European
Commission

Building a pipeline to analyse iOS devices at scale

Hack.lu Conference 2025

TLP:CLEAR

European
Commission

$whoarewe

Christophe Vandeplas

🍟 🚲 BE

Security Consultant
Open-source Developer

David Durvaux

🍟 🍺 BE

Situation Awareness
Head of Sector at
European Commission

Darío Borreguero Rincón

🌞 ⚽ ES

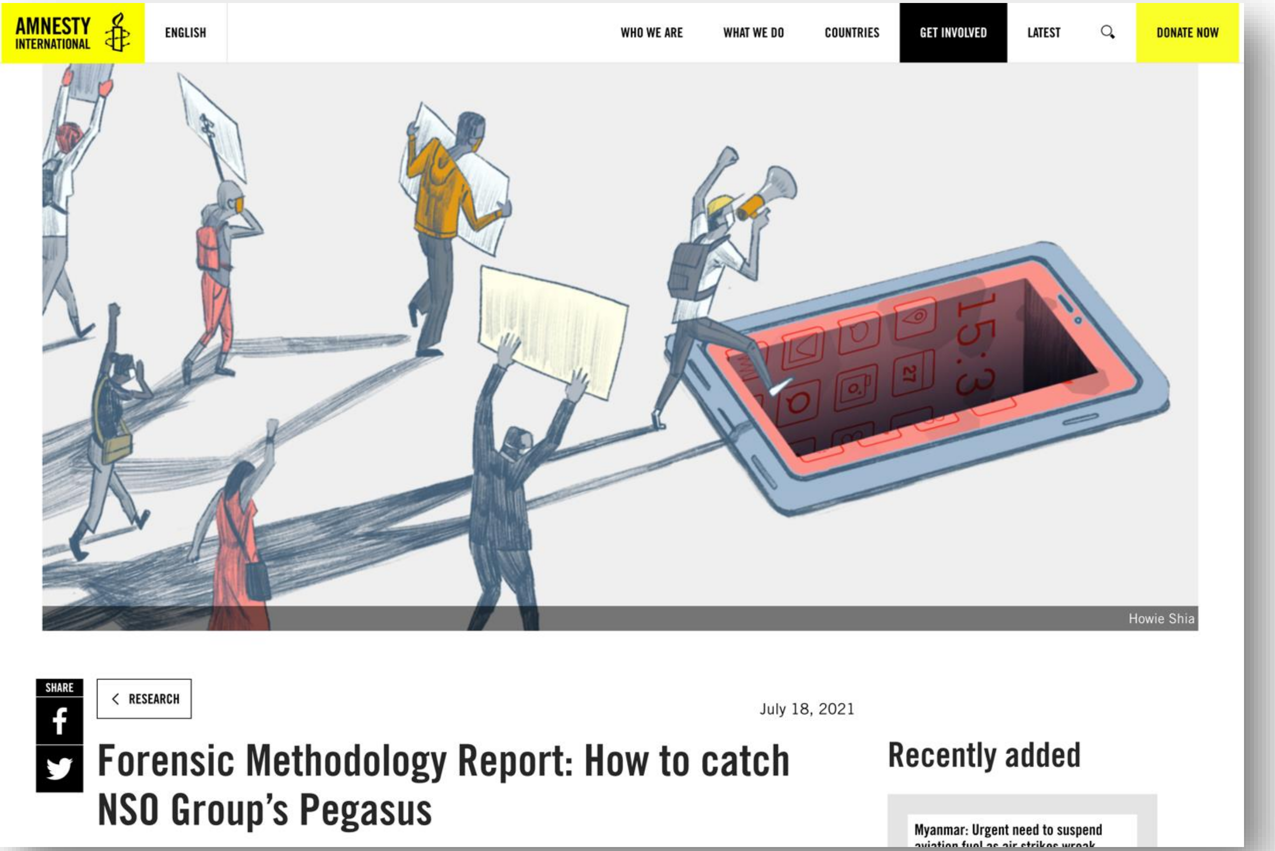
CSIRC Senior Incident
Handler at European
Commission

Agenda

- Problem statement
- The genesis
- Growing up
- Today
- Future

Problem statement

Why perform mobile device analysis?



