



## DIGITAL FORENSICS

IFSA-Butler Reimagining Europe Semester Program in Prague

**Suggested US semester credit hours:** 4 credits

**Contact hours:** 60

**Course level:** 300

**IFSA-Butler course code:** CS380-05

**Course length:** Semester

**Delivery method:** Face to face

**Language of Instruction:** English

### COURSE DESCRIPTION

The course aims to provide students with an understanding of the principles of digital forensics and the impact on commerce, society and the individual. As with a real-world crime scene, a computer system can be used as a tool to implicate criminal activity. The need to preserve the crime scene and ensure the analysis is completed in a manner conducive to the fair and unbiased pursuit of justice is of the greatest importance. Students will need to understand and review cases where the process of forensic analysis determines the absence of direct criminal intent and serves as a process to improve security and administrative processes as well as technological implementation.

### STUDENT LEARNING OBJECTIVES

Students who successfully complete this course will:

- Understand the impact of digital forensics on the social and commercial environments
- Understand the principles of evidence gathering
- Be able to plan and implement digital forensics investigations
- Be able to analyze the outcomes of digital forensics investigations
- Strengthen critical thinking skills
- Become familiar with resources available for further research on digital forensics
- Make cognitive connections between learning in this course and other learning experiences in the IFSA-Butler Reimagining Europe Semester Program in Prague

## COURSE DELIVERY

Students are expected to read or view resources in advance and be prepared to actively discuss them in class. In each meeting, the instructor will overview the topic and then facilitate a group discussion, drawing out relevant themes, following up on specific lines of inquiry, and prompting students' thoughtful engagement with the topic. Students are encouraged to bring their prior learning experiences into class discussions and to make cognitive connections between this course and others in the IFSA-Butler Reimagining Europe Semester Program in Prague whenever possible. Theories of experiential learning and integrative learning therefore undergird the dynamic learning environment of this course.

This course utilizes an interactive approach to teaching that focuses on the individual student's needs. This approach to teaching and learning aims to foster a challenging but caring environment that allows students to explore, create, and test themselves and their ideas in a safe place.

## COURSE SCHEDULE

<b>15 weeks</b>	<b>Content Delivery</b>
1	Terms definition (Weakness, exploit, malicious activity, risk, assessment, insurance) Event classification EACEWNID How to solve stuff (standards, procedures, guidelines, best practice, technical policy, administrative policy, physical policy ) Security Policies (authentication, authorization, accounting)
2	Attacks (Reconnaissance, Social Engineering, DOS, Brute force, MID, Spoofing) Security Disposal (magnetic, optic, flash)
3 -6	Simulator (GNS3), VirtualBox
7	Definitions and assumptions, Strengthening the router, ASA and strengthening ASA
8	GNS3 configuration of a site -2-site IPSec VPN, CBAC, Zone Based Firewall
9 - 10	Implementation of zone-based firewall AAA ( Authentication, Authorization and Accounting) Cisco ASA
11	Configuring ASA interfaces, firewall and site-to-site IPSec VPN between ASA and Cisco Router
12	Gathering and storing logs and data
13	Intrusion Protection System and simulation
14	Assignments

15	<b>Feedback, final results</b>
----	--------------------------------

EVALUATION METHODS

The course instructor will determine specific assignments (including paper topics), projects, and exams for the course. Your work on individual assignments and projects will be guided by grading rubrics provided by the course instructor. Your final grade in the course will be arrived at through assessment methods determined by the course instructor and according to the percentages attached to each assignment and exam by the course instructor. Participation will constitute a determined percentage of your grade. Participation includes attendance, preparation, engagement in discussion, civility, and respect.

Assignment Number	Type of Assignment	Description and Areas Assessed
1	Technical report	Procedures, Finding and Analysing Security Issues
2	Implementation and report	Implementing a Network Lockdown

**Timely Submissions**

Assignments submitted after the deadline will be accepted at the discretion of the course instructor and generally only in the event of a documented illness or emergency.

READING LIST

Cisco CCNA on Security 640-554 guidelines

Casey E – Handbook of Digital Forensics and Investigation (Academic Press, 2009) ISBN-10: 0123742676

ACADEMIC INTEGRITY

Any academic endeavor must be based upon a foundation of honesty and integrity. Students are expected to abide by principles of academic integrity and must be willing to bear individual responsibility for their work while studying abroad. Any academic work (written or otherwise) submitted to fulfill an academic requirement must represent a student’s original work. Any act of academic misconduct, such as cheating, fabrication, forgery, plagiarism, or facilitating academic dishonesty, will subject a student to disciplinary action.

IFSA-Butler takes academic integrity very seriously. Students must not accept outside assistance without permission from the instructor. Additionally, students must document all sources according to the instructions of the professor. Should your instructor suspect you of plagiarism,

cheating, or other forms of academic dishonesty, you may receive a failing grade for the course and disciplinary action may result. The incident will be reported to the IFSA-Butler resident director as well as your home institution.