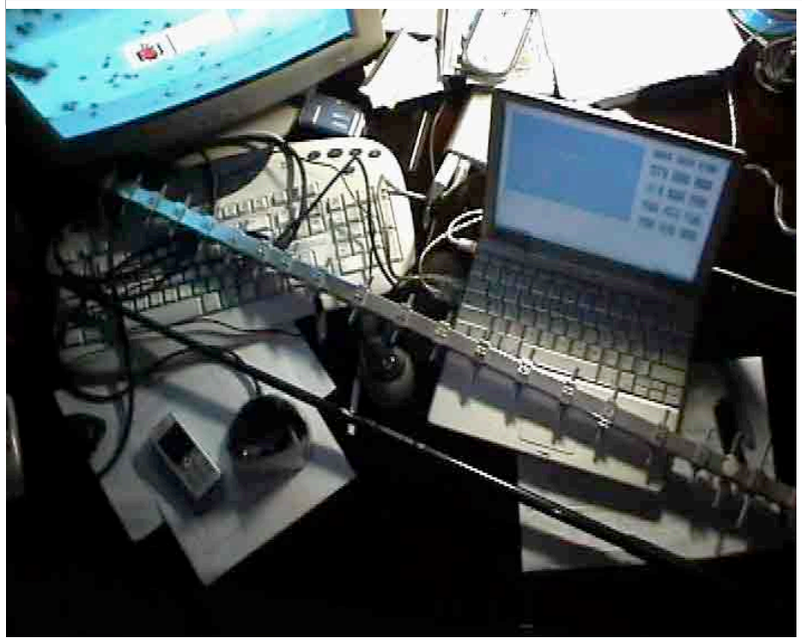
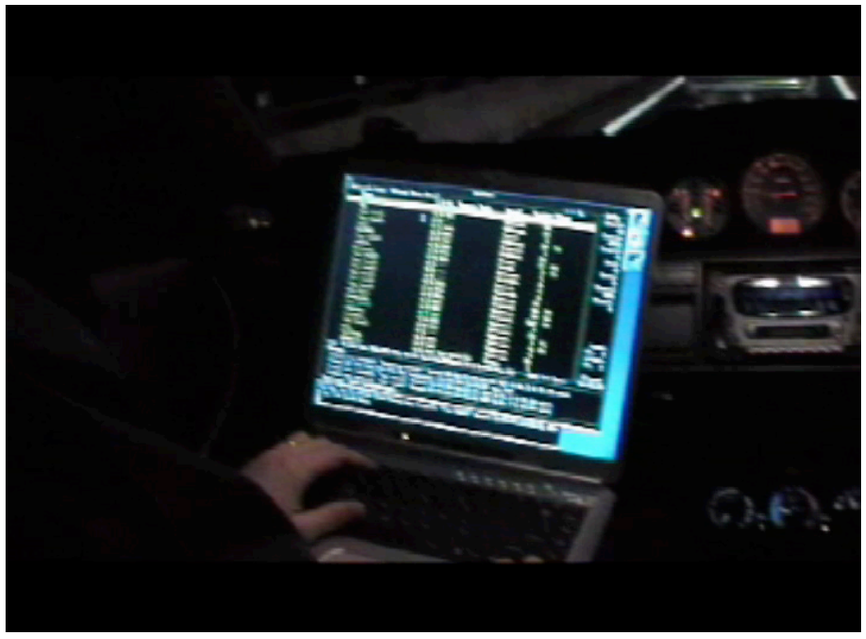
Bellua Asia Pacific

War Driving





Anthony C. Zboralski

work: z@bellua.com

Jim Geovedi

work: jim.geovedi@bellua.com

PT Bellua Asia Pacific

- Bellua Asia Pacific is a consortium of information security consultants, who are recognised experts in:
  - Information Security
  - Business Process Engineering
- Our clients benefit from our extensive network of consultants which covers more than 24 countries including:
  - *Argentina, Austria, Australia, Belgium, China, England, Finland, France, Germany, Greece, Indonesia, Malaysia, Norway, Netherlands, Poland, Romania, Russia, Sri Lanka, Thailand and the United States*.
- We are vendor neutral

PT Bellua Asia Pacific

- Bellua uses a team-based approach in every engagement to ensure access to all available resources and experiences of our professionals.
- In Jakarta, our team is comprised of 14 information security experts, including 5 BS7799 IRCA certified auditors.
- Our security consultants have many years of information security experience that include performing penetration testing, security assessments for some of the largest Asian banks and a dozen Fortune 500 companies.

