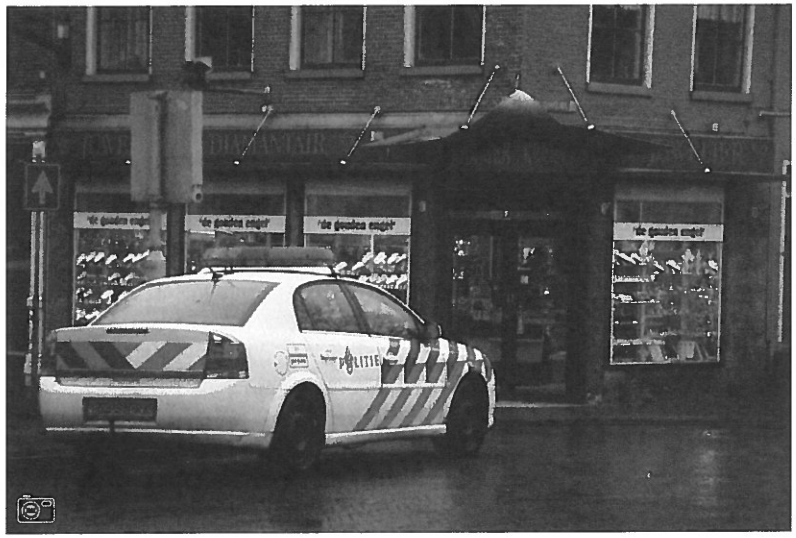
Sporen van WiFi-verkeer in apparaatgeheugens

Kennisavond voor forensisch coordinatoren

2 oktober 2014

Het onderwerp



Het onderwerp (niet)

Bron: *Renew London* persbericht

Forensisch interessante informatie

→ *Wat voor informatie vliegt er door de lucht?*

- Beacon frames (Identiteit, Locatie, Tijd)
- Probe requests (Identiteit, Locatie[1])

[1] Maar dan anders.

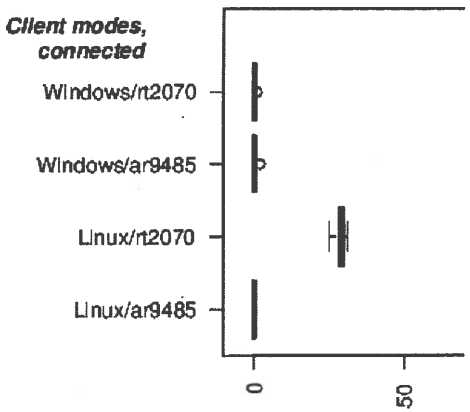
Meer info

→ *Wat blijft er achter in het vluchtige geheugen van apparaten?*

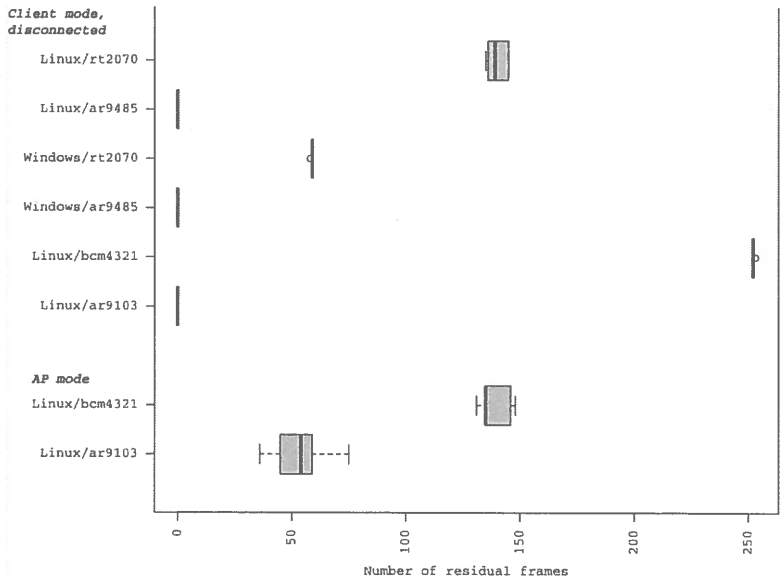
.

