



CORSO di FORMAZIONE
in
Diritto penale dell'informatica
Anno Accademico 2009-2010

LEZIONE INAUGURALE DEL CORSO

Venerdi 8 gennaio 2010

Ore 15.30 – 19.30

Moderatore : Prof. Avv. Roberto Zannotti (Diritto penale, LUMSA)

Saluti – Autorità accademiche LUMSA

Saluti Consiglio dell'ordine avvocati di Roma, Presidente Avv. Alessandro Cassiani

Intervengono:

Prefetto Prof. Carlo Mosca (Consiglio di Stato, già Prefetto di Roma); Pres. Giorgio Lattanzi* (Presidente di sezione della Corte di Cassazione); Cons. Aniello Nappi (Consigliere della Corte di Cassazione); Cons. Domenico Carcano (Consigliere della Corte di Cassazione); Dott. Pietro Saviotti (Magistrato, Procuratore Aggiunto, Procura della Repubblica, Roma); Dott. Giuseppe Corasaniti (Magistrato, Sostituto Procuratore della Procura della Repubblica, Roma); Dott. Gianluca Braghò (Referendario Corte dei Conti, ex Pool Reati informatici Procura di Milano); Avv. Stefano Grassi (Direttore della Struttura Tutela Aziendale, Poste Italiane); Dott. Luigi Montuori (Dirigente dell'Autorità Garante per la protezione dei dati personali); Dott. Francesco Modafferi (Dirigente dell'Autorità Garante per la protezione dei dati personali); Ing. Cosimo Comella (Dirigente dell'Autorità Garante per la protezione dei dati personali); Dott. Domenico Vulpiani (Dirigente Generale Polizia di Stato), Dott. Antonio Apruzzese (Direttore del servizio della Polizia Postale e delle Telecomunicazioni); Dott. Sergio Mariotti (Dirigente Servizio Polizia postale e Telecomunicazioni); Dott. Andrea Rossi (Dirigente Compartimento Polizia Postale e Telecomunicazioni, Roma); Ing. Simone Tacconi (Servizio della Polizia Postale e delle Telecomunicazioni); Vice Questore Dott. Sergio Staro*(Servizio della Polizia Postale e delle Telecomunicazioni); Magg. Marco Mattiucci (Ra.Cis, Carabinieri); Maggiore Andrea Raffaelli (R.O.S. – Carabinieri); M.llo Capo Giorgio Ruggieri (R.O.S. – Carabinieri); Col. Umberto Rapetto (Guardia di Finanza, GAT); Dott. Gerardo Costabile (IISFA - International Information Systems Forensics Association); Ing. Rocco Mammoliti (Responsabile Protezione delle informazioni, TELECOM Italia); Ing. Gianfranco Ciccarella (Telecom Italia Sparkle spa); Dott. Fabrizio Marcelli (H3G); Avv. Anna Cataleta (H3G); Prof.ssa Fiammetta Mignella Calvosa (Università LUMSA); Prof. V. Luigi Mancini (Università di Roma "La Sapienza"); Avv. Mario Ianulardo; Avv. Stefano Aterno.

Modulo I

Dal 8.1.2010 al 29.1.2010 (6 gg/3 settimane)

con tavola rotonda

I REATI INFORMATICI

Responsabili del modulo : Prof. Avv. Roberto Zannotti, Avv. Stefano Aterno

Docenti: Prof. Roberto Zannotti, Dott. Giuseppe Corasaniti, Avv. Stefano Aterno, Avv. Francesco Catullo

PREMESSE SISTEMATICHE E DOGMATICHE SUI REATI INFORMATICI

- Le condotte informatiche;
- Il bene giuridico nei reati informatici;
- Il dolo "informatico";

LA CATEGORIA DEI REATI INFORMATICI

– Le fattispecie tipiche previste dal codice penale:

- *Delitti contro l'inviolabilità del domicilio "informatico":*

- Delitto di interferenze illecite nella vita privata (art. 615 bis cp);
- Delitto di accesso abusivo a sistema informatico e telematico (art. 615 ter);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater cp);
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies c.p.)