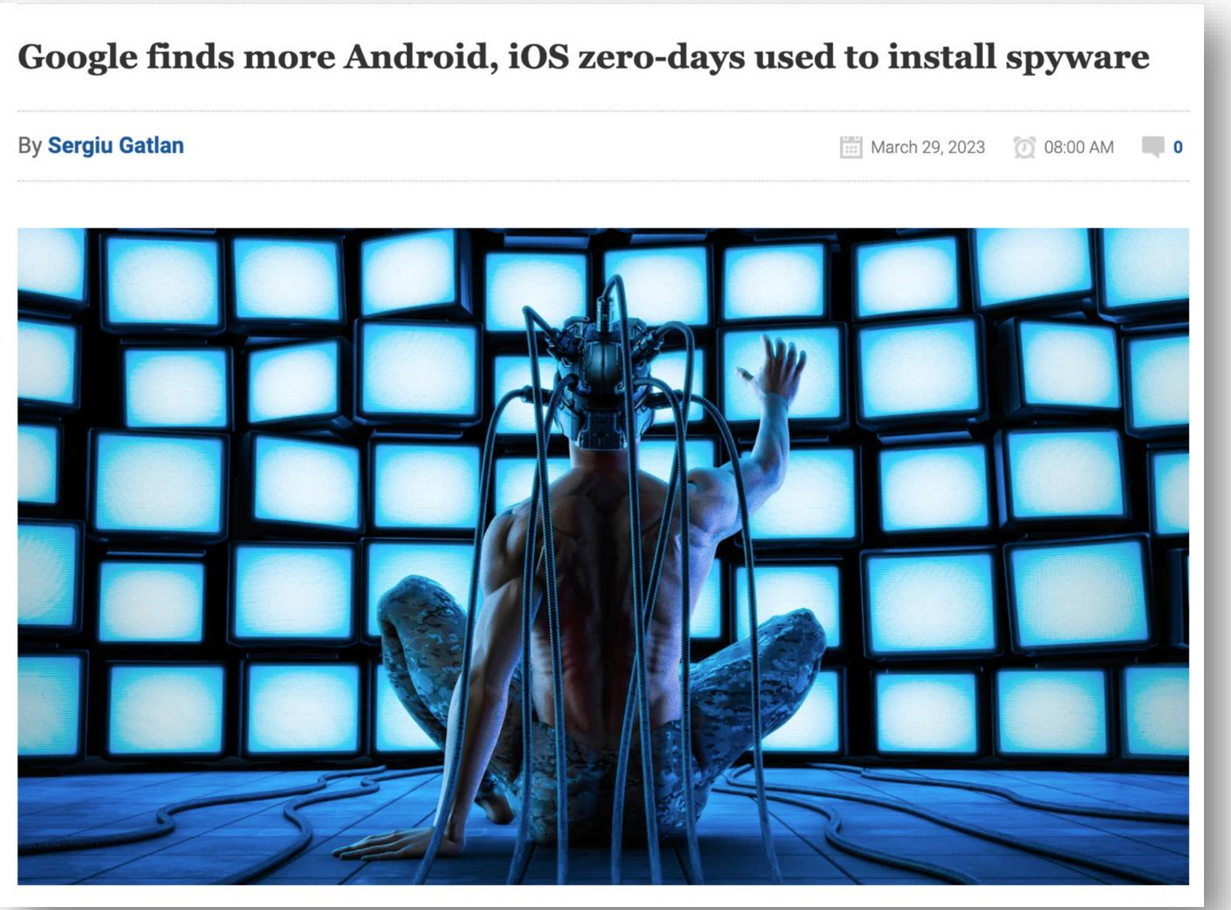
Howie Shia

July 18, 2021

Forensic Methodology Report: How to catch NSO Group's Pegasus

Recently added

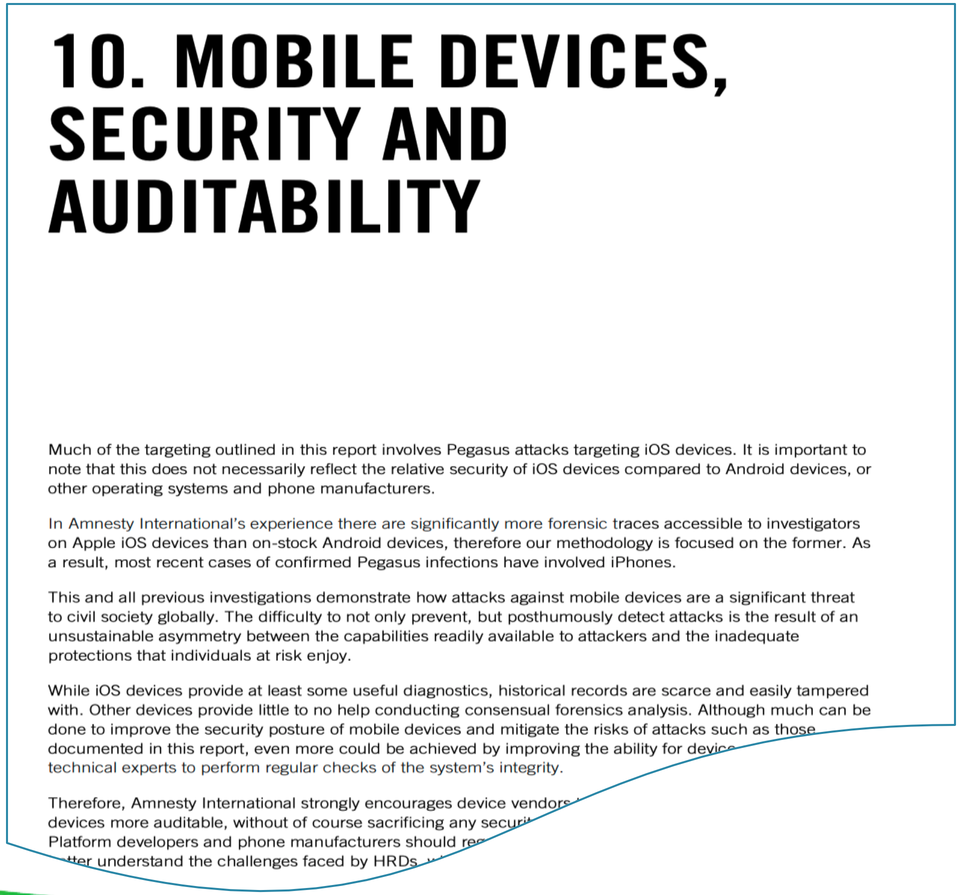
Myanmar: Urgent need to suspend aviation fuel as air strikes wreak



Google finds more Android, iOS zero-days used to install spyware

By **Sergiu Gatlan** March 29, 2023 08:00 AM 0

Let’s zoom into the Amnesty report



10. MOBILE DEVICES, SECURITY AND AUDITABILITY

Much of the targeting outlined in this report involves Pegasus attacks targeting iOS devices. It is important to note that this does not necessarily reflect the relative security of iOS devices compared to Android devices, or other operating systems and phone manufacturers.

In Amnesty International’s experience there are significantly more forensic traces accessible to investigators on Apple iOS devices than on-stock Android devices, therefore our methodology is focused on the former. As a result, most recent cases of confirmed Pegasus infections have involved iPhones.

This and all previous investigations demonstrate how attacks against mobile devices are a significant threat to civil society globally. The difficulty to not only prevent, but posthumously detect attacks is the result of an unsustainable asymmetry between the capabilities readily available to attackers and the inadequate protections that individuals at risk enjoy.

While iOS devices provide at least some useful diagnostics, historical records are scarce and easily tampered with. Other devices provide little to no help conducting consensual forensics analysis. Although much can be done to improve the security posture of mobile devices and mitigate the risks of attacks such as those documented in this report, even more could be achieved by improving the ability for device
technical experts to perform regular checks of the system’s integrity.

Therefore, Amnesty International strongly encourages device vendors
devices more auditable, without of course sacrificing any securi
Platform developers and phone manufacturers should re
tter understand the challenges faced by HRDs

- Relies on available artefacts
- Comes with a tool: Mobile Verification Toolkit (MVT)
- MVT for iOS:
  - **Filesystem Dump**: might have an impact on artefacts
  - **iTunes Backup**

The genesis

Let’s do something

but we don’t know what…

To find something

But we don’t know what…

The story

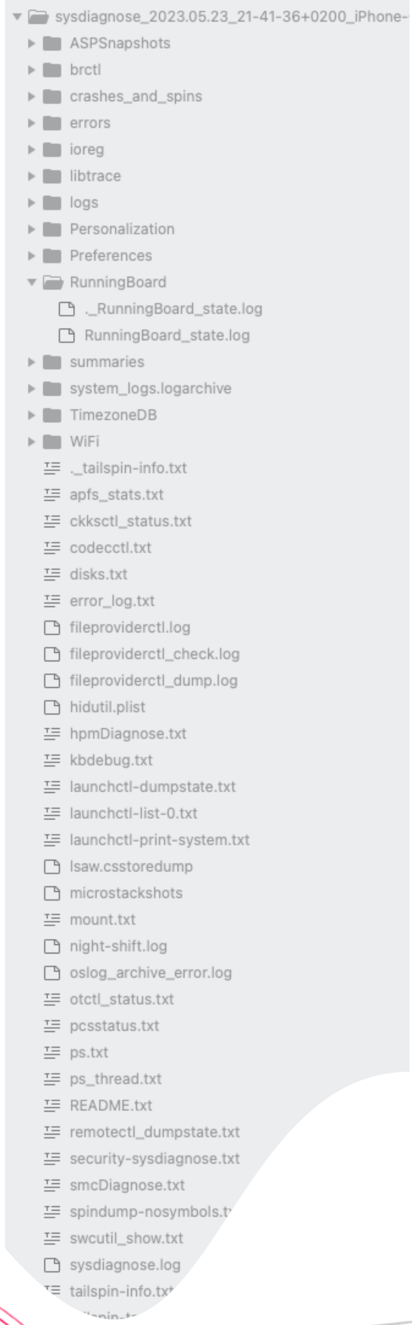
- We assumed mobile could be a target (it’s a computer after all)
- We heard (thanks Sarah) around a beer that there is something called “sysdiagnose”
- A bit of Googling showed just a few scripts for a very limited coverage
- So…

Why not simply using Amnesty MVT?

- Initially we started before ;)
- MVT has a strong emphasis on using device backup (contains private data)
- Sysdiagnose is a diagnostic feature intended to be used by Apple support and developers (minimal impact on user privacy)

