Next Generation Wireless Recon, Visualizing the Airwaves

RAPID7 UNIFIED VULNERABILITY MANAGEMENT

Joshua D. Abraham

- GISKismet / Perl

Ben Smith

- Airgraph-ng / Python

About Us

- Jabra AKA “Joshua D. Abraham”
  - Security Consultant
  - Penetration Testing, Web Application Assessments and Wireless Audits
  - Works on many Open Source Projects:
    - Backtrack LiveCD, Fierce, Nikto and PBNJ
- TheX1le AKA Ben Smith
  - Network Engineer
  - Contributes to
    - Backtrack

Agenda

- <u>**Current Wireless Tools / Methods**</u>
- Our Goals & Implementations
- Screen Shots & DEMO(s)
- Future Work / QA

Wireless Recon

- Special Thanks to:
  - Mike Kershaw “Dragorn”
  - Thomas d'Otreppe “Mister_X”
  - RBG “Graphic Arts”
  - The Folks that make Shmoocon possible
- Ph33r them!!

Wireless Recon

- Kismet (stable, devel and newcore)
  - Recon and Enumeration
- Aircrack-ng
  - Cracking WEP and WPA
- Netstumbler
  - (some people still use windows)

Kismet

- Locate / Identify AP(s)
  - BSSID, ESSID, Channel and Encryption
  - GPS data
  - Much much more....
- Locate / Identify Client(s)
  - MAC Address
  - Manufacturers
- Spectrum analysis
- Drones / open-source WIPS

Aircrack-ng

- Suite of tools for wireless testing
  - Mostly thought for wireless cracking
  - Can also be used for wireless recon
    - IE Airodump-ng

Types Recon Data

- Kismet-(stable|devel)
  - Txt, CSV, XML, GPS and pcap
- Kismet-newcore
  - Txt, NetXML, GPS and pcap
- Aircrack-ng
  - CSV, pcap
  - XML “coming soon” QUOTE “Mister_X”

Current Visualization Recon

- Gpsmap (ancient)
- Pykismet
- Kismet-earth
- kisgearth

Limitations of Current Visualization Tools

- None work with Kismet-newcore
- None work with Aircrack-ng
- Flexible representation of specific information
  - Total flexibility in the generated graphs

Agenda

- Current Wireless Tools / Methods
- **Our Goals & Implementations**
- Screen Shots & DEMO(s)
- Future Work / QA

Goals - GISKismet

- Building Visual Representations of Kismet data
- Store information from:
  - Kismet-devel and Kismet-newcore
- Correlate information in database
- Graphically represent information
- Filter out non-useful information

GISKismet - .01

- Initial PoC - Spring 08
- Only worked with Kismet-devel CSV
- Mapped data to SQLite
- Several tools
  - Create database
  - Insert data
  - Query database
- No filtering of the input data

GISKismet - .02

- Redesigned as single tool
- Parse Kismet logs
  - Kismet-devel
  - Kismet-newcore
- SQLite database

GISKismet - Filters

- Input filters
  - AP configuration data
  - Query filters on any information
    - AP configuration
    - Client information
    - GPS coordinate(s)

GISKismet - Filters(2)

- Filter input
  - Insert all AP(s) on channel 6 named Linksys
- Filter output
  - Output all AP(s) without Encryption

Goals - Airgraph-ng

- Started back in November 2008
- Wanted to learn python
- A visual way to see airodump-ng data
  - Specific graph types
  - Client Focused

Airgraph-ng - Graph Types

- CAPR (Client AP Relationship)
  - Shows links between Access points and Clients
  - Focus more on clients then Ap’s
  - Only Ap’s with clients get graphed
    - This can lead to smaller graphs then you are expecting
  - Keeps basic statics of the mapping
    - Total number of clients assoicated
    - Number of clients per AP
  - Color Based coding of each AP
    - Red = Open
    - Yellow = WEP
    - Green = WPA / WPA2

Airgraph-ng - Graph Types

- CPG (Client Probe Graph)
  - Graphs links between clients and probe requests
  - Probes are shown in blue

