

Principali informazioni sull'insegnamento	A.A. 2020/2021
Titolo insegnamento	Informatica Forense
Corso di studio	Laurea Magistrale in Sicurezza Informatica
Crediti formativi	06
Denominazione inglese	Digital Forensics
Obbligo di frequenza	No
Lingua di erogazione	Italiano

Docente responsabile	Nome Cognome	Indirizzo Mail
	Ugo Lopez	ugo.lopez@uniba.it
Luogo ed Orario di Ricevimento	Online su MS Teams dopo le lezioni e/o concordata con il docente	c/o sede Uniba – polo jonico al termine delle lezioni

Dettaglio credi formativi	Ambito disciplinare	SSD	Crediti
	Informatica	INF/01, ING-INF/05	06

Modalità di erogazione	
Periodo di erogazione	Primo Semestre
Anno di corso	II
Modalità di erogazione	In presenza e/o in DAD

Organizzazione della didattica	
Ore totali	48
Ore di corso	48 lezione in aula o in DaD
Ore di studio individuale	

Calendario	
Inizio attività didattiche	09/10/2020
Fine attività didattiche	08/01/2021

Syllabus	
Prerequisiti	Conoscenza dei principali algoritmi crittografici; conoscenza intermedia dei principali sistemi operativi e file system; conoscenza di base dei principali sistemi operativi e file system del mondo mobile; fondamenti di networking e architettura delle reti; fondamenti di web application; conoscenza generale dell'ordinamento giudiziario italiano
Risultati di apprendimento previsti (declinare rispetto ai Descrittori di Dublino) (si raccomanda che siano coerenti con i risultati di apprendimento del CdS, riportati nei quadri A4a, A4b e	Il corso si propone di formare i futuri professionisti della Digital Forensics, mettendoli in grado di conoscere modelli teorici e applicare tecniche scientifiche e rigorose, con un approccio metodologico conforme alle normative vigenti che cristallizzi gli elementi probatori digitali preservandone l'efficacia ai fini legali

A4c della SUA, compreso i risultati di apprendimento trasversali)	
Contenuti di insegnamento	<ul style="list-style-type: none"> • Definizione di Informatica Forense – Quadro normativo d’insieme e principali impianti normativi di riferimento (L.48/08, PCT, CAD, GDPR, diritto d’autore e proprietà industriale, diritto penale informatico, etc.) • I ruoli dell’informatico forense (Perito, CTP, CTU, CTPM, etc.) • Catena di custodia, integrità, autenticità e non ripudio • Hardware e Software specifici per l’informatica forense • Open Source vs Closed Source • Principali tipologie di evidenze informatiche e loro cristallizzazione (computer forensics, mobile forensics, cloud forensics, etc.) • Le fasi della Digital Forensics (acquisizione, conservazione, analisi, reporting) • Elementi di OSINT (Open Source INTelligence) – Elementi di estimo in ambito informatico • La costruzione della relazione tecnica.

Programma	
Testi di riferimento	<ul style="list-style-type: none"> • “Digital Forensics Basics”, Nihad A. Hassan, Apress, ISBN-13 (pbk): 978-1-4842-3837-0 • “Manuale del perito e del consulente tecnico nel processo civile e penale”, VIII edizione, Gennaro Brescia, Maggioli Editore, ISBN: 978-88-916-2901-2 • Materiale didattico fornito dal docente
Note ai testi di riferimento	
Metodi didattici	Didattica frontale, DaD/DDI, esercitazioni pratiche
Metodi di valutazione (indicare almeno la tipologia scritto, orale, altro)	Progetto di gruppo assegnato dal docente durante il corso, prova orale. Esonero orale a metà percorso.
Criteri di valutazione (per ogni risultato di apprendimento atteso su indicato, descrivere cosa ci si aspetta lo studente conosca o sia in grado di fare e a quale livello al fine di dimostrare che un risultato di apprendimento è stato raggiunto e a quale livello)	Al termine del corso, lo studente conoscerà i principali aspetti procedurali e le più note tecniche necessari a svolgere la professione dell’informatico forense, a supporto dei privati, della magistratura e degli organi inquirenti
Altro	