Bellua Team Experience

- British Aerospace
- Aerospatiale & Defence
- Matra-Aerospatiale
- Alcatel
- LVMH
- Axa
- Circe
- Dassault
- Eurocoptere
- GIE Carte Banquaire
- Kabelvision [Anthony]
- MPR/DPR [Anthony]

Ministry of Finance [Fetri]

Bank of Indonesia [Fetri]

Lippo Bank [Anthony]

Bank BRI [Anthony] [Agus]

Bank Mandiri [Fetri]

Bank BNI [Anthony, Kartono]

Bank Niaga [Anthony]

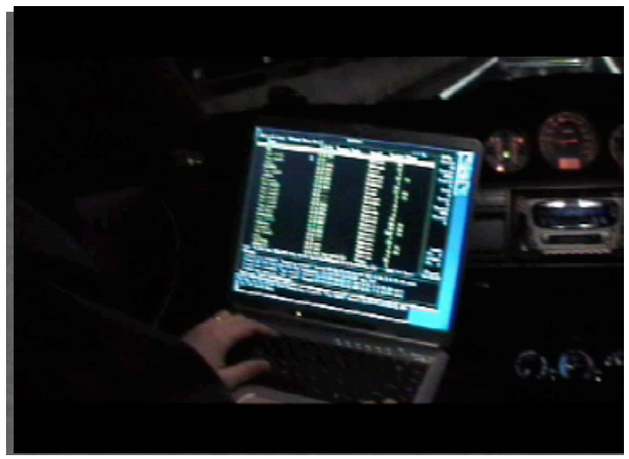
Pacomnet (Online Banking System used by Bank Bukopin and Bank Niaga) [Anthony]

CPR Bank & CPR Billet [Anthony]

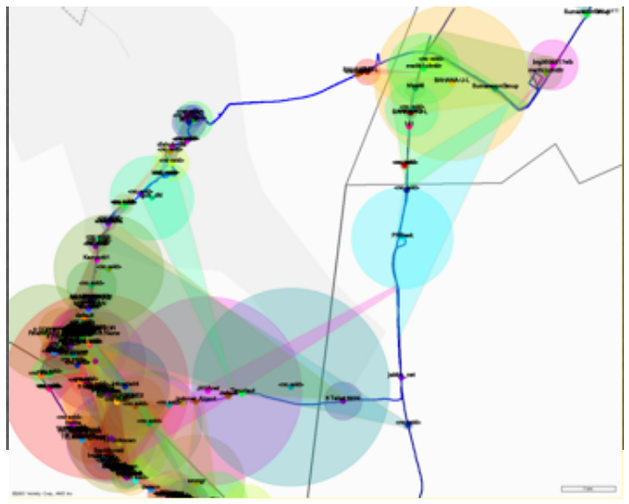
[...]

Wireless Security

- War Driving
- Wireless Honeypot
- Wireless Pen Tests
  - Infrastructure, Hotspots, Laptops...
- Wireless Social Engineering Attacks
- Targeting Bluetooth phones and PDAs



