Certificate of Advanced Studies

Digital Forensics & Cyber Investigation Specialist II

The digital transformation of society is affecting crime, criminals and criminal investigation. The Digital Forensics & Cyber Investigation (DFCI) continuing education program at BFH was created to address new education demand for skilled digital forensic and cyber investigators.

The CAS DFCI Specialist II is the final specialization needed to complete the Master of Advanced Studies (MAS) and provides you with advanced knowledge and skills in specialized domains. The topics are covered include E-Discovery, Mobile Device Forensics, Fintech Forensics, Forensic Intelligence/OSINT, and Hardware/IoT Forensics.

This final CAS contains five modules. Students must choose a minimum of four modules to complete the MAS degree. Students may also attend all five modules at no additional cost.

Berner
Fachhochschule

Inhaltsverzeichnis

23.08.2023

1 Environment

The digital transformation of society is affecting crime, criminals and criminal investigation. New cyber criminal methods using advanced technical tools and exploitation are an opportunity for criminals and a challenge for investigators. Technically complex illegal activities are being sold as services to less skilled criminals, increasing the challenge of fighting cybercrime. On the other hand, criminals face challenges trying to hide and avoid attribution. The large amount of digital traces stored across multiple locations creates an opportunity for criminal investigators.

Crime scenes are also changing. With the growth of cybercrime, crime scenes are becoming virtual, global, and multi-jurisdictional. Investigating a trans-national cyber crime scene requires investigative tools to remotely gather information, and also collaboration between entities in both the public and private sectors.

Modern physical crime scenes have a comprehensive set of digital evidence sources. In addition to PCs and notebooks, digital evidence traces can be found in mobiles, IoT devices, automobiles, smart control systems, data stored with cloud providers, and distributed on servers across the Internet. With the increase in digital and online payment systems, financial transactions are also becoming an important digital evidence source, especially in financially motivated crimes like fraud

2 Target audience

The DFCI program is designed for two groups of professionals:

- Experienced forensic investigators who want to increase their technical skills in digital forensics and cyber investigations

- Experienced engineers and technicians who want to transition into the field of digital forensics and cyber investigations.

3 Career opportunities

The DFCI program will prepare students for career opportunities in a variety of organizations:

- Law enforcement - Federal agencies, KAPOs
- Military and government - CERTs, cyber-troops
- Finance industry - fraud/cybercrime investigation teams
- Insurance industry - cyber insurance claims investigation
- Large enterprises - security and incident response teams
- Consultancy and audit - e-Discovery, accounting, "Big Four"
- IT security service providers and product vendors
- Private boutique digital forensic and investigation firms

4 Education goals

This continuing education program has practical learning objectives. Students completing the CASSpecialist II will understand concepts and have skills in specialist areas including E-Discovery, forensic analysis of Mobile Devices, clouds/VMs, hardware and IoT forensics, financial technology and crypto currency investigations, and leveraging open source Intelligence for investigations.

5 Admission Requirements

Admission into the DFCI Master of Advanced Studies (MAS) or Certificate of Advanced Studies (CAS) requires one of the following:

- a university degree or equivalent professional education degree in computer science, computer engineering, or related field

- professional experience in digital forensics or IT investigation, and a related industry certification.

If applicant qualifications are unclear or inconclusive, further information (for example, a CV) or an interview may be requested.

6 Language, location, and contact

Modules are conducted in one-week fulltime periods and taught in English. Some modules may have pre-reading recommendations. Module assignments and exams are completed by the end of the week.

