Traces of nearby device's wireless transmissions in volatile memory

DFRWS-EU '14

Wicher Minnaard

May 8th, 2014

About me

- Forensic investigator @ *Netherlands Forensic Institute* (NFI) since '11
- Finishing my Master's in *System and Network Engineering* (UvA) this summer

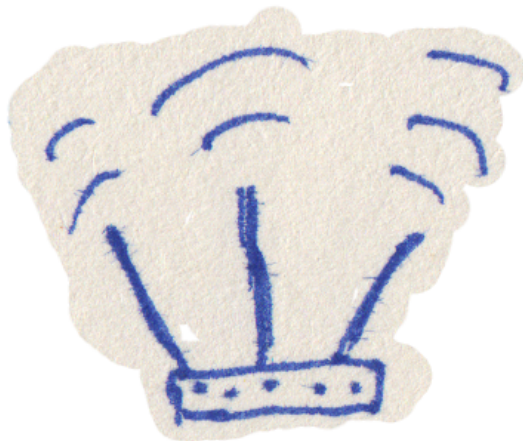
The research topic

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

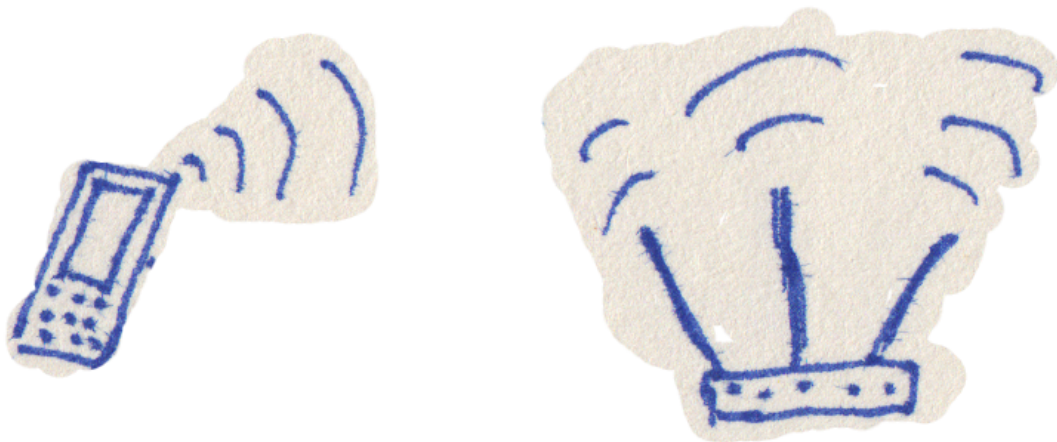
The research topic

Source: *Renew London* press release

The research topic

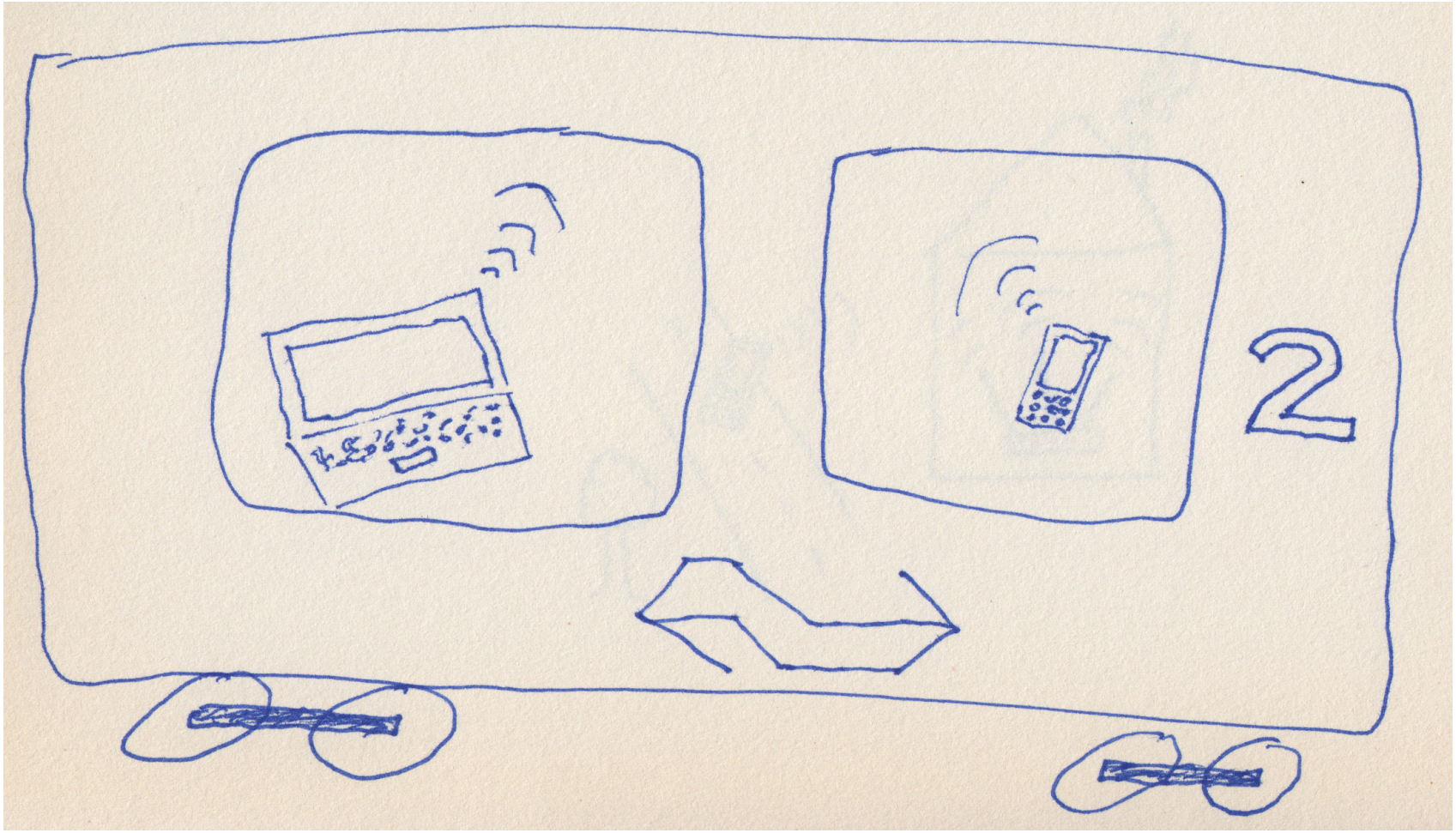


The research topic



The research topic

The research topic



The research topic

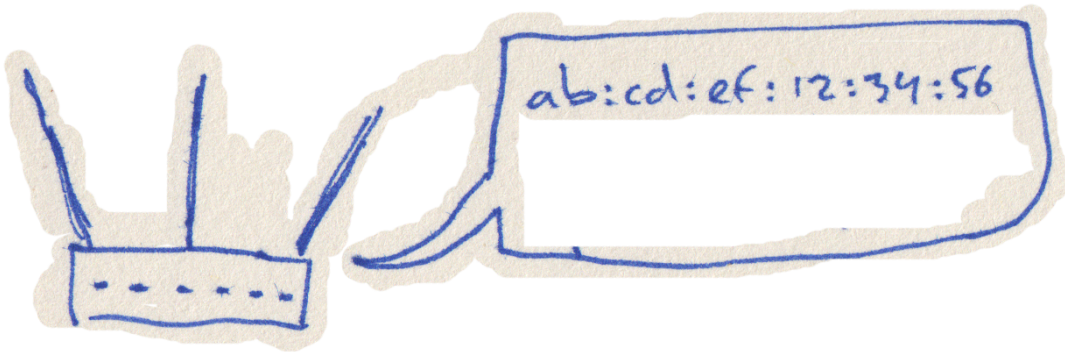
We've been receiving questions from police forces...

Any traces of interesting information?

- Beacon frames (Identity, Location, Time)
- Probe requests (Identity, Location[1])

[1] But different.

