HostileWRT

Reclaim Your Spectrum

Eugene Parkinson, Philippe Langlois

http://www.tmplab.org

http://www.p1security.com

Why HostileWRT?

- Wireless Security Audit
  - Controlled envt only
  - Inside an industrial site
  - Big number of AP to audit
- Need for Ultra-Fast setup
- Access to friends' network
  - Beware of the law! Need author.

What is HostileWRT?

- Based on OpenWRT (www.openwrt.org)
- Script to automate WiFi actions
- Packages for aircrack-ng
- WiFi networks: LoveWRT
- Great hardware: FON2

Routeur HADOPI Scandal

- This IS NOT!
- But...
  - It may be used this way...
  - ...if you don’t respect the law
- Of course, you should not

Limitations

- Small Memory
- Slow CPU
- No internet
- or rarefied (IPoICMP, IPoDNS)

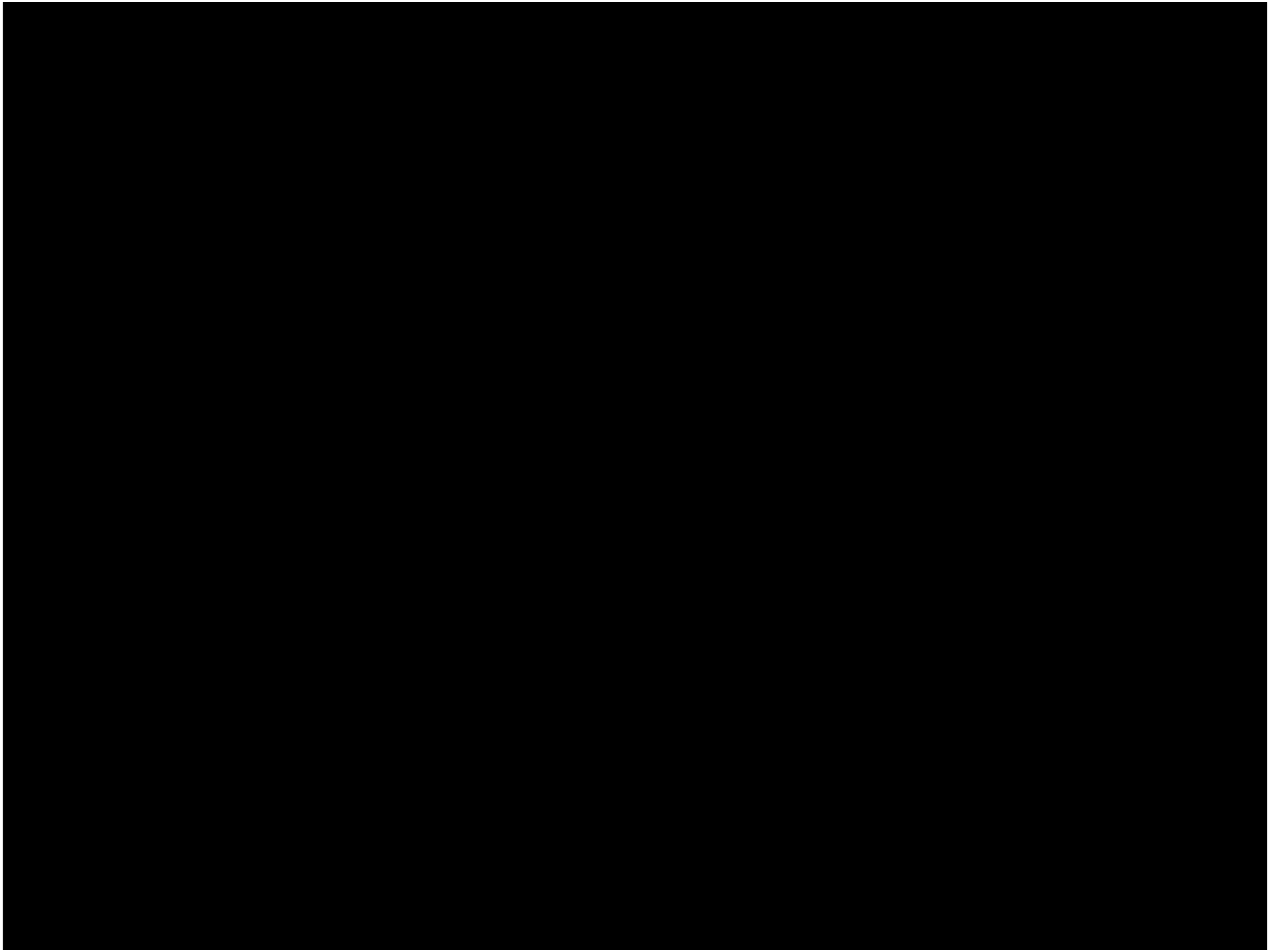
Behaviours

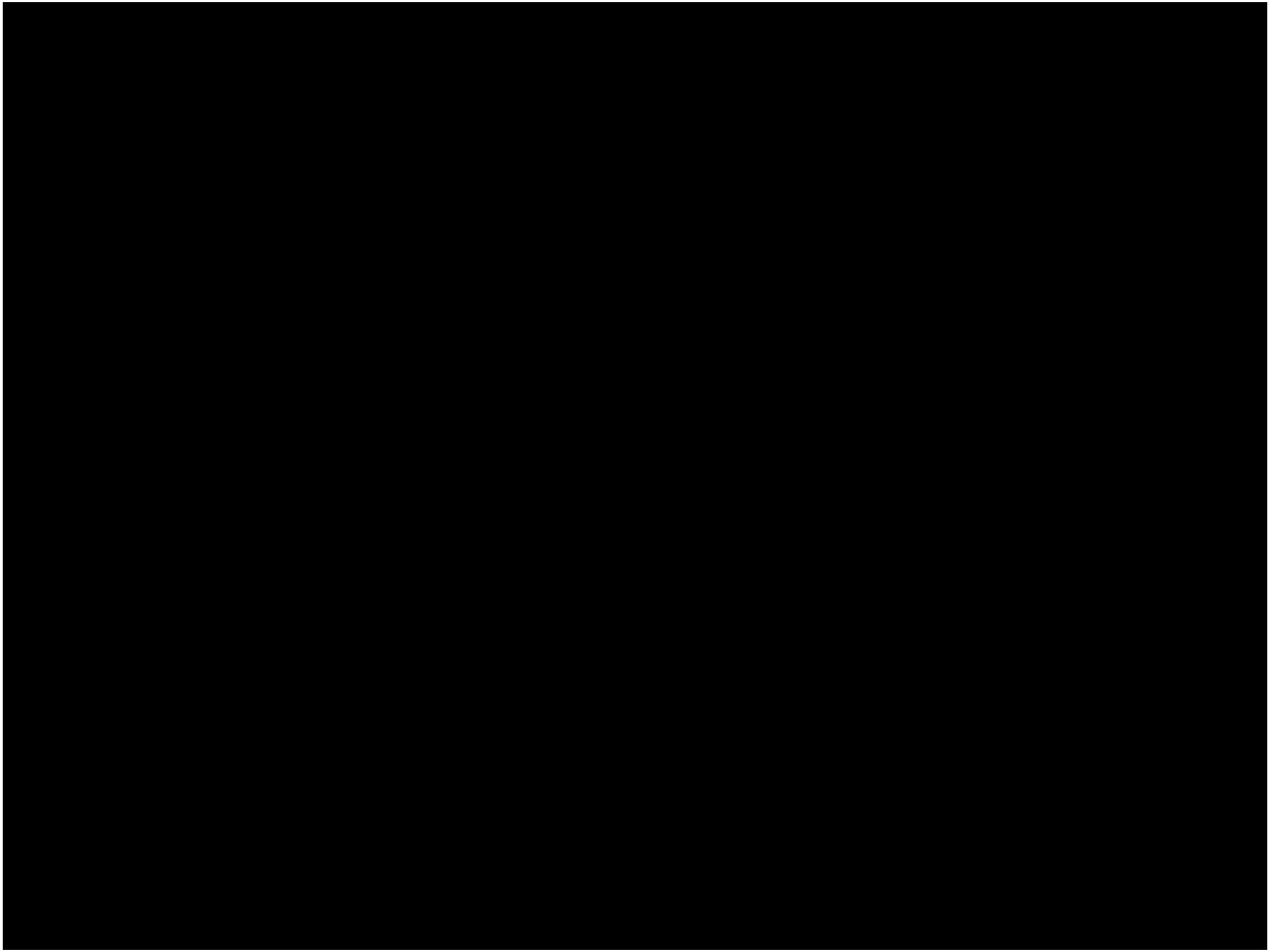
- == Modes
- Fast Setup
  - Auto-join on first crack
- Mass Audit
  - Collect and crack
  - Key size dependent? (big: crack later, small: crack now)
- Multi-ops mode
  - AP / STA / MONITOR

