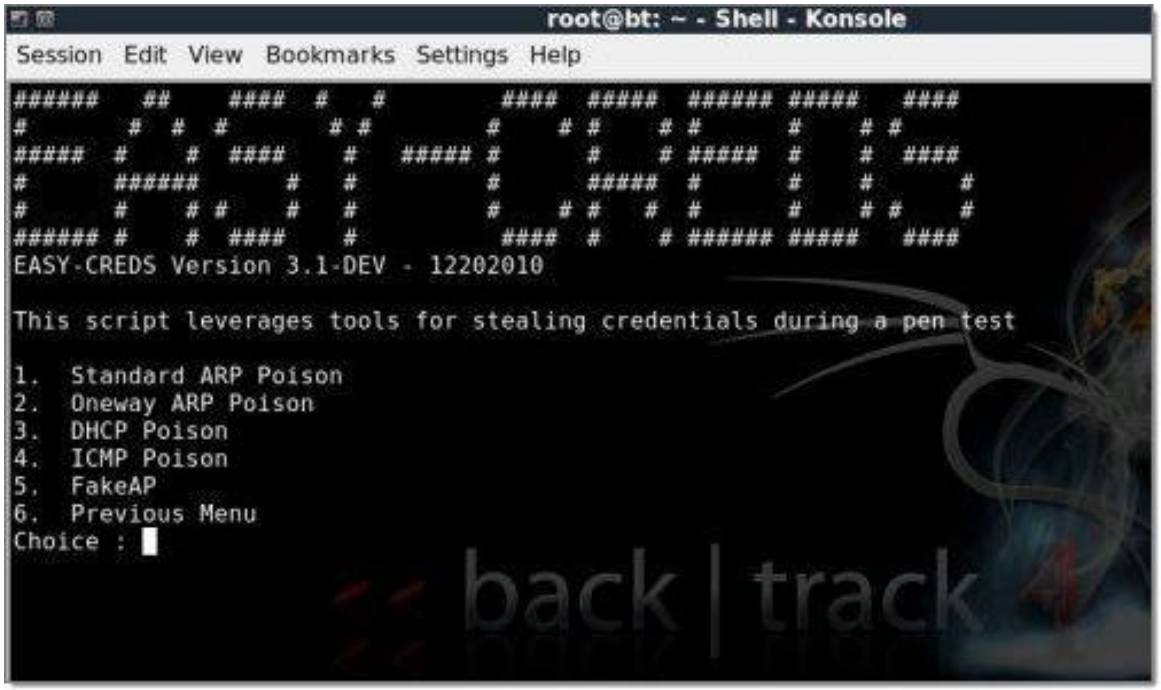
FRUITY WIFI



- Raspberry Pi – cheap alternative (~$35)
  - Fruity WiFi – Raspberry Pi version of the WiFi Pineapple