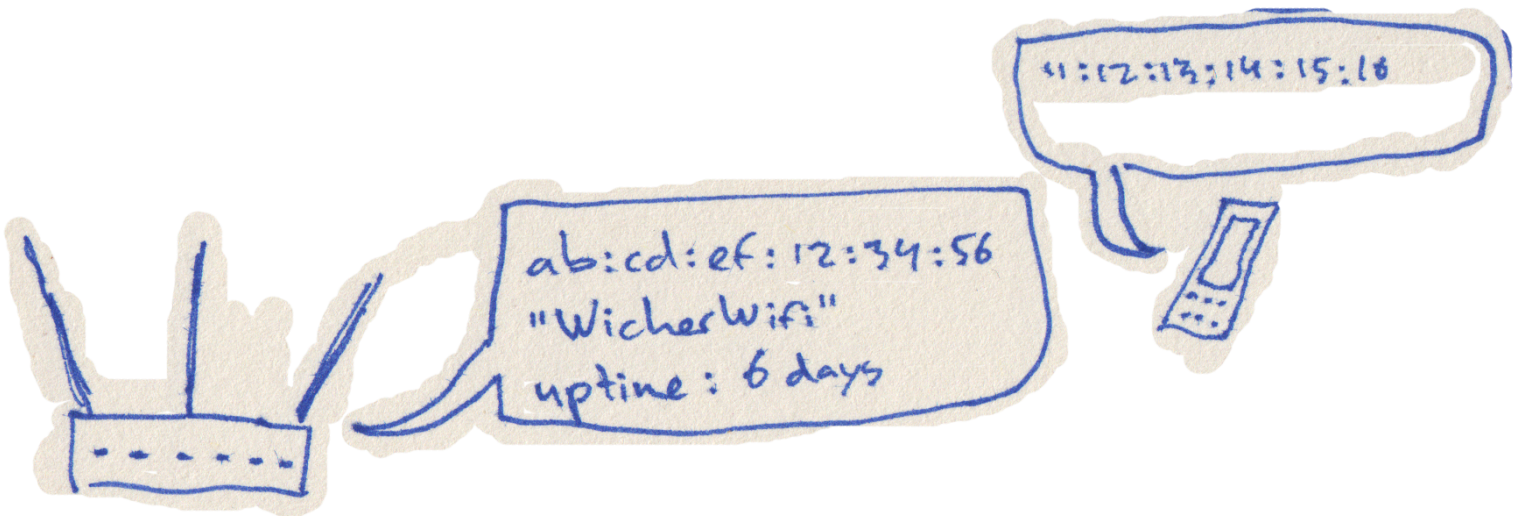
Information in beacons & probes



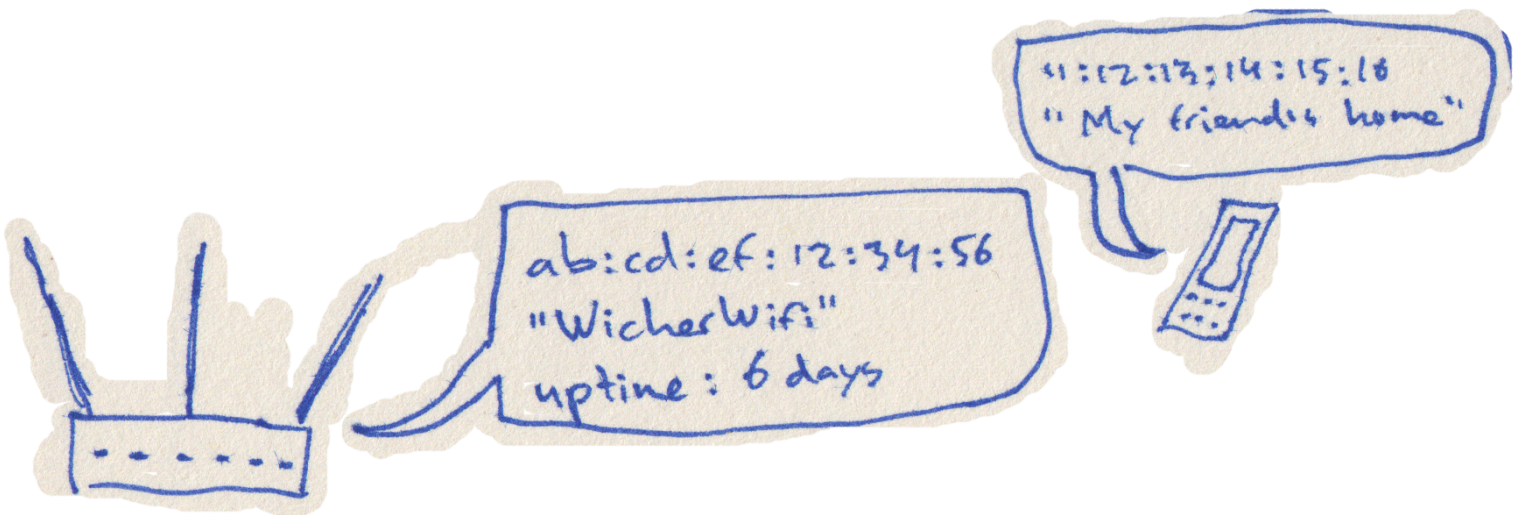
Information in beacons & probes

Information in beacons & probes

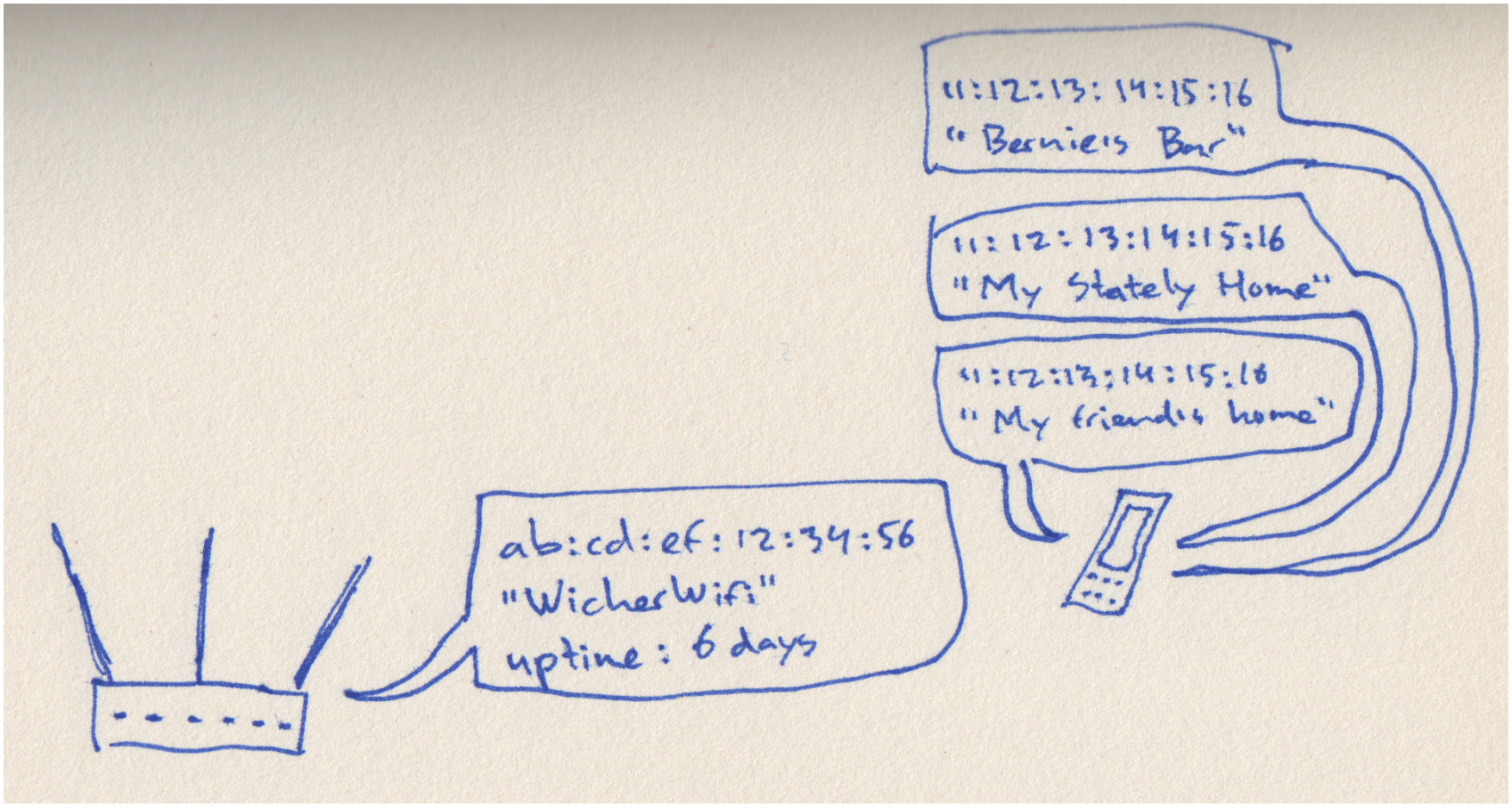
Information in beacons & probes



Information in beacons & probes



Information in beacons & probes



Retention experiment

→ *How common is the retention behaviour? Can we exclude certain device classes?*

Inject a fixed number of *unique*[2] probe request frames.

Dump subject device memory.

Search dump for injected frames.

Count them.

Repeat 10 times for each configuration.

[2] MAC and SSID fields will be pseudorandomly generated.

Retention experiment

→ *How common is the retention behaviour? Can we exclude certain device classes?*

Inject a fixed number of *unique*[2] probe request frames.

Dump subject device memory.

Search dump for injected frames.

Count them.

Repeat 10 times for each configuration.

Scripts available through the link in the paper

[2] MAC and SSID fields will be pseudorandomly generated.

Retention experiment: Subject devices

Wireless chipsets used.