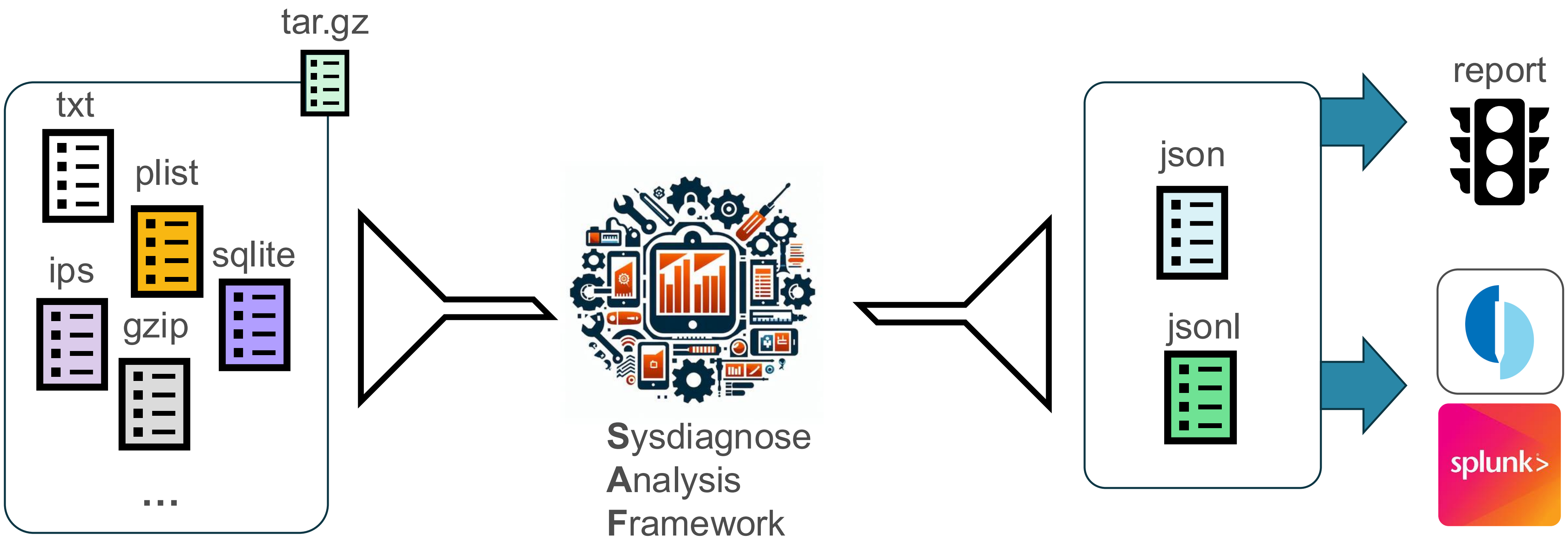
Sysdiagnose structure

- Results of commands
- ./logs : device logs including Power Logs
- ./Preferences: device preferences
- ./summaries: extract from Power Logs
- ./system_logs.logarchive: system logs
- ./WiFi: Network and Bluetooth informations
- many other info :)



```
sysdiagnose_2023.05.23_21-41-36+0200_iPhone-
  ASPSnapshots
  brctl
  crashes_and_spins
  errors
  ioreg
  libtrace
  logs
  Personalization
  Preferences
  RunningBoard
    ._RunningBoard_state.log
    RunningBoard_state.log
  summaries
  system_logs.logarchive
  TimezoneDB
  WiFi
  ._tailspin-info.txt
  apfs_stats.txt
  ckksctl_status.txt
  codecctl.txt
  disks.txt
  error_log.txt
  fileproviderctl.log
  fileproviderctl_check.log
  fileproviderctl_dump.log
  hidutil.plist
  hpmDiagnose.txt
  kbdebug.txt
  launchctl-dumpstate.txt
  launchctl-list-0.txt
  launchctl-print-system.txt
  lsaw.csstoredump
  microstackshots
  mount.txt
  night-shift.log
  oslog_archive_error.log
  otctl_status.txt
  pcsstatus.txt
  ps.txt
  ps_thread.txt
  README.txt
  remotectl_dumpstate.txt
  security-sysdiagnose.txt
  smcDiagnose.txt
  spindump-nosymbols.t
  swcutil_show.txt
  sysdiagnose.log
  tailspin-info.tx
```

Sysdiagnose Analysis Framework (SAF)



Sysdiagnose Analysis Framework (SAF)

- Feel free to
  - **Use** it
  - **Extend** it
  - **Propose** changes
  - …
- FOSS-licenced, under the European Union Public License (EUPL)
  https://github.com/EC-DIGIT-CSIRC/sysdiagnose

The outcome?

- We have a tool to parse sysdiagnose files (kind of)
- Amnesty and Citizen labs confirmed the idea to be relevant
- But…
- We (commission) have **>10k iOS/iPad OS devices** in the MDM (EC owned and BYOD)

Growing up

Our approach – Building blocks (I)

Analysis

Collection

Collection

Generating sysdiagnose

- Requires using RemoteXPC `com.apple.coredevice.feature.capturesysdiagnose` + developer mode (*) + remote debugging tricks (**), pairing certificate and local VPN
- Or requires human intervention. There are 2 methods to start sysdiagnose generation:
  - 2 volume + power buttons
  - AssistiveTouch virtual button

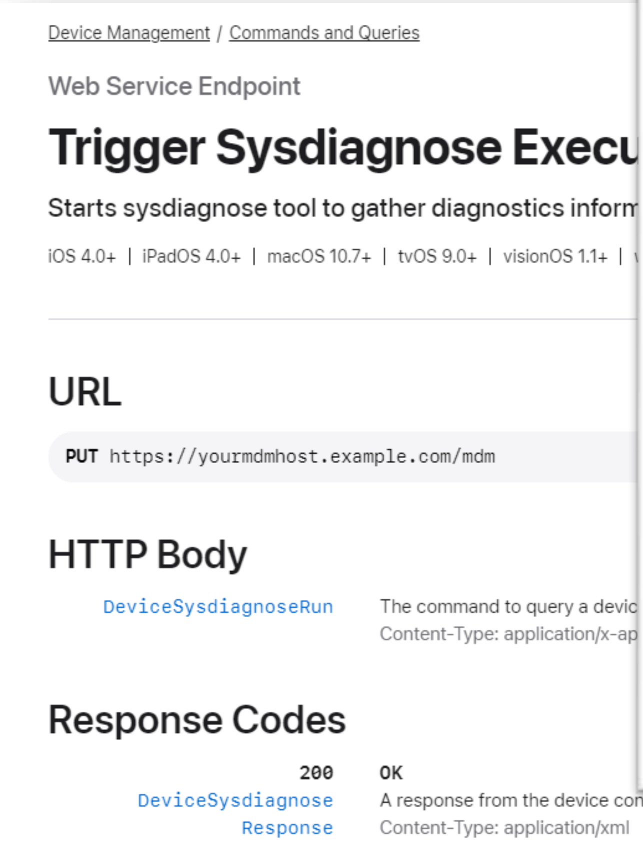
** iOS 17.4 or newer*
*** See:*
https://github.com/khcrysalis/Protokolle
https://github.com/StephenDev0/StikDebug

European Commission

Collection

Apple MDM API calls

- 2 API functions



Device Management / Commands and Queries

Web Service Endpoint

Trigger Sysdiagnose Execu

Starts sysdiagnose tool to gather diagnostics inform

iOS 4.0+ | iPadOS 4.0+ | macOS 10.7+ | tvOS 9.0+ | visionOS 1.1+ |

URL

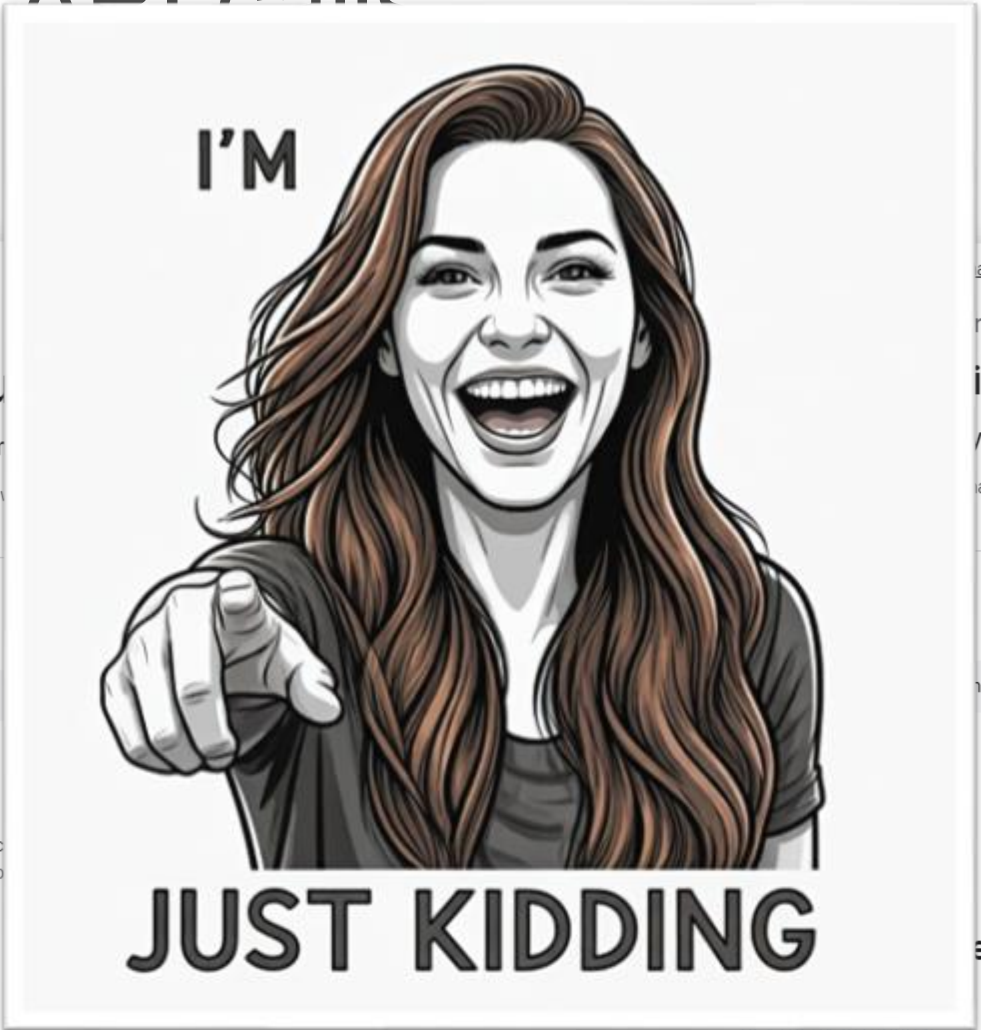
```
PUT https://yourmdmhost.example.com/mdm
```