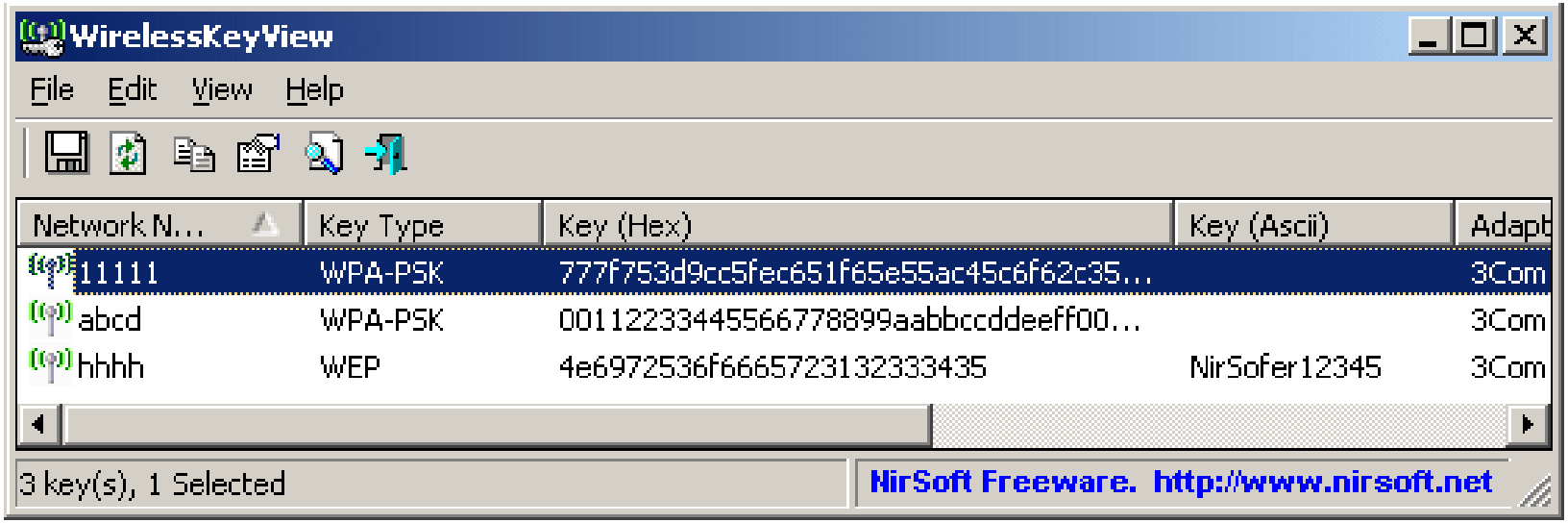
Easy-creds

AUTOMATING WIFI CLIENT ATTACKS



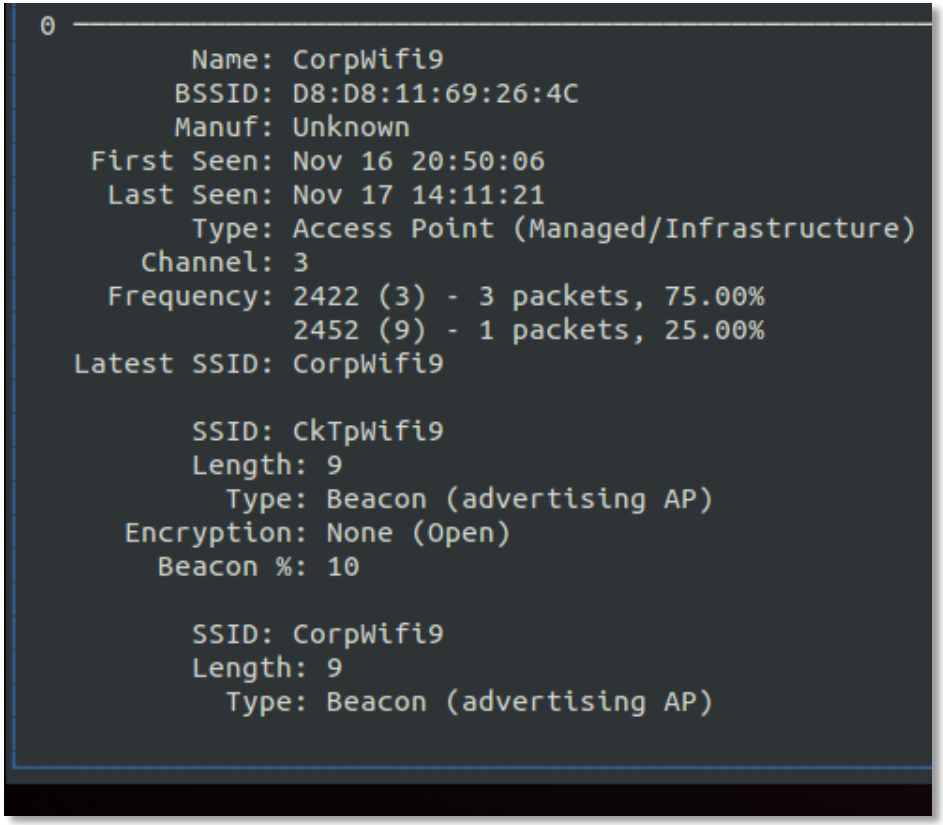
Dumping Keys

CLIENT EXPLOITING



Cracking WPA2-PSK with Pyrit

Using Kismet We've Decided on our Target Network



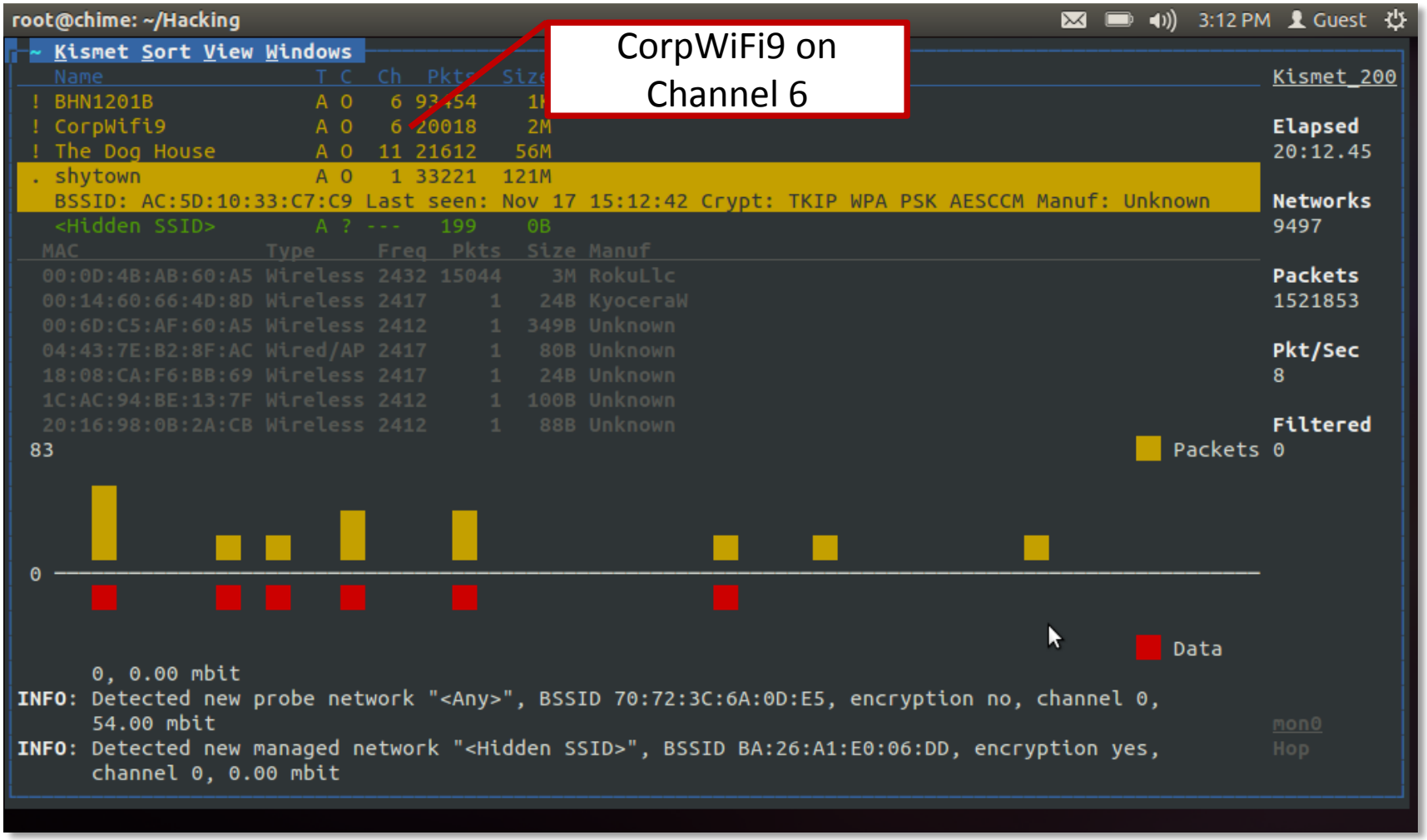
BISHOP FOX

Pyrit

https://code.google.com/p/pyrit/

Pyrit allows to create massive databases, pre-computing part of the IEEE 802.11 WPA/WPA2-PSK authentication phase in a space-time-tradeoff. Exploiting the computational power of Many-Core- and other platforms through ATI-Stream, Nvidia CUDA and OpenCL, it is currently by far the most powerful attack against one of the world's most used security-protocols.

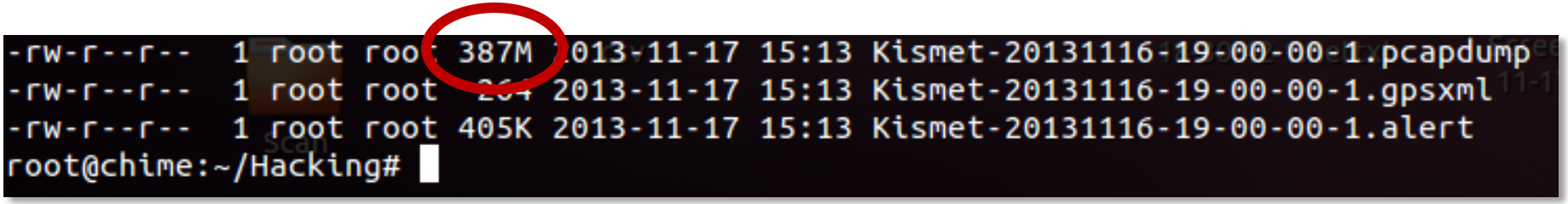
During Recon Find What Channel Your Target is on and Capture only on that Channel to Increase Your Chances of Getting a Valid WPA Handshake



BISHOP FOX

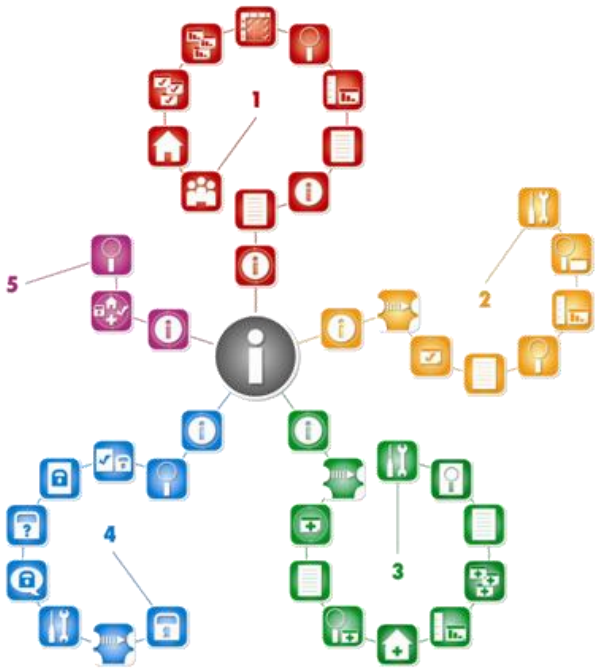
Passive Monitoring with Kismet

Running Kismet for 12 hours will capture lots of packets and PCAP files can be large.