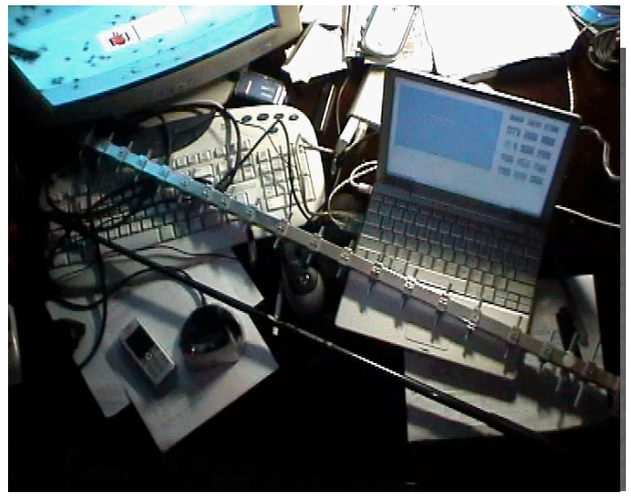
War Driving



Early Survey 2003: 500 Networks

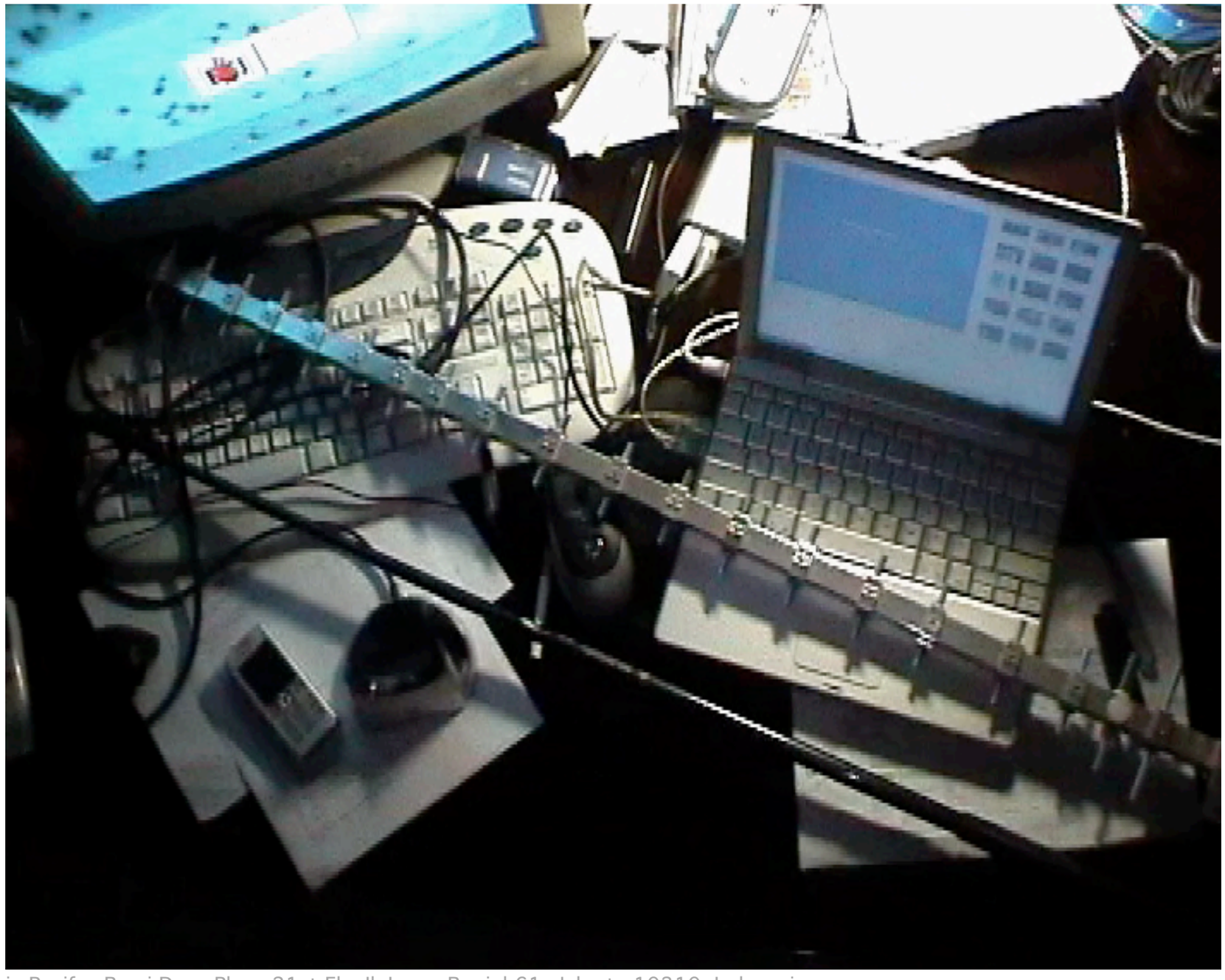
War Driving in Jakarta

- Laptop, external antennas, long range Wi-Fi card, GPS and kismet
- Thousands of wide-open networks in Jakarta
  - Infrastructure, Hotspots, WLANs (Intranet)
  - Banks, Insurance companies, government…
  - Similar results in Singapore and Kuala Lumpur