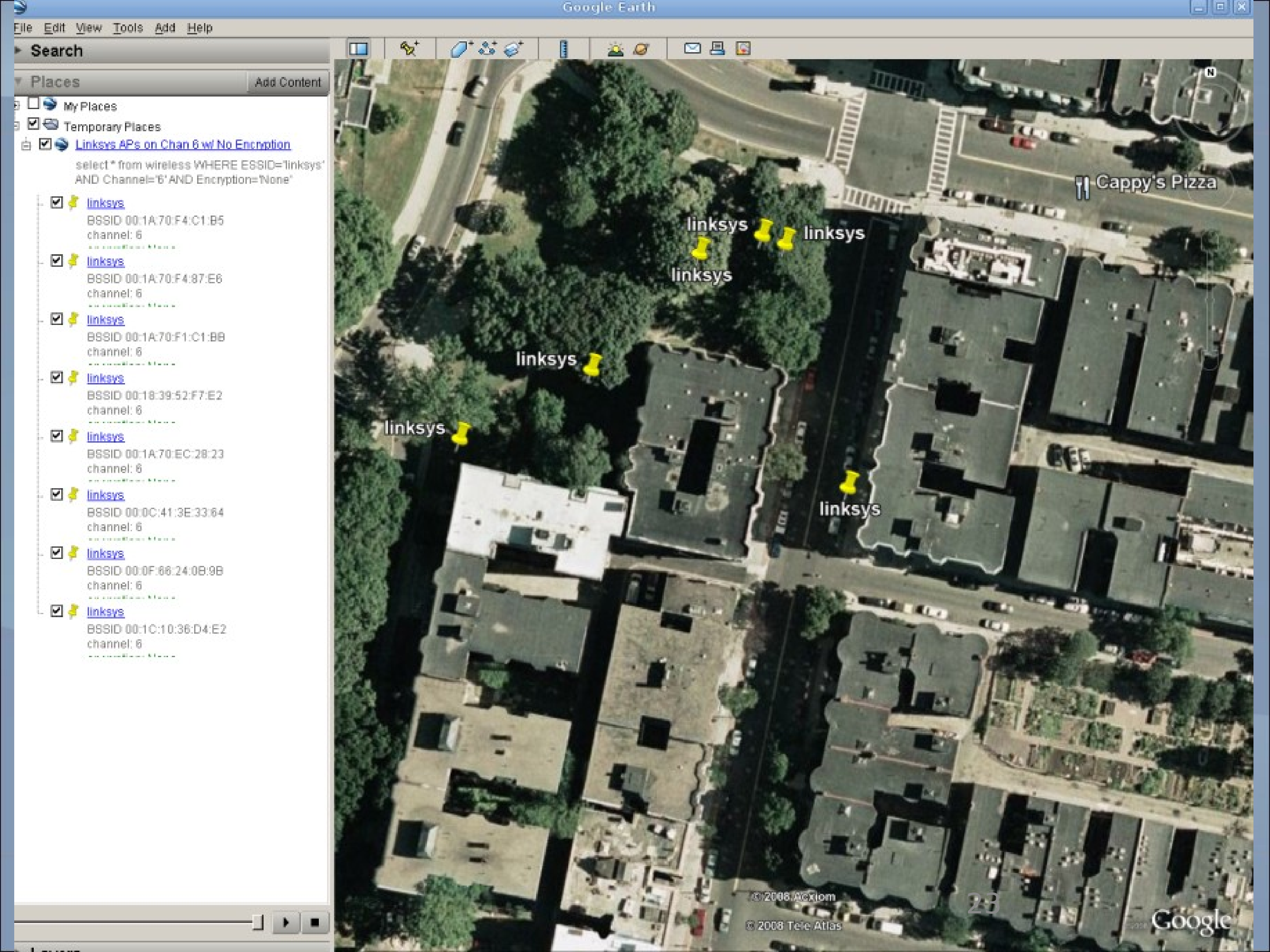
Airgraph-ng - Maltego Support

- Maltego with local transform support
- Custom Scripts written by AndrewMohawk
- Runs on both Windows and Linux
- Multiple types of transforms AP to….
  - ESSID
  - BSSID
  - Clients
  - Ip’s

Agenda

- Current Wireless Tools / Methods
- Our Goals & Implementations
- **Screen Shots & DEMO(s)**
- Future Work / QA

