Certificate of Advanced Studies

Digital Forensics & Cyber Investigation Specialist I

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 demands for skilled digital forensic and cyber investigators. The CAS DFCI Specialist I builds on the Fundamentals and Advanced CAS semesters, and provides you with the knowledge and skills needed to perform network forensic analysis, malware analysis, data analytics and visualization, and cloud/VM forensics.

Berner
Fachhochschule

Inhaltsverzeichnis

Updated: 14.04.2022

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 CAS DFCI Specialist I builds on the Fundamentals and Advanced CAS semesters, and is designed for two groups of professionals:

- Experienced forensic investigators who want to increase their technical skills in digital foren-sics and cyber investigations
- Experienced engineers and technicians who want to transition into the field of digital forensics and cyber investigations.Fliesstext

3 Education goals

This continuing education program has practical learning objectives. Students completing the DFCI Specialist I CAS will understand the concepts of modern digital forensic analysis in specialist areas including network forensic analysis, malware analysis, data analytics and visualization, and cloud/VM forensics.

This 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

As a rule, a university degree and practical experience are required for admission.

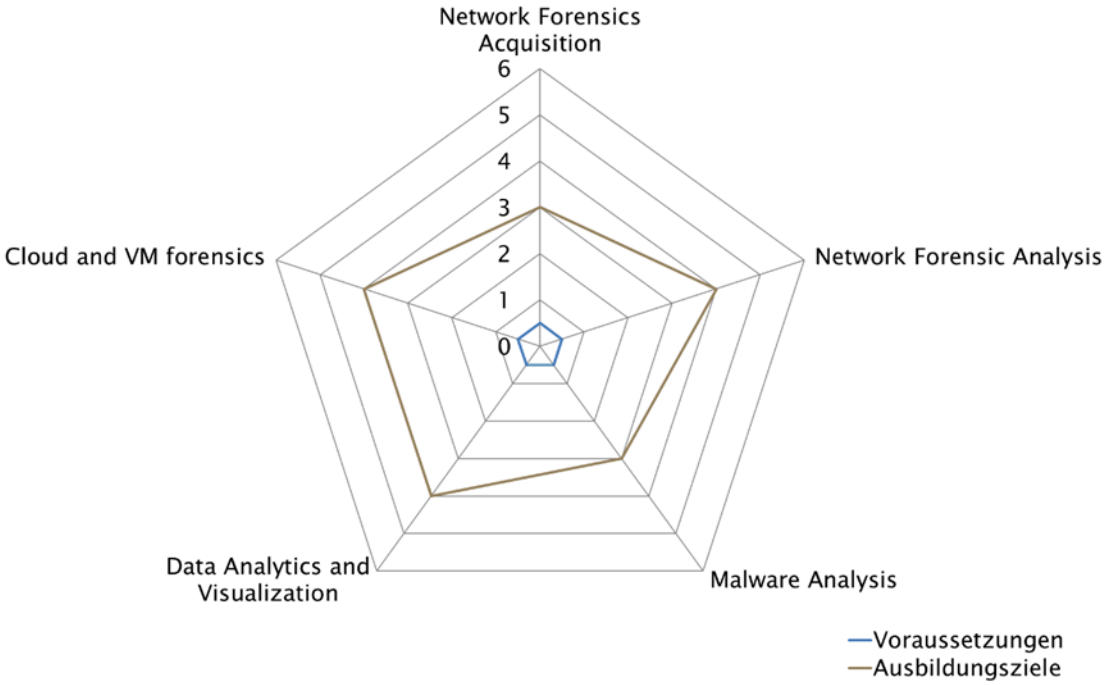
People with a high vocational training can apply, provided they have suitable professional experience and prior scientific and methodological knowledge.

If applicant qualifications are unclear or inconclusive, further information or an interview may be requested.

5 Language of instruction

The language of instruction is English.

6 Skills profile



Kompetenzstufen

1. Kenntnisse/Wissen
2. Verstehen
3. Anwenden
4. Analyse
5. Synthese
6. Beurteilung

7 Course outline

Course / Teaching unit	Lessons	Lecturers
Network Forensics	40	Reto Inversini
Malware Analysis	40	Endre Bangerter
Data Analytics and Visualization	40	Hans Hensler
Cloud and VM Forensics	40	Vassil Roussev
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 full-time 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 Network Forensics

Educational objectives	This module teaches advanced network forensics, packet capture and analysis.
Topics and content	- Network infrastructure traffic interception - Wired and wireless traffic interception - Introduction to mobile data networks (LTE, xG) - Packet capture file formats and containers - Traffic and packet analysis - Decoding and assembling protocol layers - Extraction of application data - Introduction to network encryption
Course materials	Provided in Moodle

8.2 Malware Forensics

Educational objectives	This module teaches the forensic analysis of Malware and malicious code.
Topics and content	- Static and dynamic binary analysis techniques - Debuggers, disassembly, sandboxes, basic reverse engineering - Malware identification and family categorization - DLL hooking and injection - Man-in-the-browser, web injection - Malware persistence, hiding and obfuscation

	- Botnet architectures, bot configuration files - Botnet sink-holes and disruption
Course materials	Provided in Moodle

8.3 Data Analytics and Visualization

Educational objectives	Working with big data in a forensic investigation context.
Topics and content	- Log analysis and corelation - Event reconstruction using timelines - Using Plaso to create super-timelines - Working with Big Data repositories - Correlation and relationship analysis - Statistical analysis - Advanced search techniques
Course materials	Provided in Moodle

8.4 Cloud and VM Forensics

Educational objectives	This module teaches forensics and investigations related to cloud and virtual machine technologies.
Topics and content	- Understanding cloud and virtualization technologies - Overview of commercial cloud service providers - Extracting data from cloud APIs - Analyzing server hosted virtual machines - Analyzing user installed virtual machines - Analyzing virtual desktop environments (VDIs) - Acquiring snapshots of virtual storage and memory Local (client-side) cloud artifacts
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
Network Forensics	2.5	Final exam	0 – 100 %
Malware Forensics	2.5	Final exam	0 – 100 %
Data Analytics and Visualization	2.5	Final exam	0 – 100 %
Cloud and VM Forensics	2.5	Final exam	0 – 100 %
Total weighting / Pass rate	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	Company	E-mail
Reto Inversini	Network Forensics	MELANI	reto.inversini@govcert.ch
Endre Bangerter	Malware Forensics	ThreatRay	endre.bangerter@bfh.ch
Hans Hensler	Data Analytics and Visualization	DFRWS	j.henseler@dfrws.org
Vassil Roussev	Cloud and VM Forensics	University of New Orleans	vassil@cs.uno.edu

11 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

Tel. +41 31 848 31 11
E-mail: weiterbildung.ti@bfh.ch

bfh.ch/ti/en/continuing-education/
bfh.ch/cas-dfci3