**Corso di Laurea triennale in**

**Scienze delle Investigazioni**

**Corso integrato di Mezzi di Prova e Mezzi di ricerca della Prova**

Modulo Digital Forensics

**A.A. 2022/2023 – II anno – II Semestre**

**IUS/16 - 5 Cfu (30 ore)**

**Docente: Dott. Bruno Cesena**

**Testo in italiano**

|  |  |
| --- | --- |
| **Informazioni Corso** | **CORSO INTEGRATO DI MEZZI DI PROVA E MEZZI DI RICERCA DELLA PROVA**  **MODULO DIGITAL FORENSICS**  Corso di Laurea Triennale in Scienze delle Investigazioni  Anno Accademico 2022/2023, II Anno, II Semestre  SSD IUS/16, CFU 5, ORE 30 |
| **Informazioni Docente** | Ing. Bruno Cesena.  Email: [bruno.cesena@unicz.it](mailto:bruno.cesena@unicz.it)  Orari di ricevimento: tutti i giorni delle lezioni previo appuntamento. |
| **Descrizione del corso** | Il corso ha l’obiettivo di fornire agli studenti le nozioni per l'applicazione dei principi e delle pratiche della scienza forense per la raccolta, l'esame, l'analisi e la presentazione di prove digitali. Il corso include argomenti selezionati dalla scienza forense digitale e dai domini della tecnologia dell'informazione. Esploreremo questi argomenti attraverso l'uso di vari strumenti forensi open-source e commerciali. Inoltre durante le lezioni verranno affrontati anche le problematiche inerenti l’identificazione, l’acquisizione, l’analisi e la reportistica di casi reali. |
| **Obiettivi del Corso e Risultati di Apprendimento attesi** | Al termine del corso gli studenti saranno in grado di:   * Comprendere e descrivere come la scienza forense viene applicata nell'ambito digitale; * Identificare e descrivere varie fonti di prove digitali; * Sapere come acquisire prove digitali da hard disk e dispositivi mobili * Comprendere i file system e gli artefatti; * Condurre analisi forensi sia delle immagini del disco, dispositivi mobili e Iot; * Identificare e descrivere i principi legali di base relativi alla digital forensics; * Acquisire ed analizzare prove digitali attraverso l’utilizzo di strumenti scientifici. |
| **Programma (contenuti, modalità di svolgimento).**  **Eventuale distinzione programma frequentanti – non frequentanti.** | * Domini della digital forensics * Definizione di Digital Forensics e Digital Evidence * ISO Standard * Il processo della digial forensics * La catena di custodia * Acquisizione forensi/write-blocking * Hashing * I formati forensi (DD, E01) * Partizionamento * File System FAT e NTFS * L'uso di immagini * LNK/Jumplists/Shellbags * Analisi dei dispositivi USB * Windows Events * Mobile Forensics * Introduzione alla forensics su Android e iOS * Introduzione alla Memory Analysis * Kali Linux Forensics * Kali Linux Mobile |
| **Stima dell’impegno orario richiesto per lo Studio individuale.** | 150 ore per gli studenti frequentanti.  200 ore per gli studenti non frequentanti. |
| **Metodi di insegnamento utilizzati** | Il corso prevede l’erogazione di lezioni frontali. Durante le lezioni saranno proiettate delle slides che al termine del corso saranno messe a disposizione degli studenti e costituiranno parte integrante degli appunti di lezione.  Potranno essere previsti seminari integrativi volti ad approfondire alcune delle tematiche affrontate durante le lezioni. |
| **Risorse per l’apprendimento (libri di testo consigliati, eventuali ulteriori letture consigliate per l’apprendimento, altro materiale didattico)** | Dispense e materiale inerente ai casi pratici trattati.  Consigliati:   * Il materiale di supporto e la bibliografia suggerita saranno disponibili sulla pagina web del docente * Libro: Nuove questioni di informatica forense a cura di Raffaella Brighi ISBN: 979-I2-5994-643-o |
| **Attività di supporto** | Seminari di approfondimento e presentazione di casi reali. |
| **Modalità di frequenza** | L'erogazione è prevista e strutturata nel II semestre e la frequenza, pur non avendo carattere obbligatorio, è vivamente consigliata in ragione del carattere tecnico specialistico della disciplina. |
| **Modalità di svolgimento dell’accertamento** | L’esame di profitto sarà svolto in forma scritta, con l’aggiunta di una eventuale e facoltativa prova orale.  Al fine di superare l’esame lo studente dovrà dimostrare di conoscere sufficientemente il programma nella sua interezza e di essere in grado di esprimerlo con un linguaggio soddisfacente sul piano sintattico e su quello tecnico. La mancanza totale o parziale di tali elementi basici comporterà la valutazione negativa della prova e dunque la non idoneità dello studente al superamento dell’esame. Una volta appurata invece la presenza di tali requisiti minimi, la valutazione finale dello studente, che sarà espressa in trentesimi (con voti da 18 a 30), verrà effettuata utilizzando i criteri di seguito riportati:   |  |  |  |  | | --- | --- | --- | --- | | **Votazione** | **Conoscenza e comprensione dell’argomento** | **Capacità di analisi e di sintesi** | **Utilizzo di referenze** | | Non idoneo | Importanti carenze.  Significative inaccuratezze | Irrilevanti. Frequenti generalizzazioni. Incapacità di  sintesi | Completamente inappropriato | | 18-20 | A livello soglia. Imperfezioni  evidenti | Capacità appena sufficienti | Appena appropriato | | 21-23 | Conoscenza routinaria | E’ in grado di analisi e di sintesi corrette. Argomenta in modo logico e  coerente | Utilizza le referenze standard | | 24-26 | Conoscenza buona | Ha capacità di analisi e di sintesi buone. Gli argomenti sono espressi  coerentemente | Utilizza le referenze standard | | 27-29 | Conoscenza più che buona | Ha notevoli capacità di analisi e di  sintesi | Ha approfondito gli argomenti | | 30-30L | Conoscenza ottima | Ha ottime capacità di  analisi e di sintesi | Importanti approfondimenti | |