Paper @ http://dx.doi.org/10.1016/j.diin.2014.03.013

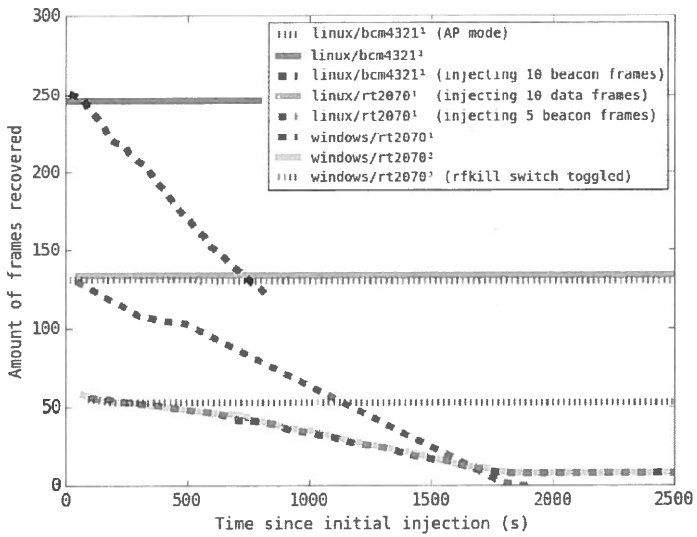
Retentie (1)


Client modes,
connected
Windows/rt2070
Windows/ar9485
Linux/rt2070
Linux/ar9485
0
50

Retentie (2)

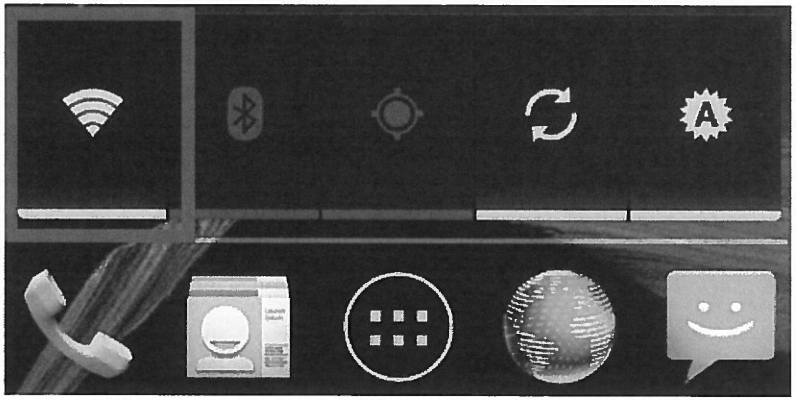

Client mode, disconnected
Linux/rt2070
Linux/ar9485
Windows/rt2070
Windows/ar9485
Linux/bcm4321
Linux/ar9103
AP mode
Linux/bcm4321
Linux/ar9103
0
50
100
150
200
250
Number of residual frames

Verval


linux/bcm4321[1] (AP mode)
linux/bcm4321[1]
linux/bcm4321[1] (injecting 10 beacon frames)
linux/rt2070[1] (injecting 10 data frames)
linux/rt2070[1] (injecting 5 beacon frames)
windows/rt2070[1]
windows/rt2070[2]
windows/rt2070[3] (rfkill switch toggled)
Amount of frames recovered
Time since initial injection (s)
0
50
100
150
200
250
300
0
500
1000
1500
2000
2500

