Bern University
of Applied Sciences

Master of Advanced Studies in Digital Forensics & Cyber Investigation

The digital transformation of society is creating new challenges and new opportunities, both for criminals and for criminal investigators. Today forensic and cyber investigators must collect and analyze digital evidence from a diverse landscape of technically complex sources. Our unique Master program gives you a wide range of practical skills needed for an exciting career in digital forensics and cyber investigation.

▶ Engineering and Information Technology

Editorial

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 or crimes involving payments for illegal products and services.

These shifts are fundamentally changing the way police, government, and industry investigators are operating, and creating a demand for new skills not offered by traditional education. The Master of Advanced Studies (MAS) in Digital Forensics & Cyber Investigation (DFCI) at BFH was created to address this education requirement and to help fill the demand for skilled digital forensic and cyber investigators.

BFH is in a unique position to provide high quality education in digital forensics and cyber investigation. We are a technically focused Swiss Applied Sciences University. Our Engineering and Information Technology (BFH-TI) department specializes in areas of IT security, cyber fraud, micro technology, medical technology and medical informatics, industrial engineering, and automotive technology. This Master program leverages existing expertise at BFH to create a digital forensics and cyber investigation MAS with a format and modules not found at other universities.

We want to improve the safety and security of society. This can be achieved by educating the next generation of digital forensics and cyber investigators, and giving them the knowledge and skills needed to effectively fight crime. I invite you to attend BFH's Master of Advanced Studies in Digital Forensics & Cyber Investigation.

Kind Regards

Prof. Dr. Bruce Nikkel

Who Should Apply?

The MAS DFCI 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.

Learning Objectives

Graduates from the MAS DFCI will understand the fundamental concepts of modern digital forensics. They will have the skills to collect and analyze digital evidence from a variety of sources, and have the ability to conduct complex cyber investigations.

Career Opportunities

The MAS DFCI prepares students for jobs in law enforcement, military, government CERTs, cyber-fraud investigation teams in the finance industry, cyber claims investigators in the insurance industry, security and incident response teams in large firms, consulting and security service providers, and specialized digital forensic and investigation firms.

Module Format

The MAS DFCI offers an approach that provides education for remote and international students. The modules combine theory and practice with extensive lab work, giving students a hands-on learning experience.

The master program is organized into 4 taught semesters (CAS) and a final master's thesis semester. Each semester consists of 4 residential 1-week blocks (modules) which are held at BFH located in the Canton of Bern, Switzerland. The regular duration for the full master programm is 2.5 years. The block format allows BFH to engage professors from around the world, bringing specialist knowledge into the classroom for an enriched learning experience. The block format also allows remote and employed students to attend modules without requiring permanent residence near the university. The pre-residential and post-residential work can be completed remotely. The full master program comprises 60 ECTS credit transfer points, 12 ECTS credits per semester. Each semester is also a self-contained study program, called a CAS (Certificate of Advanced Studies), see Details in the next sections of this brochure.

Entrance 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.

Financial Information

Tuition fees for the MAS DFCI are as follows:

- CHF 7500.- per taught semester
- CHF 4000.- Thesis supervision and defense

Total tuition cost for MAS DFCI completion: CHF 34000.-

CAS DFCI Fundamentals

Semester 1

Module 1: Digital Forensics Fundamentals

This module provides an introduction to digital forensics and digital forensic investigation. Topics covered include:

- 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

Module 2: Cyber Investigation Fundamentals

This module provides an introduction to basic Internet/cyber investigations. Topics covered include:

- 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

Module 3: Cybercrime Overview

This module provides an introduction to cybercrime and cyber facilitated crime. Topics covered include:

- 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

Module 4: Digital Forensic Acquisition

This module teaches basic digital forensic evidence acquisition. Topics covered include:

- 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

CAS Advanced Digital Forensics

Semester 2

Module 1: File System Analysis

This module teaches advanced storage and filesystem forensics. Topics covered include:

- 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

Module 2: Operating System Artifact Analysis

This module teaches the forensic analysis of Operating System specific forensic artifacts. Topics covered include:

- 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

Module 3: Application and Media File artifact Analysis

This modules teaches analysis of application artifacts and analyzing meta data inside files. Topics covered include:

- 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

Module 4: Memory Forensics

This module provides an introduction to memory forensic analysis techniques. Topics covered include:

- Dumping/acquiring memory images
- Using Volatility and Rekall 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

CAS DFCI Specialist I

Semester 3

Module 1: Network Forensics

This module teaches advanced network forensics and packet analysis. Topics covered include:

- 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

Module 2: Elective A

An elective chosen based on student interest and module availability.

Module 3: Data Analytics and Visualization

This module teaches the use of data analytics and visualization for digital forensics. Topics covered include:

- 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

Module 4: Elective B

An elective chosen based on student interest and module availability.