BISHOP FOX

DEMO

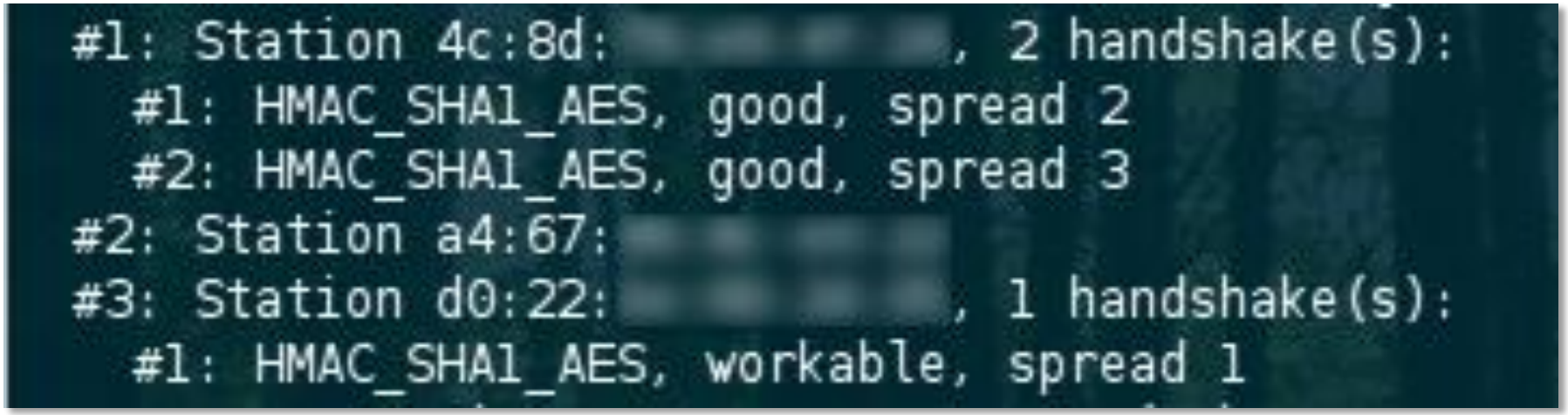


Stripping a PCAP File with Pyrit

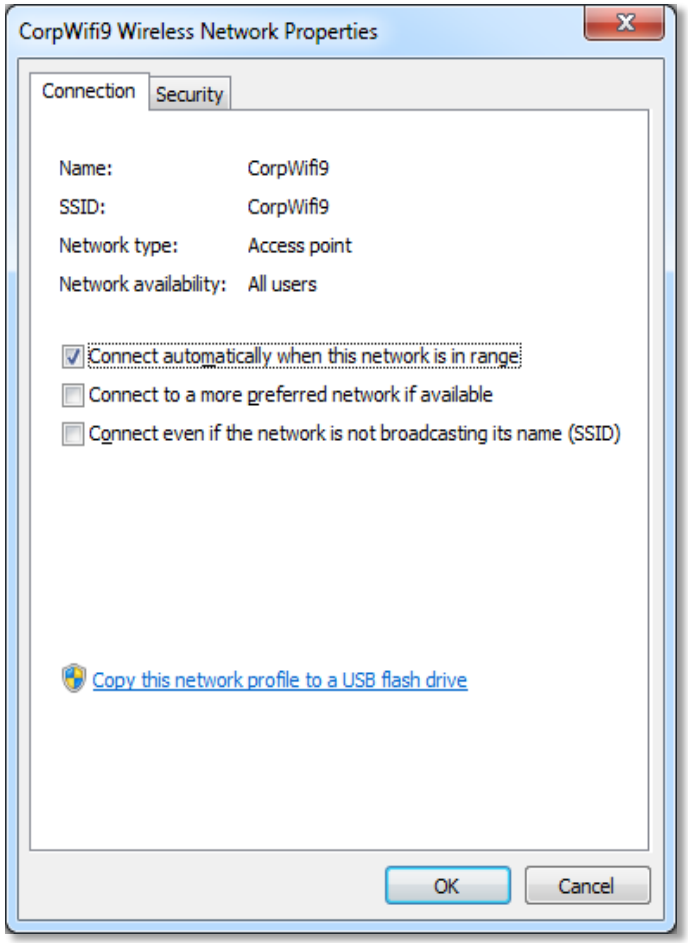
```
root@ubuntu:~/Hacking/pyrit-0.3.0/WPA2_Handshakes# ls -lah Kismet-20131116-19-00-00-1.pcapdump
-rw-r--r-- 1 root root 387M Nov 17 17:11 Kismet-20131116-19-00-00-1.pcapdump
root@ubuntu:~/Hacking/pyrit-0.3.0/WPA2_Handshakes# pyrit -r Kismet-20131116-19-00-00-1.pcapdump -o Kismet_Stripped.pcap strip
Pyrit 0.4.1-dev (svn r308) (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Parsing file 'Kismet-20131116-19-00-00-1.pcapdump' (1/1)...
/usr/local/lib/python2.7/dist-packages/cpyrit/pckttools.py:507: UserWarning: Failed to compile BPF-filter. This may be due to a bu
g in Pyrit or because your version of libpcap is too old. Falling back to unfiltered processing...
  warnings.warn("Failed to compile BPF-filter. This may be due to " \

Parsed 1522469 packets (1508121 802.11-packets), got 14245 AP(s)
```

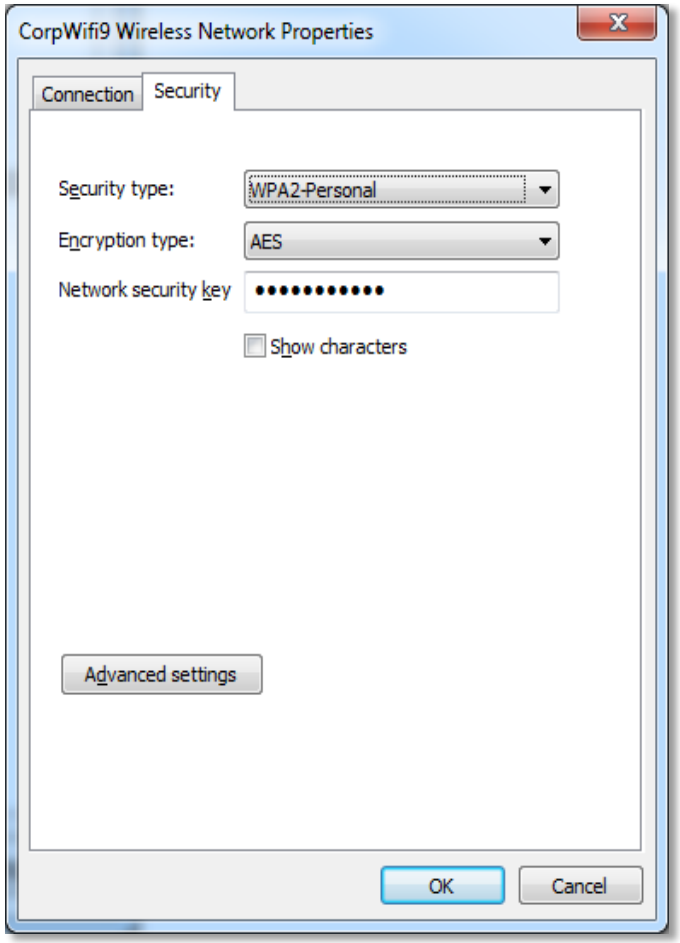
BISHOP FOX

Randomly Captured WPA2 Handshake After Running Kismet for 12 hours in my apartment