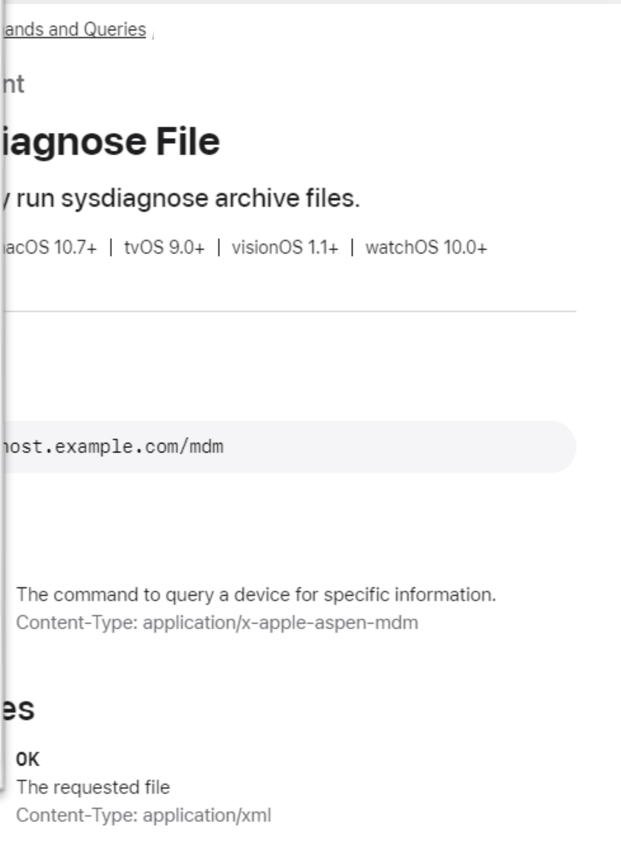
HTTP Body

DeviceSysdiagnoseRun	The command to query a devic Content-Type: application/x-ap

Response Codes

200 DeviceSysdiagnose Response	OK A response from the device confirming sysdiagnose execution is running in the background. Content-Type: application/xml





ands and Queries

nt

iagnose File

run sysdiagnose archive files.

acOS 10.7+ | tvOS 9.0+ | visionOS 1.1+ | watchOS 10.0+

```
ost.example.com/mdm
```

The command to query a device for specific information.
Content-Type: application/x-apple-aspen-mdm

es

Response	OK The requested file Content-Type: application/xml

Collection

Collecting sysdiagnose

- Requires developer mode (*), remote debugging tricks (**), pairing certificate and local VPN
- Or requires human intervention.

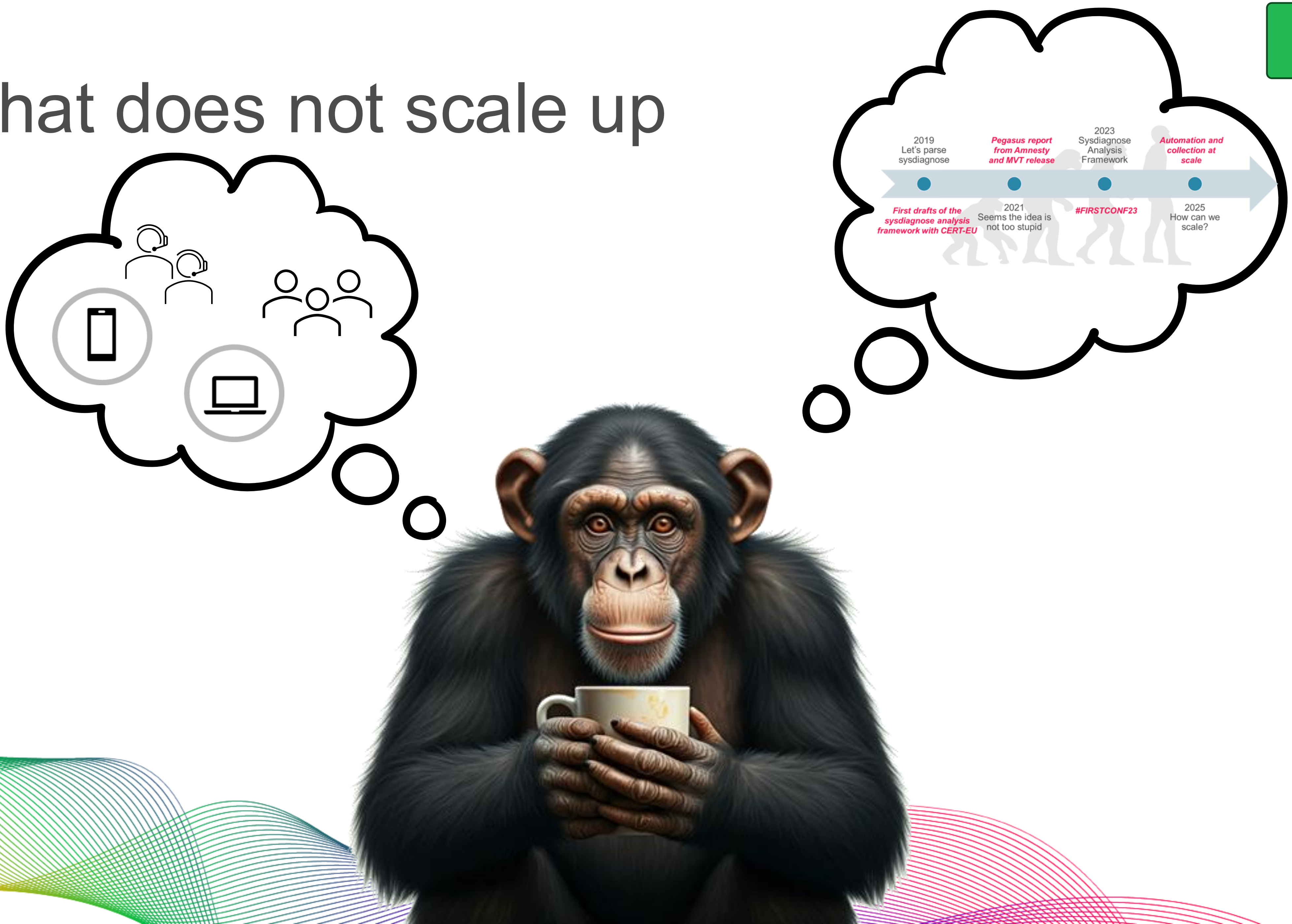
From the device directly

Using a computer

* *iOS 17.4 or newer*
** *See:*
https://github.com/khcrysalis/Protokolle
https://github.com/StephenDev0/StikDebug

That does not scale up

Collection



2019
Let's parse sysdiagnose

First drafts of the sysdiagnose analysis framework with CERT-EU

Pegasus report from Amnesty and MVT release

2021
Seems the idea is not too stupid

2023
Sysdiagnose Analysis Framework

#FIRSTCONF23

Automation and collection at scale

2025
How can we scale?

European Commission

Analysis

Collection

Our approach – EU Phone Check

- ~~Share using Shortcut~~
- iOS companion app

MQA Librarian

DWP EC Store

- Proximity support (kiosk)
- DWP application (self-service)

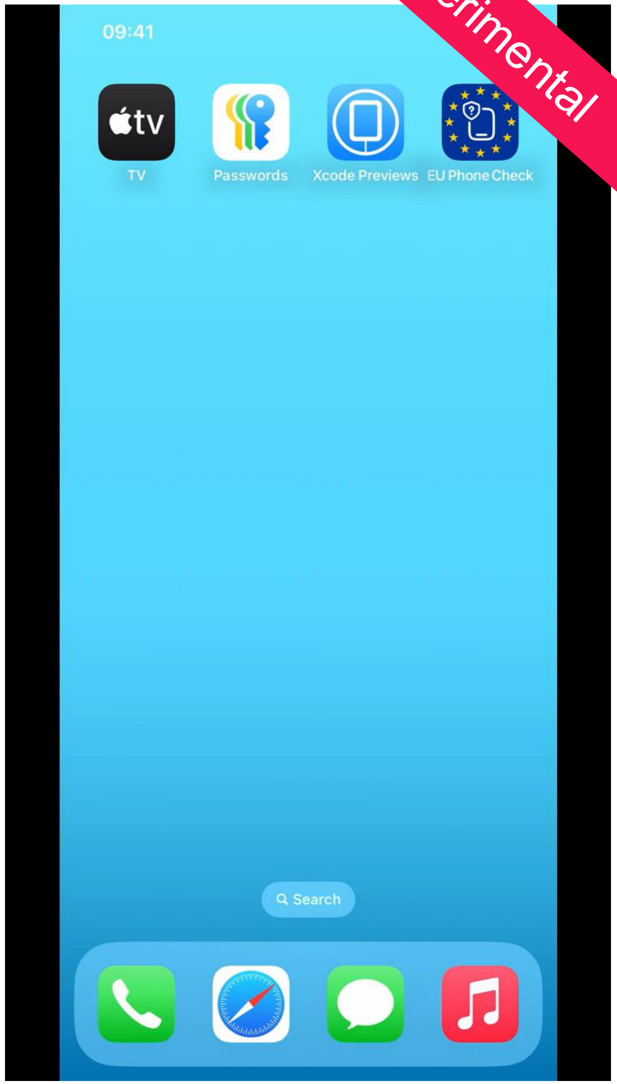
- Fallback to traditional methods
- Keep an eye on commercial products and Apple proving API function

iOS companion app

Collection

experimental

- iOS App, pushed automatically by MDM
- User Instructions
  - Generating sysdiagnose
  - Sharing sysdiagnose through App
- Monitors for sysdiagnose file creation & completion
- Uploads to server
- Lists reports



