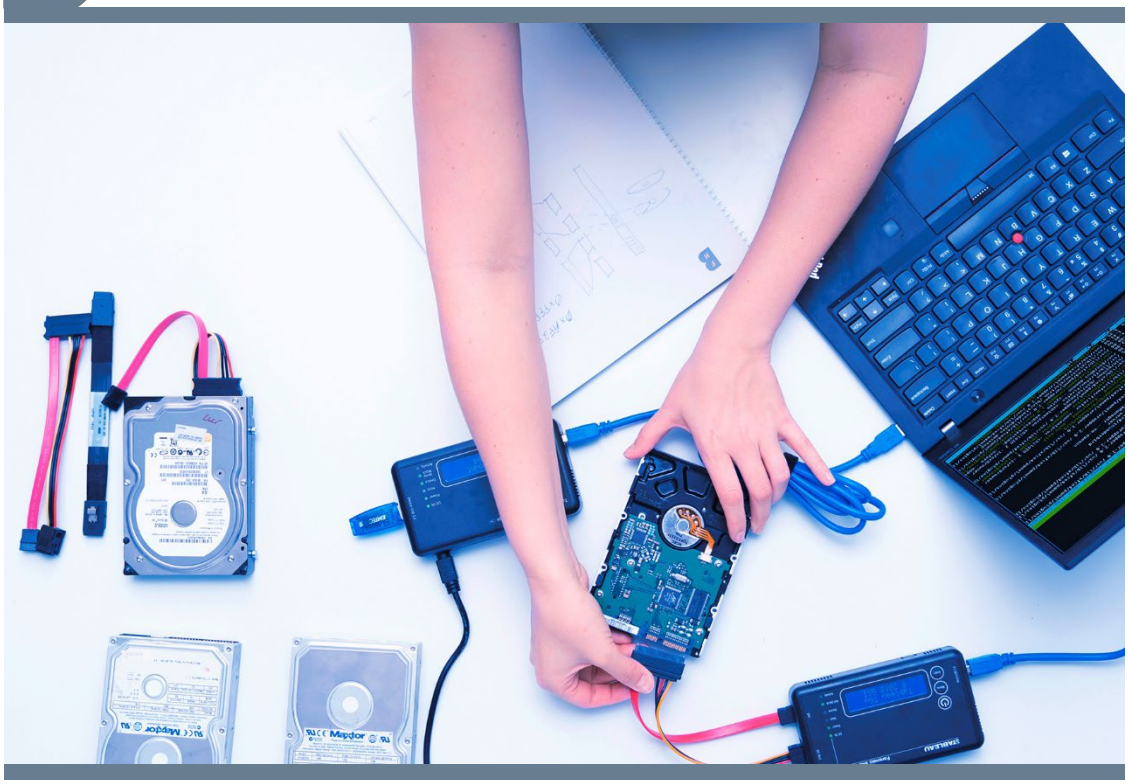


Certificate of Advanced Studies

Digital Forensics & Cyber Investigation Advanced

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 Digital Forensics & Cyber Investigation Advanced builds on the previous Fundamentals CAS and provides you with the knowledge and skills needed to perform forensic analysis of file systems, operating systems, applications, and memory.

bfh.ch/cas-dfci2

Table of contents

Updated: 22.09.22

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 Digital Forensics & Cyber Investigation Advanced is built on the CAS Digital Forensics Fundamentals, and 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 Education goals

This continuing education program has practical learning objectives. Students completing the CAS in Digital Forensics & Cyber Investigation Advanced will understand the concepts of modern digital forensic analysis in depth. They will have the skills to analyze digital evidence from a variety of sources, including file systems, operating systems, applications, and memory.

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

Admission into the MAS DFCI requires at least one of the following qualifications:

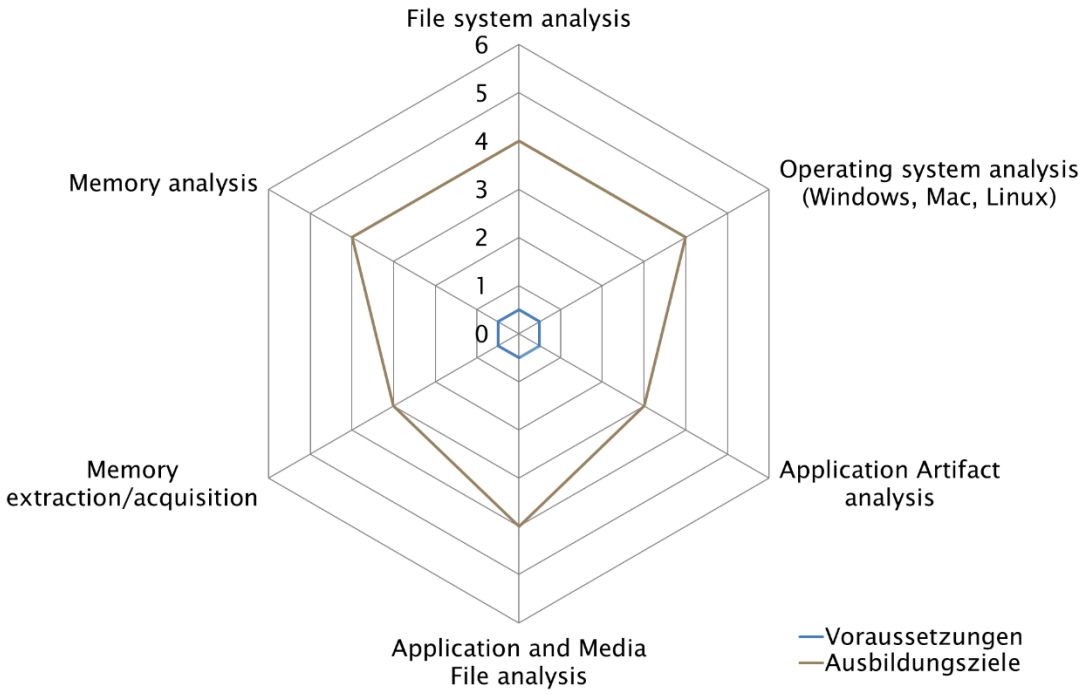
- a bachelor's degree or equivalent professional education degree in
- computer science, computer engineering, or related field
- professional experience in digital forensics or IT investigation, and a
- related industry certification.