Screenshots - GISKismet



☐ My Places

☑ Temporary Places

☑ Linksys APs on Chan 6 w/ No Encryption

```
select * from wireless WHERE ESSID='linksys'
AND Channel='6' AND Encryption='None'
```

☑ linksys
BSSID 00:1A:70:F4:C1:B5
channel: 6

☑ linksys
BSSID 00:1A:70:F4:87:E6
channel: 6

☑ linksys
BSSID 00:1A:70:F1:C1:BB
channel: 6

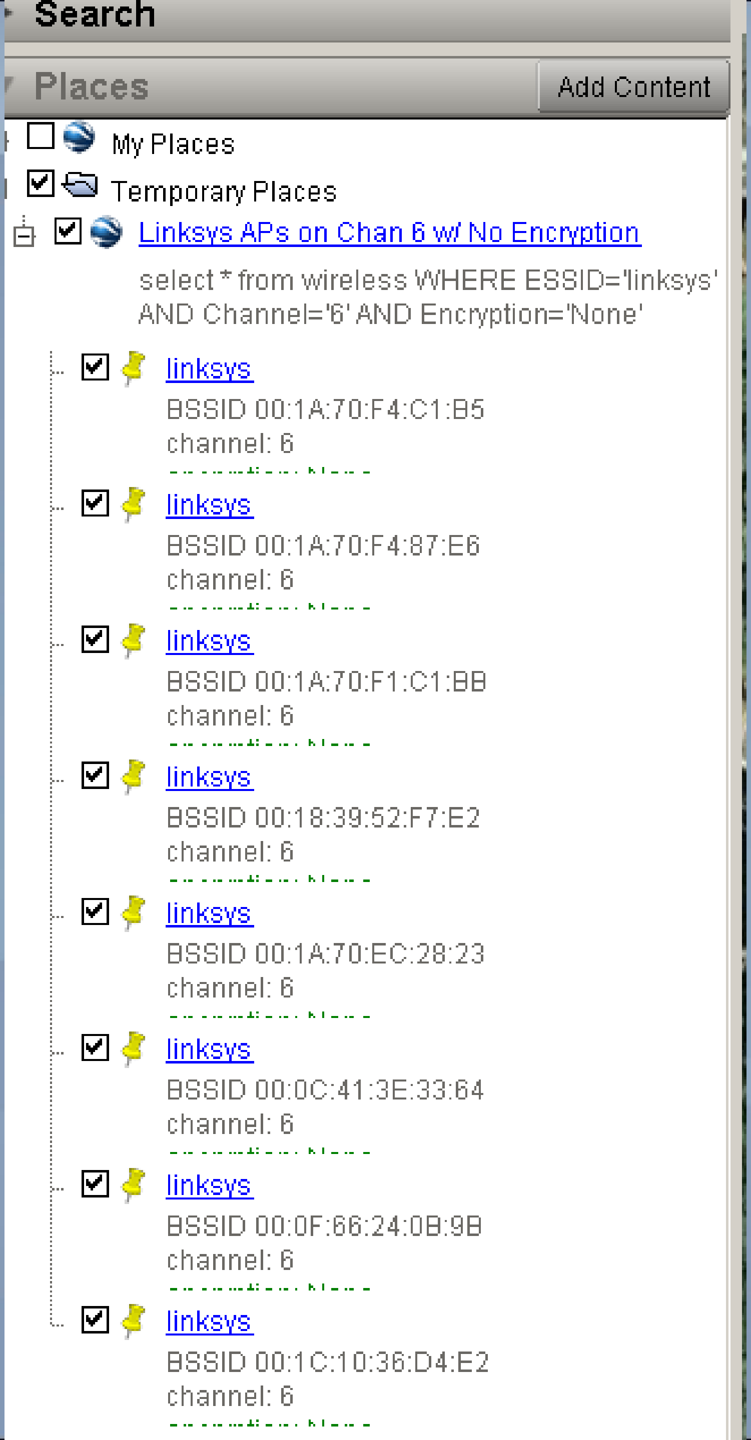
☑ linksys
BSSID 00:18:39:52:F7:E2
channel: 6