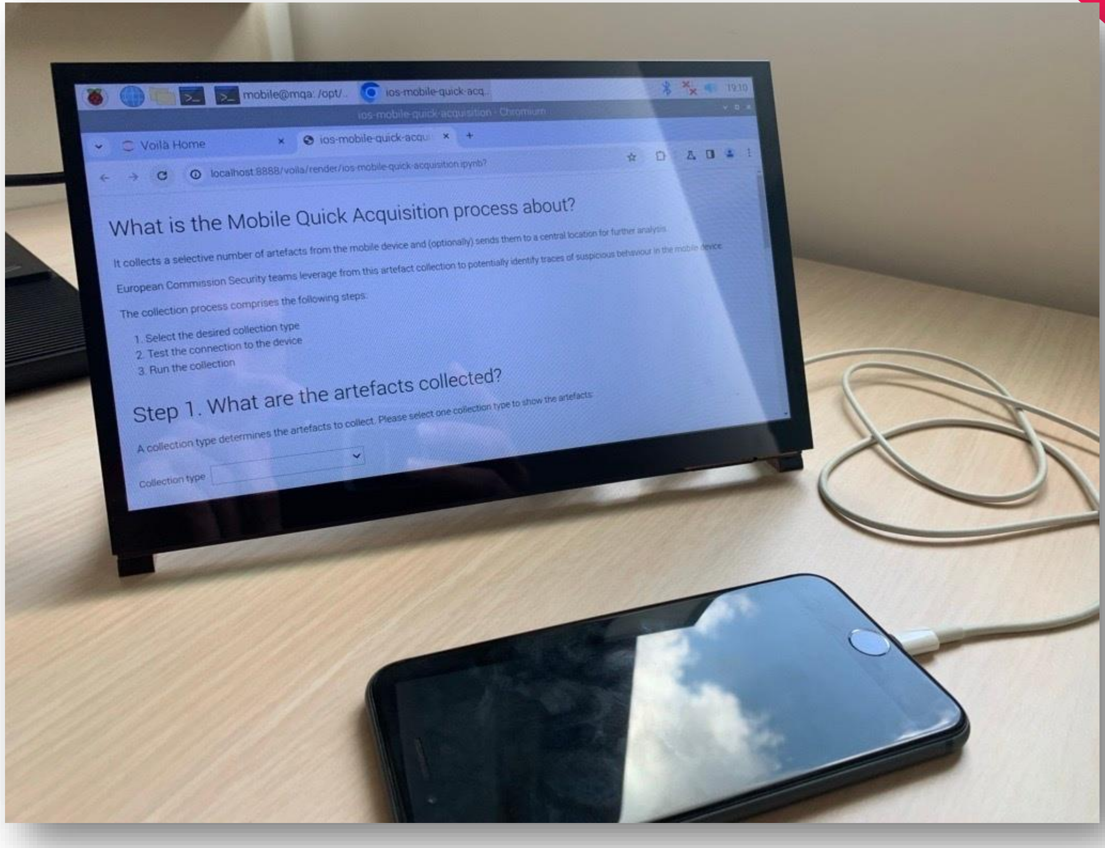
European Commission

Collection

experimental

Proximity team (Kiosk)

- IT Proximity team support
- Raspberry Pi & touchscreen
- Mobile Quick Acquisition library on a Custom UI with:
  - Instructions
  - Pre-defined acquisition profiles
  - Monitors for sysdiagnose archive creation
- Uploads data to EU-Send


Voilà Home
ios-mobile-quick-acqu
localhost:8888/voila/render/ios-mobile-quick-acquisition.ipynb?

What is the Mobile Quick Acquisition process about?

It collects a selective number of artefacts from the mobile device and (optionally) sends them to a central location for further analysis.

European Commission Security teams leverage from this artefact collection to potentially identify traces of suspicious behaviour in the mobile device

The collection process comprises the following steps:

1. Select the desired collection type
2. Test the connection to the device
3. Run the collection

Step 1. What are the artefacts collected?

A collection type determines the artefacts to collect. Please select one collection type to show the artefacts:

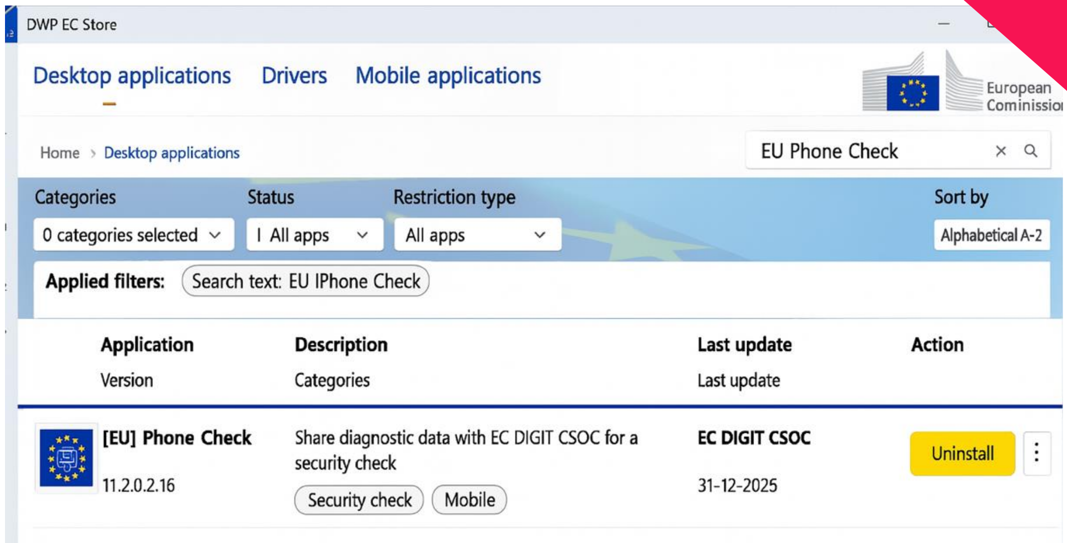
Collection type

Collection

experimental

DWP application (self-service)

- Computer app, installed via DWP EC Store
- User Instructions
  - Generating sysdiagnose
  - Trusting computer
- User plugs phone on DWP computer
- App auto-detects sysdiagnose archive creation, extracts it from phone and uploads it to EU-Send



DWP EC Store

Home › Desktop applications

EU Phone Check

Categories: 0 categories selected

Status: All apps

Restriction type: All apps

Sort by: Alphabetical A-Z

Applied filters: Search text: EU IPhone Check

Application Version	Description Categories	Last update Last update	Action
[EU] Phone Check 11.2.0.2.16	Share diagnostic data with EC DIGIT CSOC for a security check Security check Mobile	EC DIGIT CSOC 31-12-2025	Uninstall