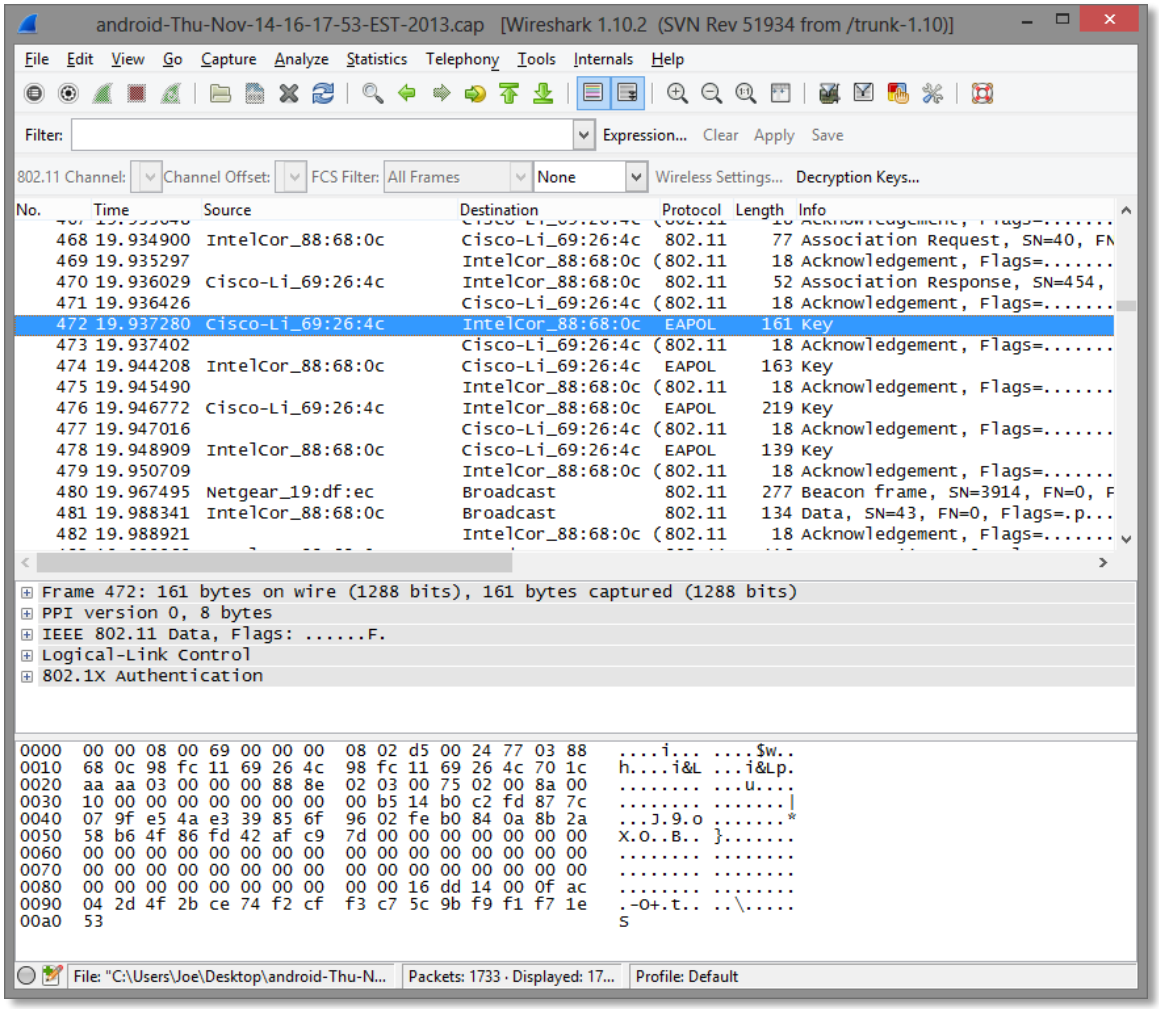
A Typical Windows 7 Wireless Client Using WPA2