- *Delitti contro l'inviolabilità dei segreti e delle comunicazioni(art. 616 – 617quater e seguenti, cp):*

- Violazione, sottrazione e soppressione di corrispondenza (art. 616 cp); analisi con particolare riferimento alle problematiche sottese al controllo della posta elettronica e al controllo della navigazione Internet dei dipendenti (vedi anche Modulo Privacy);

- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (617 *quinquies* cp)
- Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617 *sexies* cp).

-Delitti contro il patrimonio - "informatico":

- Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* cp);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-*ter* cp);
- Danneggiamento di sistemi informatici o telematici (art. 635-*quater* cp);
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies* cp);
- Ipotesi di attacchi alle infrastrutture critiche del Paese. Le tutele previste nel nostro Paese e la situazione all'estero. Il ruolo del Cnaipc e la sicurezza informatica della Pubblica Amministrazione e dei sistemi informatici istituzionali più critici. Il ruolo e la strutture dei gestori e fornitori di telefonia e degli Internet Service Provider.

- Delitti contro il patrimonio : delitti di truffa, l e cd "truffe (frodi) informatiche":

- Frode informatica (art. 640 *ter* cp): analisi delle principali tipologie di frode *on line* (es clonazione delle carte di credito e di pagamento, alterazioni dei sistemi di pagamento on line, e altro ancora);
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* cp).

- Il Phishing, il Pharming, l' sms- ishing :

- Analisi del fenomeno, condotte tipiche e analisi tecnica dei diversi tipi di frode cd Phishing, ruolo dei soggetti coinvolti (Banche e Istituti di credito, Finanziarie, Pubblica Amministrazione, Siti internet di trading on line, aste on line). Analisi giuridica e tecnica del Pharming, e dell' sms- ishing;

- Cyberlaundering (riciclaggio di denaro sporco proveniente dal Phishing e dalle truffe informatiche on line);
- **Case study** (è prevista la partecipazione di magistrati, agenti delle Forze di Polizia ed ex appartenenti alla Guardia di Finanza che hanno partecipato alle più importanti operazioni Antiphishing degli ultimi anni);

- *Delitti di falso (informatico):*

- il concetto di documento informatico nel codice penale (art. 491 bis c.p.);
- falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri) (art. 495-bis c.p.);
- *analisi e studio di tutte le sentenze della Giurisprudenza di merito e della Corte di Cassazione relative ai suddetti delitti;*
- *casi giudiziari realmente accaduti (Case study);*

QUESTO MODULO PREVEDE UNA SERIE DI SIMULAZIONI E RELAZIONI SU CASI REALMENTE VERIFICATISI

TAVOLA ROTONDA n. 1 Venerdì 29.1.2010

“Il tema dei reati informatici con particolare riferimento al phishing e alle truffe informatiche”

Moderatori : Prof. Avv. Roberto Zannotti e Avv. Stefano Aterno

Intervengono: Avv. Stefano Grassi (Direttore della Struttura Tutela Aziendale, Poste Italiane), Dott. Fabrizio Marcelli (Information Security Manager, H3G) – Dott. Giuseppe Corasaniti (Procura di Roma), - Dott. Gerardo Costabile e Dott. Giuseppe Mazzaraco (IISFA-International Information Systems Forensics Association), – Responsabile sicurezza informatica di un importante Istituto di Credito

MODULO II

Sabato 30.1.2010

I REATI COMMESSI A MEZZO DI SISTEMI INFORMATICI E TELEMATICI

Responsabili del modulo : Prof. Avv. Roberto Zannotti, avv. Stefano Aterno

Docenti : Prof. Avv. Roberto Zannotti, Avv. Stefano Aterno

Docenti Ospitati : Dott. Diego Buso e Sost. Commissario Dott. Giovanni Ledda

- I Delitti di pedopornografia on line (art. 600 ter cp e seguenti); i concetti di detenzione, cessione e condivisione di file pedopornografici;
- Esame giuridico- tecnico dell'utilizzo di sistemi di condivisione on line e peer to peer (EMULE, KAZAA; analisi di fatti realmente accaduti su Chat, email, skype, ICQ, Messenger);
- Sostituzione di persona (art. 494 cp) : il cd furto d'identità. Analisi del fenomeno con riferimenti a fatti e ipotesi realmente accadute nel mondo delle Internet Community (email, mailing list, Ebay, Facebook, Second Life Linkedin, e altre);
- Utilizzo abusivo carte di credito e di altri sistemi di pagamento;
- Diffamazione a mezzo internet con particolare riferimento alla diffamazione a mezzo BLOG; riferimenti a case study in materia di contestazioni del reato di istigazione all'odio razziale;
- Estorsione e minacce a mezzo di sistemi informatici;
- Analisi delle nuove forme lecite e illecite del Gioco d'azzardo ON LINE;
- Istigazione all'odio razziale avvalendosi di strumenti e di pubblicazioni on line (Legge Mancino);