☑ linksys
BSSID 00:1A:70:EC:28:23
channel: 6

☑ linksys
BSSID 00:0C:41:3E:33:64
channel: 6

☑ linksys
BSSID 00:0F:66:24:0B:9B
channel: 6

☑ linksys
BSSID 00:1C:10:36:D4:E2
channel: 6



☐ My Places

☑ Temporary Places

☑ Linksys APs on Chan 6 w/ No Encryption

select * from wireless WHERE ESSID='linksys' AND Channel='6' AND Encryption='None'

☑ linksys
BSSID 00:1A:70:F4:C1:B5
channel: 6

☑ linksys
BSSID 00:1A:70:F4:87:E6
channel: 6

☑ linksys
BSSID 00:1A:70:F1:C1:BB
channel: 6

☑ linksys
BSSID 00:18:39:52:F7:E2
channel: 6

☑ linksys
BSSID 00:1A:70:EC:28:23
channel: 6

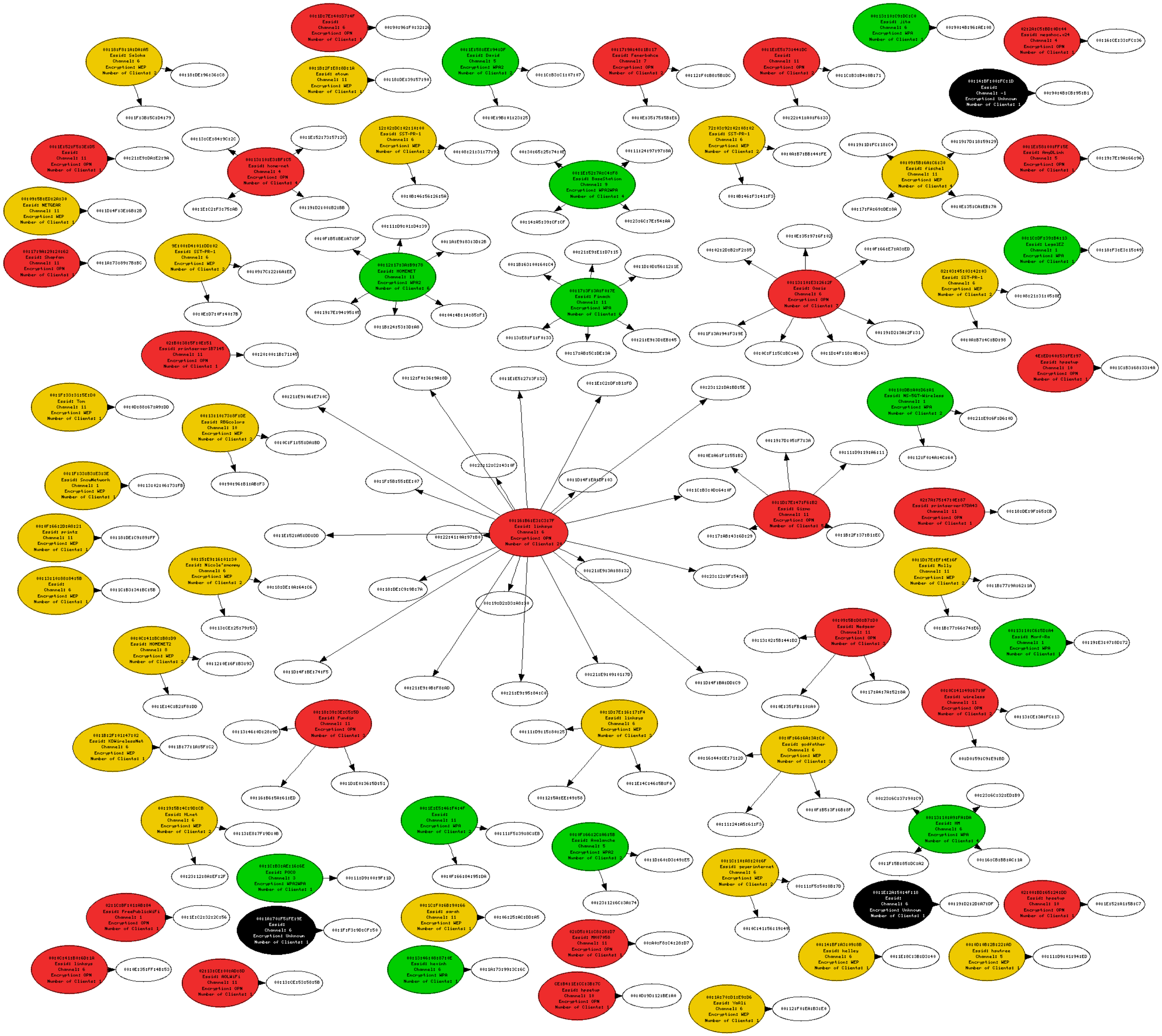
☑ linksys
BSSID 00:0C:41:3E:33:64
channel: 6

