

Coordinatore:

Prof. Avv. Giovanni Ziccardi

Cattedre di «Informatica Giuridica» e «Informatica Giuridica Avanzata», Facoltà di Giurisprudenza, Università degli Studi di Milano

Direzione Scientifica:

Prof. Alessandro Boscato, *Università degli Studi di Milano*

Prof. Danilo Bruschi, *Università degli Studi di Milano*

Prof. Maria Teresa Carinci, *Università degli Studi di Milano*

Prof. Elena Ferrari, *Università degli Studi dell'Insubria*

Prof. Mario Jori, *Università degli Studi di Milano*

Prof. Gaetano Aurelio Lanzarone, *Università degli Studi dell'Insubria*

Prof. Cesare Maioli, *Università degli Studi di Bologna*

Prof. Andrea Rossetti, *Università degli Studi di Milano - Bicocca*

Prof. Giovanni Ziccardi, *Università degli Studi di Milano*

Corpo Docenti:

Esponenti del mondo accademico: Prof. Danilo Bruschi, *Professore Ordinario di sistemi operativi e sicurezza, Dipartimento di Informatica e Comunicazione, Università degli Studi di Milano, CLUSIT, Cert-It* – Prof. Maria Teresa Carinci, *Professore Ordinario di diritto del lavoro, Facoltà di Giurisprudenza, Università degli Studi di Milano* – Prof. Elena Ferrari, *Professore Straordinario di database systems e security, Dipartimento di Informatica e Comunicazione, Università degli Studi dell'Insubria* – Prof. Mario Jori, *Professore Ordinario di filosofia del diritto e informatica giuridica, Facoltà di Giurisprudenza, Università degli Studi di Milano* – Prof. Gaetano Aurelio Lanzarone, *Professore Ordinario di logica computazionale, sistemi intelligenti, epistemologia, deontologia ed etica dell'informatica, Dipartimento di Informatica e Comunicazione, Università degli Studi dell'Insubria* – Prof. Cesare Maioli, *Professore Ordinario di informatica giuridica, Facoltà di Giurisprudenza, CIRSFID, Università di Bologna* – Prof. Alessandro Boscato, *Professore Associato di diritto del lavoro, Facoltà di Giurisprudenza, Università degli Studi di Milano* – Prof. Andrea Rossetti, *Professore Associato di filosofia del diritto e informatica giuridica, Università degli Studi di Milano - Bicocca* – Prof. Giovanni Ziccardi, *Professore Associato di informatica giuridica e informatica giuridica avanzata,*

Facoltà di Giurisprudenza, Università degli Studi di Milano

– Prof. Luca Lupària, *Ricercatore in procedura penale, Facoltà di Giurisprudenza, Università degli Studi di Milano* – Dott.

Mattia Monga, *Ricercatore presso il Dipartimento di Informatica e Comunicazione, Università degli Studi di Milano* – Dott.

Pierluigi Perri, *Assegnista di Ricerca in informatica giuridica presso la Facoltà di Giurisprudenza dell'Università degli Studi di Milano*

– Dott. Ing. Antonio Savoldi, *Università degli Studi di Brescia, Facoltà di Ingegneria, Dipartimento di Elettronica per l'Automazione (DEA)* – Dott. Stefano Zanero, *Assegnista di Ricerca presso il Dipartimento di Elettronica e Informazione (DEI) del Politecnico di Milano*

Avvocati: Avv. Stefano Aterno, *Avvocato in Roma, Docente di informatica forense, Università La Sapienza, Roma* – Avv. Antonio Gammarota, *Avvocato in Bologna, Docente di informatica forense presso la Facoltà di Giurisprudenza dell'Università di Bologna* – Avv. Matteo Giacomo Jori, *Avvocato in Milano*

Esponenti delle Forze dell'Ordine: Ten. Col. Antonio Gorgoglione, *Polizia Tributaria di Milano* – Magg. Stefano Lombardi, *Polizia Tributaria di Milano* – Ten. Col. Cesare Maragoni, *Polizia Tributaria di Milano* – Magg. Ing. Marco Mattiucci, *RACIS, Arma dei Carabinieri* – Dott. Angelo Parente, *Direttore Tecnico Principale, Compartimento Polizia Postale e delle Comunicazioni per la Lombardia, Milano* – Dott. Sergio Russo, *Commissario Capo della Polizia di Stato, Responsabile del Settore Operativo del Compartimento Polizia Postale e delle Comunicazioni Emilia Romagna* – Dott.ssa Fabiola Treffiletti, *Vice Questore Aggiunto, Compartimento Polizia Postale e delle Comunicazioni per la Lombardia, Milano*

Magistrati – Dott. Gianluca Braghò, *Procura della Repubblica presso il Tribunale di Milano, pool reati informatici* – Dott. Francesco Cajani, *Procura della Repubblica presso il Tribunale di Milano, pool reati informatici* – Dott. Massimiliano Carducci, *Procura della Repubblica presso il Tribunale di Milano, pool reati informatici*

Professionisti e computer forensics expert:

Claudio Agosti, *ricercatore indipendente e computer forensics expert* – Dott. Donato Caccavella, *computer forensics expert, Docente di informatica forense, Facoltà di Giurisprudenza, Università di Bologna* – Dott. Gerardo Costabile, *Responsabile della Sicurezza Logica di Poste Italiane Spa e Presidente dell'Italian Chapter dell'IISFA - International Information Systems Forensics Association* – Andrea Ghirardini, *ricercatore indipendente e computer forensics expert* – Alberto Ornaghi, *ricercatore indipendente e computer forensics expert* – Alessio Pennasilico, *ricercatore indipendente e computer forensics expert*

Sede del corso

Università degli Studi di Milano

Facoltà di Giurisprudenza

Via Festa del Perdono n. 7

20122 Milano

Ammissione

Le domande di ammissione devono essere presentate nei termini e con le modalità previste dal bando disponibile sul sito <http://www.unimi.it/studenti/corsiperff/5411.htm>

Quota di iscrizione

La quota di iscrizione è di 750 Euro

Durata

Il corso di 70 ore si articola – nel periodo gennaio-marzo 2008 – su moduli giornalieri di 5 ore in aula il giovedì pomeriggio (14:00 – 19:00) e di 4 ore in laboratorio informatico il venerdì mattina (9:00 – 13:00).

Alla fine del corso verrà rilasciato dall'Università degli Studi di Milano un attestato di partecipazione dopo lo svolgimento di una prova finale e la verifica della frequenza.

Per informazioni

Presidenza della Facoltà di Giurisprudenza
Segreteria Didattica
Via Festa del Perdono, 7 – 20122 Milano
Tel. 02-5031.2473/2694/2087
Fax 02-5031.2475
infomaster.giurisprudenza@unimi.it
www.computerforensics.unimi.it



UNIVERSITÀ DEGLI STUDI DI MILANO
FACOLTÀ DI GIURISPRUDENZA

*Istituto di Filosofia e Sociologia del Diritto
Cattedre di «Informatica Giuridica» e «Informatica Giuridica Avanzata»*

2007 – 2008 prima edizione

Corso di perfezionamento in COMPUTER FORENSICS E INVESTIGAZIONI DIGITALI

Tecniche e strategie informatico-giuridiche
di gestione degli incidenti informatici

PROGRAMMA DEL CORSO

Gennaio 2008

INVESTIGARE: LE BASI

In aula: 1. Le basi di ogni strategia investigativa. La scena del crimine: analisi, interpretazione, *modus operandi*. La *forensics* come scienza. Le tecniche comuni, i principi di base, gli errori più ricorrenti. 2. Le strategie investigative tipiche della magistratura inquirente in ambito informatico, i principi generali di reperimento delle fonti di prova e la *forensics* durante le indagini preliminari. La *forensics* nella fase dibattimentale. 3. Teoria e prassi organizzativa e legale delle investigazioni informatiche aziendali. Le strategie investigative all'interno del tessuto aziendale, la prevenzione e la repressione dei comportamenti illeciti, l'individuazione dei responsabili, i rapporti con le Forze dell'Ordine e con le autorità.

In laboratorio: 4. Il computer, le memorie di massa e il *file system* in un'ottica investigativa: individuazione, repertazione, documentazione delle operazioni effettuate.

LA FORMAZIONE DEL COMPUTER FORENSICS EXPERT E LA COMPUTER FORENSICS ETHICS

In aula: 1. I percorsi accademici per la formazione del *computer forensics expert*. 2. Il percorso formativo professionale del *computer forensics expert*: competenze, certificazioni, iscrizione all'albo dei periti, formazione informatico-giuridica. 3. La *computer forensics ethics* e i comportamenti responsabili. I principi etici, i codici etici, le regole di comportamento, i rapporti con i colleghi, la concorrenza sleale.

In laboratorio: 4. Assicurare una fonte di prova. L'uso del software per la crittografia e la firma digitale, la firma dei *file* e dei supporti, il *time*

stamping, introduzione all'*hash*, i problemi di collisione del md5, la «firma» pratica di un *file* e di un supporto, la fissazione di un flusso di dati, l'uso di strumenti software e hardware.

IL COMPUTER, LE AZIONI DELL'INDAGATO E LA LORO ANALISI

In aula: 1. I mezzi di ricerca della prova sul luogo e sul computer di un indagato: ispezioni, perquisizioni e sequestri. Simulazione di un sequestro. Casistica relativa a materiale perdopornografico. 2. L'analisi forense delle immagini e dei video connessi allo sfruttamento sessuale dei minori: strategie di indagine, attività di contrasto, diffusione e detenzione. 3. I rapporti con le compagnie telefoniche e i *provider*, la gestione delle comunicazioni, dei tabulati, delle conversazioni, delle e-mail.

In laboratorio: 4. Il computer collegato in rete e l'analisi delle attività e del traffico di rete: la nozione di *file di log*, gli *Intrusion Detection System*, la ricostruzione temporale degli avvenimenti, l'interpretazione dettagliata su computer di terzi delle attività commesse.