Modulo III

Dal 5.2.2010 al 19.2.2010

(5 gg / 2 settimane e mezzo)

con tavola rotonda

**PRINCIPI GENERALI SULLA PRIVACY E SUL TRATTAMENTO DEI DATI PERSONALI ; REATI
CONTRO LA RISERVATEZZA DEI DATI PERSONALI E DEI DATI SENSIBILI. SANZIONI PENALI
E AMMINISTRATIVE**

Responsabili del modulo : Prof. Avv. Roberto Zannotti, Avv. Stefano Aterno

Docenti : Dott. Luigi Montuori (Dirigente dell'Autorità Garante per la protezione dei dati personali), Ing. Cosimo Comella (Dirigente dell'Autorità Garante per la protezione dei dati personali), Dott. Francesco Modafferi (Dirigente dell'Autorità Garante per la protezione dei dati personali); Avv. Stefano Aterno

- Cenni sui principi generali del Codice sulla protezione dei dati personali (D.lgs 196 del 2003);
- Misure di sicurezza in ambito privacy: analisi e commento di alcune norme del codice privacy e dell'Allegato B (Documento Programmatico sulla sicurezza e protezione dei dati sensibili);
- Amministratori di sistema: perché e quali soluzioni tecniche per garantire la riservatezza?
- Alcuni provvedimenti del Garante Privacy in materia di amministratori di sistema, data retention, dati sanitari e dati sensibili, videosorveglianza; dati personali e libertà di stampa, consulenti e avvocati, indagini difensive ; direct marketing, marketing selvaggio, "rottamazione di un PC, istruzioni pratiche per una cancellazione sicura dei dati, sullo smaltimento dei rifiuti di apparecchiature elettriche ed elettroniche;
- I nuovi obblighi dei consulenti tecnici delle parti processuali in materia di trattamento dei dati processuali e degli atti di indagine;

- Il reato di trattamento illecito dei dati personali (art. 167 DLgs 196/2003): analisi della fattispecie, esame delle questioni problematiche; esame e studio della Giurisprudenza di merito e della Suprema Corte di Cassazione; le recentissime sentenze della Corte di Cassazione. Il nocumento e non solo; case study dei più importanti e noti fatti relativi all'illecito trattamento dei dati personali ed alle violazioni in materia di privacy;
- Il delitto di omessa adozione delle misure di sicurezza (art. 169 dlgs 196/2003);
- La data retention, normativa e sua applicazione : dal “decreto Pisanu (2005) al dlgs 109 del 2008 (direttiva Frattini: principi e definizioni); l'acquisizione dei tabulati di traffico telefonico e telematico; rapporti tra sicurezza e privacy.

TAVOLA ROTONDA n. 2 venerdì 19 febbraio 2010

“PRIVACY e BILANCIAMENTO DEGLI OPPOSTI INTERESSI: SICUREZZA E BUSINESS : c'è spazio per un equilibrio reale ed effettivo ?”

Moderatori : Dott. Luigi Montuori - Avv. Stefano Aterno

Interverranno: Dott. Francesco Modafferi (Nucleo attività ispettive Autorità Garante della privacy); Dott. Gerardo Costabile (Tutela Aziendale e Sicurezza Logica, Poste italiane), Dott. Pietro Saviotti (Procura della Repubblica di Roma); Dott. Alberto Cisterna (Magistrato, Direzione Nazionale Antimafia); Dott. Fabrizio Marcelli (Information Security Manager, H3G); Avv. Anna Cataleta (Privacy Manager, H3G); Dott. Sergio Mariotti (Servizio Polizia Postale - Cnaipc) - Dott. Andrea Rossi (Dirigente Compartimento di Roma Polizia Postale); ing. Rocco Mammoliti (Responsabile Protezione delle informazioni - TELECOM Italia);