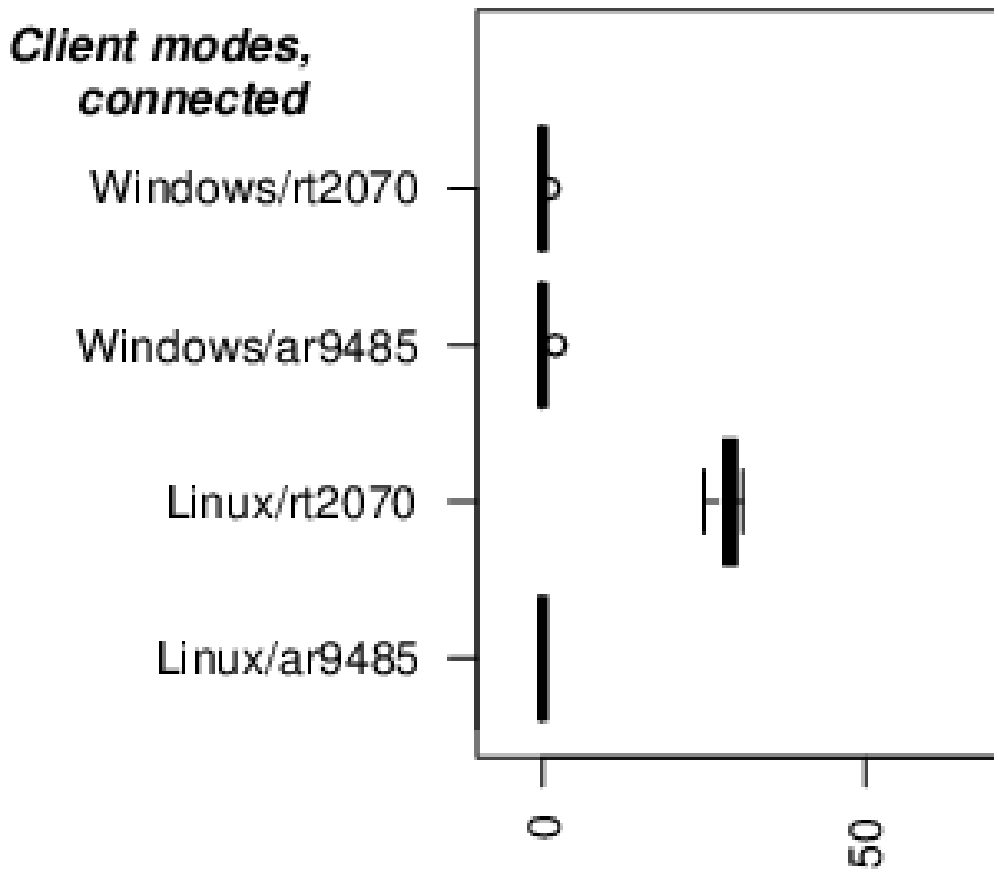
Chipset	Interface	Host system	Description
bcm4330	SDIO	Samsung Galaxy Nexus	A Broadcom chip on an ARM smartphone board, brcmfmac driver.
bcm4321	PCI	D-link DSL-2740B	On a Broadcom MIPS wifi router board (bcm6358), b43 driver.
ar9103	AMBA	TP-Link TL-WR1043ND	On an Atheros MIPS wifi router board (ar9132), ath9k driver.
ar9485	PCIe	HP Pavilion DM1-4000SD	An Atheros adapter, part of the laptop. Linux driver: ath9k, Windows manufacturer driver version: "9.2.0.427".
rt2070	USB	HP Pavilion DM1-4000SD	A Ralink chip inside a D-link DWL-G122 (rev.E1) USB adapter. Linux driver: rt2800usb, Windows manufacturer driver version: " v3_60_s0038".

Host system configuration.

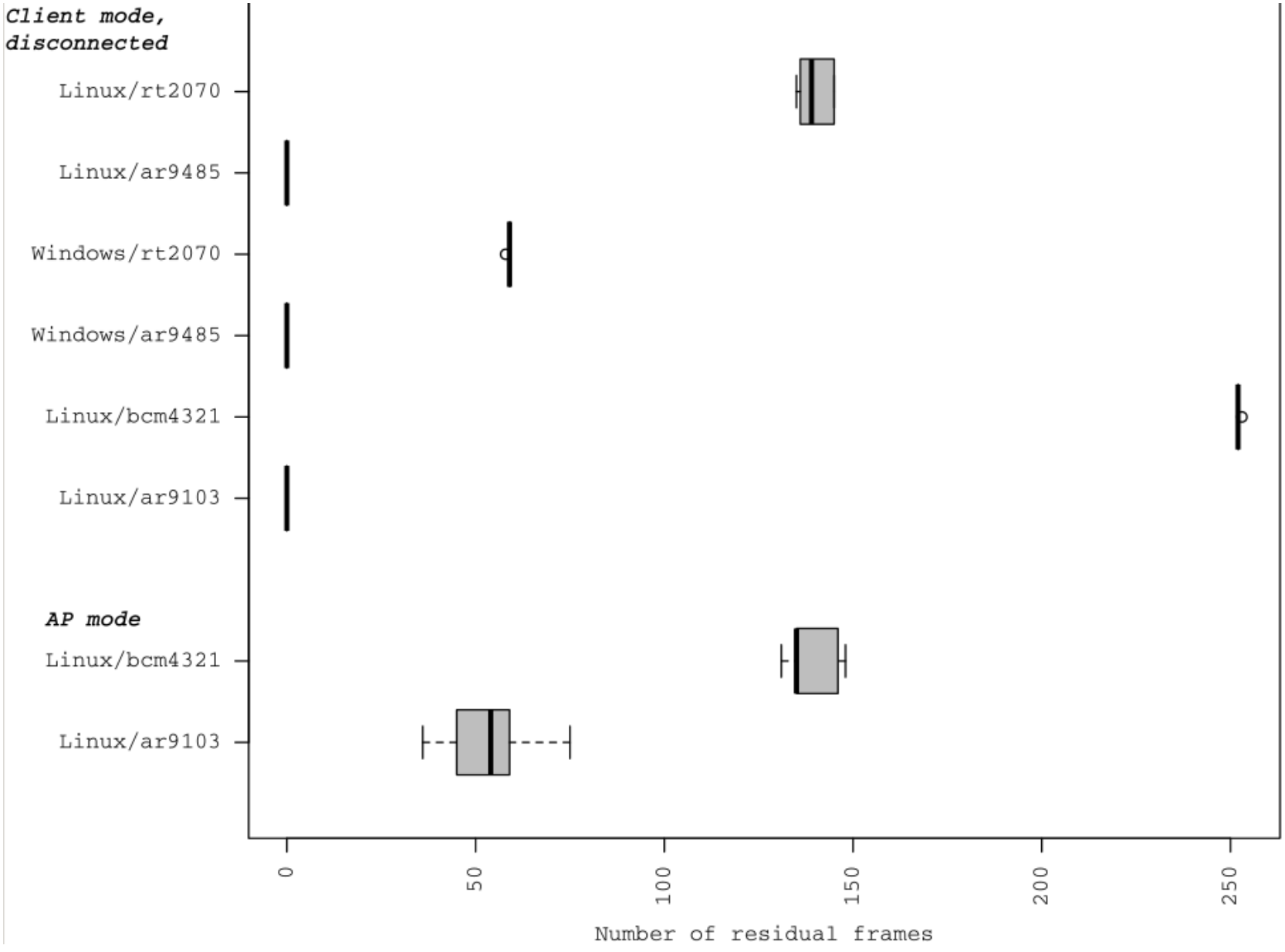
Host system	Description
Galaxy Nexus	Equipped with the Replicant 4.0-0003 fully open source Android-compatible firmware (Linux kernel with Android userspace). Memory is dumped with LiME r17 (Sylve et al., 2012), using TCP over ADB. This system has 768 MB of RAM.
DSL-2740B TL-WR1043ND	Running OpenWRT 12.09—a Linux distribution targeted at networking equipment and embedded systems. Memory is dumped over TCP using LiME r17. Both systems have 32 MB of RAM.
Pavilion DM1-4000SD	Windows 7 Home Premium, 32-bit, build 7601 (SP1). Memory is limited to 512 MB and its contents are acquired using crash dumps. For the decay tests memory is dumped over TCP using KnTDD 2.3.0.2733. 32-bit Linux through the SystemRescueCD live-cd distribution with kernel 3.4.52, limited to 256 MB RAM, which is dumped over TCP using LiME r17.

Mix of different buses, chipsets, drivers and OSes (Windows 7, and three Linux flavours).