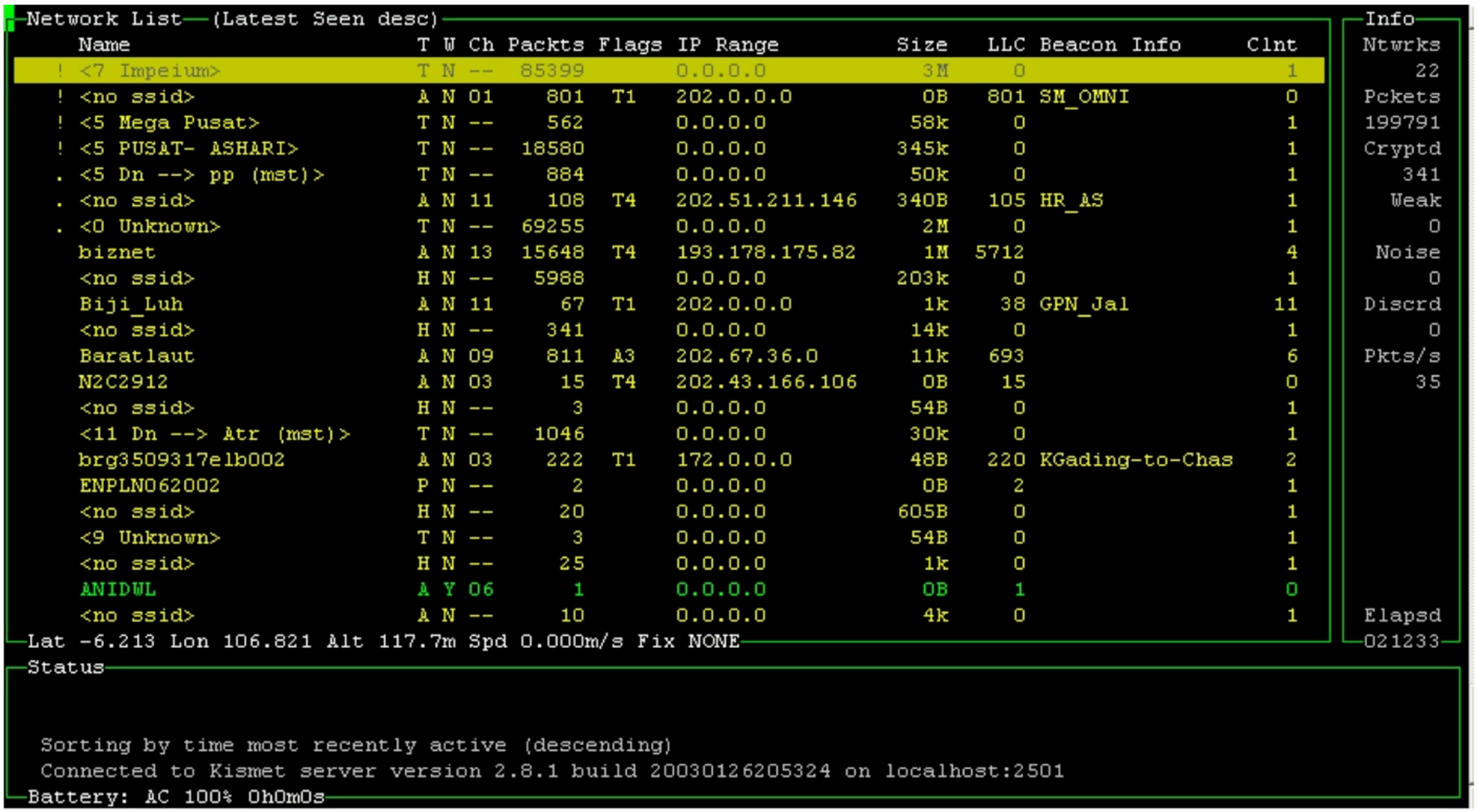


War Driving in Jakarta, 12/2004

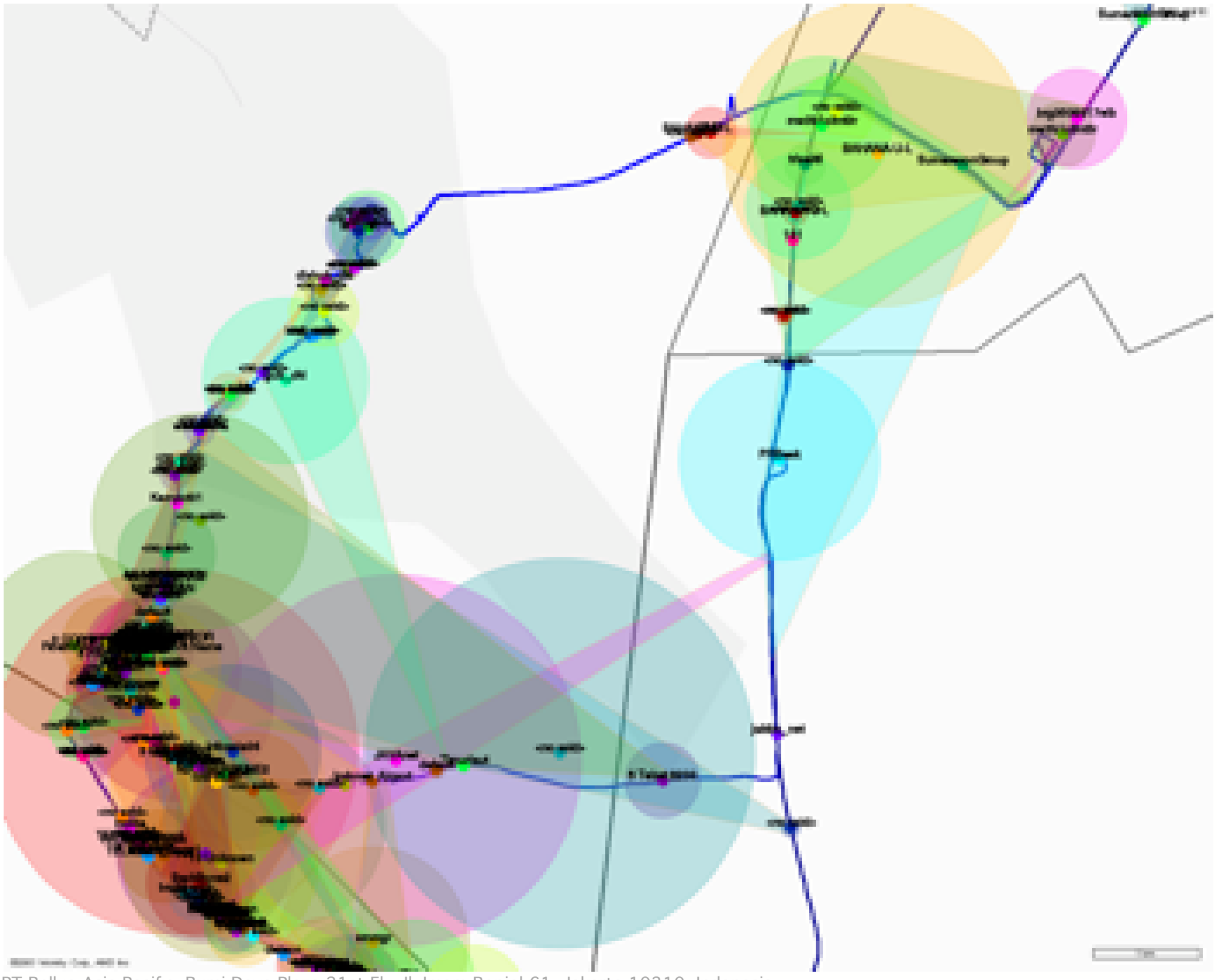
War Driving in Jakarta



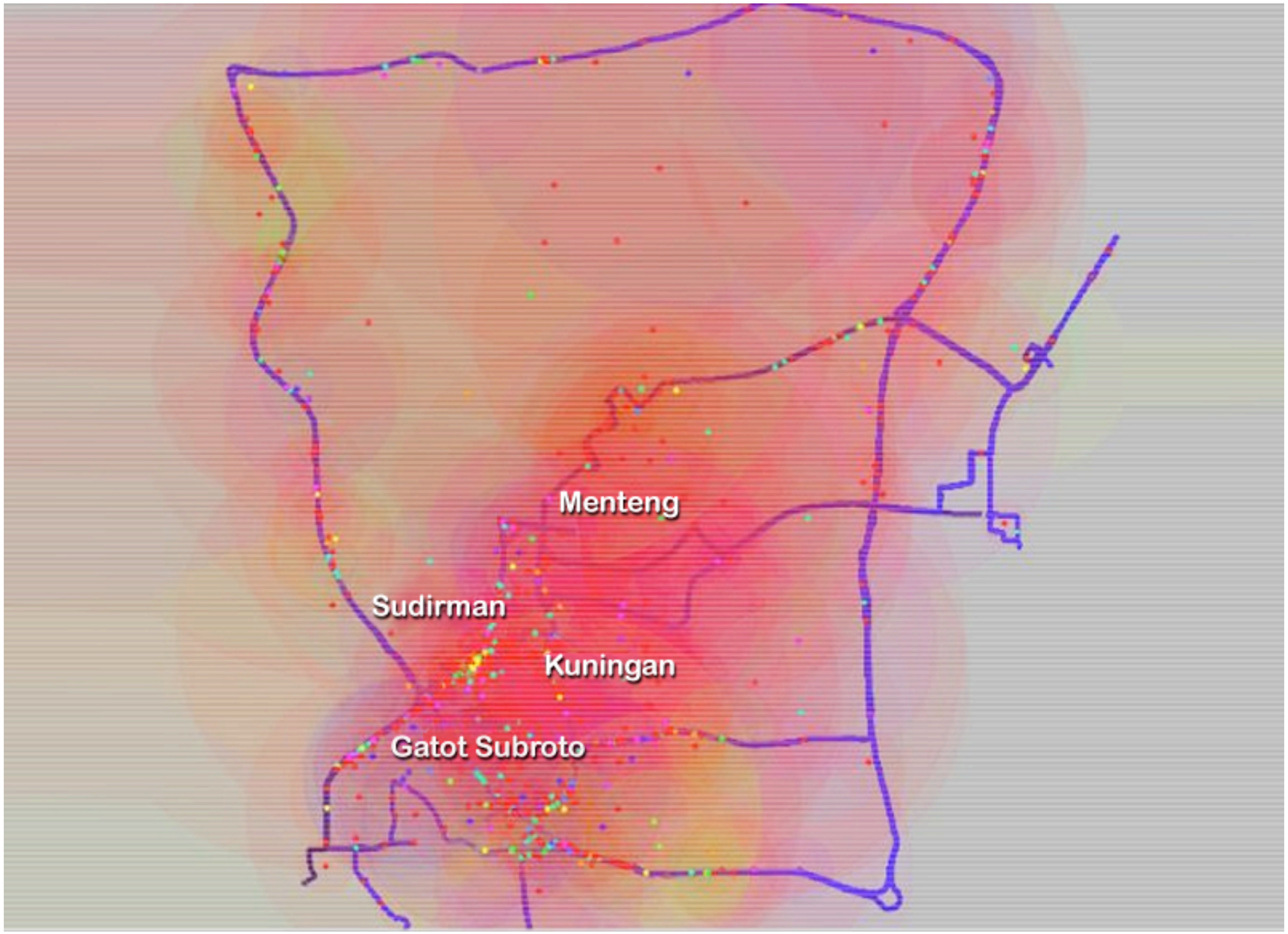
Identifying Networks with Kismet



War Driving in Jakarta



Jakarta Wireless 2003



