EUROPEAN DEFENCE AGENCY

Fact sheet

www.eda.europa.eu

Deployable Cyber Evidence Collection and Evaluation Capability (DCEC2)

© Leonardo

Digital Forensics is a technology area that is well-established in a civilian context. Such technologies enable cybersecurity analysts to collect information and conduct investigations in response to cyber-attacks.

Given its increasing importance and the general need for improving the resilience of military communication and information systems, deployable digital forensics for military operations has been identified as a key capability to be developed for EU-led crisis management within the EU Common Security and Defence Policy (CSDP).

Cyber forensics is defined as the process of extracting information and data from computers to serve as digital evidence to prove and legally prosecute cybercrime. Yet, on the military side, probably one of the tactical advantages that cyber forensics can provide is to help understanding adversaries' decision-making process, and to reduce the time required for incident response. For the military context, cyber forensic exploitation teams must be enabled to work remotely or to deploy with forensic exploitation laboratories. Their functional operation must be scalable, modular, and agile to support a commander's needs, and must be configured in line with the operational infrastructure.

Objectives

The main objective is to deliver a deployable forensics technology demonstrator for military operations. An analysis of the state-of-the-art of digital forensics science, technology and practice will be performed, looking for a functional relevance to the defence sector. Also, an identification of technology trends and solutions in a roadmap, including anti-forensics measures and examination of future technologies will be carried out. The chief benefit will be to identify research activities for short, medium and long-term planning.

Finally, an architecture compliant with the NATO Architecture Framework will be developed for a deployable digital forensics capability able to be used in CSDP operations and missions.

Benefits

In order to make the 2017 CARD trial run a success, EDA developed a methodology presented to Member States' Capability Directors in September 2017, based on the following elements and procedural steps:

- **Usability**
  - Accelerate information seizing. Enabling fast, initial screening of investigative targets in order to estimate their evidentiary value
  - Ease of operation. Minimize operators required skills to pursue at least evidence collection and fast analysis

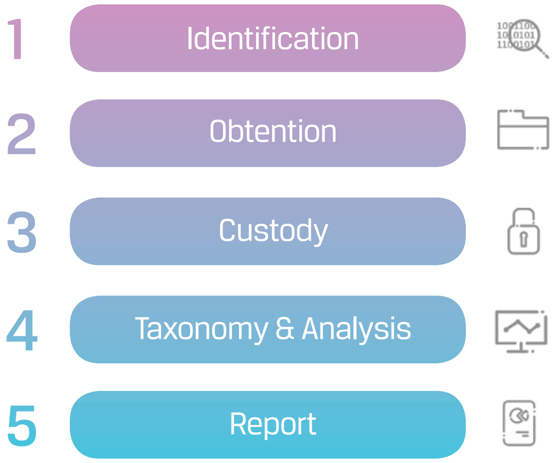
- **Building a Secure Communication Channel to SOC/NOC infrastructures** where deep analysis can be performed and transmitted information serves as a Cyber Intelligence Enabler to feed Cyber Military Strategy

- **Energy consumption, low weight and dimensions of DCEC2**: A self-sufficient energy forensics device

- **Modular deployable forensics capability** with a modular architecture ready to augment its functionality on-demand.

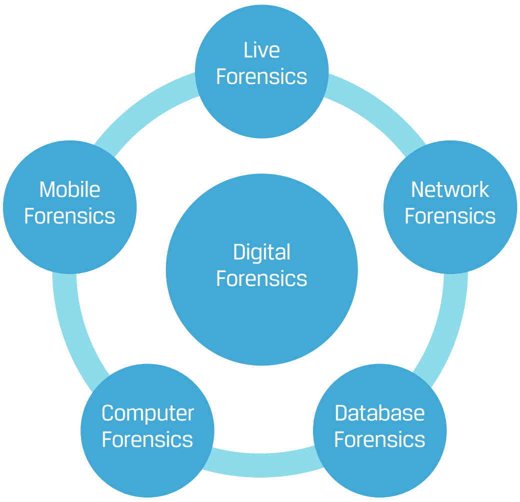
Digital Forensics Investigation Process

- Computer, Mobile, Database, Network and Live forensics functionalities
- Facilitating phases 1 to 3 of digital forensics investigation by providing automation
- Optionally leaving phases 4 and 5 to an on-premises (reach-back) phase, supported by experts
- Easing fast searching for sensitive information (triage)
- Providing hands-on training to operators on Foresee, Engage Empower, Protect (FEEP) Cyber Range.



Addressing Main Digital Forensics Areas

- **Computer Forensics** is the practice of collecting, analysing and reporting on digital data in a way that is legally admissible
- **Live Forensics** considers the value of the data that may be lost by powering down a system and collecting it while the system is still running
- **Database Forensics** relates to forensic study of databases and their related metadata
- **Network Forensics** is the capture, recording, and analysis of network events at specific point(s) in the network in order to discover the source of security attacks or other problem incidents
- **Mobile Forensics** relates to the recovery of digital evidence or data from a mobile device under forensically sound conditions.



Last update: 20 February 2018