Retention experiment: Results



Retention experiment: Results



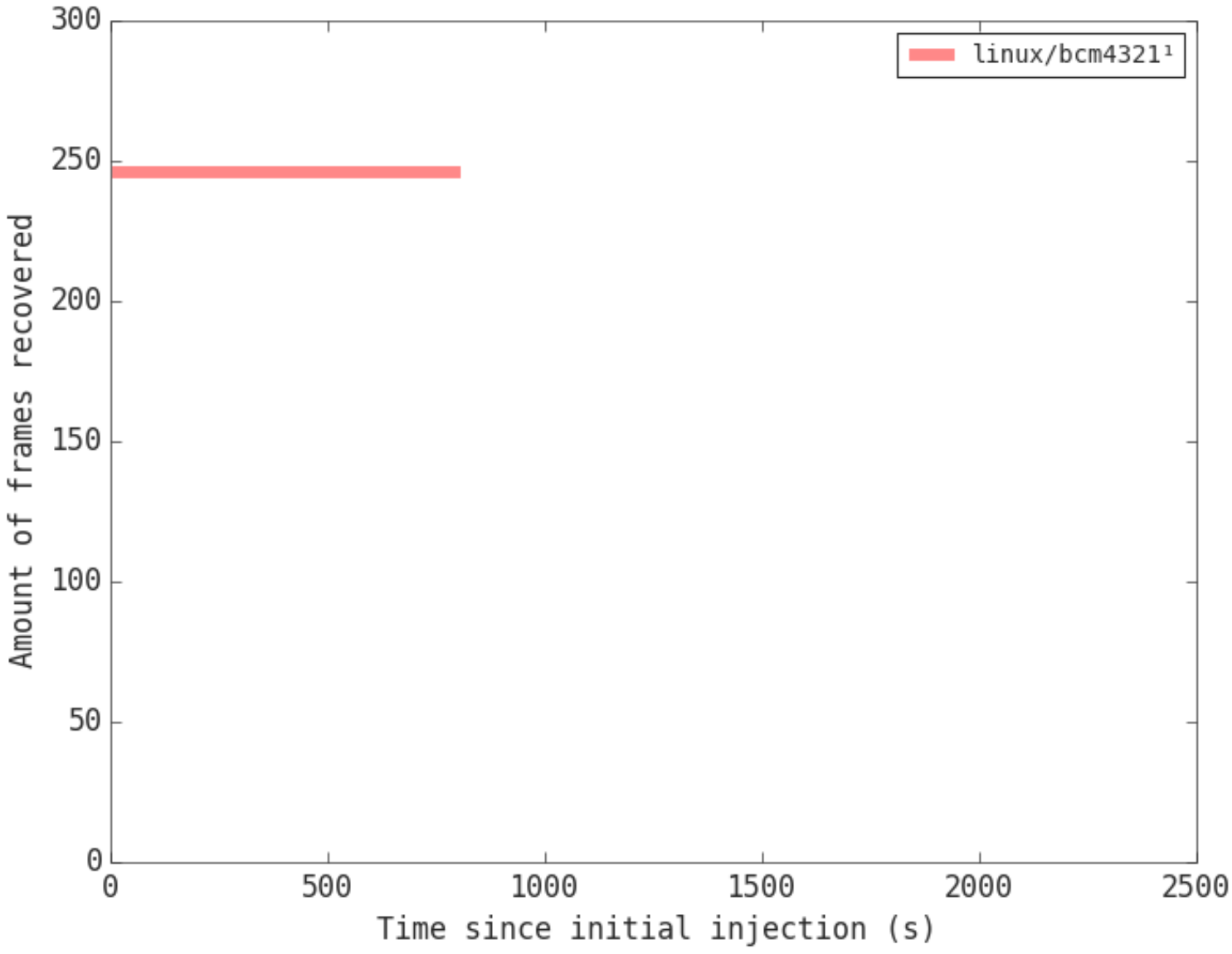
Retention experiment: Interim observations

1. Retention behaviour is not tied to one particular mode, bus, chipset, driver, or OS.
2. Seems to be a function of driver/firmware boundary architecture; hard to generalize.
3. Except... for the distinction between Linux SoftMAC/HardMAC drivers; `#include mac80211.h`