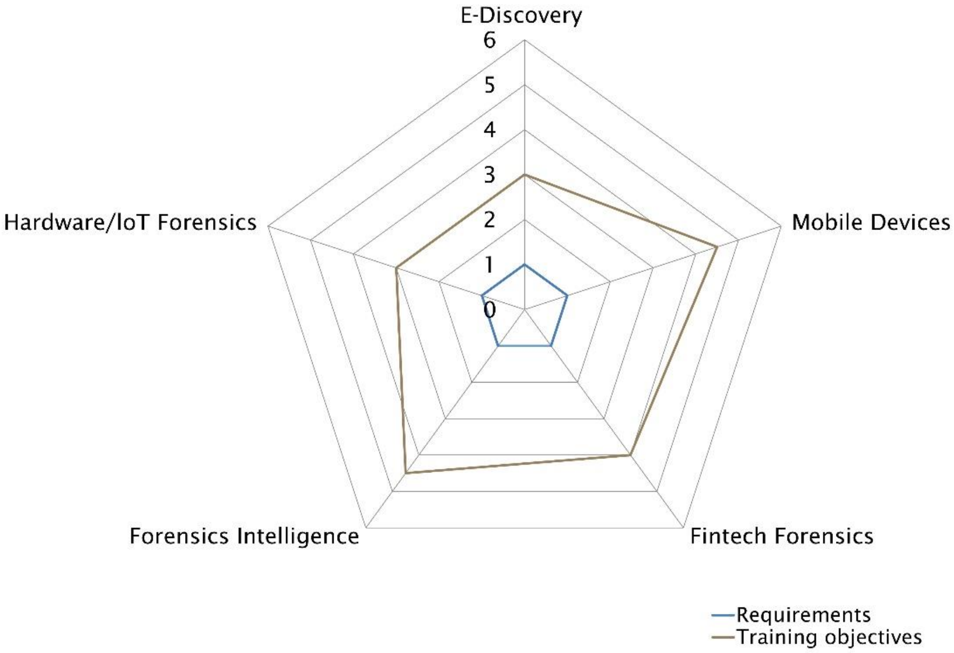
The location of taught classes is the Switzerland Innovation Park, Aarbergstrasse 46, in Biel/Bienne. More information can be found here: https://www.bfh.ch/en/about-bfh/locations-facilities/locations/biel-aarbergstrasse-46/

Some modules allow remote attendance, however, onsite attendance is strongly recommended (better teaching experience, building friendships with your student colleagues and teachers).

Please see the schedule for the latest dates and onsite availability.

Berner Fachhochschule, Weiterbildung, Aarbergstrasse 46 (Switzerland Innovation Park Biel/Bienne),
2503 Biel,
Telefon +41 31 848 31 11, E-Mail weiterbildung.ti@bfh.ch.

7 Skills profile



Skill levels

1. Proficiency/knowledge
2. Comprehension
3. Application
4. Analysis
5. Synthesis
6. Appraisal

8 Course outline

Course / Teaching unit	Lessons	Hours	Lecturers
E-Discovery	40		Iréne Wilson
Mobile Device Forensics	40		Chris Hargreaves
Fintech Forensics	40		Peter Waelti
Forensic Intelligence	40		Reto Inversini et al.
Hardware Forensics	40		Edouard Forler
Total	**160**		

This final CAS of the MAS requires 4 of 5 modules to be completed. Students may choose any 4 modules or take all 5 (without additional cost).

Completion of the MAS requires a Master Thesis (can be written in your preferred language, as agreed by the expert performing the assessment)

The CAS comprises a total of 12 ECTS credits. For the individual courses, time for self-study, exam preparation, etc. must be taken into account as needed.

Please see the schedule for the latest dates and onsite availability.

9 Module descriptions

The individual modules that make up this programme are described below.

A module may include a variety of teaching methods such as lectures, seminars, case studies, practical labs, assignments, etc.

9.1 E-Discovery

Educational objectives	This module covers the Electronic Discovery processes in corporate legal and litigation investigations.
Topics and content	– Introduction to civil investigations and litigation – Concepts of E-Discovery, client privilege – Electronic Discovery Reference Model (EDRM) – Corporate document retention and legal IT – Electronically stored information (ESI) – Document/record identification and preservation – Data pre-processing and processing – Review, production, and presentation
Course materials	Provided in Moodle

9.2 Mobile Device Forensics

Educational objectives	This module teaches the analysis of mobile devices such as smart phones and tablets.
Topics and content	– Extracting data from mobile devices – Using Faraday cages in a forensic environment – Logical and physical extraction – Analyzing mobile apps and app stores – Rogue apps and mobile malware – IOS forensic artifacts – Android forensic artifacts – Network telemetry analysis
Course materials	Provided in Moodle

