European Security and Defence College
Doc: ESDC/2024/65
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2025**	Activity number **279**	**Digital Forensics Investigator**	ECTS **1**

Target audience	Aim
The participants should be mid-ranking to senior military or civilian officials dealing with cyber incident response, security operations centre and cybersecurity professionals from EU Institutions, Bodies and Agencies as well as EU Member States and the Western Balkans.	The aim of the course is to prepare the participants to analyse, evaluate and collect artefacts of cybersecurity incidents and to identify the root causes of cyber incidents and malicious actors. Furthermore, this course will allow the mid-ranking to senior officials to exchange their views and share best practices on security operation centres (SOCs) and computer security incident response teams (CSIRTs) topics by improving their knowledge, skills and competencies. By the end of this course, the participants will learn how to acquire and use specific tactics, techniques, procedures and tools and will develop skills to deal with large-scale cyber-attacks in a windows network/domain.
Open to: • EU Member States / EU Institutions Bodies and Agencies • Candidate Countries	

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber and the EU's Policy on Cyber Defence	• *Specialised cyber course, at tactical, operational, and strategic level.* • *Linked with the strategic objectives of Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning Outcomes

Knowledge	LO1- Describe digital forensics recommendations and best practices LO2- Describe digital forensics standards, methodologies and frameworks LO3- Describe digital forensics analysis procedures LO4- Select malware analysis tools LO5- Discuss Cybersecurity related laws, regulations and legislations

Skills	L06- Collect digital artefacts LO7- Use malware analysis tools LO8- Identify, analyse and correlate cybersecurity events LO9- Develop and communicate, detailed and reasoned investigation reports
Responsibility and Autonomy	LO9- Apply digital forensics investigation policy, plans and procedures LO10- Identify, recover, extract, document and analyse digital evidence LO11- Preserve and protect digital evidence and make it available to authorised stakeholders LO12- Inspect environments for evidence of unauthorised and unlawful actions LO13- Systematically and deterministic document, report and present digital forensic analysis findings and results LO14- Select and customise forensics testing, analysing and reporting techniques

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model: it makes use of *level 1 evaluation* (*based on participants' satisfaction with the course*) and *level 3 evaluation* (*assessment of participants' long-term change in behaviour after the end of the course*). *Evaluation feed-back* is given in the level 1 evaluation on the residential modules.

In order to complete the course, the participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential modules, including their syndicate sessions and practical activities as well as on their completion of the eLearning phases: course participants must finalise the autonomous knowledge units (AKUs) and pass the tests (*mandatory*), scoring at least 80% in the incorporated out-test/quiz. **However, no formal verification of the learning outcomes is foreseen; proposed ECTS is based on participants' workload only**.

The Executive Academic Board takes these factors into account when considering the award of *Certificates* to participants. Module leaders provide an evaluation report for each residential module. The Course Director is responsible for overall coordination, with the support of the ESDC Secretariat, and drafts the *final evaluation report, which* is presented to the Executive Academic Board.

Course structure

The residential module is held over 5 days.

Main Topic	**Suggested Working Hours (required for individual learning)**	**Suggested Contents**
1. Introduction to digital forensics analysis	4(2)	• Identify, collect, examine, and analyse digital data while preserving the integrity of the information and maintaining a strict chain of custody for the data
3. Collecting artefacts	15(6)	• File system forensics • Registry forensics • Memory forensics • Email forensics • Browser forensics • USB forensics
4. Analysing the artefacts	15(6)	• Evidence examination • Procedures to retrieve, copy and store evidences
5. Hunting the threat	15(4)	• Malware analysis tools • Threat alerts and Triage • Types of malware analysis • Stages of malware analysis
6. Presenting the artefacts	2	• Document, report and present digital forensic analysis findings and results

TOTAL	51 (18)	

Material

Required:
AKU 104: Module 3 – Experience a security incident
AKU 104: Module 8 – Review Organisational Controls
AKU 104: Module 9 – Review Technical Controls

Recommended:

- *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union (**NIS 2**)*
- *EU Policy on Cyber Defence, JOIN(22) 49 final, 10.11.2022*
- *The EU's Cybersecurity Strategy for the Digital Decade (December 2020)*
- *The EU Cybersecurity Act (June 2019)*
- *The EU Cyber Diplomacy Toolbox (June 2017)*
- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*
- *Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)*

Methodology

The course is based on the following methodology: Presentations, Panels talks, Q&A and/or workshops

Additional information

Pre-course questionnaire on learning expectations and possible briefing topic from the specific area of expertise may be used.

All course participants have to prepare for the residential module by going through the relevant eLearning preparatory phase, which is mandatory. The materials proposed for supplemental (eLearning) study will reflect current developments in the field of cyber security/cyber defence in general and EU policies in particular.

The Chatham House Rule is applied during all residential phase of the course: "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".