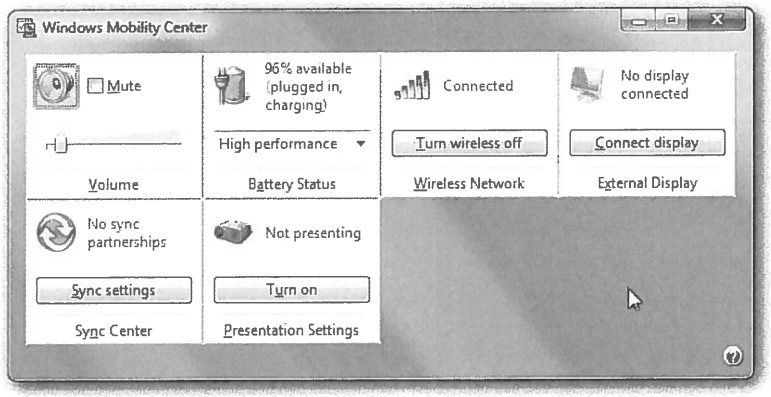
Voor in de praktijk

- Verval hangt af van 'drukte' in de ether (broadcast-verkeer).
  - → *zorg dus voor radiostilte op de plaats delict...*
- Uitzetten van de wifi (RFKILL) is een handige conserveringsmethode (knopjes, Windowstoets+X)



Voor in de praktijk

- Verval hangt af van 'drukte' in de ether (broadcast-verkeer).
  - → *zorg dus voor radiostilte op de plaats delict...*
- Uitzetten van de wifi (RFKILL) is een handige conserveringsmethode (knopjes, Windowstoets+X)

