

EC's journey

on building a digital forensic capacity for Apple mobile devices

BE-CYBER 2025

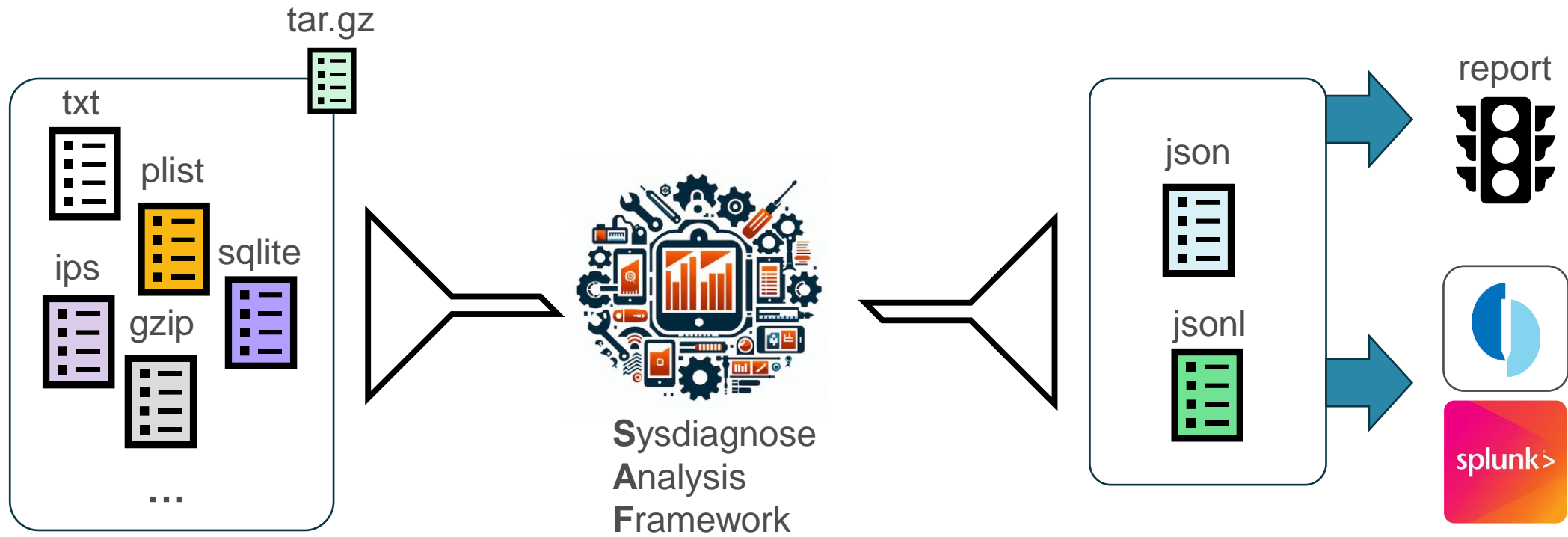
The genesis

Let's do something
but we don't know what...

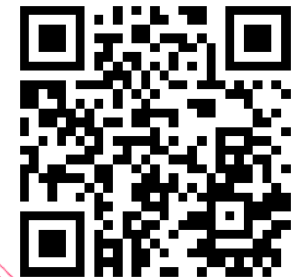
To find something
But we don't know what...



Sysdiagnose Analysis Framework (SAF)