Modulo IV

Inizio 20.2.2010 fino al 6.3.2010 (5 gg / 3 settimane e mezzo)

ELEMENTI BASE DI COMPUTER FORENSICS E SCIENZA DELL'INVESTIGAZIONE CON L'USO DI NUOVE TECNOLOGIE. LE INTERCETTAZIONI TELEFONICHE E TELEMATICHE

Responsabili : Prof. Avv. Roberto Zannotti, Avv. Stefano Aterno, Dott. Donato Caccavella, Dott. Gerardo Costabile

Docenti: *Prof. Dott. Donato Caccavella, Dott. Gerardo Costabile, Dott. Giuseppe Mazzaraco, Massimiliano Graziani;*

Docenti ospitati: *Ing. Gianfranco Ciccarella (Telecom Italia Sparkle spa– Executive Vice President); Magg. Andrea Raffaelli e M.Ilo Capo Giorgio Ruggieri (Arma dei Carabinieri Nucleo Tecnologico , R.O.S.);*

- Concetti elementari di informatica
- Concetti e semplici definizioni per comprendere cosa sono e come funzionano : i sistemi informatici, i virus, worm, spyware, i trojan, cookies, malware, gli active X, gli script dannosi e tante altri software;
- Cosa sono i file di LOG; i tabulati telefonici e telematici;
- L'importanza dell'indirizzo di Internet Protocol
- La crittografia: cos'è e come si utilizza, i software più comuni, segreti e problematiche; il suo rapporto con la protezione dei dati, come possibile strumento della criminalità e come strumento per la riservatezza dei documenti;
- Tecniche di intrusione e attacco ad un sistema informatico
- La rilevanza di una corretta analisi di "*computer forensics*";
- Come si acquisiscono con modalità forensi i dati di un computer; la network forensics;
- Il cd *tracciamento* delle e-mail e dei siti internet;

- Il concetto di prova informatica che resiste al giusto processo;
- Il sequestro del computer da parte dell' Autorità Giudiziaria;
- Il momento dell'acquisizione del contenuto del computer;
- Una corretta acquisizione e una corretta formazione della prova;
- Il sequestro e l'acquisizione di un sito web (esempio di scuola : un caso di diffamazione a mezzo web)
- La mobile e phone forensics;
- Le intercettazioni telematiche; concetto e analisi delle modalità tecniche di intercettazione di una email;
- Il ruolo del tecnico informatico e del responsabile della sicurezza fisica e informatica di una grande azienda dopo le recenti modifiche introdotte nella L. 231 del 2001 dalla legge 18 marzo 2008 n. 48;
- Strutturazione, stesura e discussione di una consulenza e di una perizia tecnica in un giudizio penale in tema di *computer forensics*;
- Intercettazioni informatiche e telematiche Voip – Skype;
- Il punto di vista dell'avvocato: le indagini e le strategie in materia di investigazioni difensive informatiche . Come cambia il ruolo del difensore;

QUESTO MODULO PREVEDE SIMULAZIONI IN AULA E DIMOSTRAZIONI SULL'USO DEGLI STRUMENTI D' INDAGINE DA PARTE DI CONSULENTI E FORZE DI POLIZIA - SIMULAZIONI DI UN ATTACCO INFORMATICO- SIMULAZIONE DI UN ATTACCO AD UN FILE CRIPTATO

Ing. Gianfranco Ciccarella (Telecom Italia Sparkle):

Sicurezza delle Reti:

- Introduzione ai problemi di sicurezza delle reti (attacchi di sicurezza, meccanismi di sicurezza, servizi di sicurezza, modello per la sicurezza di rete, metodi di difesa)
- Cifratura/Crittografia (il problema dell'autenticazione, cenni sugli algoritmi di cifratura/crittografia, posizionamento dei dispositivi di cifratura, crittografia a chiave pubblica)
- Autenticazione (servizio di autenticazione, firma digitale, certificati utente, procedure di autenticazione)
- Sicurezza IP e Web (approcci alla sicurezza per il protocollo TCP/IP, IP sec, applicazioni IP sec)