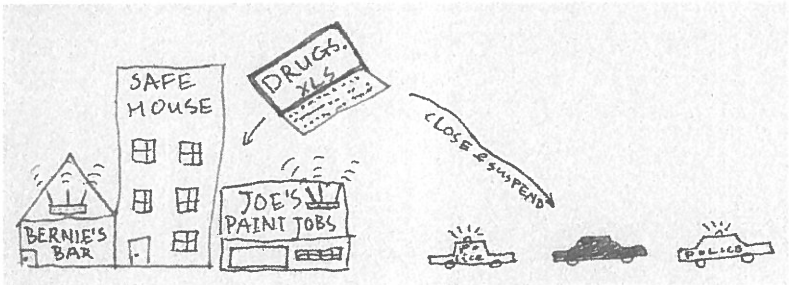


Een voorbeeldscenario

Een voorbeeldscenario

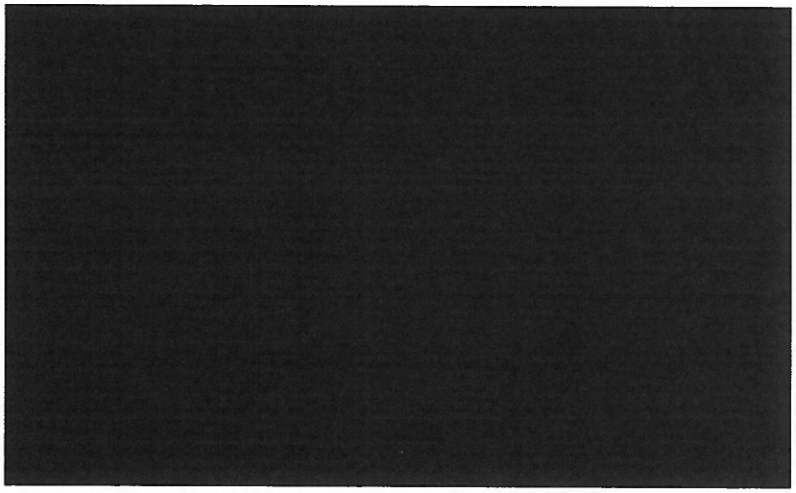
Een voorbeeldscenario

Een voorbeeldscenario



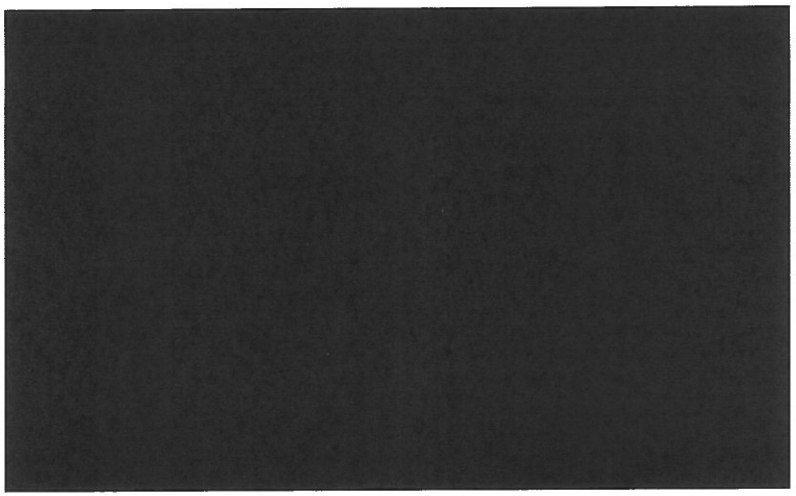
Welke informatie zouden we kunnen ontlenen aan de probe requests en beacon frames die we in het geheugen van de laptop vinden?

Een scenario met echt materiaal (1)



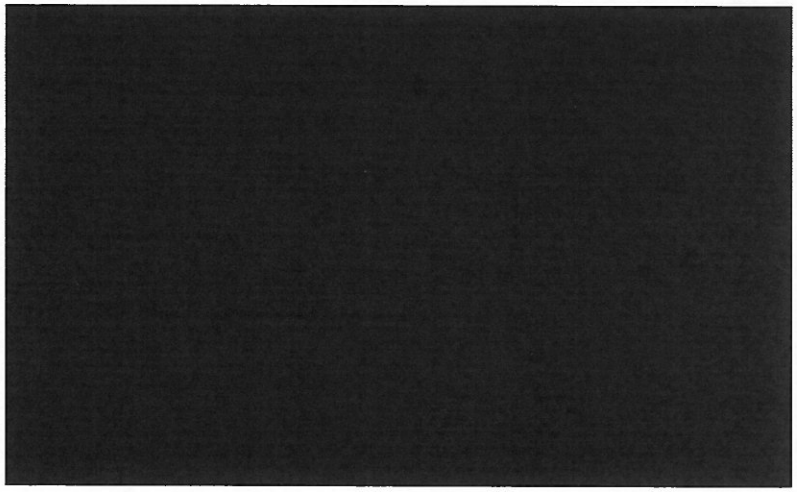
10.2.e

Een scenario met echt materiaal (2)



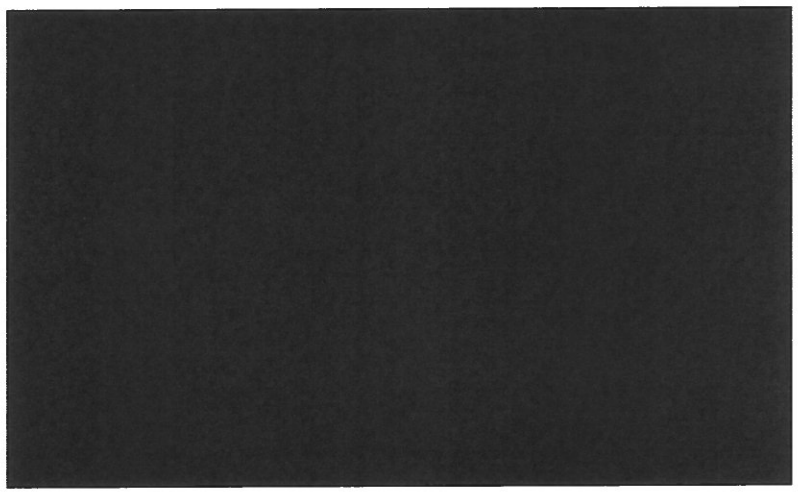
10.2.e

Een scenario met echt materiaal (3)