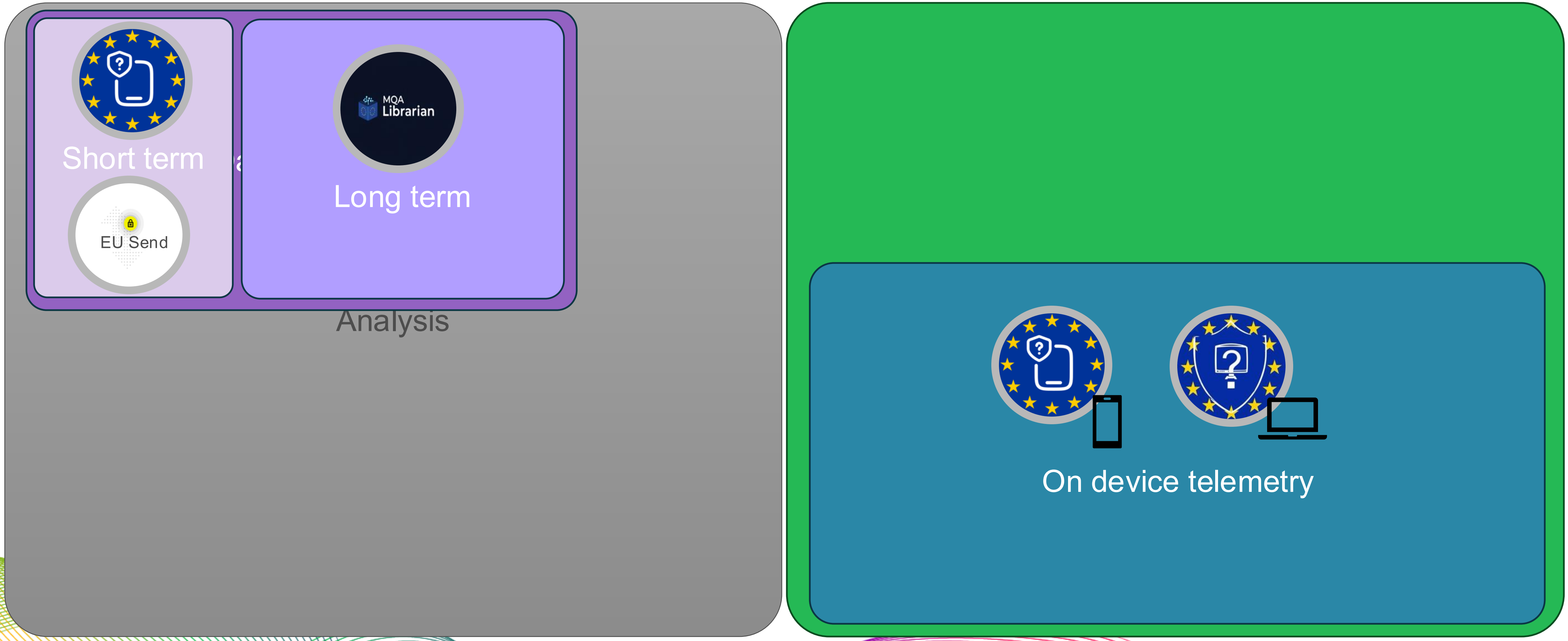
Collection

Other

- Eager to see more Off The Shelf apps
- Eager to have Apple to add MDM API commands to allow to generate + collect forensic artefacts remotely
- … ?

European Commission

Our approach – Building blocks (II)



Short term

Long term

Analysis

On device telemetry

Time for Data analytics

- You have data (collection)
- You can convert the data (SAF)
- Now do something with it !

Data analytics

- SAF: analyser
- Splunk
- Timesketch
- Grep, jq, yara …

splunk>

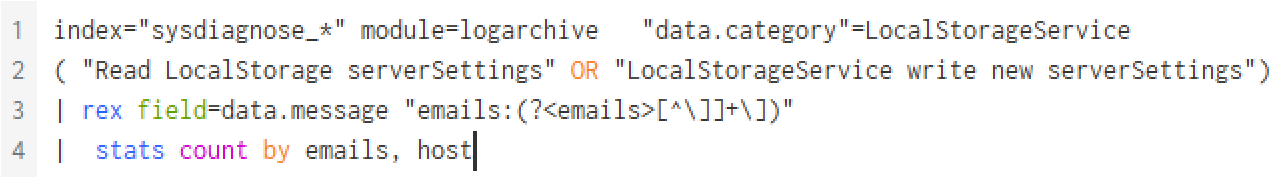
timesketch

Digital Forensics Timeline Analysis

Analysis

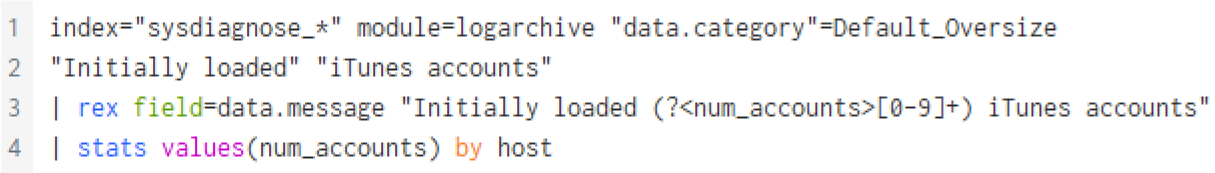
Examples

- Accounts linked to phone



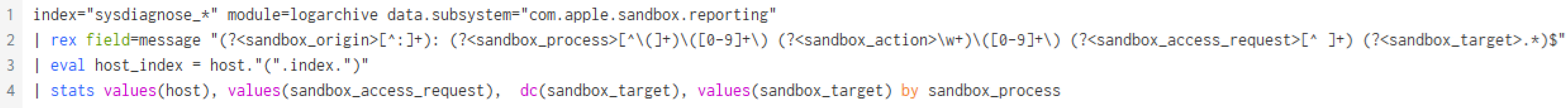
```
index="sysdiagnose_*" module=logarchive   "data.category"=LocalStorageService
( "Read LocalStorage serverSettings" OR "LocalStorageService write new serverSettings")
| rex field=data.message "emails:(?<emails>[^\]]+\])"
|  stats count by emails, host
```

- iTunes accounts (+ evolution)



```
index="sysdiagnose_*" module=logarchive "data.category"=Default_Oversize
"Initially loaded" "iTunes accounts"
| rex field=data.message "Initially loaded (?<num_accounts>[0-9]+) iTunes accounts"
| stats values(num_accounts) by host
```

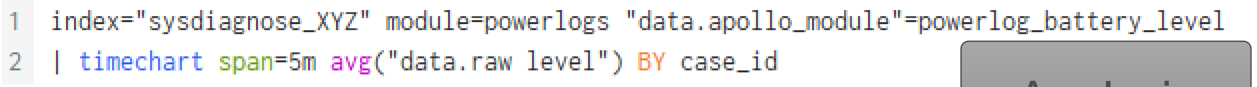
- Sandbox violations



```
index="sysdiagnose_*" module=logarchive data.subsystem="com.apple.sandbox.reporting"
| rex field=message "(?<sandbox_origin>[^:]+): (?<sandbox_process>[^\(]+)\([0-9]+\) (?<sandbox_action>\w+)\([0-9]+\) (?<sandbox_access_request>[^ ]+) (?<sandbox_target>.*)$"
| eval host_index = host."(".index.")"
| stats values(host), values(sandbox_access_request),  dc(sandbox_target), values(sandbox_target) by sandbox_process
```

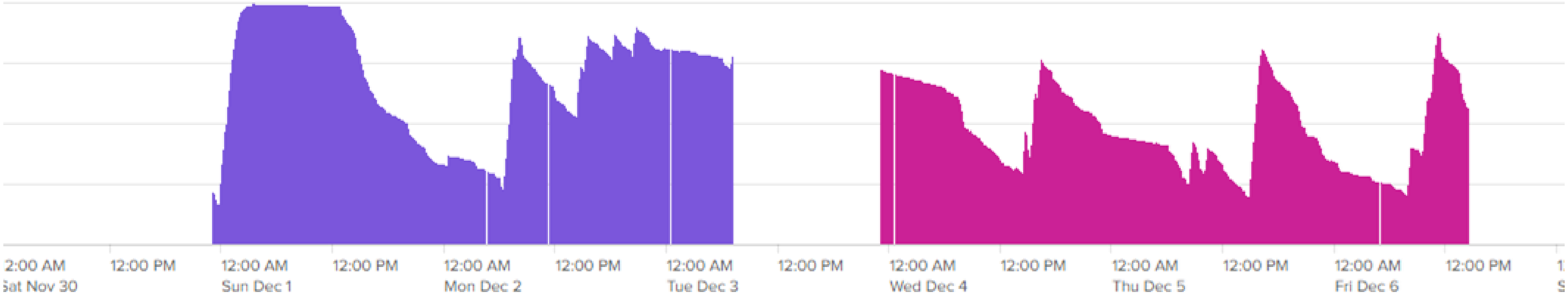
European Commission

- Battery consumption
  (2 snapshots of same device)

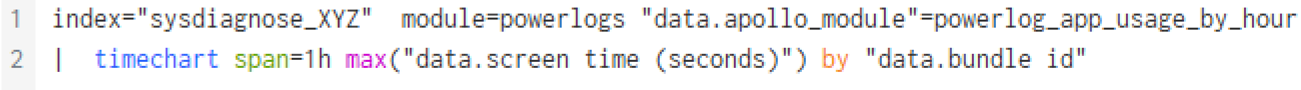


```
index="sysdiagnose_XYZ" module=powerlogs "data.apollo_module"=powerlog_battery_level
| timechart span=5m avg("data.raw level") BY case_id
```