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

5 Venue

Bern University of Applied Sciences, Continuing Education, Aarbergstrasse 46, 2502 Biel,
Tel. +41 31 848 31 11, E-mail office.ti-be@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
File System Analysis	40	Chris Hargreaves
Operating System Artifact Analysis	40	John Sheppard
Application and Media File Analysis	40	Angelo Mathis/Vera Thueler
Memory Forensic Analysis	40	Slavo Greminger
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 File System Analysis

Educational objectives	This module teaches advanced storage and filesystem forensics.
Topics and content	– Overview of partition schemes (MBR, GPT) – Identification and analysis of partition tables – Identification and analysis of filesystems – Using The Sleuth Kit (TSK) and Autopsy – Recovering deleted files and deleted partitions – Using hashsets and the NSRL databases – Extracting slack space and unallocated blocks – Carving unstructured data – Decrypting filesystems and directories
Course materials	– Provided in Moodle

8.2 Operating System Artifact Analysis

Educational objectives	This module teaches the forensic analysis of Operating System specific forensic artifacts.
Topics and content	– MS Windows artifacts – Apple OSX artifacts – Linux distribution artifacts – OS specific databases – Users, groups, system configuration – Cached and persistent data – system logs (event logs, syslog, systemd journal) – Installed software packages – Backups, synchronization
Course materials	– Provided in Moodle

8.3 Application and Media File artifact Analysis

Educational objectives	Application and Media File artifact Analysis.
Topics and content	– Analysis of application specific forensic artifacts – Client and server applications – Application configuration – Cached and persistent application data – History, application logs, temporary data – synchronization, backup, cloud telemetry – Analyzing meta data inside files (EXIF) – Identifying and analyzing application file content – File and application layer encryption
Course materials	– Provided in Moodle

8.4 Memory Forensics

Educational objectives	This module provides an introduction to memory forensic acquisition and analysis techniques.
Topics and content	– Dumping/acquiring memory images – Using Volatility and other tools to analyze memory – Memory introspection of running processes – Established network connections, listening sockets – Finding cryptographic keys and passwords – Extracting file fragments with carving memory data – Analyzing hibernation, swap, and page files – Analyzing OS generated core/crash dumps
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
File System Analysis	2.5	Final exam	0 – 100 %
Operating System Artifact Analysis	2.5	Final exam	0 – 100 %
Application Forensics	2.5	Final exam	0 – 100 %
Memory Forensics	2.5	Final exam	0 – 100 %
Total weighting / Pass rate	10		0 – 100 %

Each student can achieve a pass rate of 0 to 100% for each proof of proficiency. The weighted sum of the pass rates per topic and the weighting of the topic results in an overall pass rate between 0 and 100%. The weighted average of the success rates for each assessment is converted to a grade between 3 and 6. The grade 3 (averaged success rate less than 50%) means failed. Grades 4, 4.5, 5, 5.5 and 6 (averaged success rate between 50% and 100%) are passing grades.

10 Lecturers

First name / Last name	Course	Company	E-mail
Chris Hargreaves	File System Forensics	Oxford University	chris@hargs.co.uk
John Sheppard	Operating System Forensics	Waterford Institute of Technology	johnsheppardnid@dfrws.org
Angelo Mathys / Vera Thueler	Application Forensics		
Slavo Greminger	Memory Forensics	SWITCH-CERT	slavo.greminger@switch.ch

11 Organisation

CAS supervisor:
Bruce Nikkel
Tel.: +41 32 321 63 77
E-mail: bruce.nikkel@bfh.ch

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
Department of Engineering and Information Technology
Continuing Education
Aarbergstrasse 46
CH-2503 Biel

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

bfh.ch/ti/weiterbildung
bfh.ch/ti/cas-dfci2