☑ linksys
BSSID 00:0F:66:24:0B:9B
channel: 6

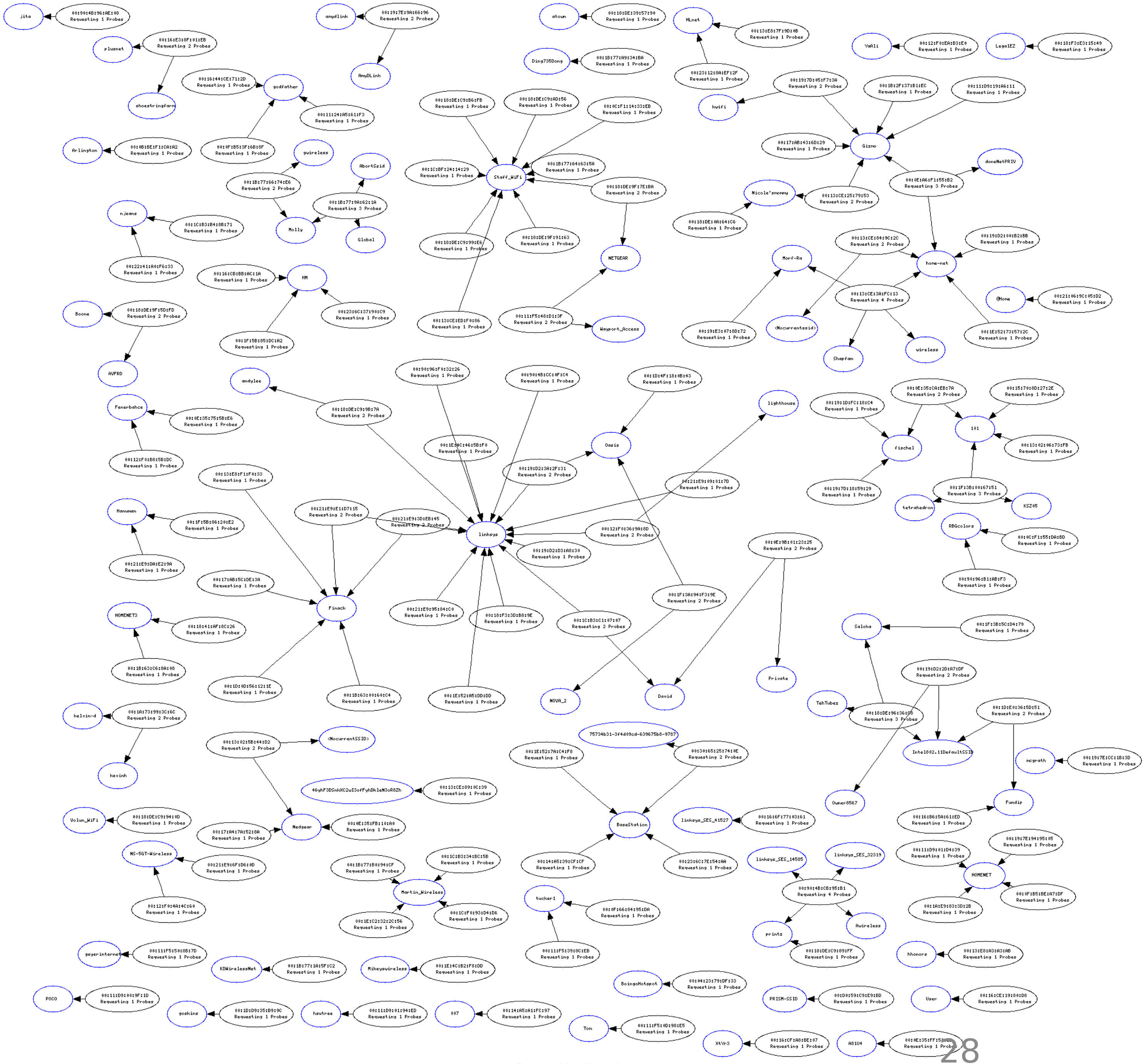
☑ linksys
BSSID 00:1C:10:36:D4:E2
channel: 6