Febbraio 2008

COMPUTER FORENSICS E AVVOCATURA

In aula: 1. La *computer forensics* per l'avvocato: aspetti maggiormente rilevanti. La *computer & network forensics* nell'ambito delle attività di investigazione difensiva.

In laboratorio: 2. Le attività di investigazione difensiva da un punto di vista tecnico. Il problema dell'accesso al materiale oggetto di indagine. Gli errori più comuni sulle analisi già effettuate. I rapporti con l'avvocatura e la magistratura nelle indagini difensive. I limiti etici nell'attività del tecnico.

IL SOFTWARE UTILIZZATO, LA PREPARAZIONE DELLA MODULISTICA, LE PRASSI E LE LINEE GUIDA

In Aula: 1. Illustrazione delle linee guida rilevanti e contestualizzazione in merito all'ordinamento italiano dei modelli internazionali di linee guida. I moduli delle *best practice*. Esempi di modulistica originale. La gestione della *timeline* e della catena di custodia.

In laboratorio: 2. Illustrazione delle distribuzioni *live* più comunemente adoperate per l'analisi forense e la stesura di perizie o di consulenze tecniche:

COMUNICAZIONI, MOBILE, CONSOLE E MP3 PLAYER FORENSICS

In aula: 1. La *mobile forensics*. Tutela delle comunicazioni, perquisizioni personali, la disciplina delle comunicazioni e della *privacy*, la *forensics* sui telefoni cellulari, sui palmari, sulle console e sugli MP3 player.

In laboratorio: 2. La *forensics* delle SIM/USIM card. Stato dell'arte e presentazione delle caratteristiche presenti in *tool* commerciali ed *open-source*; analisi fisica delle SIM/USIM card, estrazione della parte standard del *filesystem* da una SIM/USIM card ed interpretazione dei file standard, analisi della parte non standard di un *filesystem* di una SIM/USIM card, *data hiding* in una SIM/USIM e contromisure da adottare. 3. La *forensics* delle immagini digitali. Stato dell'arte dei *tool* usabili per occultare dati sensibili in un'immagine JPEG, applicazioni illecite derivanti dal *data hiding*, contromisure: la steganalisi delle immagini JPEG: 4. La *forensics* dei PDA e degli *smartphone*. Tecniche standard per acquisire gli elementi di prova. Tecniche di *antiforensics* utilizzate: approcci e soluzioni. Il problema del *data hiding* nel *firmware*: approcci e soluzioni.

Marzo 2008

LA COMPUTER FORENSICS NELLE DINAMICHE PROCESSUALI DELL'AVVOCATO: PERIZIE, CONSULENZE TECNICHE, ESAMI, CONTROESAMI

In aula: 1. Strutturazione, stesura e discussione di una perizia/consulenza tecnica in un giudizio penale in tema di *computer forensics*. 2. L'esame e il controesame nell'ottica del legale: quali domande porgere, come veicolare contenuti altamente tecnici e informatici in maniera fruibile per il giudice, come gestire e interpretare le eventuali trascrizioni. 3. Preparazione del proprio consulente tecnico all'esame e al controesame in udienza.

In laboratorio: 4. Analisi di un caso reale e

redazione di una perizia. Termini da utilizzare, concetti da evidenziare, informazioni superflue da evitare. Analisi comparata di diverse perizie in tema di *forensics*. Struttura del documento, obblighi e strategie nella redazione della stessa.

Ottava settimana

IL RAPPORTO CON L'INDAGATO E CON I PRESENTI SULLA SCENA DI UN CRIMINE TECNOLOGICO

In aula: 1. Le domande da porgere durante l'attività investigativa in loco, il primo rapporto con la vittima, *fac simile* di modelli utilizzati e di informazioni da documentare. 2. Gli interventi investigativi presso le aziende o i *provider* e le compagnie telefoniche. Richieste di tabulati relativi ad un'utenza telefonica, di flussi telematici, la fornitura delle informazioni da parte dei provider di telefonia e la loro interpretazione, analisi dei tabulati e dei *file di log*.

In laboratorio: 3. *Anti-forensics*, instaurazione di un canale di comunicazione crittografato non intercettabile, protezione delle informazioni con tecniche crittografiche o steganografiche.

Nona settimana

COMPUTER FORENSICS IN AZIENDA: TUTELA DEL DIPENDENTE E GARANZIE

In aula: 1. *Forensics* aziendale. Tutela del lavoratore nel corso delle investigazioni interne ed aziendali. Limiti di invasività del *software* e di azioni di controllo. Rapporto con le rappresentanze sindacali, lo statuto dei lavoratori e il Garante per la protezione dei dati personali.

In laboratorio: 2. Intercettazioni. Le intercettazioni di dati e di comunicazioni, gli strumenti *software* per il controllo delle attività del dipendente e della postazione.

Prima settimana

Terza settimana

Sesta settimana

Seconda settimana

Quarta settimana

Settima settimana

Quinta settimana