Modulo V

Dal 12.3.2010 al 27.3.2010 (6 gg / 3 settimane)

con n. 2 tavole rotonde

CENNI DI PROCEDURA PENALE IN TEMA DI INDAGINI INFORMATICHE

Responsabili : Prof. Avv. Roberto Zannotti, Avv. Stefano Aterno

Docenti: *Cons. Aniello Nappi (Consigliere di Cassazione); Dott. Pietro Saviotti (Procuratore Aggiunto, Roma), Dott. Francesco Cajani (Sostituto Procuratore, Procura di Milano), Dott. Pasquale Bronzo (Ricercatore, Università La Sapienza di Roma).*

Docenti Ospitati: M.Ilo Davide D'Agostino (Guardia di Finanza)

- Le nuove norme introdotte dalla legge n. 48 del 2008: esame e interpretazione del dettato normativo
- Le norme in materia di perquisizioni on line, sequestro e ispezioni di sistemi informatici e telematici
- Come cambiano le indagini informatiche delle forze di polizia ;
- Le prime sentenze dei tribunali di merito e della Corte Suprema di Cassazione
- Come cambia il ruolo delle parti processuali e dei loro consulenti davanti a questo tipo di reati
- La giurisdizione e la competenza territoriale nei reati informatici
- La pratica e la dottrina sulla prova scientifica in relazione all'acquisizione degli elementi di prova digitale

TAVOLA ROTONDA n. 3 venerdì 26.3. 2010

“Indagini informatiche, strumenti normativi e norme di garanzia ai sensi delle norme del codice di procedura penale e della giurisprudenza”

Moderano : il Prof. Avv. Roberto Zannotti e il Cons. Dott. Giuseppe Corasaniti (Pubblico Ministero, Roma).

Interverranno: Dott. Pietro Saviotti (Procuratore aggiunto, Roma), Dott. Francesco Cajani (Pubblico Ministero Procura di Milano); Pres. Giorgio Lattanzi* (Presidente di sezione della Corte di Cassazione); Dott. Gianluca Braghò (Referendario Corte dei Conti, ex Pool Reati informatici Procura di Milano); Magg. Marco Mattiucci (RACIS, Roma), Dott. Andrea Rossi (Dirigente del Compartimento Polizia Postale, Roma) ; Cons. Ercole Aprile (Magistrato, Tribunale di Lecce); Dott. Pasquale Bronzo (Ricercatore, Università di Roma, La Sapienza); Dott. Gerardo Costabile (Tutela Aziendale, Sicurezza Logica, Poste Italiane); Avv. Prof. Luca Luparia (Università di Milano); Avv. Paolo Galdieri; Avv. Stefano Aterno.

TAVOLA ROTONDA n.4 sabato 27.3. 2010

La prova scientifica “informatica”

Moderatore: Prof. Avv. Roberto Zannotti

Interverranno: Cons. Aniello Nappi (Consigliere della Corte di Cassazione); Cons. Domenico CARCANO (Consigliere di cassazione); Cons. Ercole Aprile (Magistrato Tribunale di Lecce); Cons. Rocco Blaiotta *(Consigliere di Cassazione); Dott. Gianluca Braghò (Referendario Corte dei Conti, ex Pool Reati informatici Procura di Milano); Prof. Avv. Pier Francesco BRUNO; Dott. Pasquale Bronzo (Ricercatore, Università di Roma, La Sapienza); Avv. Prof. Luca Luparia (Università di Milano);

Modulo VI

Dal 9.4.2010 al 30.4.2010 (7 gg /4 settimane)

COMPUTER FORENSICS AVANZATA e SCIENZA DELL’INVESTIGAZIONE INFORMATICA.

Analisi investigative digitali, esperienze delle forze di polizia e dei consulenti di parte

Responsabili : Prof. Avv. Roberto Zannotti, Avv. Stefano Aterno

Coordinatore: Dott. Gerardo Costabile (Poste Italiane – ex investigatore , m.llo Guardia di Finanza)

Docenti: Dott. Gerardo Costabile, Dott. Giuseppe Mazzaraco, Dott. Donato Caccavella, Massimiliano Graziani,

Docenti ospitati: Dott. Sergio Mariotti (Servizio Polizia Postale - Cnaipc); Dott. Andrea Ghirardini, Ing. Litiano Piccin, Dott. Andrea Mandarino (Polizia di Stato), Ing. Simone Tacconi (Servizio di Polizia Postale e delle Comunicazioni, Roma) ; Magg. Marco Mattiucci (RACIS, Roma);