DEMO - GISKismet

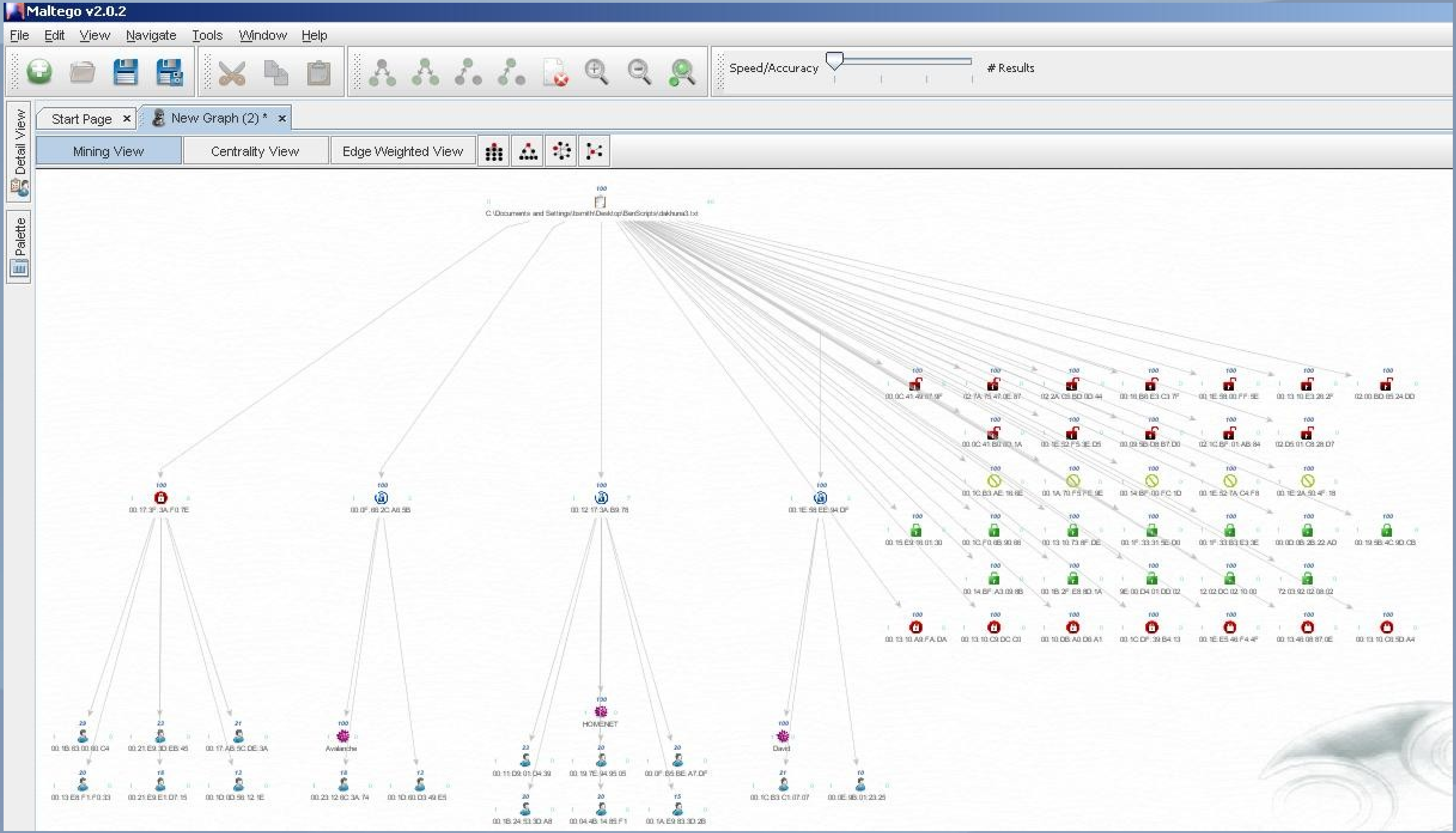
Screenshots - Airgraph-ng



Generated by Airgraph-ng
64 Access Points and
141 Clients are shown



Generated by Airgraph-ng
124 Probes and
255 Clients are shown


Maltego v2.0.2
File Edit View Navigate Tools Window Help
Speed/Accuracy
# Results
Detail View
Palette
Start Page
New Graph (2) *
Mining View
Centrality View
Edge Weighted View
100
C:\Documents and Settings\bsmith\Desktop\BenScripts\dakhuna3.txt
00:17:3F:3A:F0:7E
00:0F:66:2C:A6:5B
00:12:17:3A:B9:78
00:1E:58:EE:94:DF
00:1B:63:00:60:C4
00:21:E9:3D:EB:45
00:17:AB:5C:DE:3A
00:13:E8:F1:F0:33
00:21:E9:E1:D7:15
00:1D:0D:58:12:1E
Avalanche
00:23:12:6C:3A:74
00:1D:60:D3:49:E5
HOMENET
00:11:D9:01:D4:39
00:19:7E:94:95:05
00:0F:B5:BE:A7:DF
00:1B:24:53:3D:A8
00:04:4B:14:85:F1
00:1A:E9:83:3D:2B
David
00:1C:B3:C1:07:07
00:0E:9B:01:23:25
00:0C:41:49:07:9F
02:7A:75:47:0E:87
02:2A:C9:BD:0D:44
00:16:B6:E3:C3:7F
00:1E:58:00:FF:5E
00:13:10:E3:28:2F
02:00:BD:65:24:DD
00:0C:41:B0:0D:1A
00:1E:52:F5:3E:D5
00:09:5B:D8:B7:D0
02:1C:BF:01:AB:84
02:D5:01:C8:28:D7
00:1C:B3:AE:16:8E
00:1A:70:F5:FE:9E
00:14:BF:00:FC:1D
00:1E:52:7A:C4:F8
00:1E:2A:50:4F:18
00:15:E9:18:01:30
00:1C:F0:6B:90:66
00:13:10:73:8F:DE
00:1F:33:31:5E:D0
00:1F:33:B3:E3:3E
00:0D:0B:28:22:AD
00:19:5B:4C:9D:CB
00:14:BF:A3:09:8B
00:1B:2F:E8:8D:1A
9E:00:D4:01:DD:02
12:02:DC:02:10:00
72:03:92:02:08:02
00:13:10:A9:FA:DA
00:13:10:C9:DC:C0