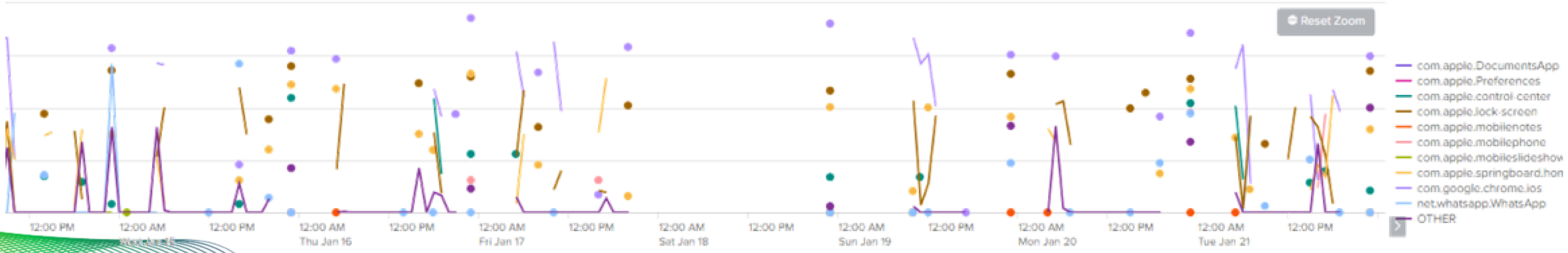
Analysis



- App usage



```
index="sysdiagnose_XYZ"  module=powerlogs "data.apollo_module"=powerlog_app_usage_by_hour
|  timechart span=1h max("data.screen time (seconds)") by "data.bundle id"
```



Examples

- Treasures in unifiedlogs / logarchive (containing a 2-3 day timeframe)

Activity	1 482 769
Log	11 065 315
Loss	792
Signpost	203 478
Simpledump	28 414
Statedump	20 222

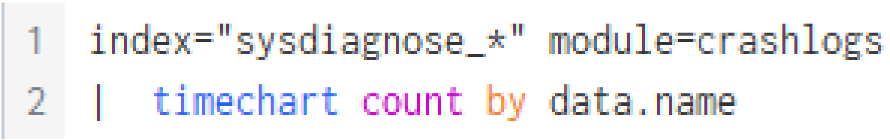
Debug	29 070
Default	9 973 320
Error	281 182
Fault	149 436
Info	632 307

https://www.ios-unifiedlogs.com/post/ios-unified-logs-parsing-all-my-sql-queries

Analysis

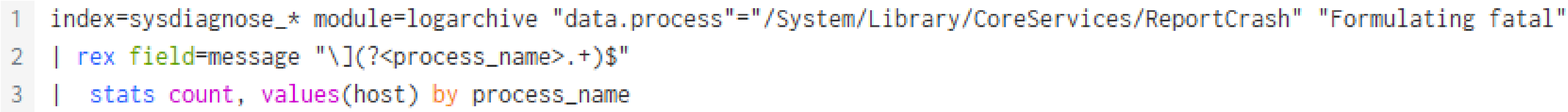
Example: Crashlogs

- Crashlogs (long history, easily tampered)



```
index="sysdiagnose_*" module=crashlogs
|  timechart count by data.name
```

- Logarchive (short history, more difficult to tamper)

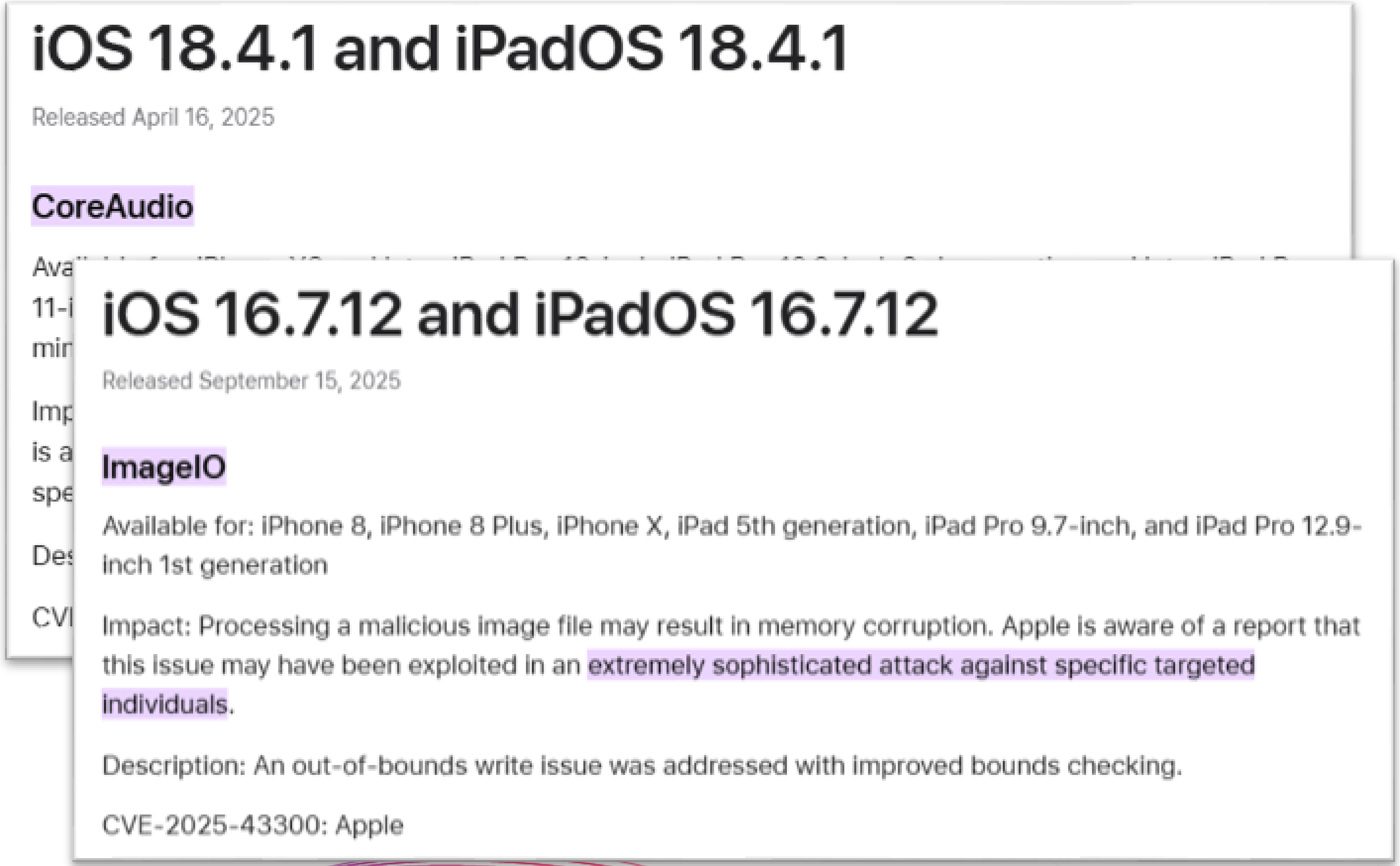


```
index=sysdiagnose_* module=logarchive "data.process"="/System/Library/CoreServices/ReportCrash" "Formulating fatal"
| rex field=message "\](?<process_name>.+)$"
|  stats count, values(host) by process_name
```

Analysis

Example: Crashlogs

- Apple Security updates mention components:
  - Accessibility
  - CoreAudio
  - ImageIO
  - Messages
  - RPAC
  - WebKit
  - …