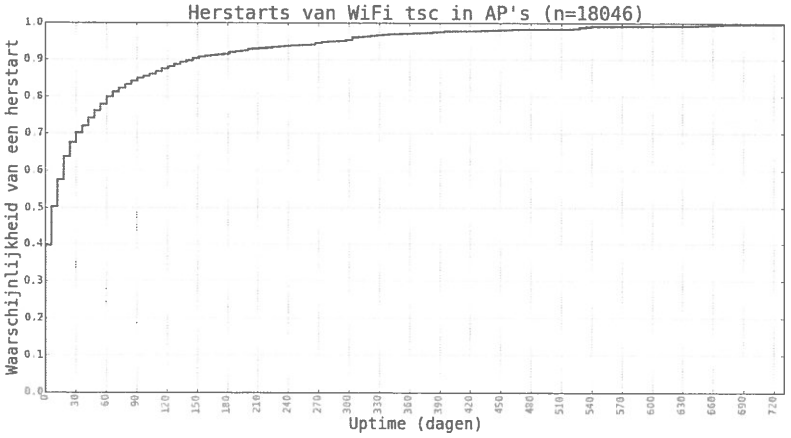
10.2.e.

Een scenario met echt materiaal (4)



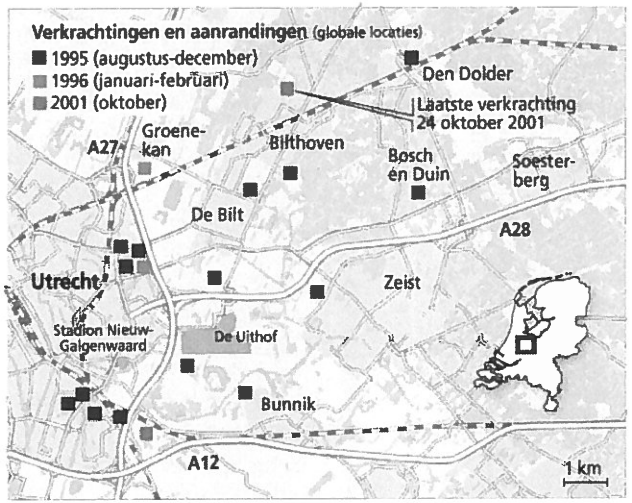
10.2.e.

Een scenario met echt materiaal (5)

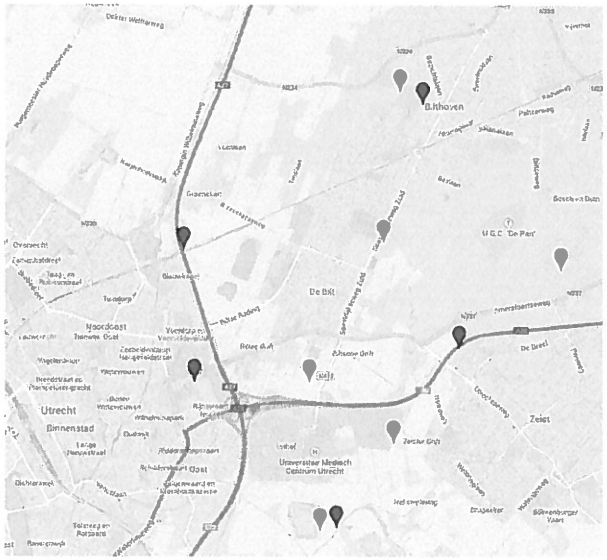


De Utrechtse serieverkrachter

Waar sloeg de Utrechtse serieverkrachter toe?



Radiodrukte



Radiodrukte

Radiodrukte: Bilthoven

Radiodrukte: Groenekan

Radiodrukte: Groenekan

Radiodrukte: Groenekan