But we don't use Wireless!

- Pen Testing a Major Bank using Wireless
- Bridged Neighbouring networks
- Open WAP on Executive Floor
- Rogue Access Points
- Clear-Text Wireless link from Data Centre to DRC

What did we find...

- ATM Transactions
- Username and passwords
- Confidential e-mails
- SQL queries and results

- Oops, we're in again...

ATM Transactions over Wireless!

Censored

Credit Cards Information

Censored

User names and passwords

Censored

Credit Card Centre over Wireless!

Censored

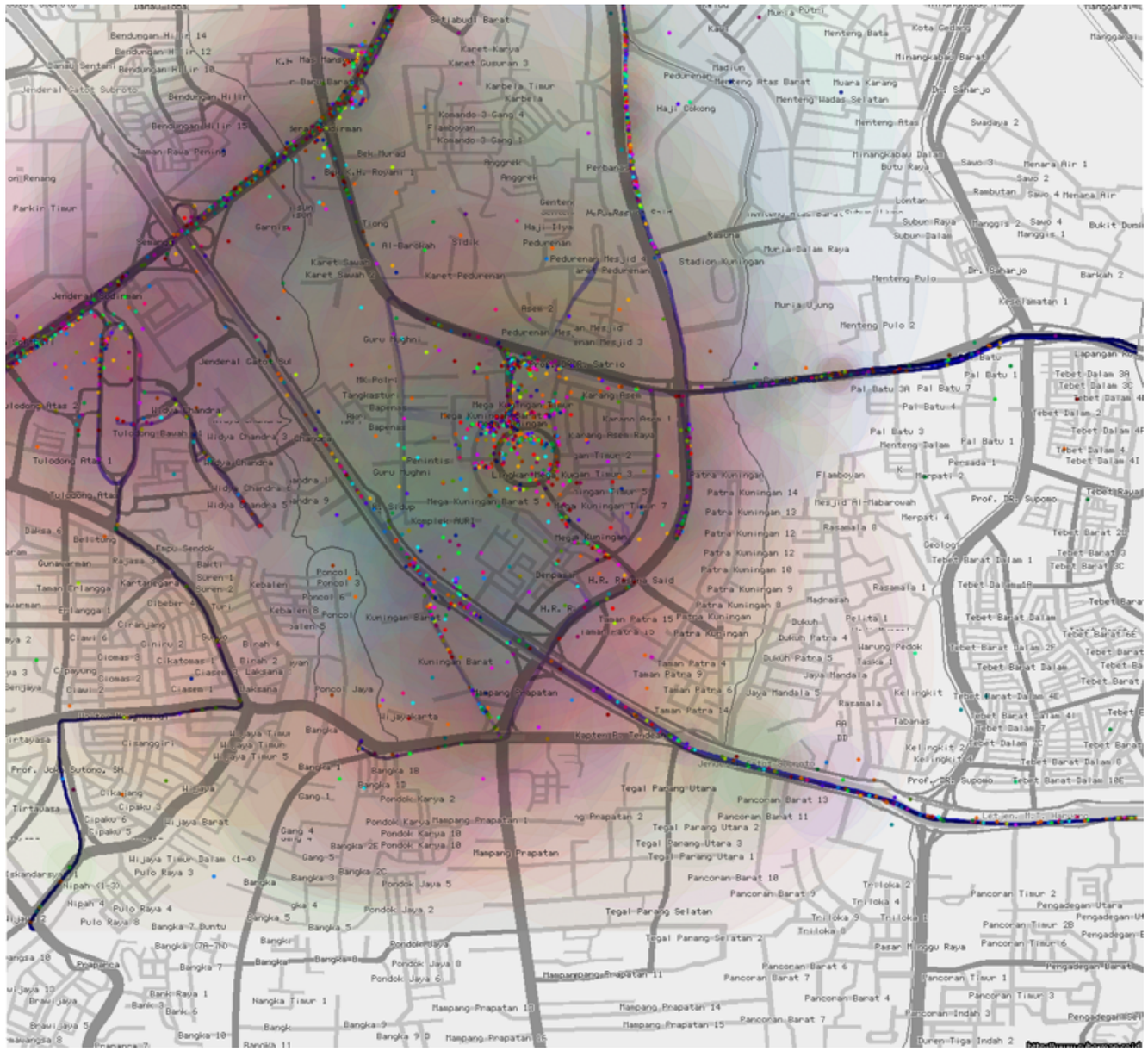
“but we don’t use wireless ?!?”

