

Principali informazioni sull'insegnamento	
Titolo insegnamento	Informatica forense
Corso di studio	Sicurezza Informatica
Crediti formativi	6 CFU
Denominazione inglese	Digital Forensics
Obbligo di frequenza	
Lingua di erogazione	Italiano

Docente responsabile	Nome Cognome	Indirizzo Mail
	Ugo LOPEZ	u.lopez@ugolopez.it

Dettaglio credi formativi	Ambito disciplinare	SSD	Crediti
		INF/01, ING-INF/05	6

Modalità di erogazione	
Periodo di erogazione	I semestre
Anno di corso	Il anno
Modalità di erogazione	Lezioni frontali

Organizzazione della didattica	
Ore totali	
Ore di corso	48
Ore di studio individuale	

Calendario	
Inizio attività didattiche	Inserire da segreteria
Fine attività didattiche	

Syllabus	
Prerequisiti	Conoscenza informatica di base, conoscenza dei rudimenti del diritto processuale penale e civile
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 A4c della SUA, compreso i risultati di apprendimento trasversali)	<ul style="list-style-type: none"> • <i>Conoscenza e capacità di comprensione</i> • <i>Conoscenza e capacità di comprensione applicate</i> • <i>Autonomia di giudizio</i> • <i>Abilità comunicative</i> • <i>Capacità di apprendere</i>
Contenuti di insegnamento	<u>INTRODUZIONE AL CORSO</u> <ul style="list-style-type: none"> • Organizzazione del corso e informazioni generali

- Materiale didattico
- Organizzazione dell'esame
- Orario e modalità di ricevimento

PARTE 1 - INTRODUZIONE ALL'INFORMATICA FORENSE

- 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

PARTE 2 - PROCEDURA E NORMATIVA

- La consulenza tecnica nel codice di procedura civile
 - CTU e CTP
 - Procedure da seguire
 - Adempimenti e operazioni di consulenza tecnica
 - Verbale e relazione
 - Cause di nullità della consulenza
 - Responsabilità del consulente
- La perizia e la consulenza nel codice di procedura penale
 - CTPM, Perito, Perito di parte, Ausiliario
 - Principio di facoltatività della prova
 - Poteri e facoltà del perito
 - Valutazione della perizia

- Responsabilità del perito
- Incidente probatorio
- Accertamenti tecnici ripetibili e non ripetibili
- Verbale e relazione
- Cause di nullità della consulenza

PARTE 3 –L'INFORMATICA FORENSE

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

	<ul style="list-style-type: none"> • Open Source INTElligence (OSINT) <ul style="list-style-type: none"> ○ NATO Open Source Intelligence Handbook ○ Open Source Data ○ Open Source INFormation (OSINF) ○ Open Source INTElligence (OSINT) ○ Validated OSINT (OSINT-V) ○ Il ciclo OSINT • Cenni su altri settori della Digital Forensics (Mobile Forensics, Network Forensics, Cloud Forensics, analisi celle telefoniche, etc.)
--	--

Programma	
Testi di riferimento	<p>“Digital Forensics Basics”, Nihad A. Hassan, Apress, ISBN-13 (pbk): 978-1-4842-3837-0</p> <p>“Manuale del perito e del consulente tecnico nel processo civile e penale”, VIII edizione, Gennaro Brescia, Maggioli Editore, ISBN: 978-88-916-2901-2</p> <p>Materiale didattico fornito dal docente</p>
Note ai testi di riferimento	
Metodi didattici	Lezioni frontali, lezioni laboratoriali, esercitazioni pratiche
Metodi di valutazione (indicare almeno la tipologia scritto, orale, altro)	Progetto assegnato dal docente + prova orale
<p>Criteria 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)</p>	<ul style="list-style-type: none"> • <i>Conoscenza e capacità di comprensione</i> Lo studente avrà consapevolezza dell’ambito di applicazione dell’Informatica Forense, delle sue fasi, delle sue metodiche e dei limiti normativi e applicativi • <i>Conoscenza e capacità di comprensione applicate</i> Lo studente apprenderà le principali tecniche e metodiche dell’Informatica Forense con piena capacità di applicazione pratica • <i>Autonomia di giudizio</i> 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 propostogli • <i>Abilità comunicative</i> 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,

	<p>etc.) le analisi svolte</p> <ul style="list-style-type: none">• <i>Capacità di apprendere</i> 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
Altro	