



Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	Informatica Forense	
Corso di studio	Laurea Magistrale in Sicurezza Informatica	
Anno Accademico	2022/23	
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)	06 CFU	
Settore Scientifico Disciplinare	INF/01, ING-INF/05	
Lingua di erogazione	Italiano	
Anno di corso	Secondo	
Periodo di erogazione	Secondo semestre	
Obbligo di frequenza	La frequenza è fortemente raccomandata	
Sito web del corso di studio	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica	

Docente/i	
Nome e cognome	Ugo Lopez
Indirizzo mail	ugo.lopez@uniba.it
Telefono	347/9395069
Sede	Dipartimento di Informatica - Sede di Taranto, Via Alcide De Gasperi
Sede virtuale	Piattaforma ADA - https://elearning.di.uniba.it/
Sito web del docente	
Ricevimento (giorni, orari e modalità, es. su appuntamento)	Su prenotazione: https://bookme.name/ugolopez/uniba Codice Teams del corso: q36q2wa

Syllabus



Obiettivi formativi	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
Prerequisiti	Le seguenti conoscenze preliminari facilitano ed accelerano la comprensione degli argomenti dell'insegnamento: <ul style="list-style-type: none">• Conoscenza informatica di base• Conoscenza dei rudimenti del diritto processuale penale e civile<ul style="list-style-type: none">o Si consiglia la lettura di:<ul style="list-style-type: none">o http://www.tribunale.reggiocalabria.giustizia.it/docs/80006750808/pagine/ALLEGATO_IL%20PROCESSO%20CIVILE...IN%20PILLOLE.pdf introduzione al diritto processuale civileo https://ripetiamodiritto.com/uncategorized/introduzione-all-a-procedura-penale/ introduzione al diritto processuale penale
Contenuti di insegnamento (Programma)	<p><u>INTRODUZIONE AL CORSO</u></p> <ul style="list-style-type: none">• Organizzazione del corso e informazioni generali• Materiale didattico• Organizzazione dell'esame• Orario e modalità di ricevimento <p><u>PARTE 1 – INTRODUZIONE ALL'INFORMATICA FORENSE</u></p> <ul style="list-style-type: none">• Definizione di informatica forense• Obiettivi dell'informatica forense• Esempi di casi mediatici• Principali categorie nell'informatica forense• Utenti dell'informatica forense• Il metodo scientifico• La prova digitale• La catena di custodia• Il processo di acquisizione della prova <p><u>PARTE 2 – PROCEDURA E NORMATIVA</u></p> <ul style="list-style-type: none">• La consulenza tecnica nel codice di procedura civile<ul style="list-style-type: none">o CTU e CTPo Procedure da seguireo Adempimenti e operazioni di consulenza tecnicao Verbale e relazioneo Cause di nullità della consulenzao Responsabilità del consulente• La perizia e la consulenza nel codice di procedura penale<ul style="list-style-type: none">o CTPM, Perito, Perito di parte, Ausiliarioo Principio di facoltatività della provao Poteri e facoltà del peritoo Valutazione della periziao Responsabilità del peritoo Incidente probatorioo Accertamenti tecnici ripetibili e non ripetibilio Verbale e relazioneo Cause di nullità della consulenza <p><u>PARTE 3 – L'INFORMATICA FORENSE</u></p>



- Concetti tecnici introduttivi
 - Rappresentazione dei dati
 - Hash
 - Tipi di memoria
 - Principali tipologie di file system
 - Networking

- Principali software e hardware per l'informatica forense
 - Principali Hardware per la Digital Forensics
 - Distribuzioni Linux
 - Software Open Source e gratuiti
 - Il valore probatorio dell'Open Source nella Digital Forensics
 - Software commerciali
 - Tecnologie di virtualizzazione
 - Laboratory Information Management System
 - Altro software

- La scena del crimine e l'acquisizione di elementi di prova
 - Strumenti dell'ausiliario
 - Ordine di volatilità
 - Documentare la scena del crimine
 - Trasporto delle periferiche digitali

- L'acquisizione della prova
 - Formato RAW
 - Acquisizione di memoria volatile
 - Acquisizione di memoria non volatile
 - Acquisizione di periferiche "non-standard" (NAS, HD cifrati, etc.)

- Fase di analisi
 - Analisi di periferiche di massa
 - Analisi di memoria RAM
 - Windows Forensics
 - Creazione di una timeline
 - Recupero di file cancellati
 - Data carving
 - Account utente
 - Analisi del registro di sistema
 - Analisi Windows non-standard (prefetch, thumbnail, Ink, etc.)
 - Web browser forensics
 - Email forensics

- Tecniche antiforensi
 - Steganografia
 - Distruzione di dati con tecniche antirecupero
 - Crittografia
 - Anonimizzazione
 - Tecniche antiforensi non-standard