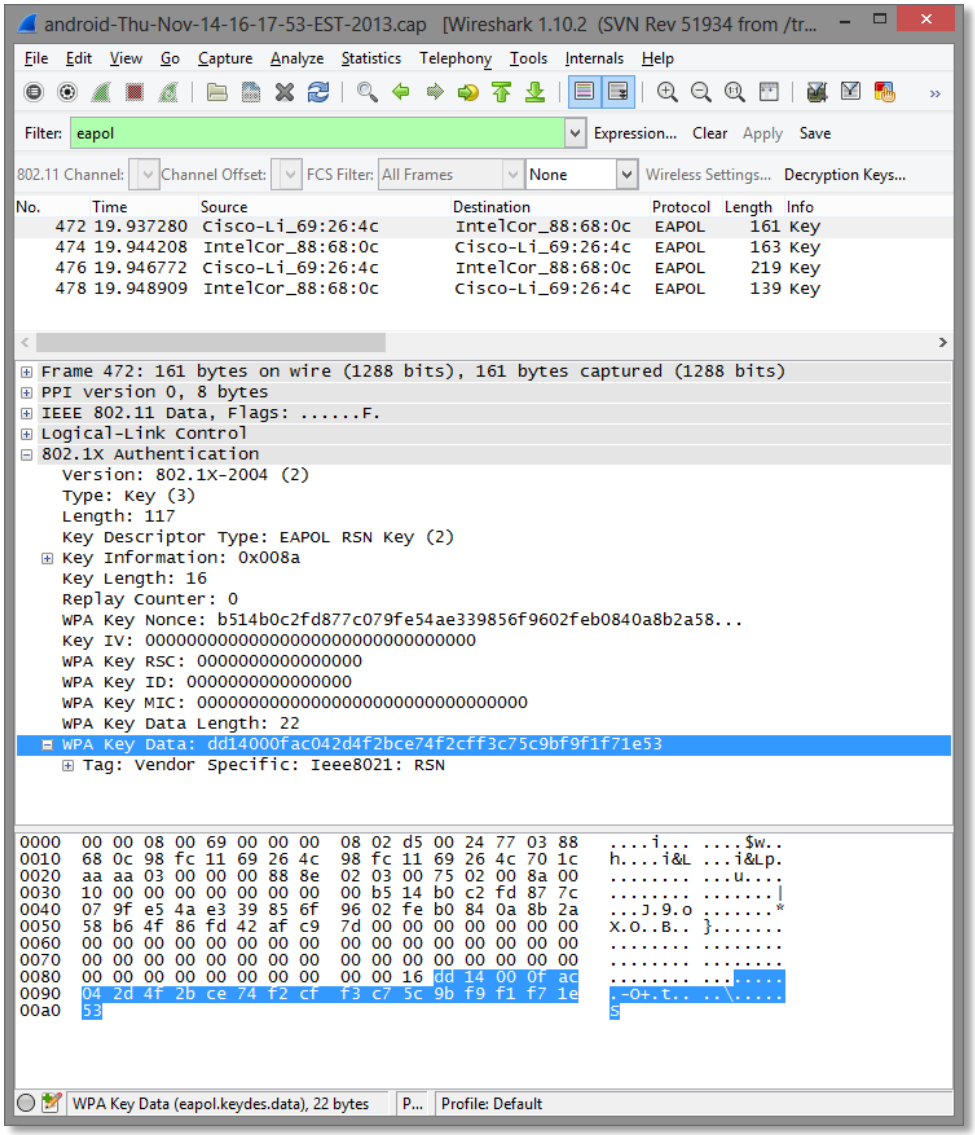
BISHOP FOX

WPA 4-Way Handshake



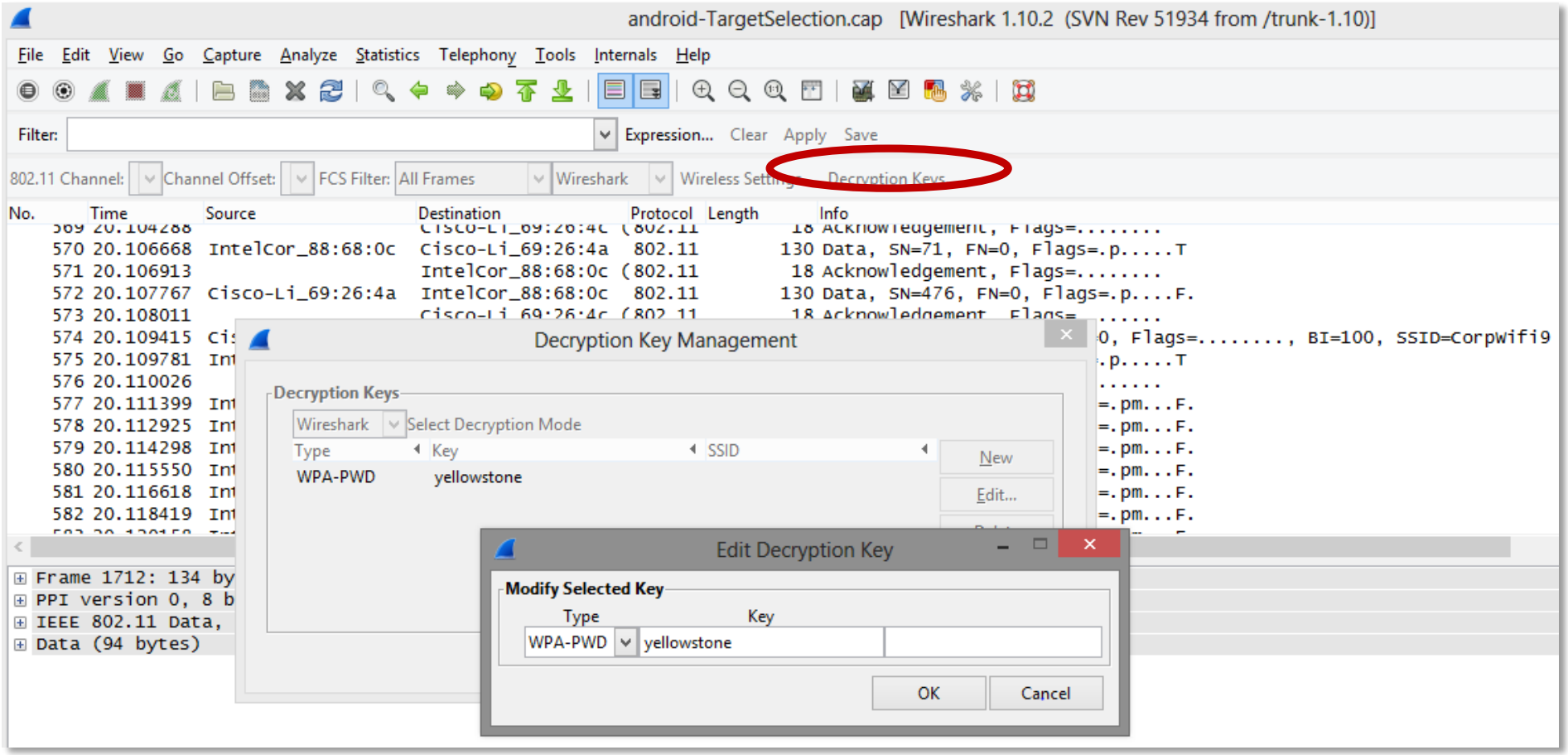
BISHOP FOX

WPA 4-Way Handshake



BISHOP FOX

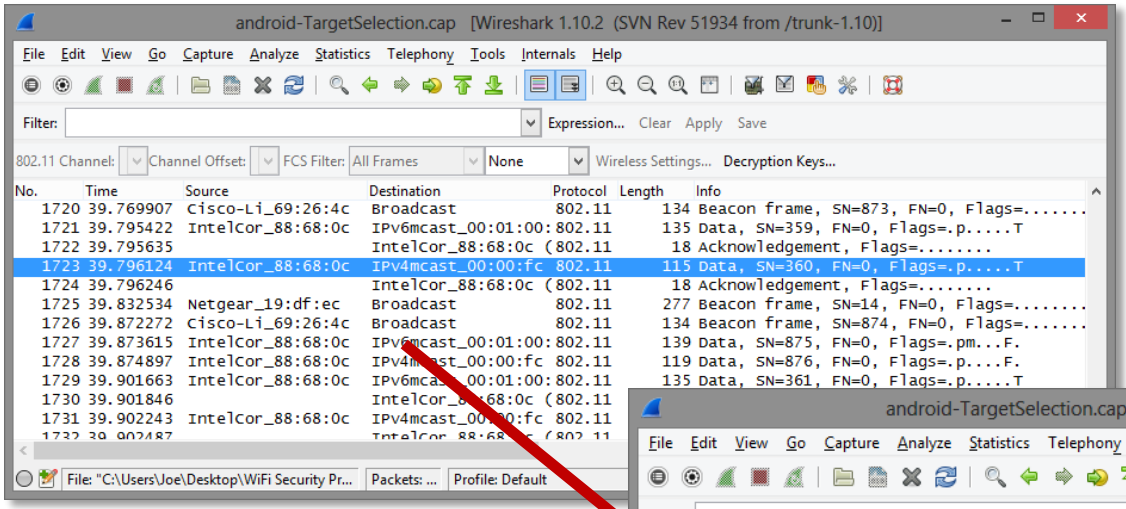
Decrypting WPA Packet Captures with Found Key in Wireshark