CAS DFCI Specialist II

Semester 4

Module 1: Mobile Device Forensics

This module teaches the analysis of mobile devices such as smart phones and tables. Topics covered include:

- 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

Module 2: Elective A

An elective chosen based on student interest and module availability.

Module 3: Social Media Investigation

This modules covers the investigation of social media platforms. Topics covered include:

- Overview of popular social media platforms
- Extracting data from APIs
- Account/profile analysis
- Group membership and relationships
- Multiple account linkage
- User attribution
- Client application configuration
- Locally cached artifacts

Module 4: Elective B

An elective chosen based on student interest and module availability.

Elective Modules*

Module: Malware Forensics

This module provides an introduction to malware analysis:

- 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

Module: IoT and Hardware Forensic Analysis

This module covers forensic analysis of hardware and IoT devices. Topics covered include:

- Introduction to micro-electronics
- Chip pinouts and interfaces
- Chip programmers and adapters
- Accessing device memory via JTAG interfaces
- Chip-off techniques for non-volatile storage devices
- Embedded linux systems
- Single-board microcontrollers (Arduino)
- Extracting data stored on IoT devices

*subject to student demand and professor availability

Module: Industrial Forensics

This module teaches industrial control systems and medical device forensics. Topics covered include:

- Introduction to industrial control systems, Industry 4.0
- SCADA systems and standards
- Location and contents of interesting industrial data
- Attacks against industrial control systems
- Introduction medical device technologies
- Extracting data from medical devices and implants
- Consumer wearable health monitoring devices
- Interpreting medical data

Module: Cloud and VM Forensics

This module teaches forensics related to cloud technologies. Topics covered include:

- 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

*subject to student demand and professor availability

Elective Modules*

Module: Encryption and Forensics

This module teaches the challenges and techniques for managing encrypted data. Topics covered include:

- Introduction to encryption algorithms and implementations
- Network encryption
- Application specific encryption systems
- SSD hardware encryption
- Filesystem and block level storage encryption
- Folder encryption and containers
- File encryption
- Password and key recovery techniques

Module: Anti-Forensics and Anonymity Investigations

This module teaches methods used to subvert forensic investigations. Topics covered include:

- Understanding onion routing (TOR) and P2P networks
- Analyzing darknet servers and clients
- Underground forums and markets
- Anti-forensic techniques
- Anonymizers and relaying techniques
- Bullet-proof hosting and takedown resistant infrastructure
- Steganography and data hiding
- Data destruction methods

*subject to student demand and professor availability

Module: Financial Technology Forensics

This module teaches investigative tecniques related to financial technologies. Topics covered include:

- 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

Module: E-Discovery

This module teaches electronic discovery for legal litigation investigations. Topics covered include:

- 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

*subject to student demand and professor availability

Elective Modules*

Module: Commercial Products

This module provides an overview of commercial forensic and investigation products and services. This product showcase is presented by a variety of companies and includes:

- Forensic acquisition and analysis
- Data corelation and analysis
- Storage forensics
- Mobile forensics
- Cloud forensics
- Social Media investigations
- Other investigation tools

Module: Forensic Intelligence

This module teaches the use of intelligence to guide forensic investigations. Topics covered include:

- 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

*subject to student demand and professor availability

Module: Vehicle and Drone Forensics

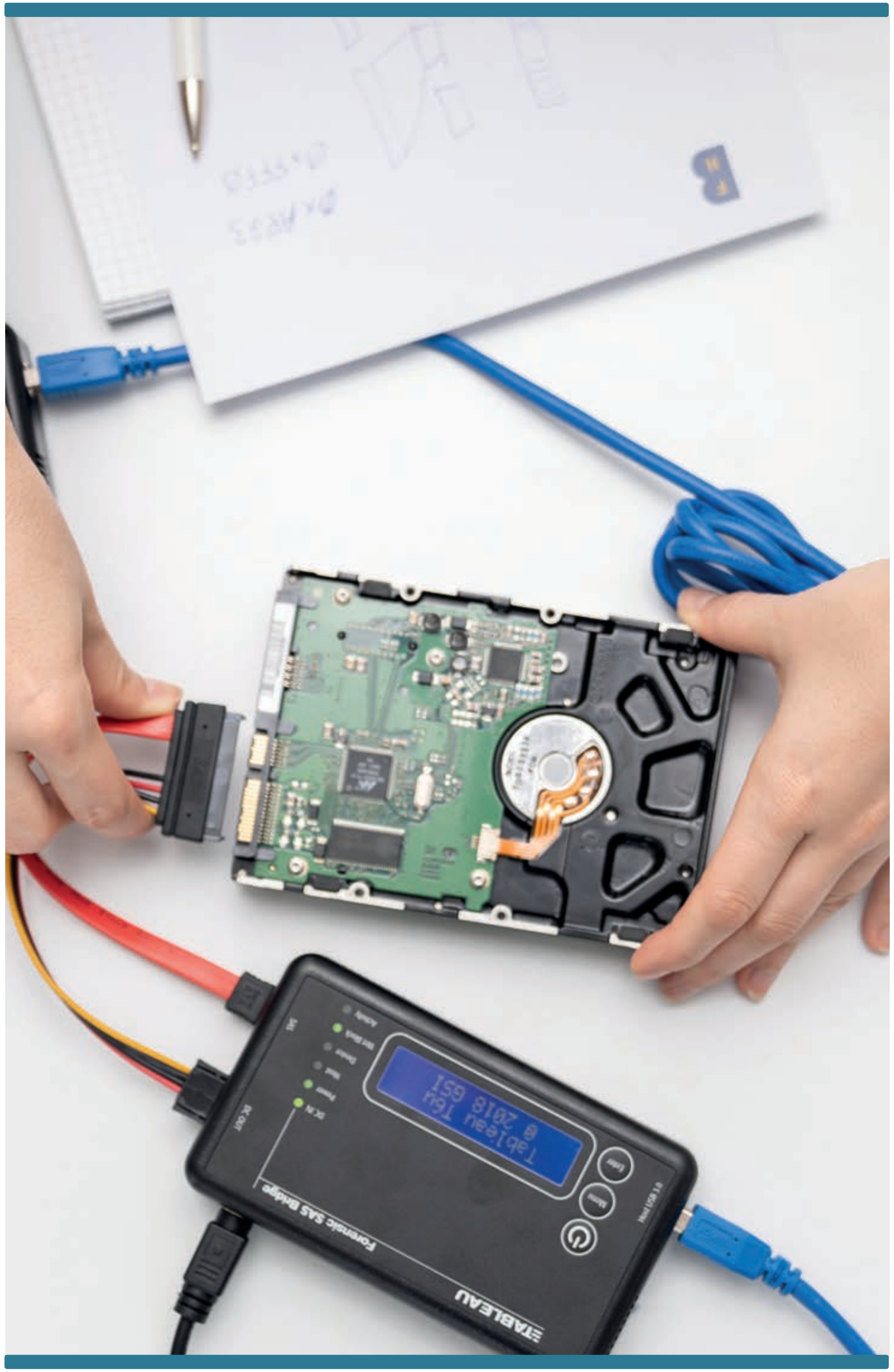
This module provides an introduction to automobile and drone forensics. Topics covered include:

- Introduction to automotive electronics
- Controller Area Networks (CAN)
- Extracting stored data from vehicle electronic systems
- GPS, geolocation and navigation data
- Introduction to drone technologies
- Accessing and extracting stored data from drones
- Forensic analysis of drone photos, flight paths, and configuration data
- Identifying other devices paired or associated with drones

Module: Technical Investigation Support (LEA Only)

This module is available only for students employed by Law Enforcement Agencies and teaches effective digital forensics and cyber investigation support. Topics covered include:

- Approaching providers and corporations for support
- Making evidence preservation/hold requests
- Quick and effective online takedown requests
- Private sector investigative collaboration
- Multi-jurisdictional cooperation with other agencies
- Intelligence sharing and public-private partnerships
- Writing technical MLATs



Master’s thesis

The research and write-up of the Thesis requires one full semester of work. This includes:

- choosing a thesis topic
- writing a thesis proposal
- finding a Thesis advisor
- conducting the research project work
- writing up the dissertation
- the Thesis defense.

The master’s thesis is started after completion of the first four semesters (16 modules total). The expected workload for completing the master thesis is minimum 360 hours.
Depending on the external examiner/expert, the dissertation and thesis defense may also be in German or French.
During Semester 5 students may also attend elective modules that were unavailable during semesters 3 and 4.

Contact Information

If you are interested in more information about the MAS in Digital Forensics & Cyber Investigation, please visit our web site: bfh.ch/mas-dfci

If you have additional questions about administration or technical information, please email us at: dfci@bfh.ch

Bern University of Applied Sciences
Master of Advanced Studies in
Digital Forensics & Cyber Investigation

Legal notice:

This brochure is for general orientation. In case of doubt, the wording of the statutory provisions and regulations shall prevail. We reserve the right to make changes without prior notice. November 2019.

Bern University of Applied Sciences
Engineering and Information Technoloy
Continuing Education
Wankdorffeldstrasse 102
3014 Bern

Phone +41 31 848 31 11

office.ti-be@bfh.ch
bfh.ch/mas-dfci

swissuniversities