00:10:DB:A0:D8:A1
00:1C:DF:39:B4:13
00:1E:E5:46:F4:4F
00:13:46:08:87:0E
00:13:10:C8:5D:A4

DEMO - Airgraph

- CAPR Graph
  - Demo
- CPG Graph
  - Demo
- Maltego
  - Demo

Agenda

- Current Wireless Tools / Methods
- Our Goals & Implementations
- DEMO(s)
- **Future Work / QA**
- World Domination!

Future Work

- Easier / Additional filters
- Graphic engines
  - Maltego
  - Google Earth
  - Additional / Alternative engines ...

Future Work - GISKismet

- Access Point Location correction
  - Single AP / Multiple APs
  - Multiple Log files
  - Tracking over time (think PBNJ)
  - Correctly pinpoint location
- GIS fully incorporated
  - Spatial data representations
- Alternative graphing software
  - GoogleEarth requires net

Future Work - Airgraph

- Show all data in a single graph
- Smaller images
- More graph types
- Filtering engine
  - Time aware
  - GPS Support
  - Grouping based on channel or encryption type
  - Bssid / Essid Filters
- Kismet newcore Support
- Better statistics about the graphs

Questions??

Where to Find us

- Joshua D. Abraham
  - jabra@spl0it.org
- Ben Smith
  - thex1le@gmail.com

Oh wait, did we forget something???

Want some fresh code ?

GISKismet .02 Released!

- http://www.giskismet.org
- http://my-trac.assembla.com/giskismet/

Airgraph-ng

Currently in aircack-ng svn

http://trac.aircrack-ng.org/svn/branch/airgraph

Aicrack-ng 1.0RC2 Release

Backtrack 4 Beta