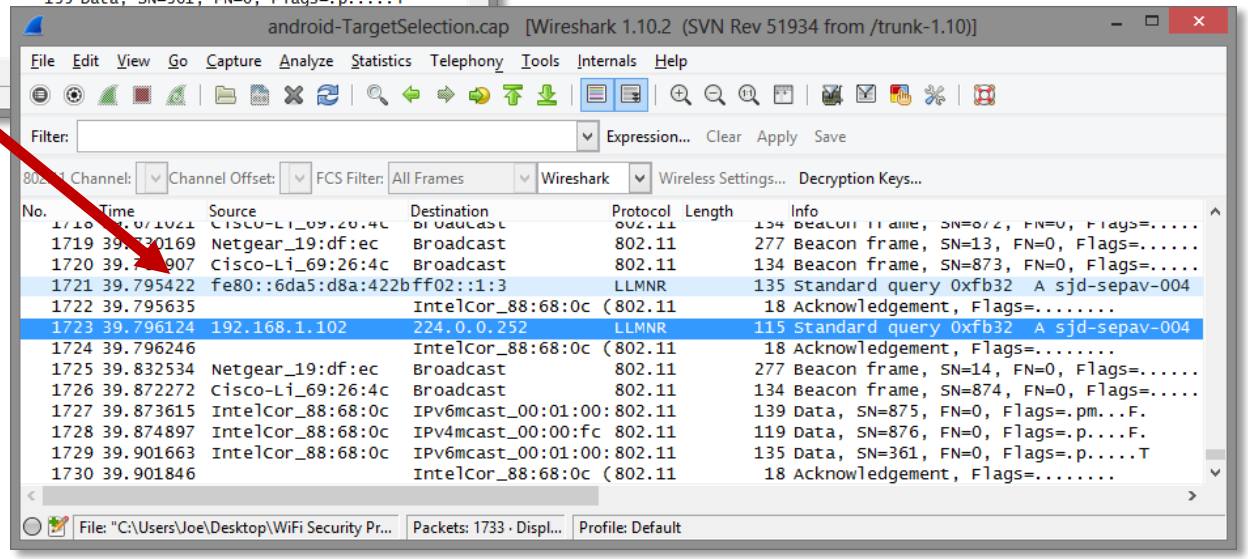
BISHOP FOX

Before and After Decryption in Wireshark

Before Applying WPA Key

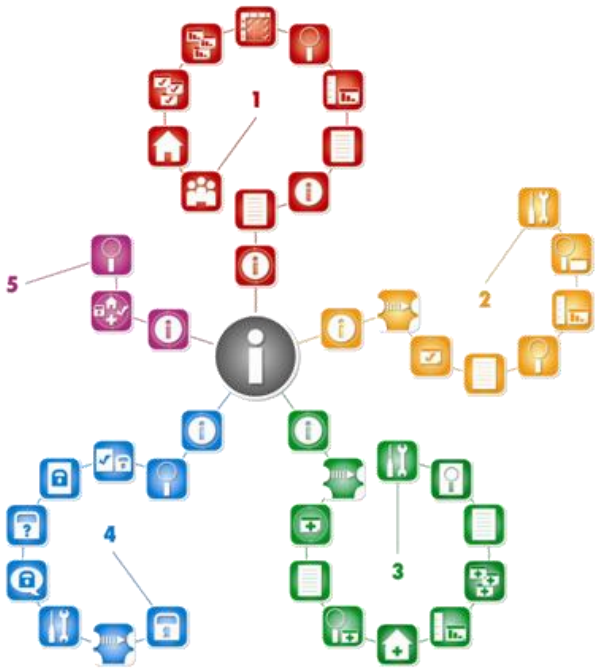


After Applying WPA Key



BISHOP FOX

Mobile WiFi Security Tools



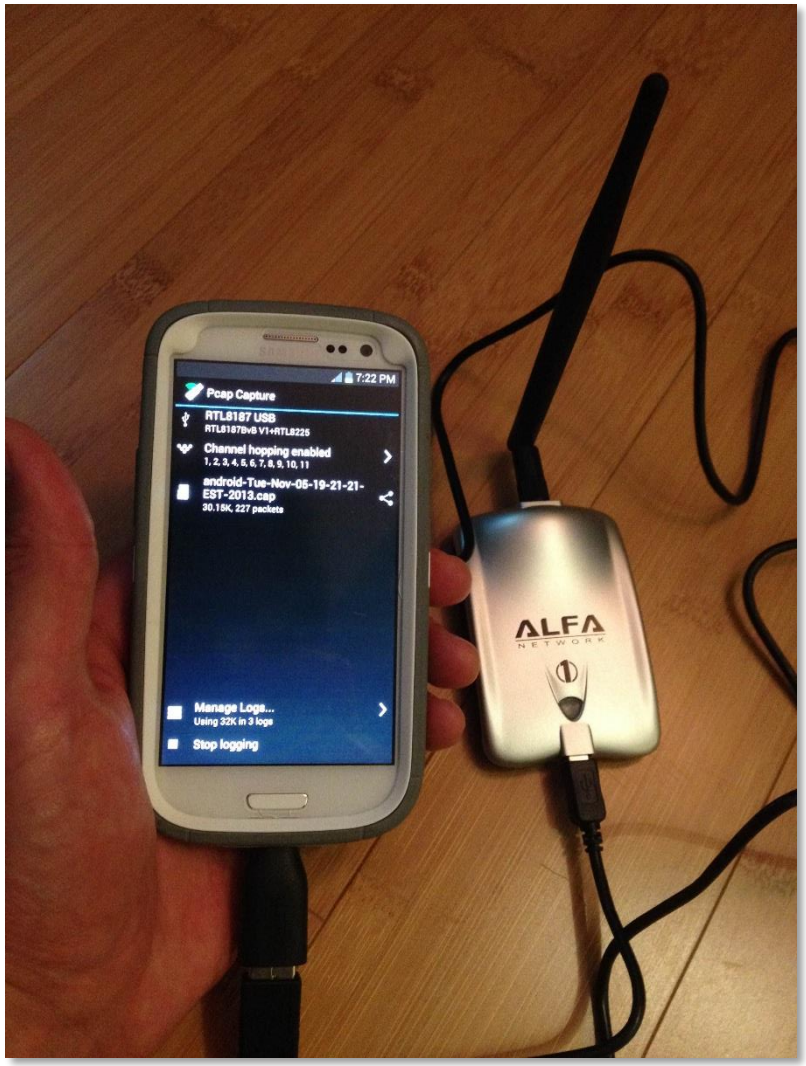
Popular Mobile WiFi Hacking Tools

WiFi Sniffing on Android in Monitor Mode
http://www.kismetwireless.net/android-pcap/

Password Sniffing & Session Hijacking Using dSploit
http://dsploit.net/

iphone-wireless https://code.google.com/p/iphone-wireless/wiki/Stumbler

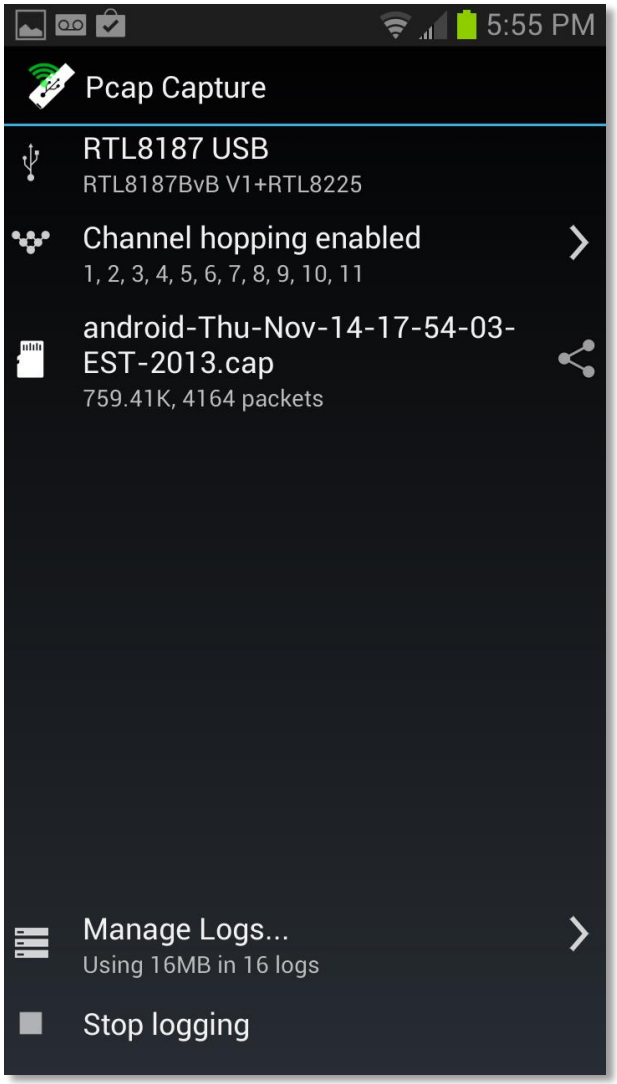
More Discreet Monitoring Using Alpha 1 802.11b/g



Model Number AWUS036H. This uses the RTL8187 Wireless Chipset.