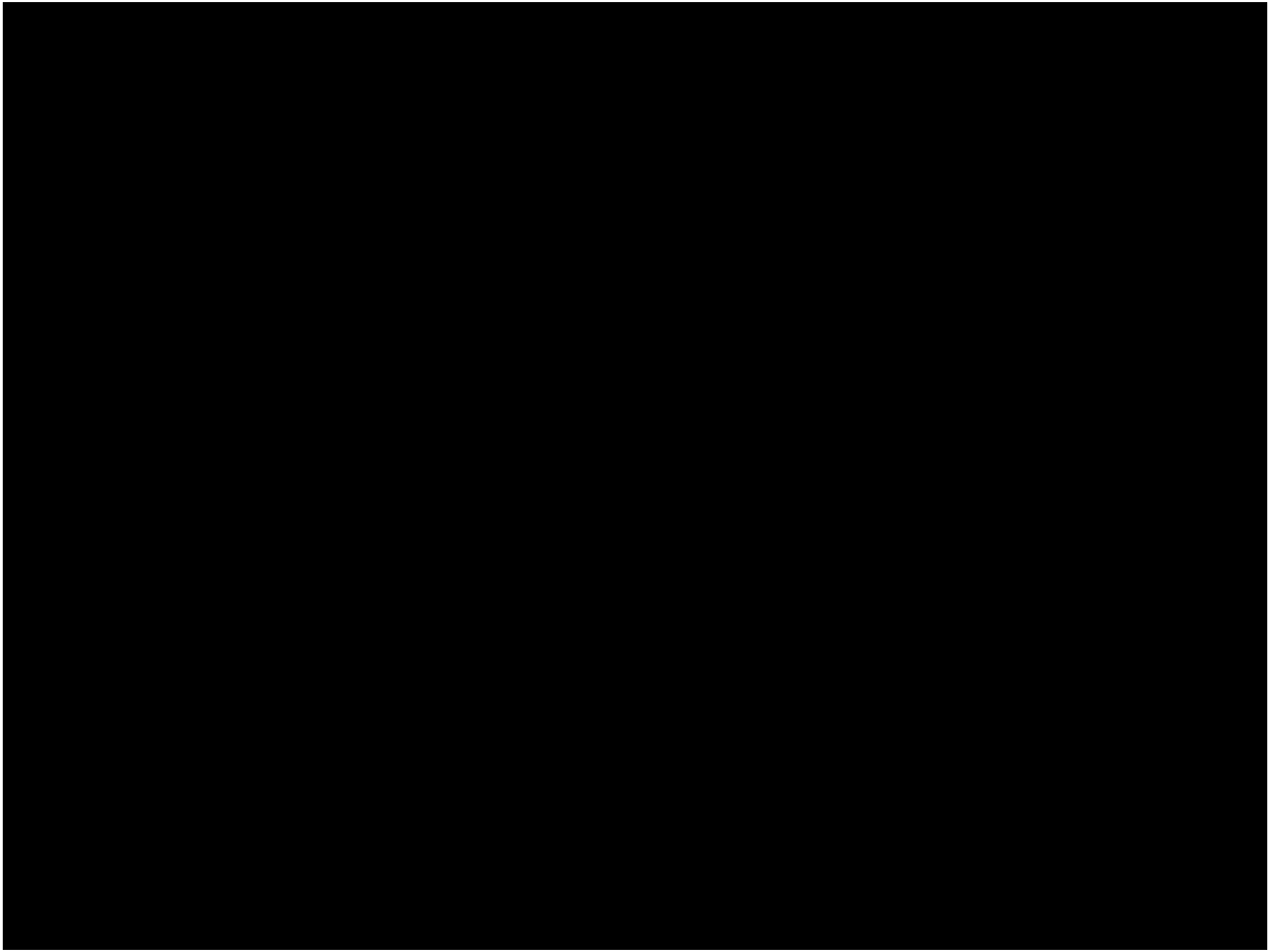
Plug-ins

- Hooks
  - For each event
  - On start
  - On WEP attack working
  - On WEP attack start
  - On WEP key found
- Open Generic Model
  - On client detect