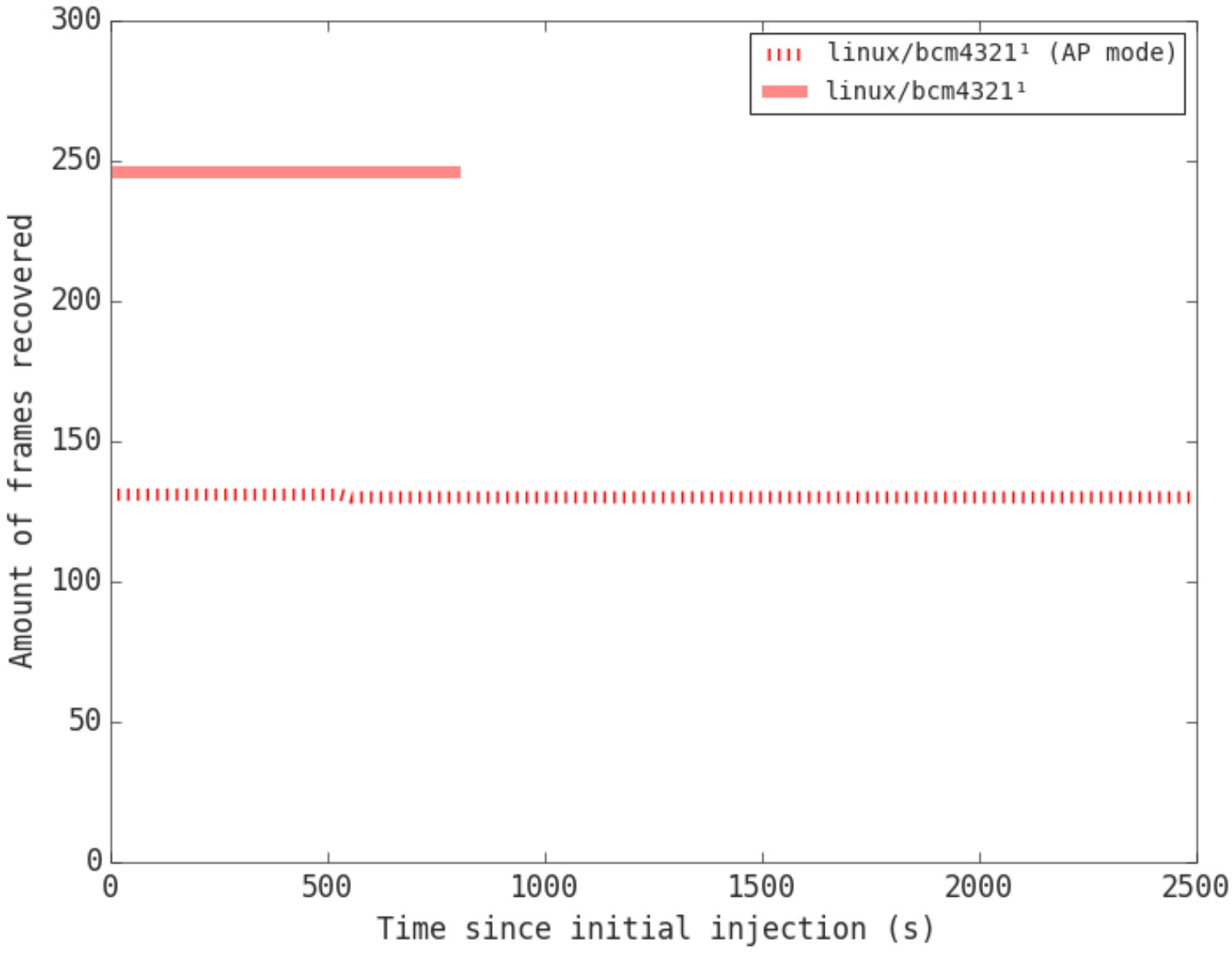
Decay experiment

$\rightarrow$ *So how volatile are these traces?*

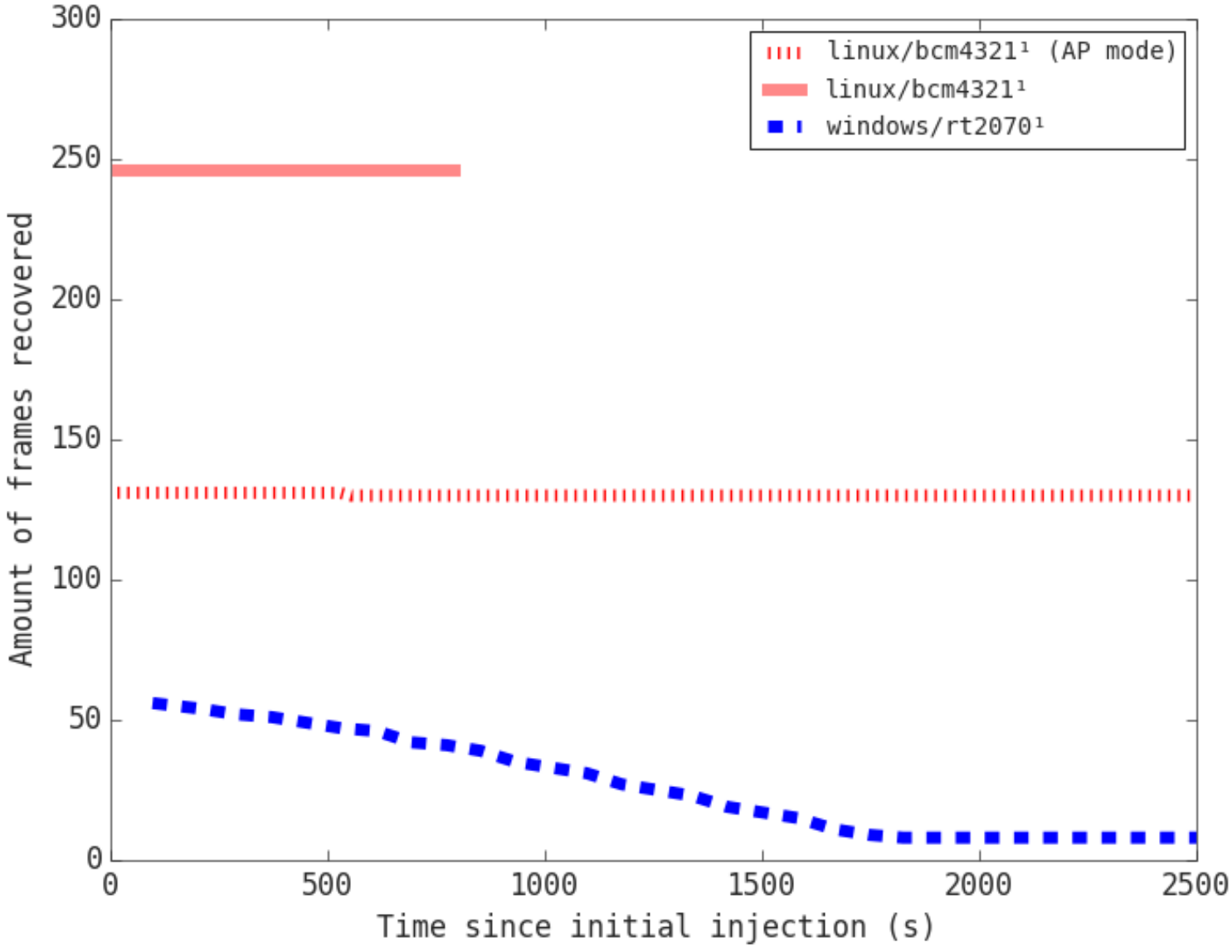
Decay experiment



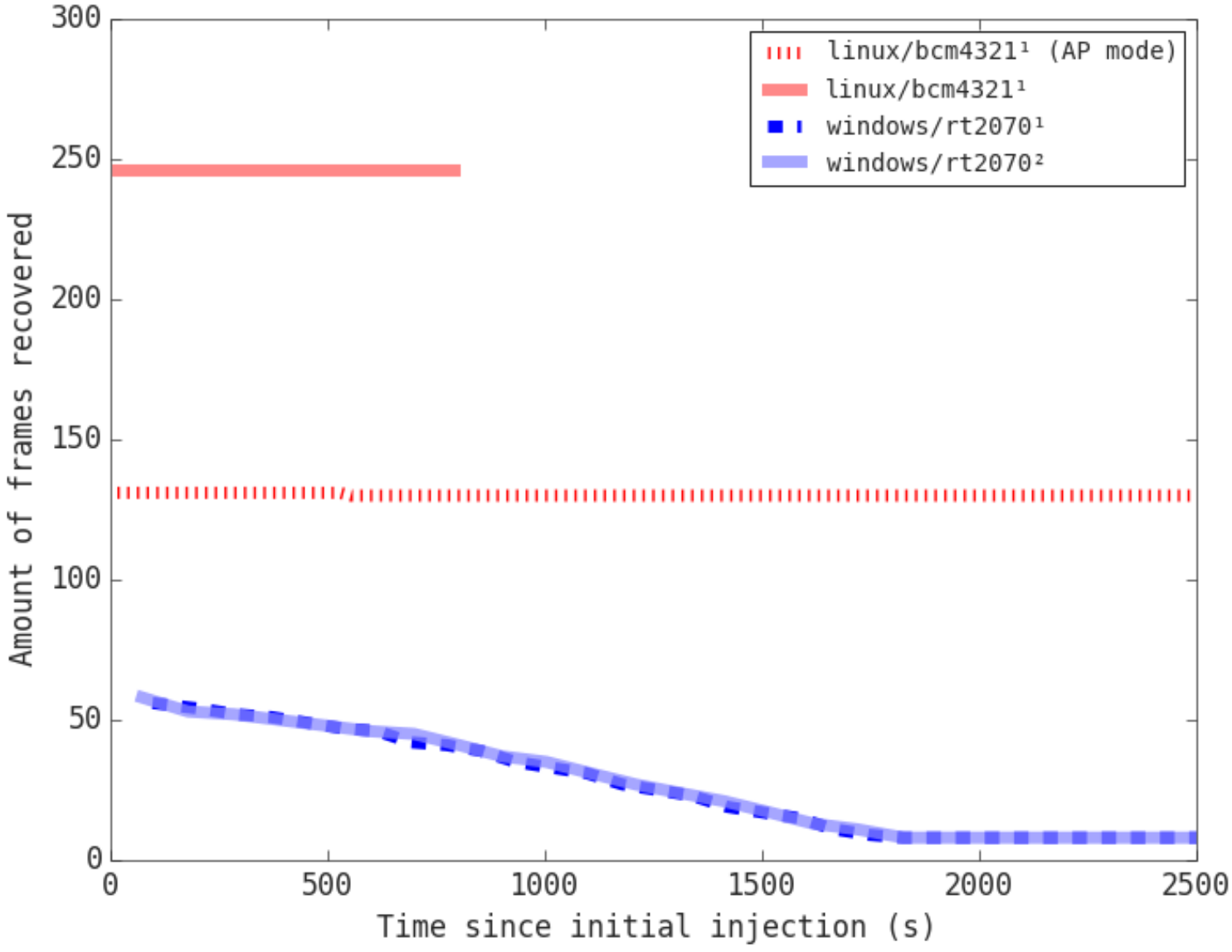
Decay experiment



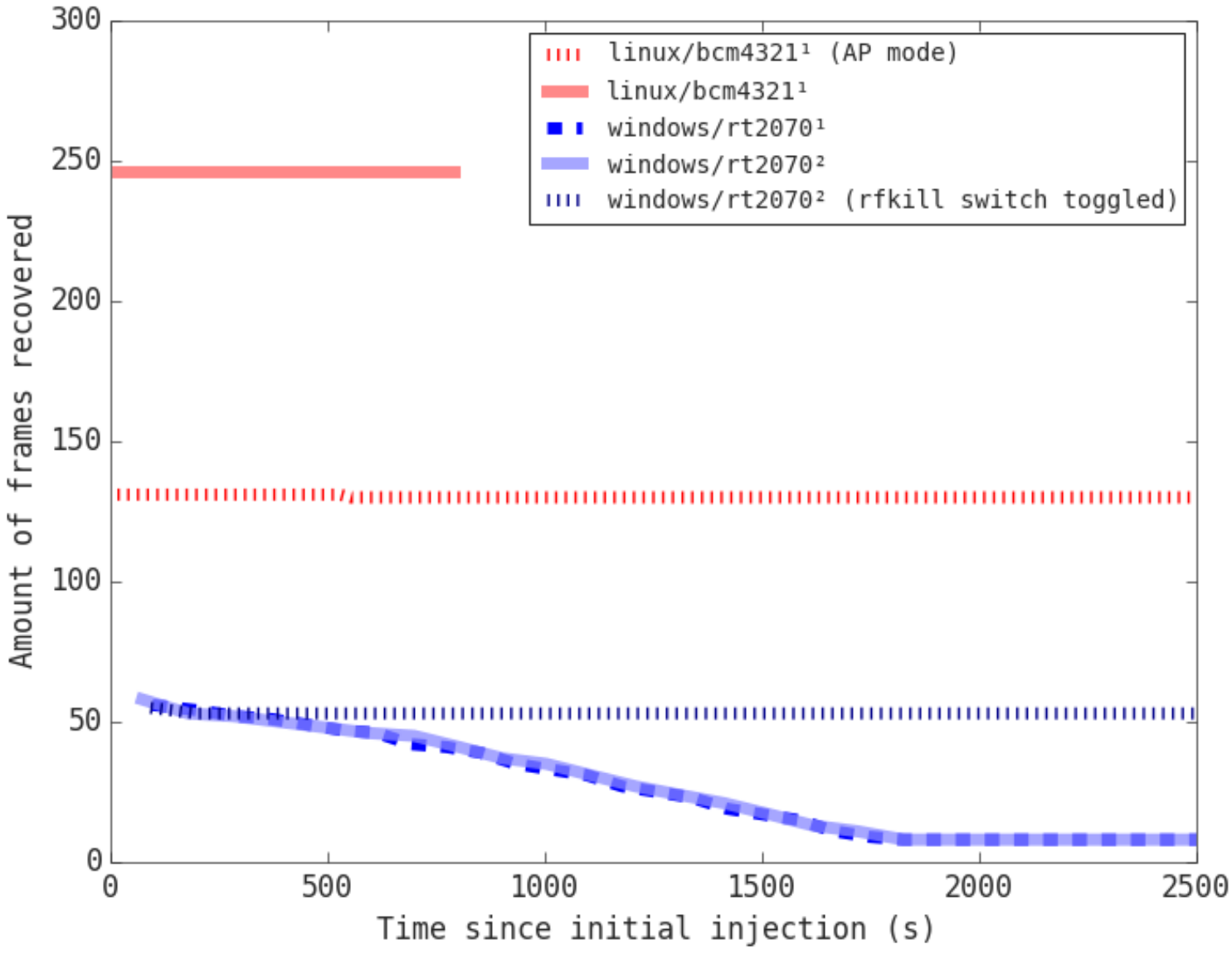
Decay experiment



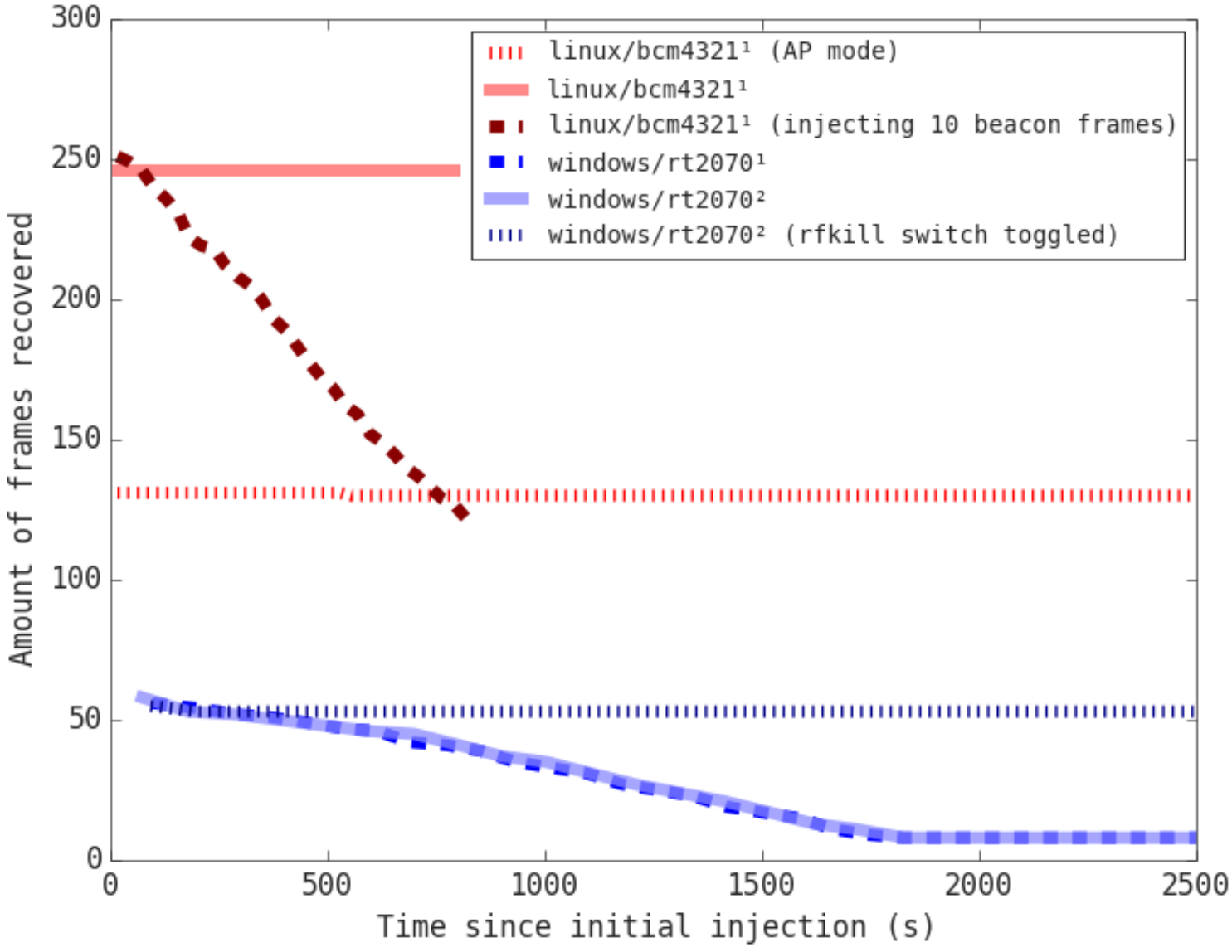
Decay experiment