- Information Forensics nel panorama giuridico internazionale ed italiano: le varie definizioni
- Modalità di acquisizione dei dati su hard disk
- Le linee guida internazionali e le differenze con il comparto italiano: IACIS guidelines
- La Chain of custody
- Acquisizione delle fonti di prova digitale sul web
- Incidente informatico aziendale: modalità di formazione delle prove
- Log files e accountability: l'uso della firma digitale
- I quesiti al consulente in Information Forensics
- Cenni all'Information Intelligence e motori semantici
- Case study italiani: caso Vierika, Fineco, Chieti etc
- Hashing: Md5 e Sha1
- Collisioni degli hash
- Blocchi hardware in scrittura
- Blocchi software
- Analisi di un sistema Windows
- Utilizzo di macchine VMWare per replicare il computer originale
- Registry: Tool e programmi per analizzare il database centralizzato di Windows nel migliore dei modi
- Particolarità dei file system supportati: Data Hiding e Alternative data stream
- Registry Event viewer
- File di swap
- Caching delle password

- Internet Explorer
- Outlook Express
- Metadata
- Case study: metodologia e processi in alcuni casi reali
- intercettazioni informatiche e telematiche Voip – Skype
- Progettare un laboratorio di information forensics
- Utilizzo dei seguenti software:
 - Helix Knoppix (parte Windows e Linux)
 - Raccolta di dati da un sistema Unix
 - Autopsy <http://www.digital-evidence.org/>
 - FTK <http://www.accessdata.com/products.htm>
 - Encase <http://www.encase.com/>
 - Ilook investigator
- Information forensics con Linux:
 - Sistema operativo Linux e fondamenti di informatica
 - Comandi utili per l'analisi forense: "awk", "sed", "grep", "find", "strings"
 - Linux: installazione e live cd
 - Tecniche di duplicazione di RAM e dischi
 - Boot con sistemi Linux Live CD, e l'uso di software come "dd", "dcfldd", "air" o "Adepto".
 - Acquisizione dischi RAID
- Sessione specifica Filesystem:
 - FAT: Il sedecimale dei sistemi Microsoft dal DOS sino a oggi
 - NTFS: File system avanzato derivato da HPFS usato dalla famiglia NT, 2k e Vista
 - ext2/3: File system classico di Linux
 - reiserfs: File system journaled usato in Linux

- UFS: Per i sistemi BSD
- ZFS: Sun Microsystem

CASE STUDY DI INFORMATION FORENSICS:

- Esame del layout del disco: sessione su come controllare la veridicità della partition table e verificare che non vi siano zone non assegnate dello stesso. Sono stati trattati i sistemi di indirizzamento CHS e LBA;
- Gestione a più livelli: E' stato mostrato quando effettuare una analisi a livello di raw device, di slack space e di file esadecimale. In tutti i casi vengono esaminati i pro e i contro delle singole scelte;
- Esame del file system: sia software forensi dotati di GUI (Autopsy Browser e phyflag sia i tool specifici per i più noti esadecimale oltre, naturalmente, alle utility che compongono lo sleuth Kit Raw Device Slack Space, Swap e Hibernation;
- Le tecniche di file carving per recuperare i dati dove fallisca l'analisi a livello di file system. Uso di editor esadecimale per l'esame del disco a basso livello;
- Comandi linux e programmi specialistici: come usare comandi specifici per trovare le informazioni necessarie ed estrapolarle dal contesto;

FORENSICS SU ALTRI MEDIA

CD e DVD:

Masterizzazioni single session e multisession

Multisession e analisi forense

Disaster recovery di un supporto ottico

FORENSICS DI *DEVICE* NON CONVENZIONALI

Macchine fotografiche digitali

Apple iPod

Sony PSP

Lettori mp3

Videocamere/videosorveglianza

NETWORK FORENSICS

Raccolta di reperti da una rete

Protocolli di rete e analisi del traffico

Indagini sui router

Security Event & Incident Management in Azienda

CASI ED ESPERIENZE SUL CAMPO DELLE FORZE DI POLIZIA (i casi saranno anonimizzati).

Qualche fuori programma divertente e interessante tipico del digital Forenseser.