Demo & Internals







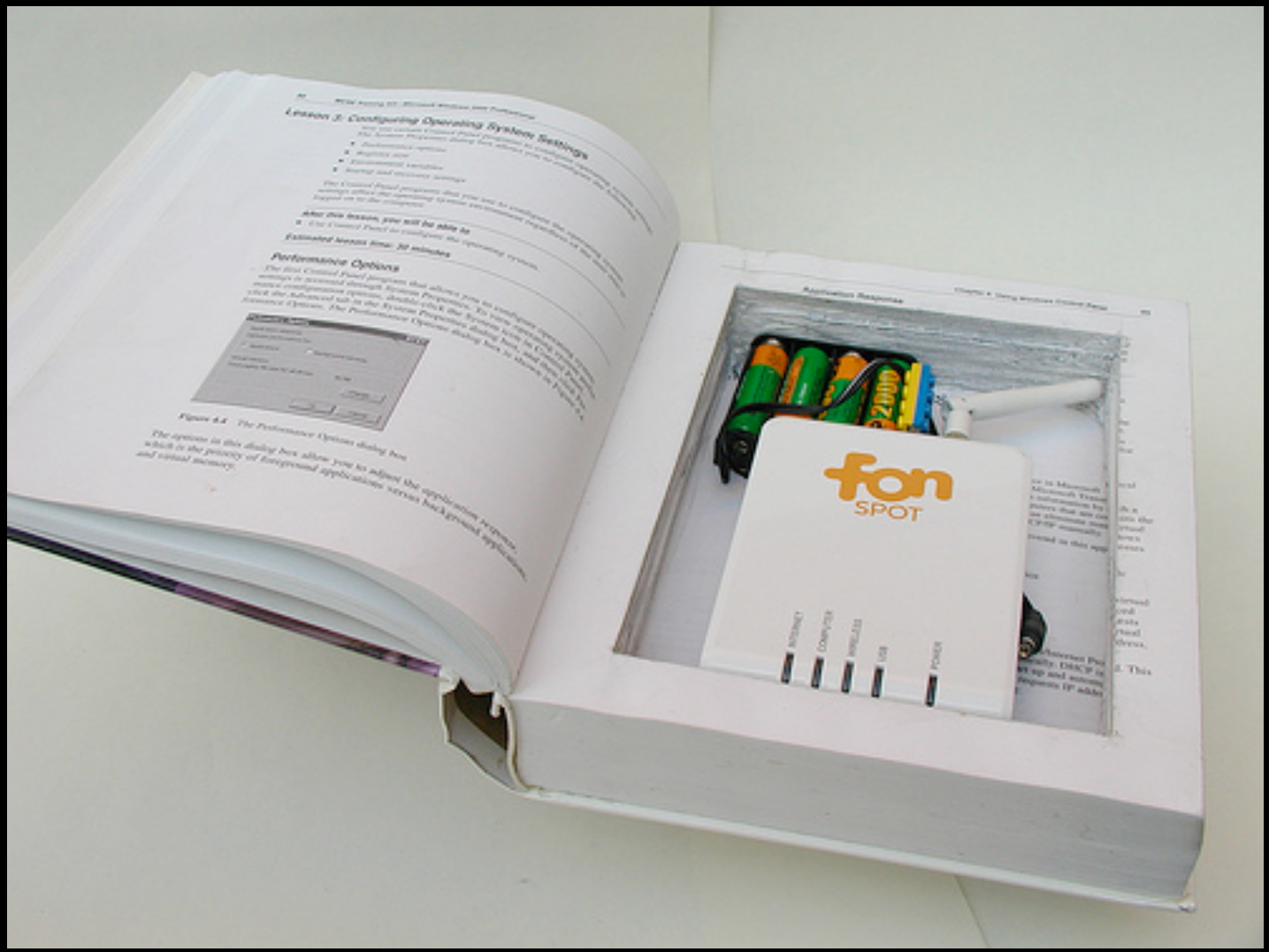
Roadmap

- What works
  - Scan
  - WEP crack
  - Client Mode (stability?)
  - AP Mode (channel changing)
- What's next
  - Web UI, QA
  - Resistant WEPs, WPA with Kalk

Hacks: Mobile

- Batteries
- Car, Bicycle-based
- FridaV example
  - Already using OpenWRT
- Thanks to Ljudmila hackerspace

Hacks: Hiding



Hacks: Antennas

- Omni
- HSB Mighty Waveguide hacks
- NZ DIY antennas
- Coffee box
- Is THIS ridiculous???
- Yagi

Hacks: Connecting things

- GPIO: SPI, I2C
- Chemical Sensors
  - Thanks Sebastien B.
- Radioactivity diodes
  - Thanks M

SSID to Wordlists

- New in 0.3.2
- Guess the best dictionaries for your country
- SSID list gives fingerprint
  - SSID patterns, FR: Livebox_
- You can contribute for your Country
  - Hint: .hr, .pl, .hu, ...

Bugs

- NO STORAGE ON FLASH!!!!
  - Pwweez don't crash your AP
- Newest AP (Fon2N?)
- airdecloak-ng
- None other known... :)

Future

- Mesh networks (BABEL?!)
- Datagram control (BOTmode)
- Captive portal fishing test
- Reliable IPoDNS, IPoICMP
- Anonymous Browsing (TOR?)
- Industrial solution (reporting, mgmt, dual approach)

Help Needed

- Developpers
- Testers
- Real-world experience feedback
- IPoXXX endpoints / exit nodes
- Resistant WEP tricks
- WPA Crypto+FPGA Genius? (K!LK!)

Credits

- The OpenWRT project
- XXX for FONbook on batteries
- Loloster
- All the /tmp/lab crew

Thanks! Merci!

Work In Progress @ /tmp/lab

Come meet us

http://www.tmplab.org

http://www.p1security.com