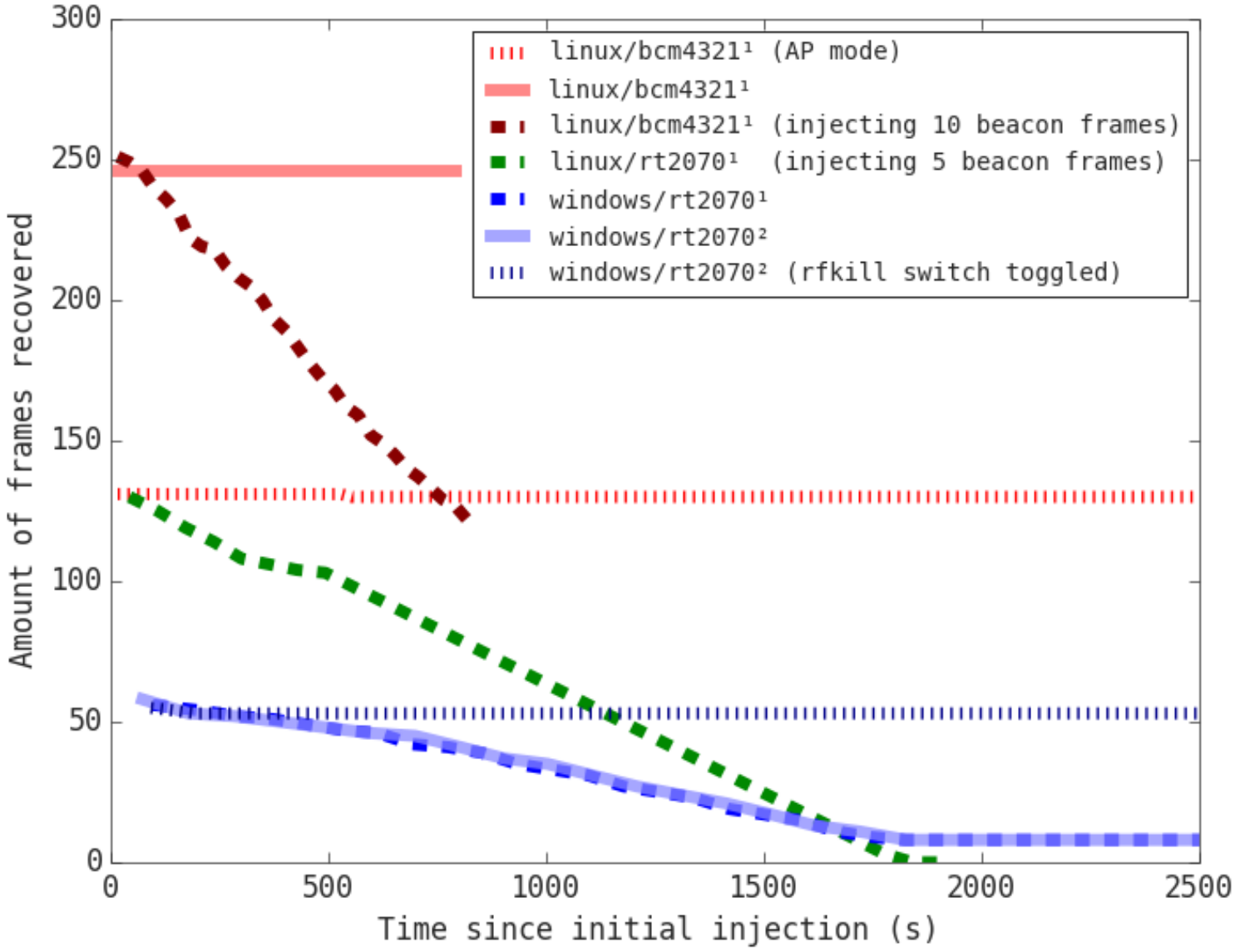
Decay experiment



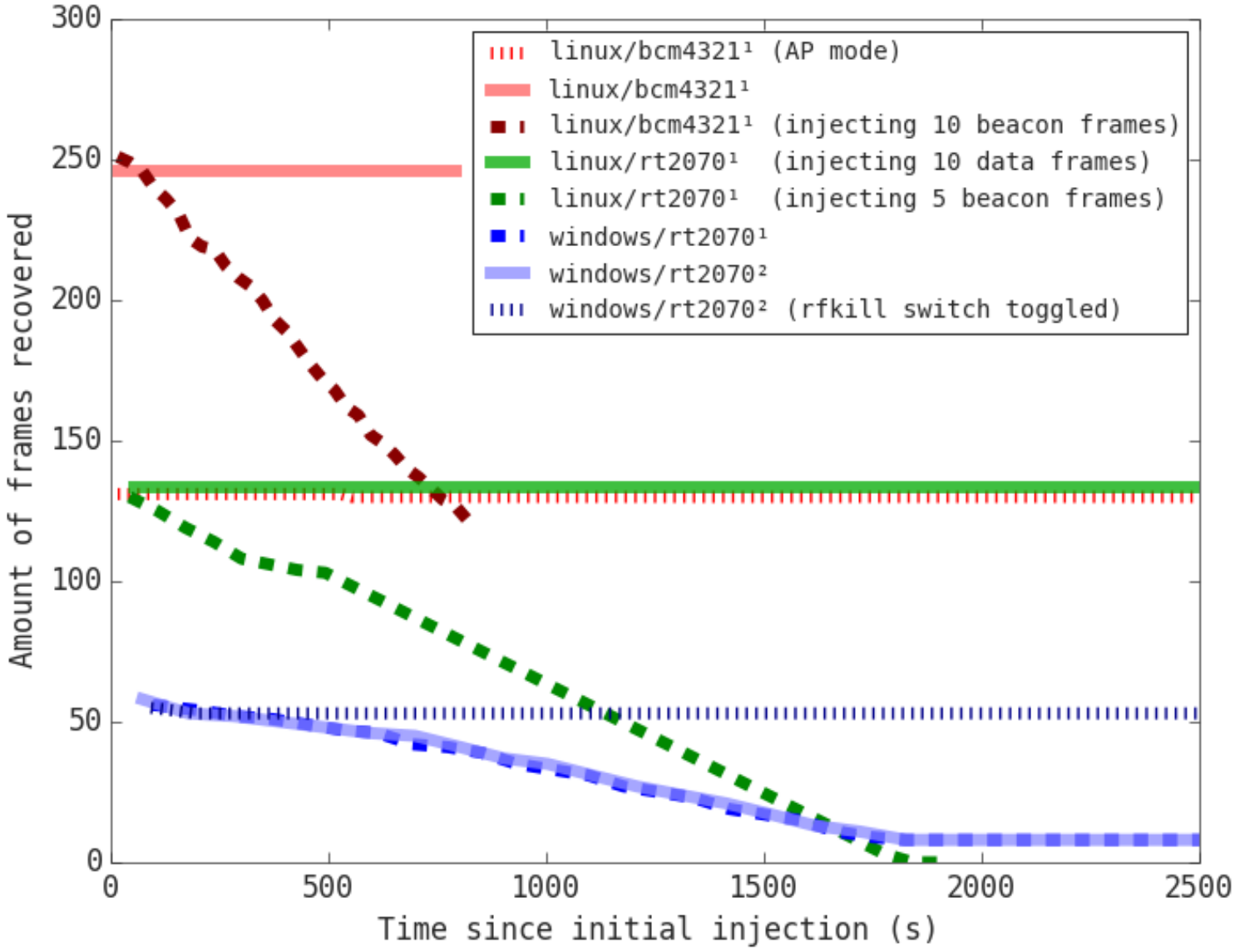
Decay experiment



Decay experiment



Decay experiment



Decay experiment: Interim observations

1. Broadcast traffic seems to be destructive.
2. Unrelated unicast data frames do not seem to be.
3. Odd behaviour of `Windows/rt2070`
4. Sidenote: `HIBERFIL.SYS`