- Open Source INTElligence (OSINT)
 - NATO Open Source Intelligence Handbook



	<ul style="list-style-type: none">o Open Source Datao Open Source INFORMATION (OSINF)o Open Source INTELLIGENCE (OSINT)o Validated OSINT (OSINT-V)o Il ciclo OSINT <p>Cenni su altri settori della Digital Forensics (Mobile Forensics, Network Forensics, Cloud Forensics, analisi celle telefoniche, etc.)</p>		
Testi di riferimento	<ul style="list-style-type: none">• “Digital Forensics Basics”, Nihad A. Hassan, Apress, ISBN-13 (pbk): 978-1-4842-3837-0<ul style="list-style-type: none">o Su questo libro, lo studente potrà studiare gli argomenti tecnici relativi alle <u>parti uno e tre</u> del programma• “Manuale del perito e del consulente tecnico nel processo civile e penale”, VIII edizione, Gennaro Brescia, Maggioli Editore, ISBN: 978-88-916-2901-2<ul style="list-style-type: none">o Su questo libro, lo studente potrà studiare gli argomenti relativi alla <u>parte due</u> del programma• Materiale didattico fornito dal docente <p>Gli studenti che lo desiderano possono ottenere i testi in prestito dalla Biblioteca. Può convenire verificarne la disponibilità mediante il Sistema Bibliotecario di Ateneo https://opac.uniba.it/easyweb/w8018/index.php? e contattare la biblioteca per concordare il prestito.</p>		
Note ai testi di riferimento			
Organizzazione della didattica			
Ore			
Totali	Didattica frontale	Pratica (laboratorio, progetto, esercitazione, altro)	Studio individuale
150 ore	48 ore		102 ore
CFU/ETCS			
06 CFU	06 CFU		

Metodi didattici	
	Lezioni frontali, presentazione casi d'uso

Risultati di apprendimento previsti	
--	--



Conoscenza e capacità di comprensione	<ul style="list-style-type: none">Lo studente avrà consapevolezza dell'ambito di applicazione dell'Informatica Forense, delle sue fasi, delle sue metodiche e dei limiti normativi e applicativi
Conoscenza e capacità di comprensione applicate	<ul style="list-style-type: none">Lo studente apprenderà le principali tecniche e metodiche dell'Informatica Forense con piena capacità di applicazione pratica
Competenze trasversali	<ul style="list-style-type: none">Autonomia di giudizio<ul style="list-style-type: none">Lo studente sarà in grado di classificare situazioni reali, applicando le tecniche più corrette caso per caso e cercando di estrarre il maggior numero di informazioni necessarie al fine della risoluzione del caso propostogliAbilità comunicative<ul style="list-style-type: none">Lo studente sarà in grado di realizzare relazioni e perizie sintetiche ed efficaci, in grado di illustrare anche a "non tecnici" (avvocati, magistrati, giuristi, periti di altre discipline, etc.) le analisi svolteCapacità di apprendere in modo autonomo<ul style="list-style-type: none">Lo studente, in un contesto in continua evoluzione, saprà affrontare situazioni "non-standard" con capacità e consapevolezza necessarie per reperire ed utilizzare ulteriori risorse di auto-formazione

Valutazione	
Modalità di verifica dell'apprendimento	Progetto assegnato dal docente + prova orale
Criteri di valutazione	<ul style="list-style-type: none">Conoscenza e capacità di comprensione: lo studente sarà valutato attraverso richiesta esposizione orale relativa alle parti procedurali del corsoConoscenza e capacità di comprensione applicate: agli studenti viene richiesto di realizzare un'applicazione in linea con gli obiettivi del corsoAutonomia di giudizio: verrà valutata attraverso l'analisi di casi di studio durante l'esposizione oraleAbilità comunicative: le proprietà di linguaggio e la precisione del lessico specifico costituiranno la modalità di valutazione durante la prova orale, così come l'analisi della qualità della documentazione a supportoCapacità di apprendere: verrà valutata attraverso l'analisi delle modifiche richieste dal docente all'applicazione realizzata
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	Il voto finale dell'esame è espresso in trentesimi. L'esame è superato con un voto minimo di 18/30. Il voto è determinato prendendo in considerazione completezza, correttezza e padronanza nell'esposizione degli argomenti trattati
Altro	Si suggerisce agli studenti di affidarsi esclusivamente alle informazioni/comunicazioni fornite sui siti ufficiali del Dipartimento di Informatica, ovvero sui gruppi social solo se costituiti e amministrati esclusivamente dai docenti dei relativi insegnamenti:



- <https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea>
- <https://www.uniba.it/it/ricerca/dipartimenti/informatica>
- <https://elearning.di.uniba.it/>

I programmi degli insegnamenti sono disponibili qui:

- <https://programmi.di.uniba.it/>

Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei Regolamenti didattici e manifesti degli studi disponibili nel sito:

- <https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea>

Si suggerisce agli studenti di diffidare delle informazioni e dei materiali circolanti su siti o gruppi social non ufficiali, poiché spesso sono risultati non affidabili, non corretti o incompleti. Per ogni dubbio, chiedere un incontro al docente secondo le modalità previste per il ricevimento.

- <https://elearning.di.uniba.it/>

- Contatto con il docente: canale MS Teams 1r9310u