Censored

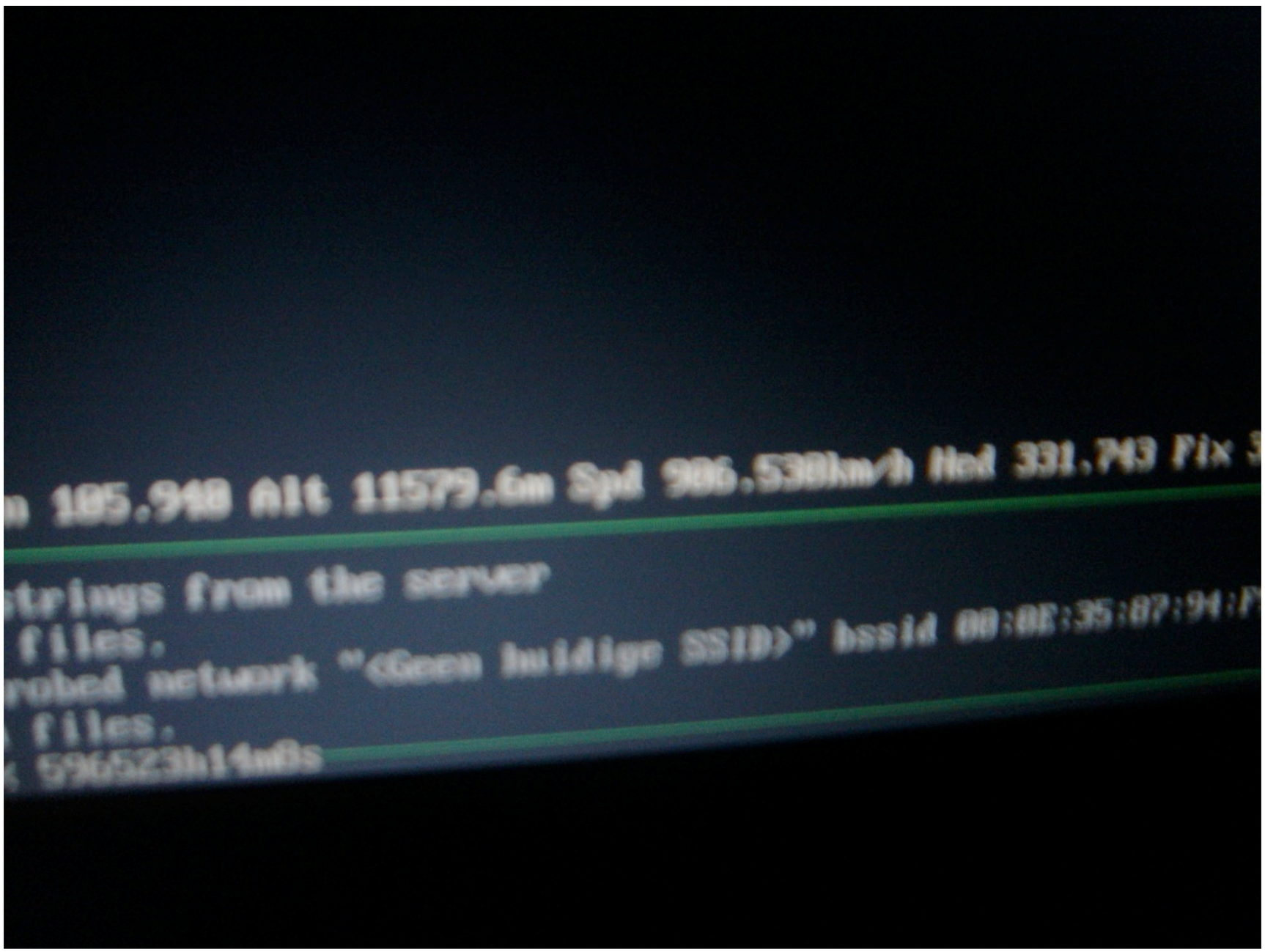
Wireless Security Survey

- Identification and GPS Mapping of:
  - Authorised Wireless Access Points
  - Intrusion attempts
  - Rogue Wireless Access Points
  - Neighbouring Wireless Access Points
  - Wireless-enabled Laptops
  - Bluetooth Devices (Phones, Printers, Modems, Fax machines...)