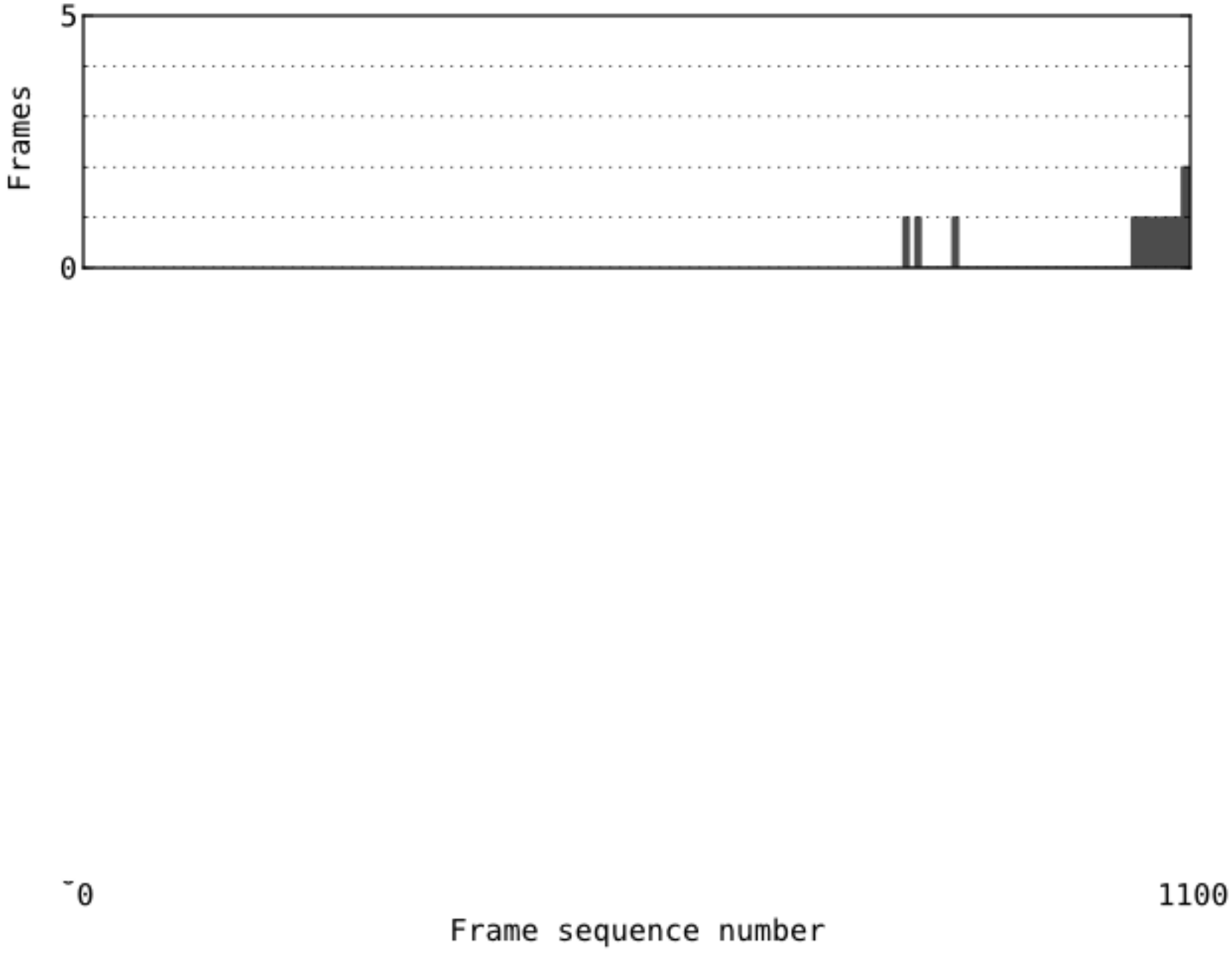
Amplification

$\rightarrow$ *What about derivative traces? Traces of just the MAC or SSID?*

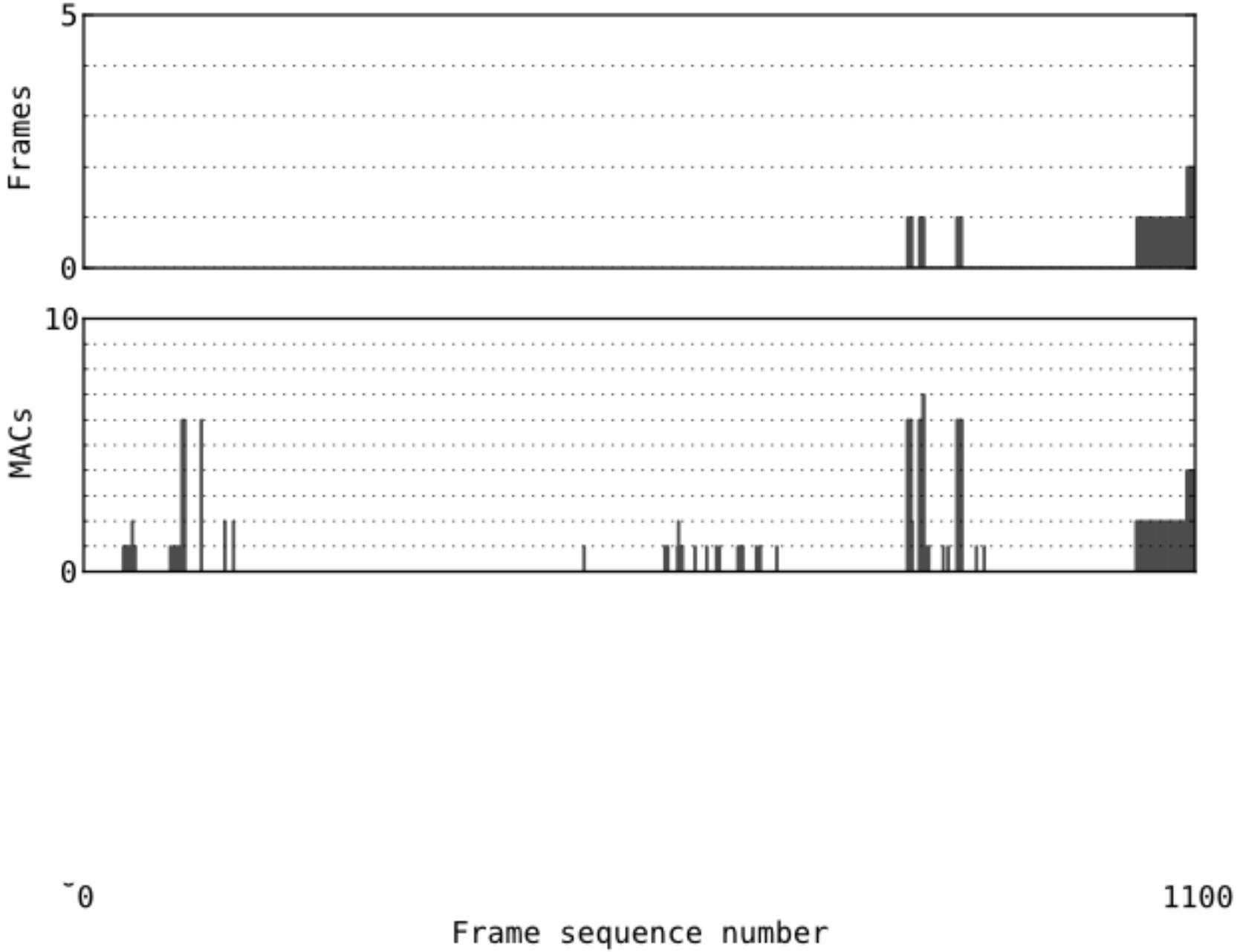
Amplification

→ *What about derivative traces? Traces of just the MAC or SSID?* Only seen on Windows, for beacons, whenever the *wlanext.exe* process is present.

