FIGHTING CRIME AND TERRORISM

PITCH SESSION

Organisation Presentation

http://nicc.fgov.be/ (NL)
http://incc.fgov.be/ (FR)

- **Location:** *Belgium, Brussels*
- *National forensic institute: main tasks:*
  - Criminal case work: evidence analysis and expert reports
  - R&D to support local and federal LEAs and magistrates
  - Training and education, international collaboration (e.g. via ENFSI)
  - National criminalistics data bases
- **Experience:**
  - ISEC/ENFSI MP: http://s-five.eu/ : forensic image/video enhancement
  - H2020-2016-FCT: http://asgard-project.eu/ : digital forensics
  - ISFP-2016-AG-IBA-ENFSI : ValiD/STEFA: digital forensics tool validation
  - Submitted proposals: 1x SU-FCT02: "SFERA", 1x SU-FCT03: "CRISTE"
- **Contact***:*
  - *Dr. ir. Patrick De Smet: patrick.desmet@just.fgov.be*
  - *Researcher/Forensic Expert; tel.: +32 2 240 05 00 (NICC central)*

Targeted Topic

SU-FCT03-2019	Information and data stream management to fight against (cyber)crime and terrorism

Operational Needs

Our 3 major needs

What?

1. *"Correct and complete" processing of huge amounts of data,*
2. *Optimized big data analysis workflows with continuously updated results,*
3. *(Beyond) state-of-the-art user-friendly tools for real-life decryption and password cracking.*

Why?

1. *Today large amounts of raw ("problematic") data remain not properly processed, or result in error propagation*
2. *Preventing imminent attacks and pre-meditated crimes in general*
3. *E.g. case work related to non-cooperative or deceased suspects or victims*

Project Idea

Big & Better Data Forensics ("BB-D-4N6"):

- ***Error robust** tools and big data platform*
- ***Forensic tool validation and QA performance analysis***
  (extending (far) beyond traditional software testing)
- *Use-case **optimized workflows:** highly scalable, parallelized, pipelined methods, tools and platform;*
- *On-the-fly **inter-tool collaboration***
  *and **"ASAP" user-interaction***
- *State-of-the-art **AI/Machine Learning methods***
  (including robustness and forensic QA analysis)

Contribution

What NICC can provide:

- *Skills and experience in software based digital forensics for:*
  - File (system) (meta-)data recovery and robustness testing
  - State-of-the-art methods for data recovery and repair
  - Tool testing and validation in digital forensics

- *Example tools:*
  - JPGcarve: carving and reassembly of fragmented JPEG pictures
    https://ieeexplore.ieee.org/document/7230269/
  - PNGcarve: carving and reassembly of fragmented PNG images
    (under further dev. within ASGARD project)
  - MFTcarve: reconstructing corrupted MicroSoft NTFS file system meta-data
  - Tool for visualization and (reporting on) examination of device data dumps
  - Early prototype tools for recovery/repair of incomplete data (headerless JPG & PNG, headerless/damaged GIF, headerless/damaged/incomplete H.265 video)