Short Advanced Studies (SAS)[1]

Memory Forensics

The digital transformation of society is creating new challenges and new opportunities, both for criminals and for criminal investigators. Today digital forensics and cyber investigators must collect and analyze digital evidence from a diverse landscape of technically complex sources. Our unique Digital Forensics and Cyber Investigation (DFCI) Short Advanced Study (SAS) programs give you a wide range of practical skills needed for an exciting career combating, analyzing and investigating cyber criminal activity.

The Memory Forensics SAS provides an introduction to memory forensic acquisition and analysis techniques. It covers dumping memory images, using tools to introspect running processes, identify established network connections, listening sockets, finding interesting data fragments and files with carving, and more.

[1]Short Advanced Studies (SAS) are short qualifying training courses designed for a specialist audience seeking to face new challenges in direct dialogue with experts (1-9 ECTS).

Berner
Fachhochschule

Table of Contents

1 Portrait 3
2 Career opportunities 3
3 Target audience 3
4 Education goals 4
5 Requirements 4
6 Factsheet 5
7 Content + Learning objectives 5
8 Proof of proficiency 5
9 Lecturers 5
10 Organisation 6

Berner
Fachhochschule

1 Portrait

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 increasing challenges trying to hide and avoid attribution. The large amount of digital traces stored across multiple locations and devices creates an opportunity for criminal forensic investigators.

Crime scenes are also changing. With the growth of cybercrime, crime scenes are becoming virtual, global, and multi-jurisdictional. Investigating a transnational 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 array 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, social media, 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, ransomware, and extortion.

Our unique Digital Forensics and Cyber Investigation (DFCI) Short Advanced Study (SAS) programs give you a wide range of practical skills needed for an exciting career combating, analyzing and investigating cyber criminal activity.

2 Career opportunities

The DFCI SAS programs prepare students for career opportunities in a variety of organizations who depend on forensic investigation capabilities. For example:

- Law enforcement - Federal agencies, KAPOs
- Military and government – NCSC, CERTs, cyber-troops
- Finance industry – fraud and 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

3 Target audience

The DFCI SAS programs are 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.

4 Education goals

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

The Memory Forensics SAS provides an introduction to memory forensic acquisition and analysis techniques. It covers dumping memory images, using tools to introspect running processes, identify established network connections, listening sockets, finding interesting data fragments and files with carving, and more.

5 Requirements

Admission into the DFCI SAS program requires one of the following qualifications:

- a bachelor's degree or equivalent professional education degree in computer science, computer engineering, or related technical 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.

6 Factsheet

Short Advanced Studies (SAS)	Memory Forensics
Degree/Certificate	Short Advanced Studies (SAS) Memory Forensics
Duration	One week, 5 days
Schedule	See website
Application deadline	Up to 1 month before the course begins
ECTS credits	3 ECTS-Credits
Costs	CHF 2'500.00
Teaching language	English
Location	remote
School	School of Engineering and Computer Science

7 Content + Learning objectives

The Memory Forensics SAS provides an introduction to memory forensic acquisition and analysis techniques. The content includes:

- 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

8 Proof of proficiency

To receive 3 ECTS (European Credit Transfer and Accumulation System) academic credits, students must demonstrate their knowledge by successfully completing assignments, projects, and final exam as required by the lecturer. Students who attend all classes but do not complete the assessment work will receive a certificate of attendance equivalent to 40 CPE (Continuing Professional Education) hours.

9 Lecturers

Name	Organisation	E-mail
Slavo Greminger		slavo.greminger@bfh.ch

10 Organisation

SAS Supervisor:
Slavo Greminger
E-Mail: slavo.greminger@bfh.ch

SAS Coordination:
Miriam Patwa
Phone: +41 31 848 58 68
E-mail: miriam.patwa@bfh.ch

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

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

bfh.ch/ti/weiterbildung

Berner
Fachhochschule