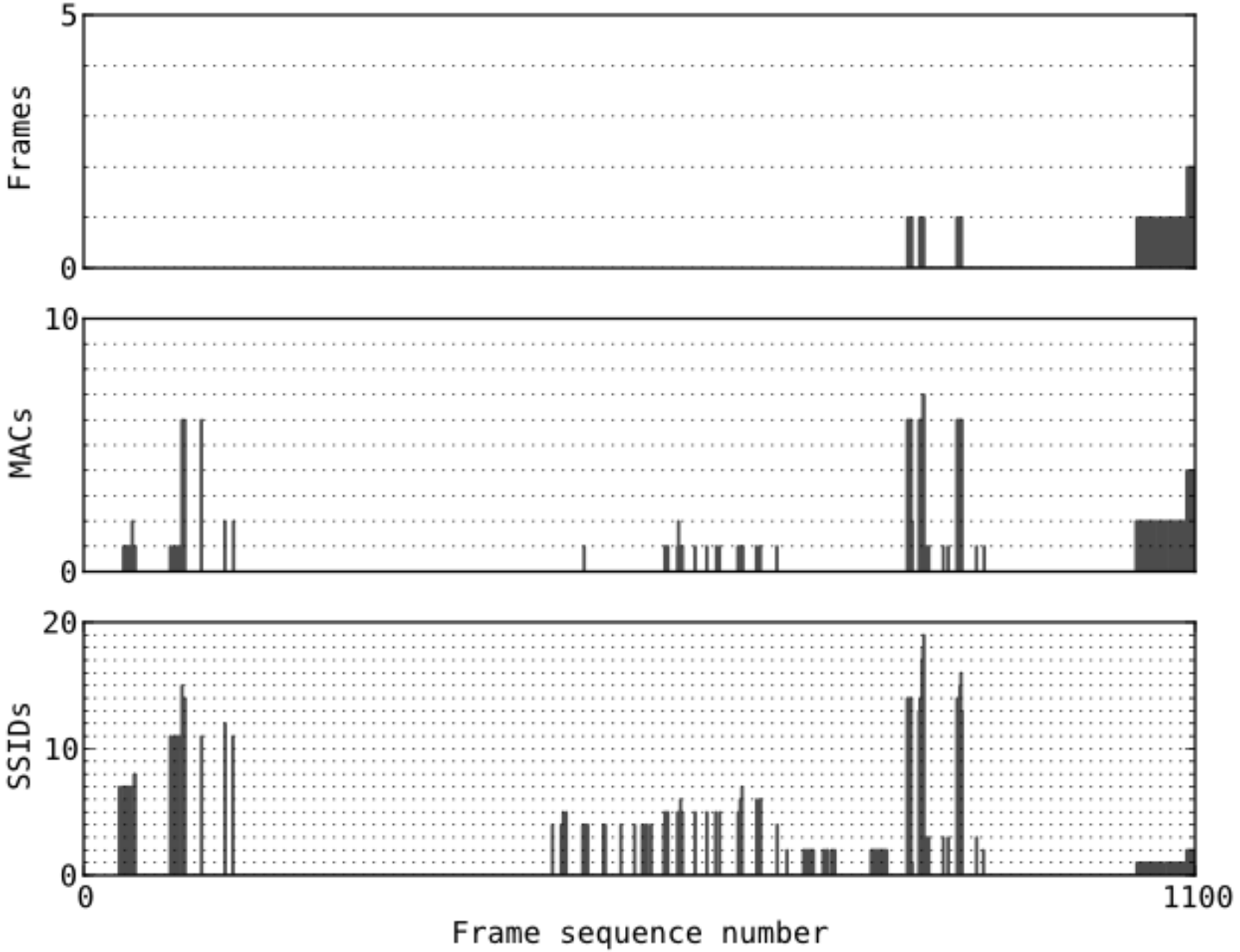
Amplification



Amplification



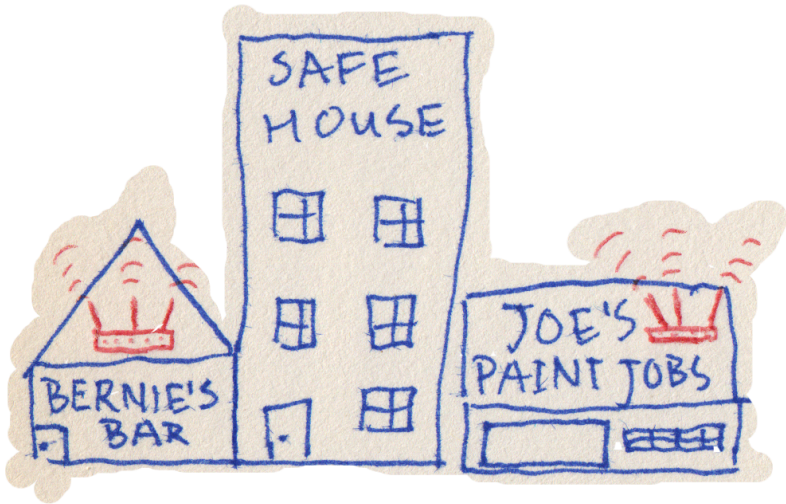
Amplification



Usability of trace type in "real-world" scenarios

1. Traces are common, but fragile.
2. Given a memory dump, carving for probes and beacons is essentially device-agnostic, and *almost free*
3. Opportunities will be rare, but will often be *identifiable*.

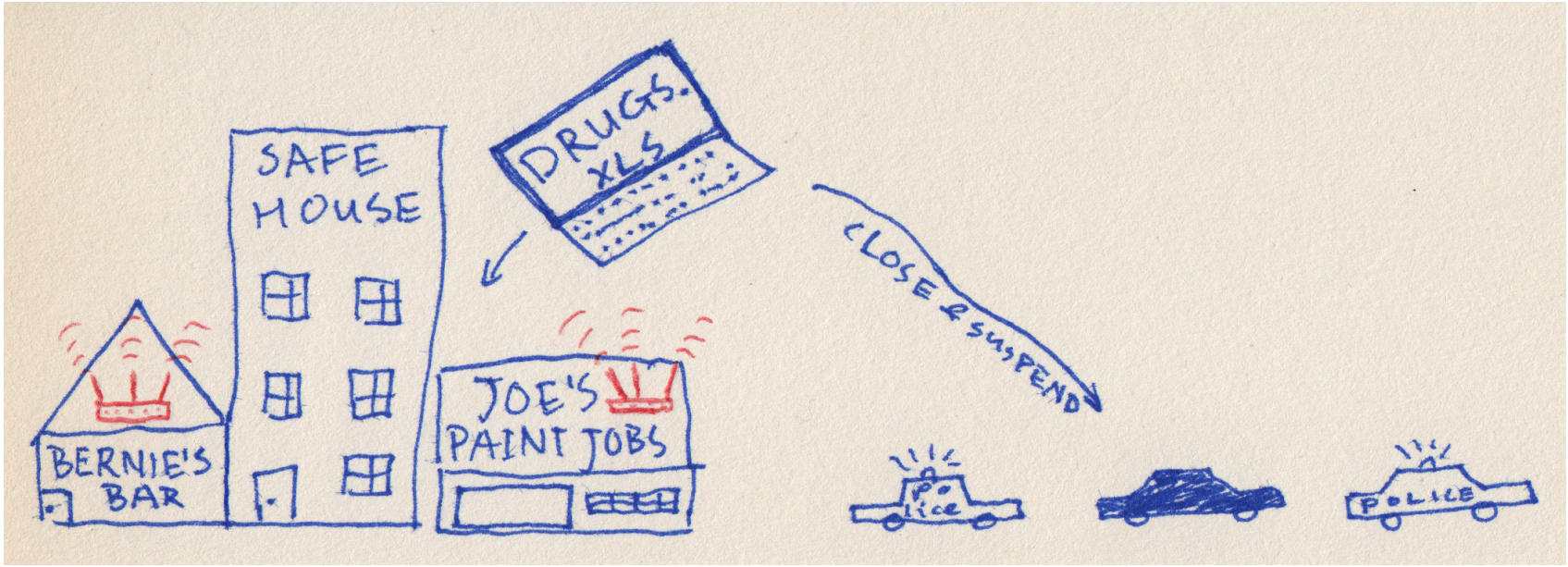
An urban opportunity



An urban opportunity

An urban opportunity

An urban opportunity



Retrievable through beacon frames carved from laptop physmem:

- Location approximation of safe house
- Time at which beacons were generated (if second beacon sample is acquired at a known time)

Open questions

- What about Apple laptops?
- What about Bluetooth?
- What about `wlanext.exe`?