<https://github.com/EC-DIGIT-CSIRC/sysdiagnose>



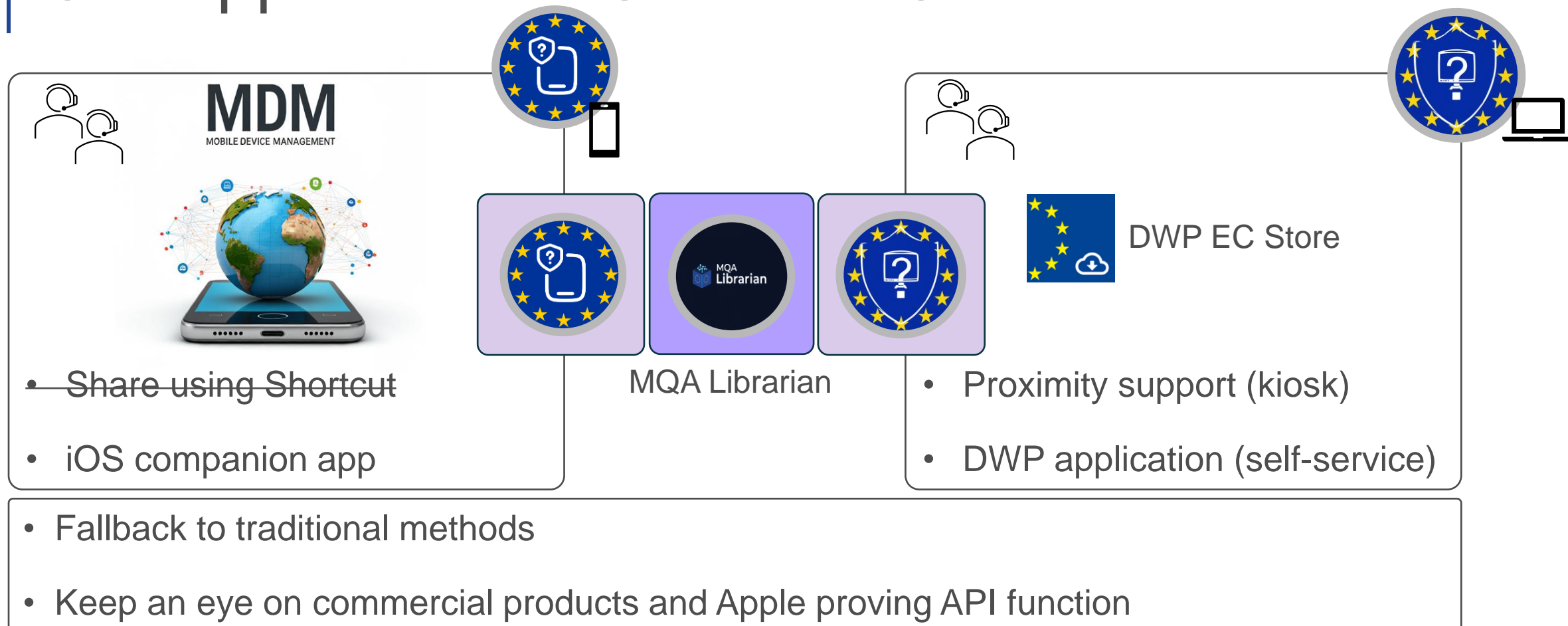
Growing up

We can do 1 device but...

We have >10k devices ☹️



Our approach – EU Phone Check



Overview of the architecture

Analysis

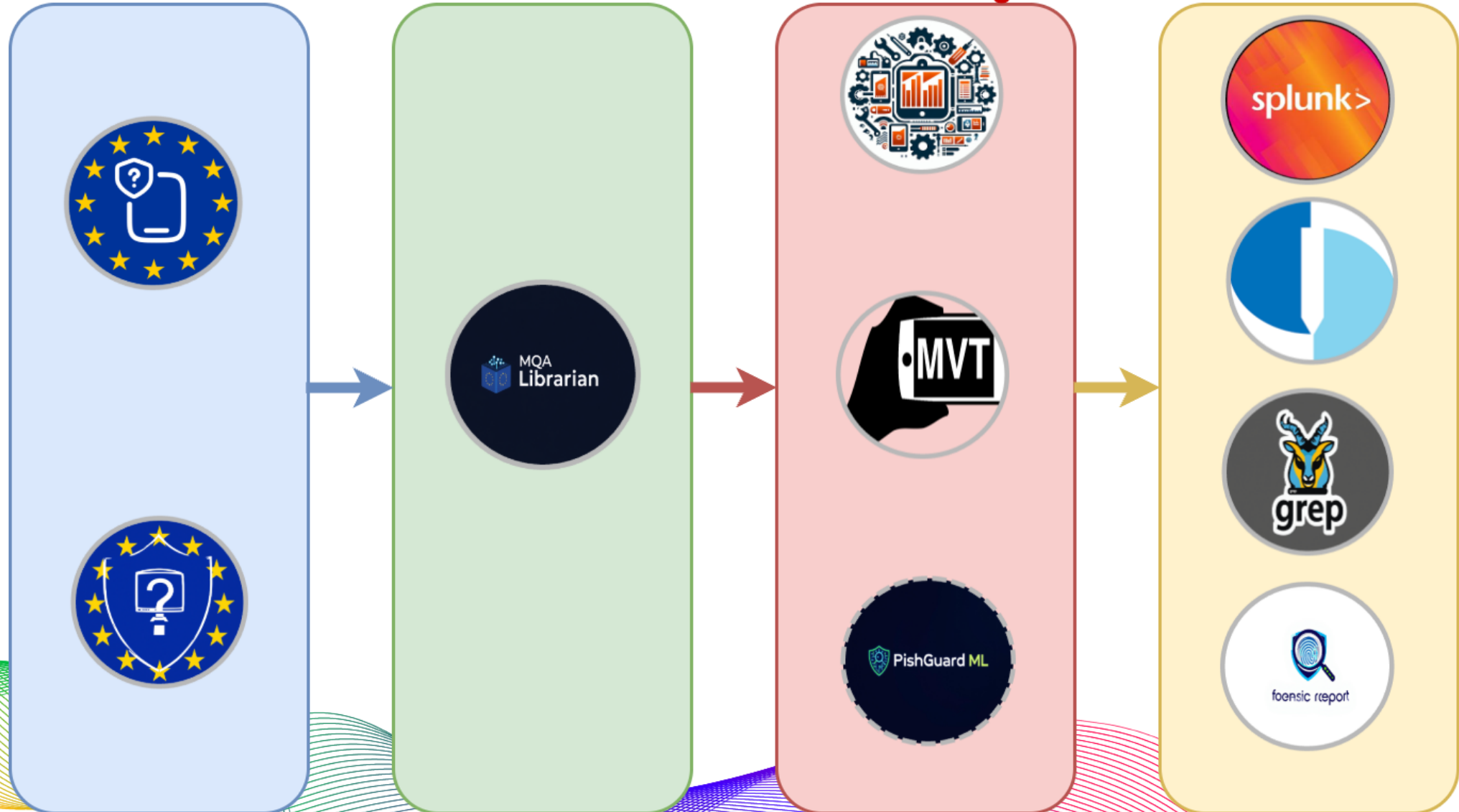
Collection

Collection

Evidence
Indexation

Evidence
Processing

Analysis



Today



Future



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

iOS companion app



- 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

