Certificate of Advanced Studies

Digital Forensics & Cyber Investigation Fundamentals

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 Digital Forensics Fundamentals gives you an introduction to digital forensics, and provides the fundamental knowledge needed to understand cyber criminal activity, conduct cyber investigations, and collect digital forensic evidence.

Berner
Fachhochschule

Table of contents

Updated: 06.03.24

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 Requirements, education goals

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.

This continuing education program has practical learning objectives. Students completing the CAS Digital Forensics Fundamentals will understand the concepts of modern digital forensics, they will have the fundamental knowledge and skills needed to understand cyber criminal activity, conduct cyber investigations, and collect digital forensic evidence.

5 Language, Location, 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.

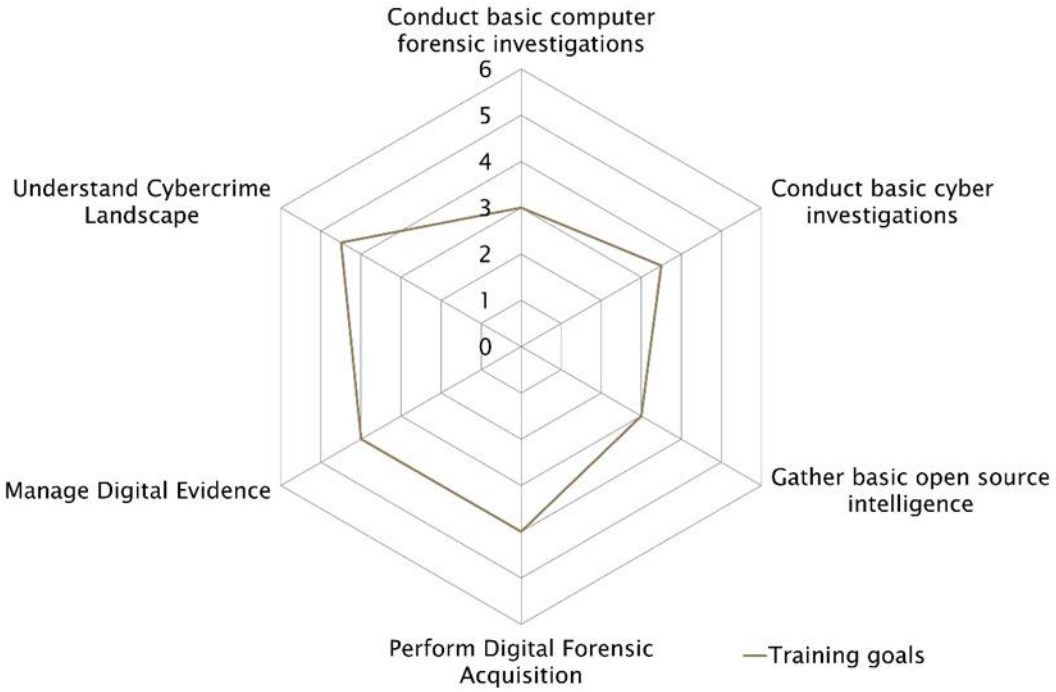
The location of taught classes is the Switzerland Innovation Park, Aarbergstrasse 46, in Biel/Bienne. More information can be found here: https://www.bfh.ch/en/about-bfh/locations-facilities/locations/biel-aarbergstrasse-46/.

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.

University of Applied Sciences, School of Engineering and Computer Science
Continuing Education, Aarbergstrasse 46 (Switzerland Innovation Park Biel/Bienne), 2503 Biel,
Telephone +41 31 848 31 11, E-mail weiterbildung.ti@bfh.ch.

6 Skills profile



Skill levels

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

7 Course outline

Course / Teaching unit	Lessons	Lecturers
Digital Forensics Fundamentals	40	Ryan Pittman
Cyber Investigation Fundamentals	40	Frank Breitinger
Cybercrime Overview	40	Mauro Vignati
Digital Forensic Acquisition	40	Mark Scanlon
Total	**160**	

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.

Modules are conducted in one-week fulltime periods. Please see the schedule for the latest dates.

8 Course 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.

8.1 Digital Forensics Fundamentals

Educational objectives	This module provides an introduction to digital forensics and digital forensic investigation.
Topics and content	– Introduction to forensic science – History of digital forensics – Current scope of digital forensics research – Laws and regulations relevant to digital forensics – Concepts of digital evidence and digital traces – Digital forensic standards and processes – Incident response and crime scene triage – Equipment and capabilities of digital forensic laboratories
Course materials	Provided in Moodle

8.2 Cyber Investigation Fundamentals

Educational objectives	This module provides an introduction to basic Internet/cyber investigations.
Topics and content	– Overview of Internet technologies (protocols, layers) – Introduction to investigation methodology – Investigating DNS, Whois, registrars, registries – Basic open source intelligence (OSINT) – Network mapping, reconnaissance, and scanning – Investigating IPv4, IPv6, TLDs, ccTLDs, gTLDs – Basic Email, VoIP, IM analysis – Network encryption – Attribution and event reconstruction
Course materials	Provided in Moodle

8.3 Cybercrime Overview

Educational objectives	This module provides an introduction to cybercrime and cyber facilitated crime.
Topics and content	– Criminal motivation – History of cybercrime – Criminal actors – Crime fighting organizations – Cyber fraud, phishing, identity theft – Data theft and leaks, Privacy and surveillance – Unauthorized access and intrusions – Disruption and denial of service
Course materials	Provided in Moodle

8.4 Digital Forensic Acquisition

Educational objectives	This module teaches basic digital forensic acquisition and evidence management skils.
Topics and content	• Overview of computer architectures • Storage technologies and interfaces • Concepts of forensically sound imaging • Forensic write-blockers • Managing digital evidence • Cryptographic hashing • Preserving and verifying evidence integrity • Forensic acquisition formats and containers
Course materials	Provided in Moodle

9 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
Digital Forensics Fundamentals	2.5	Final exam	0 – 100 %
Cyber Investigation Fundamentals	2.5	Final exam	0 – 100 %
Cybercrime Overview	2.5	Final exam	0 – 100 %
Digital Forensic Acquisition	2.5	Final exam	0 – 100 %
Total weighting / Pass rate	10		0 – 100 %
Grade	10		**3 - 6**

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

10 Lecturers

First name / Last name	Course	E-mail
Ryan Pittman	Digital Forensics Fundamentals	ryan@pittman@bfh.ch
Frank Breitinger	Cyber Investigation Fundamentals	frank.breitinger@bfh.ch
Mauro Vignati	Cybercrime Overview	mauro.vignati@bfh.ch
Mark Scanlon	Digital Forensic Acquisition	mark.scanlon@bfh.ch

11 Organisation

CAS supervisor:
Prof. Dr. Bruce Nikkel
E-mail: 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

During the course of the CAS, adjustments may be made to the content, learning objectives, lecturers and certificates of competence. It is the responsibility of the lecturers and the course director to make adjustments to the course of a CAS based on current developments in a subject area, the specific prior knowledge and interests of the participants, as well as for didactic and organizational reasons.

Bern University of Applied Sciences
School of Engineering and Computer Science
Continuing Education
Aarbergstrasse 46 (Switzerland Innovation Park Biel/Bienne)
2503 Biel
Telephone +41 31 848 31 11
E-mail: weiterbildung.ti@bfh.ch

bfh.ch/ti/en/continuing-education/
bfh.ch/cas-dfci1