# FACULTY OF ENGINEERING
# STUDY COURSE DESCRIPTION

| | |
|---|---|
| **Course Title**: | **Digital Forensics I** |
| **Course code (LAIS):** | **MKI_025** |
| **Study programme:** | **CYBERSECURITY ENGINEERING** |
| **Level of Study programme:** | ☐ 1st level professional higher education<br>☐ Professional Bachelor<br>☒ Professional Master<br>☐ PhD level |
| **Type of Study programme:** | ☐ Compulsory course (Part A)<br>☒ Professional specialization courses (Part B, compulsory)<br>☐ Professional specialization optional courses (Part B, optional)<br>☐ Elective courses (Part C) |

| **Course Workload:** | Credits | ECTS | Academic hours | Contact hours | Independent work hours |
|---|---|---|---|---|---|
| | 2 | 3 | 80 | 24 | 56 |

| | |
|---|---|
| **Course Author/ Tutor:** | **Viesturs Bambans**<br>Academic position, M.sc. Information Security and Assurance – Major: Forensic Investigation.<br><br>Consultation: according to the schedule for each semester |
| **Course Form:** | Full time |
| **Study year, semester:** | 2018./2019.       2.sem. |
| **Language:** | Latvian and English |
| **Prerequisites for the Course:** | Understanding of the TCP/IP and OSI Network Models. Working knowledge of the Win. OS and its Registry. Installation and configuration of a network devices. VPN Configuration. File systems. |
| **Course Summary:** | Learn: Digital Forensic Methodology and Terminology. Legal and ethical principles of Digital Forensics. Introduction into Cyberpsychology. Recognize the components of crime. Methodology for collecting and storing Digital Forensic evidence. Introduction to the basic principles of interviewing and interrogation. To acquire skills in using the equipment and software used by Digital Forensics, which is certified by professional organizations and government regulations. Acquiring Digital Forensics Evidence from the OS Environment, Cloud Computing, and Mobile Devices. Anti-Forensic methods, equipment and software. To acquire the skills that would help to prepare an Evidence Report addressed for use in the business environment and in the public administration environment. |
| **Course Methods:** | Lectures, practical workshops, discussions, group work |
| **The Type of Final examination** | Exam |
| **Requirements for Credits:** | Practical work 60%, final exam 40% |
| **Course Contents:** | The background knowledge needed to work and study in the Digital Forensic field<br>What is Digital Forensics. History of development. Digital Forensic Basic Principles: Components of Crime - Loss or Injury (Murder), Criminal liability, Offender. CyberPsychology; Laws concerning Digital Forensics – in Latvia, EU and USA; Ethics of Digital Forensic; Location and analysis of Digital Forensic evidence; Anti-Forensics technics. |

| | Learning Outcomes | The evaluation methods and criteria |
|---|---|---|
| **Learning Outcomes** | **Knowledge** | |
| | Student knows and understand the basic of Components of Crime, Criminal liability | lectures, practical classes, seminars, discussions, group work |
| | **Skills** | |
| | Students are able to find, collect, use relevant sources of digital evidence | lectures, practical classes, seminars, discussions, group work |
| | **Competency** | |
| | The student is able to analyze, evaluate forensic samples and make suggestions for appropriate forensic methods | practical classes, seminars, discussions, group work |

| | |
|---|---|
| **Course Compulsory literature:** | Soufiane Tahiri, "Mastering Mobile Forensics", May 2016, ISBN 9781785287817<br>Craig Ball, "Electronic Discovery Workbook 2016" http://www.craigball.com/Ball_E- |

| | | Discovery_Workbook_Ver.%2016.0818.pdf | | | |
|---|---|---|---|---|---|
| **Course additional literature:** | | James Lyle, NIST "Computer Forensics Tool Testing Handbook", https://www.cftt.nist.gov/CFTT-Booklet-08112015.pdf <br> Craig Ball, "Introduction to Digital Computers, Servers and Storage ": http://www.craigball.com/Intro_Computers_2015.pdf | | | |
| Course approval date: | | | | | |
| Course last revision date: | | | | | |

## Study Course Plan:

| Date* | Theme | Academic hours | | Study Form |
|---|---|---|---|---|
| | | contact lessons | Independent work hours | |
| | The background knowledge needed to work and study in the Digital Forensic field –Computer System Ecosystems - What is Digital Forensics. History of development. Digital Forensic Basic Principles | 4 | | Lecture, situation analysis, discussions |
| | Components of Crime - Loss or Injury.Murder), Criminal liability, Offender; CyberPsychology; Interviews and Interrogation Methodology. | 4 | | Lecture, situation analysis, discussions |
| | Laws concerning Digital Forensics – in Latvia, EU and USA – regulating, Ethics of Digital Forensic, Presenting Digital Forensic evidence in a cases govern by - Civil Court, Criminal Investigation, Intellectual Property Loss, Administrative Violations. | 4 | | Lecture, situation analysis, discussions |
| | Management of a Digital Evidence: Acquisition; Transport; Storage; Access Control – Least privilege and Wall of China; Destroying of Evidence. | 4 | | Lecture, situation analysis, discussions |
| | Location and analysis of Digital Forensic evidence | 2 | 6 | Individual project work |
| | Analyzing damaged files: Files which are sustained Logical and/or Physical damage; Analysis of known files | 2 | 30 | Individual project work |
| | Digital Forensic analysis | | 20 | Group project work |
| | Group project | 4 | | Open book exam |
| | *Hours total:* | *24* | *56* | |

*\* The date is specified before the implementation of the course*