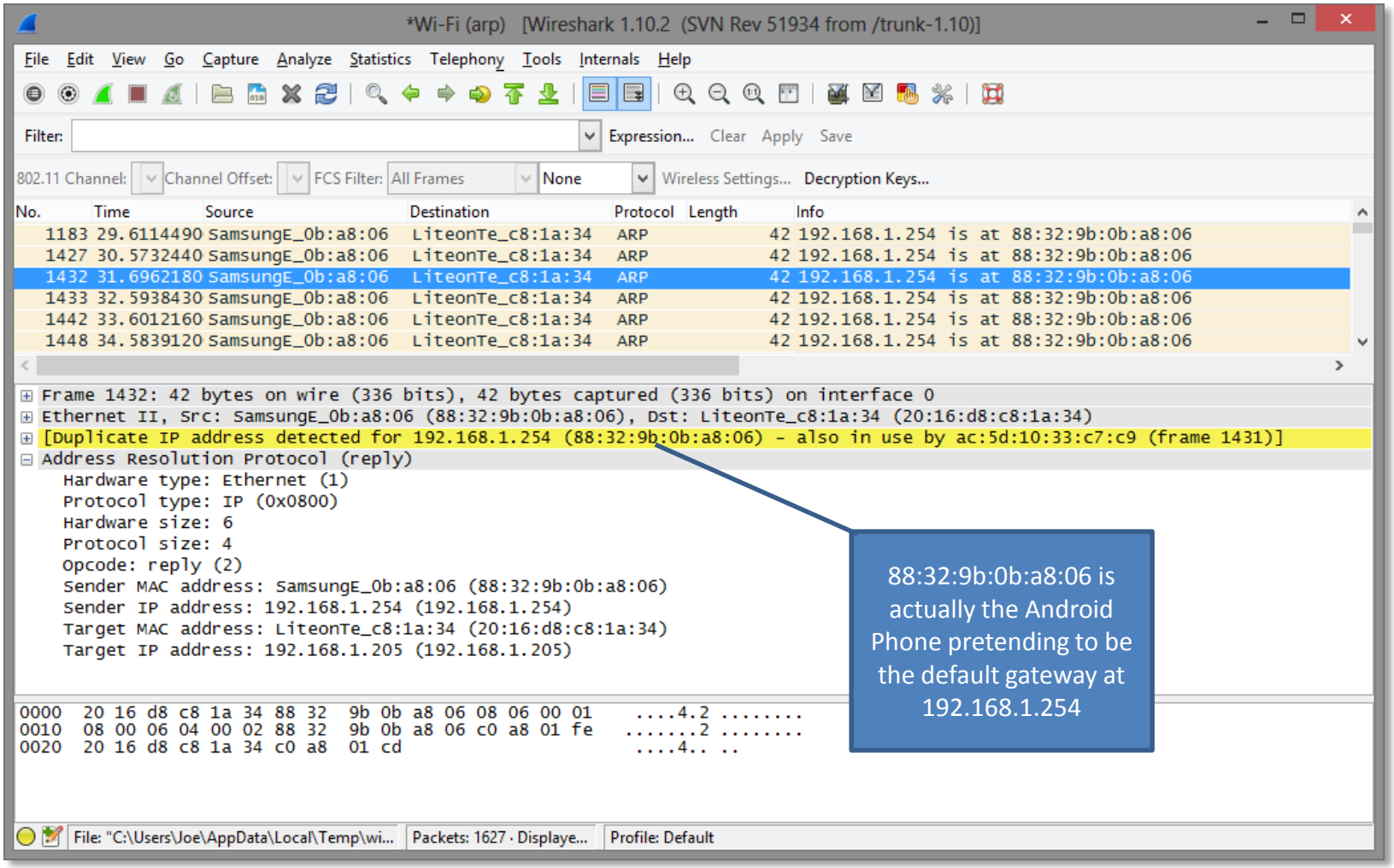
BISHOP FOX

Android PCAP Monitor Mode on a Galaxy S3



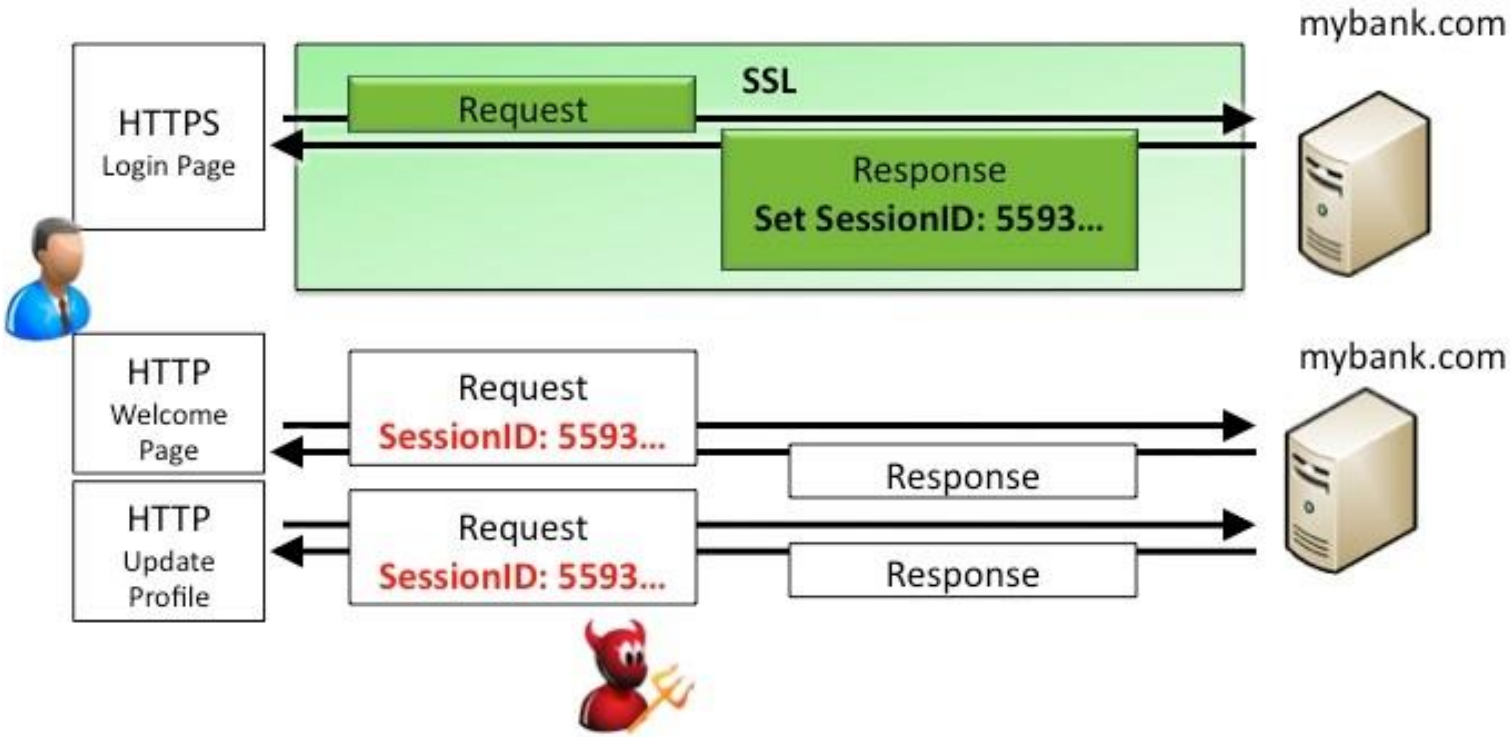
BISHOP FOX

Arp Spoofing & Detection

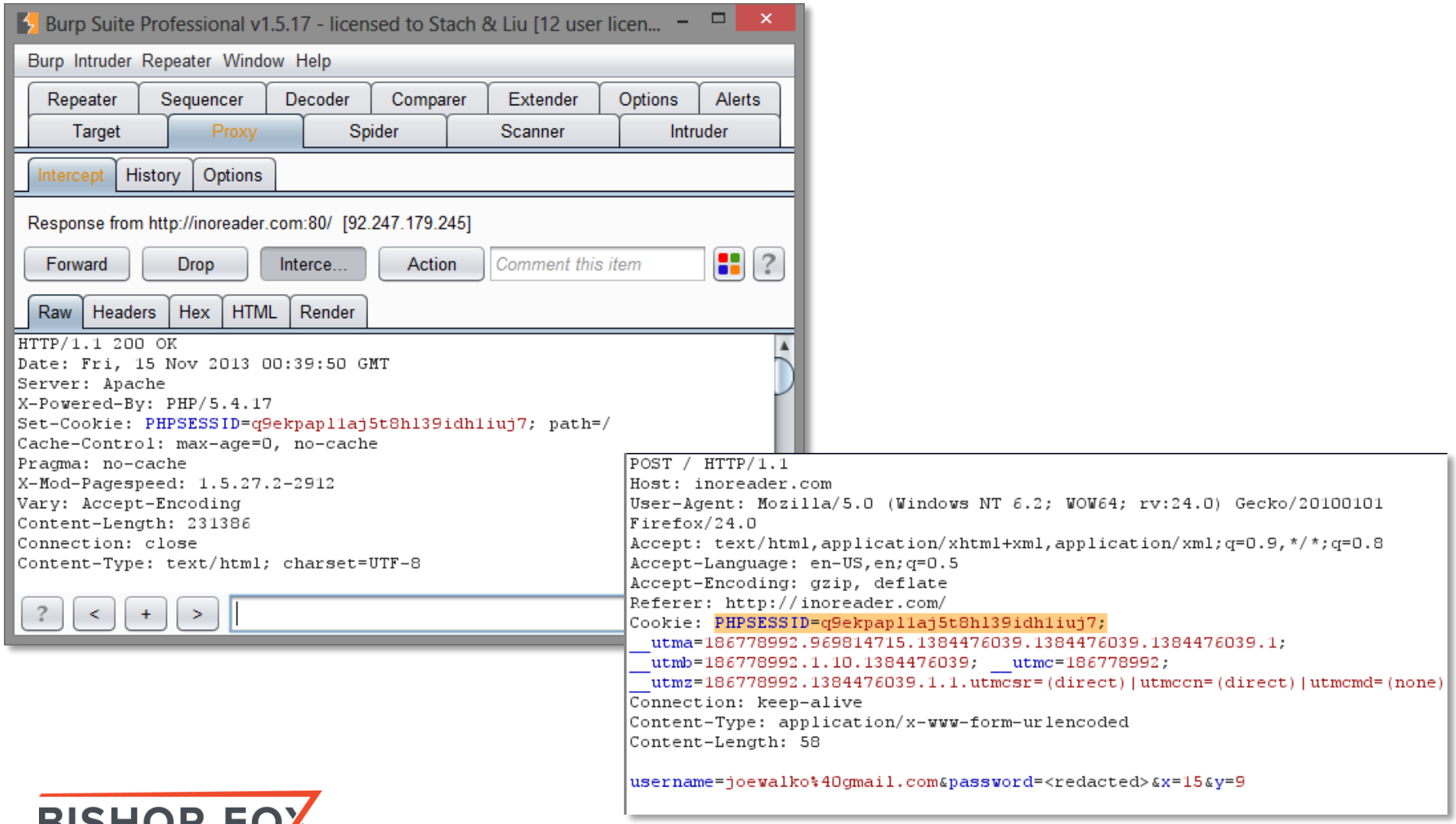


BISHOP FOX

Stealing Unencrypted Session IDs



Web Session Hijacking using dSploit



BISHOP FOX

PwnPad

NEXUS 7 PENTEST DEVICE

Toolkit includes:

Wireless Tools

- Aircrack-ng
- Kismet
- Wifite
- Reaver
- MDK3
- EAPeak
- Asleap
- FreeRADIUS-WPE
- Hostapd

Bluetooth Tools:

- bluez-utils
- btscanner
- bluelog
- Ubertooth tools

Web Tools

- Nikto
- W3af

Network Tools

- NET-SNMP
- Nmap
- Netcat
- Hping3
- Macchanger
- Tcpdump
- Tshark
- Ngrep
- Dsniff
- Ettercap-ng
- SSLstrip
- Hamster & Ferret
- Metasploit
- SET
- Easy-Creds
- John (JTR)
- Hydra
- Pyrit
- Scapy

Defenses

AVOID BEING PROBED

Defenses

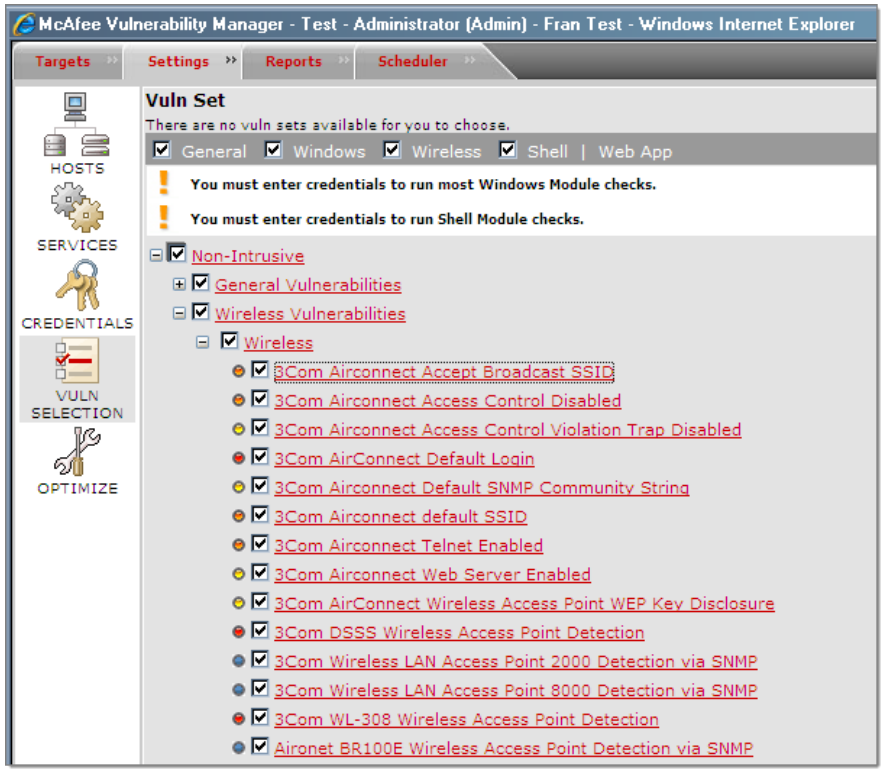
RECOMMENDATIONS

- Conduct regular wireless assessments
- Employ strong encryption and authentication methods
- Employ wireless IDS/IPS
- Secure wireless clients (laptops, phones, …)

Defenses

RECOMMENDATIONS

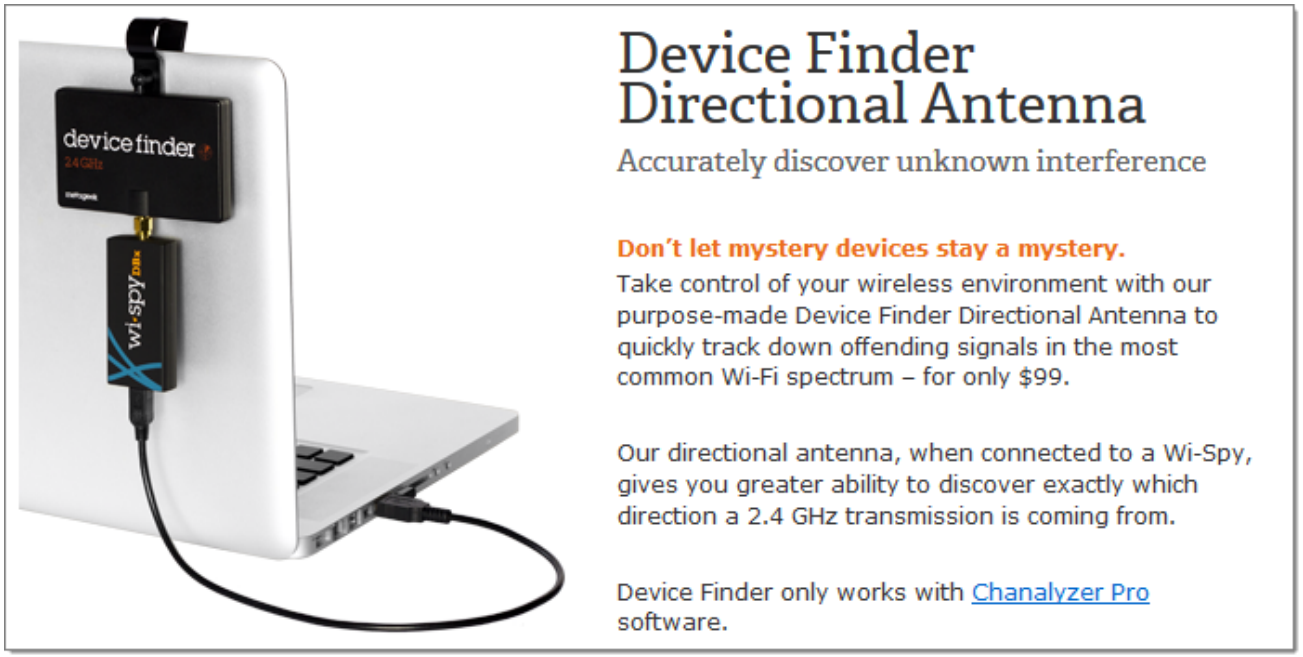
Use "wireless checks" of network vulnerability scanners



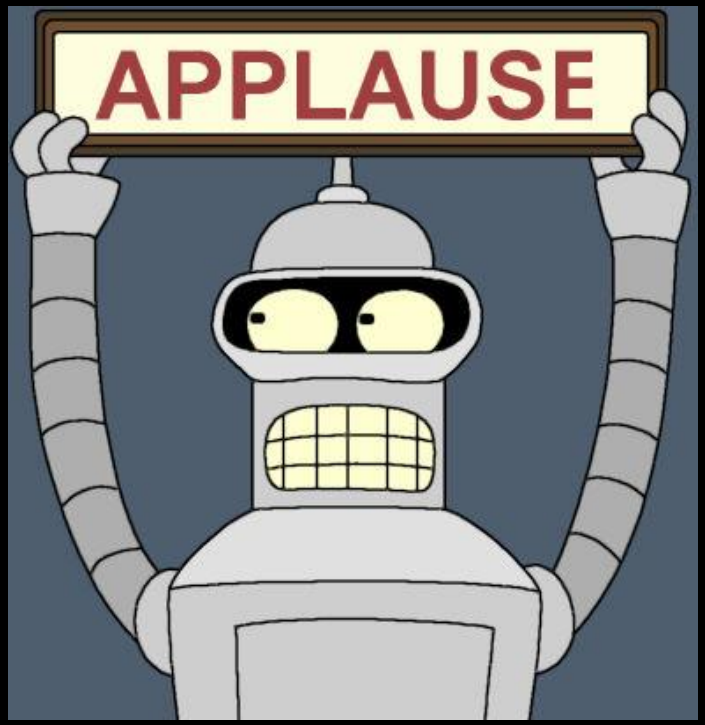
Defenses

RECOMMENDATIONS

Physically track down rogue access points and malicious devices



Thank You



Bishop Fox – see for more info:
http://www.bishopfox.com/

BISHOP FOX