9.3 FinTech Forensics

Educational objectives	This module teaches investigative tecniques related to financial technologies
Topics and content	– Technical analysis of digital payment systems – Traditional financial transactions (SWIFT messages, IBANs) – Crypto and virtual currencies (Bitcoin, etc) – Online money laundering methods – Cyber fraud investigation of phishing attacks – Forensic analysis of banking malware – Investigating social engineering fraud – Other online fraud scams (BEC, CEO impersonation, advance fee fraud)
Course materials	Provided in Moodle

9.4 Forensic Intelligence

Educational objectives	This module teaches the use of intelligence to guide forensic investigations.
Topics and content	– Understanding evidence vs. intelligence – Intelligence gathering models – Evidentiary properties of intelligence data – Advanced Open Source Intelligence (OSINT) – Assessing intelligence reliability and accuracy – Identifying and assessing intelligence sources – Using intelligence data to guide investigations – Exchanging and sharing intelligence – Social media investigation
Course materials	Provided in Moodle

9.5 Hardware Forensics

Educational objectives	This module covers forensic analysis of hardware and IoT devices.
Topics and content	– Introduction to electronics and interfaces – Accessing device memory via JTAG interfaces – Chip-off techniques for non-volatile storage devices – Embedded linux systems – Single-board computers and microcontrollers (Raspberry/Arduino) – Extracting data stored on IoT devices – Industrial control systems and medical device forensics – Drones and vehicle forensics (CAN bus)
Course materials	Provided in Moodle

10 Proof of proficiency

To gain the 12 ECTS credits, students must demonstrate proficiency by successfully completing all coursework (examinations, project work), in accordance with the following list:
:

Proof of proficiency	Weighting	Type of qualification	Student pass rate
E-Discovery (ElectiveA)	2.5	Final exam	0 – 100 %
Mobile Device Forensics	2.5	Final exam	0 – 100 %
Fintech Forensics	2.5	Final exam	0 – 100 %
Forensic Intelligence (ElectiveB)	2.5	Final exam	0 – 100 %
Hardware Forensics	2.5	Final exam	0 – 100 %
Total weighting / Pass rate	10 (best 4 marks if 5 modules are taken)		0 – 100 %

Students must choose four modules to complete the CAS. Students enrolled in the MAS are allowed to take all five modules at no additional cost. MAS students who complete all 5 modules are graded from the 4 highest results.

The weighted average of the pass rates of the individual competency certificates is converted into a grade between 3 and 6. Grade 3 (average pass rate of less than 50%) is unsatisfactory.
Grades 4, 4.5, 5, 5.5 and 6 (average pass rate between 50% and 100%) are sufficient

11 Lecturer

Name, Surname		E-Mail
Chris Hargreaves		chris.hargreaves@bfh.ch
John Sheppard		john.sheppard@bfh.ch
Angelo Mathis		angelo.mathis@bfh.ch
Slavo Greminger		slavo.greminger@bfh.ch

12 Organisation

CAS supervisor:
Prof. Dr. Bruce Nikkel
Email: bruce.nikkel@bfh.ch
Threema: DC2JN4YK
Mobile: +41 79 255 6316

CAS administration:
Miriam Patwa
Tel: +41 31 848 58 68
E-Mail: miriam.patwa@bfh.ch

Changes may be made to content, learning objectives, lecturers and required proficiency levels. The lecturers and the Head of Studies are authorised to make adjustments to a CAS on the basis of current developments in a subject area, the specific previous knowledge and interests of the students, or for didactic and organisational reasons.

Bern University of Applied Sciences
School of Engineering and Computer Science
Continuing Education
Aarbergstrasse 46 (Switzerland Innovation Park Biel/Bienne)
2503 Biel

Tel. +41 31 848 31 11
Email: weiterbildung.ti@bfh.ch

bfh.ch/ti/weiterbildung