iOS 18.4.1 and iPadOS 18.4.1

Released April 16, 2025

CoreAudio

Ava
11-i
mir

Imp
is a
spe

Des

CVI

iOS 16.7.12 and iPadOS 16.7.12

Released September 15, 2025

ImageIO

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

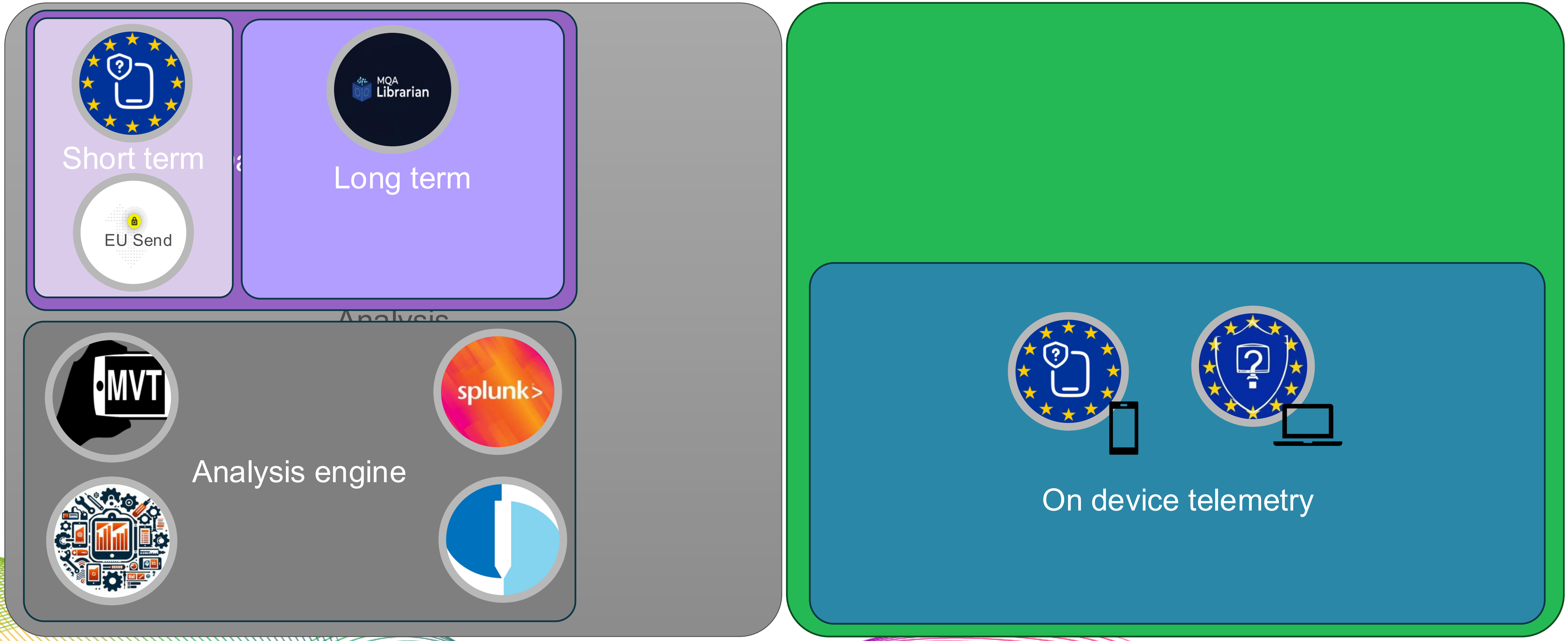
Impact: Processing a malicious image file may result in memory corruption. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals.

Description: An out-of-bounds write issue was addressed with improved bounds checking.

CVE-2025-43300: Apple

Today

Our approach – Building blocks (III)



Short term

EU Send

Long term

Analysis

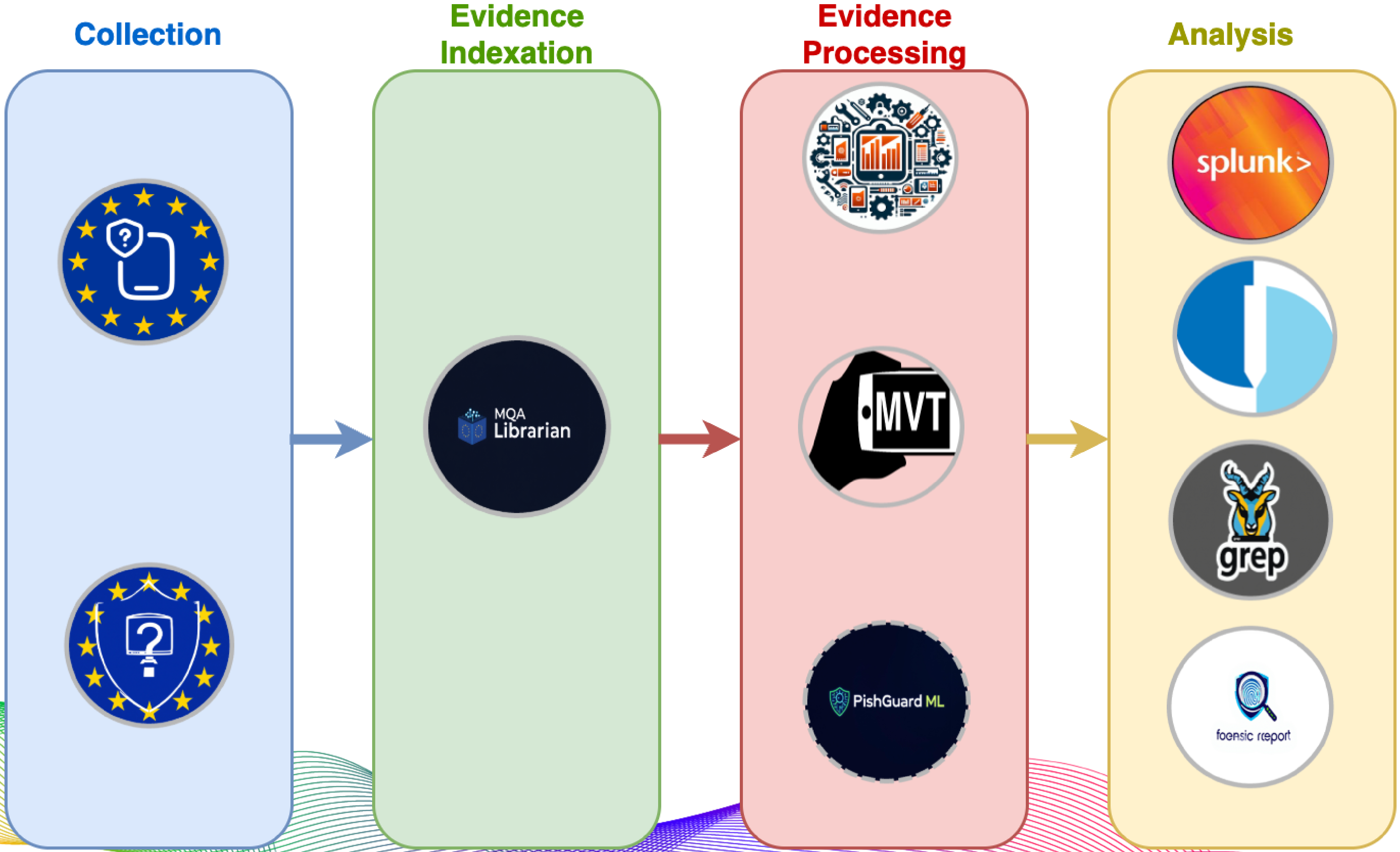
Analysis engine

On device telemetry

Overview of the architecture

Analysis

Collection



Collection

Evidence Indexation

Evidence Processing

Analysis

We didn’t stop there

- The Commission has kicked off a **Mobile Device Security (MDS) Programme**, led by DG DIGIT that involves several DGs, aiming to develop:
  - **A risk-based mobile security policy**, foreseeing security by design and by default across the lifecycle of mobile device applications.
  - **Capabilities in cybersecurity operations for mobile devices**, namely in the areas of threat hunting, threat intelligence, malware analysis, forensics, cybersecurity monitoring, vulnerability management and cybersecurity incident response.
  - **Collaboration** within and outside of the Commission.

Future

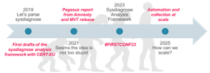
Future

Analysis Collection

Confirm the effectiveness of the approach

Release in Open Source as many pieces as possible

open source


2019
Let's parse sysdiagnose
First drafts of the sysdiagnose analysis framework with CERT-EU
Pegasus report from Amnesty and MVT release
2021
Seems the idea is not too stupid
2023
Sysdiagnose Analysis Framework
#FIRSTCONF23
Automation and collection at scale
2025
How can we scale?

Do this AT SCALE

Extend the secure digital workplace to mobile devices. Detect attacks and compromises targeting the mobile devices. Respond to incidents related to mobile devices

What do we still miss?

- Clearer timestamp from Apple Threat Notifcation straight in the notification
- Trusted group sharing IOC, detection techniques…
  - Other organisation working on similar tools – **we are stronger together**
- [DREAM] official support from Apple & Google and how to check integrity of mobile devices

In the plans

- Continue to support the sysdiagnose analysis framework (SAF) with
  - New artifacts (crash logs, unified logs…)
  - New iOS / iPad OS versions
- Release more in open-source
  - Splunk Technical Addon for SAF
  - iOS Companion App
- Workshop at hack.lu

Thank you

Source code:

- **Sysdiagnose Analysis Framework (SAF): https://github.com/EC-DIGIT-CSIRC/sysdiagnose**
- **Splunk Technical Add-On: https://github.com/EC-DIGIT-CSIRC/ec_digit_saf_ta**

Christophe Vandeplas
@cvandeplas

christophe.vandeplas@ext.ec.europa.eu

David Durvaux
@ddurvaux

david.durvaux@ec.europa.eu

Darío Borreguero Rincón
@darizotas

dario.borreguero-rincon@ec.europa.eu