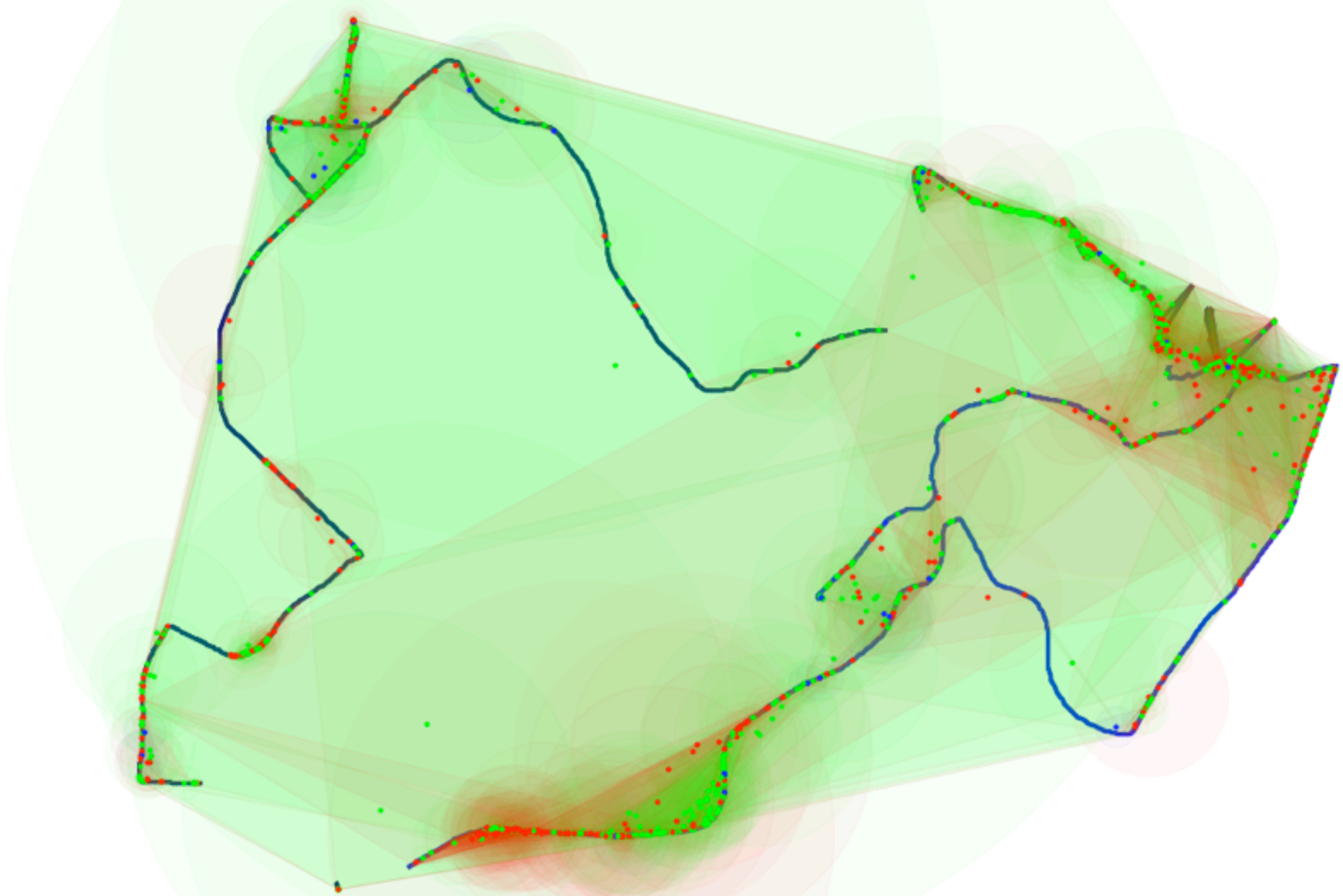
Jakarta Wireless 2005



On the way to KL



War Driving KL - HITBSecConf 2005



Wireless Controls and Policies

- ISO 17799:2005
  - 10.6.1 c) Network Controls
  - 10.8.1 e) Procedures for the use of wireless
  - 11.4.2 User Authentication for external connections
  - 11.4.5 Segregation in Networks
  - 11.7.1 Mobile Computing and communications
  - 11.7.2 Teleworking
- Policies
  - Wireless disabled unless approved, War Driving, Production Use and Fail-over, Wireless Transmission of Confidential Information...

Conclusion

- Implementation details are abstracted
- Wireless networks increase the level of existing risks and threats
- Vendors and service providers give a false sense of security
- Not just a technical issue

Thank you