Nota Bene: più volte, in altri casi, questi docenti hanno integrato il programma con esempi pratici dando spazio anche a sessioni di discussione su specifici temi particolarmente interessanti. I discenti hanno così potuto assistere a scuole di pensiero e metodologie analoghe anche con strumenti diversi.

Modulo VII

Dal 7.5.2010 al 15.5.2010 (4 gg/ 2 settimane)

Con tavola rotonda

INTERNET, COPYRIGHT E LA NORMATIVA PENALE SUL DIRITTO D'AUTORE

Responsabili : Prof. Avv. Roberto Zannotti, Avv. Prof. David Terracina

Docenti : Avv. Prof. David Terracina e Avv. Guido Scorza

- Principi e concetti generali della legge che protegge il diritto d'autore
- Il reato di illecita duplicazione di un'opera dell'ingegno protetta dalla LDA (art. 171 e ss della legge sul diritto d'Autore);
- Il reato di illecita duplicazione dei programmi per elaboratore (art. 171 bis LDA)
- Aspetti giuridici e tecnici del *Peer to Peer*. Utilizzo illecito dei diversi software esistenti: EMULE, KAZAA, Bittorrent, Imesh , Winmx .
- I DRM – *Digital Right Management*
- I creative commons e la diversa tutela del diritto d'autore
- Analisi e interpretazione delle recenti motivazioni della Giurisprudenza di merito e della Corte di Cassazione;
- Caso Peppermint;
- Cases Study

TAVOLA Rotonda n. 5 sabato 15 .5.2010 -

“Diritto d’autore, l’uso dell’Internet e delle nuove tecnologie : censure e divieti eccessivi o tutela della proprietà intellettuale?”

Moderatore : Avv. Prof. David Terracina

Interverranno: Dott. Giuseppe Corasaniti (Sostituto Procuratore, Procura di Roma), Vice Questore Dott. Sergio Staro *(Servizio della Polizia delle Telecomunicazioni); Prof. Giovanni Ziccardi*(Università Statale di Milano), Avv. Guido Scorza (Università di Roma, La Sapienza), Avv. Maurizio Mandel (SIAE)* (verranno invitati altri soggetti del mondo del software libero, associazioni dei consumatori e altre allo scopo di assicurare un ampio dibattito).

Modulo VIII

Dal 21.5.2010 al 29.5.2010 (4 g /2 settimane)

con tavola rotonda

LA RESPONSABILITÀ DEGLI ENTI IN ITALIA

Docenti: Prof. Avv. Roberto Zannotti, Avv. Prof. David Terracina

- La responsabilità degli enti in Italia. La legge 231 del 2001 e le modifiche successive;
- I reati previsti dalla legge 231 del 2001. In particolare i reati finanziari e contro la Pubblica amministrazione;
- Profili di diritto sostanziale: il problema dei gruppi di imprese;
- Modelli organizzativi e prevenzione dei reati. Le prime pronunce giurisprudenziali;
- L’organo di vigilanza previsto dalla l. 231 del 2001. Finalità, compiti e responsabilità dei componenti;
- L’attività investigativa e la tutela cautelare;
- Il ruolo dell’avvocato penalista nella preparazione del modello organizzativo;

TAVOLA ROTONDA n. 6 del 29.5.2010

“La Responsabilità penale dell’azienda e i modelli organizzativi: il punto di vista delle imprese”

Moderatori : Prof. Avv. Roberto Zannotti

Partecipano: Avv. Prof. David Terracina (Presidente, tra gli altri de l'Organo di Vigilanza ex L. 231/2001 PRADA spa); Avv. Stefano Grassi (Direttore della Struttura Tutela Aziendale, Poste Italiane); Dott. Gerardo Costabile (IISFA - International Information Systems Forensics Association); Responsabile auditing GESTORE TELEFONICO*; Ing. Rocco Mammoliti (Responsabile Protezione delle informazioni, TELECOM Italia); Avv. Anna Cataleta (Privacy Manager, H3G); Dott. Donato Caccavella (consulente tecnico); Responsabile sicurezza informatica (Istituto di Credito);

(E' prevista la partecipazione di importanti AZIENDE)

Modulo IX

Venerdi 4.6.2010

CRIMINALITA' INFORMATICA E PSICOLOGIA DEL CRIMINALE INFORMATICO

Docenti:

Cap. Andrea Ceccobelli (Guardia di Finanza – GAT) - Vice Questore Dott. Sergio Staro* (Servizio Polizia postale e Telecomunicazioni)

- Breve storia della criminalità della rete; gli hackers e la loro storia; i crackers ed altri generi di criminali informatici;
- Come si sta evolvendo la criminalità in Rete;
- Le grandi organizzazioni criminali;
- La lotta al cybercrime a livello internazionale; la cooperazione tra le forze dell'ordine.
- Le misure di contrasto;
- Un'esperienza ventennale nella lotta al cybercrime;

Modulo X

Sabato 5.6.2010

SOCIAL NETWORK : SECOND LIFE, FACEBOOK E ALTRI : DAL VIRTUALE AL REALE. LA CRIMINALITÀ SUI SOCIAL NETWORK E IPOTESI DI CONTRASTO E DI DIFESA

Responsabili : Prof. Avv. Roberto Zannotti, Avv. Stefano Aterno

Docenti : Dott. Alessandro Rossetti (GDF), Avv. Antonino Attanasio

e Avv. Mario Ianulardo

- I Social Network: quali sono, cosa sono, come funzionano e prospettive di sviluppo;
 - L'utilizzo dei social network per vari scopi: gli utilizzi leciti e quelli illeciti;
 - Condotte criminose, reati e indagini su Facebook e Second Life;
 - Anonimato e invisibilità degli Avatar su Second Life;
 - Analisi e commento dei regolamenti e delle clausole dei social network. Facebook, Second Life e altri;
 - Il processo e il sistema sanzionatorio su Second Life e su altri social network;
-
- I docenti contrassegnati con l'asterisco non hanno ancora confermato la loro presenza.
 - **E' in fase di organizzazione un evento di chiusura del corso con consegna degli attestati.**

NOTE ORGANIZZATIVE E REGOLAMENTARI:

Sede e Svolgimento delle lezioni

LUMSA ROMA - Facoltà di Giurisprudenza
Roma, Via Pompeo Magno, 22

Periodo e orario:

Gennaio 2010 – Giugno 2010

- 147 ore
- 41 giorni di lezione (tavole rotonde comprese)
- venerdì dalle 15.00 alle 19.00 - sabato dalle 9.15 alle 12.30

La frequentazione del corso consente il rilascio di:

- n. 24 crediti formativi per la professione forense rilasciati dal Consiglio dell'Ordine degli avvocati d Roma
- n. 42 CPE (Continuing Professional Education) per coloro che sono già certificati o che intendono conseguire Certificazioni internazionali
- CFU n. 25 crediti formativi universitari
- il corso è consigliato per la preparazione della certificazione CIFI

Iscrizioni:

-SCADENZA 4 GENNAIO 2010

L'ammissione al Corso, fino al raggiungimento del numero massimo di posti disponibili, avverrà sulla base della valutazione della documentazione pervenuta, secondo l'ordine di arrivo delle iscrizioni all'indirizzo comunicato;

La domanda di iscrizione, corredata della documentazione richiesta, dovrà essere inviata presso la segreteria APDI in via Tibullo 11, interno 15, Roma 00193.

Il modulo di iscrizione è disponibile sul sito www.lumsa.it (nell'area didattica - master e corsi di perfezionamento) <http://www.masterlumsa.it/corsi/corsi-formazione/diritto-penale-dellinformatica.html>

- sul sito dell' www.apdi.it
- e sul sito di IISFA www.iisfa.it
-

QUOTA DI ISCRIZIONE:

Il Costo: 2.100,00 euro (1600,00 per il corso e 500,00 per costi di segreteria ed amministrativi).

Sono previsti sconti sull'importo di euro 1.600,00 euro nel caso di iscrizioni cumulative o società/istituzioni che iscrivano più di un dipendente.

Lo sconto è del 20% sulla quota del secondo iscritto e di tutti gli iscritti successivi al primo.

Ottenuta l'iscrizione al Master, in caso di eventuale rinuncia, non si ha diritto alla restituzione delle rate pagate.

MODALITÀ DI PAGAMENTO:

- 1.600,00 euro (su richiesta pagabili in due rate) da versare sul c/c Bancoposta 99831786
IBAN: IT09P076010320000099831786
Intestato a: Associazione Avvocati penalisti d'impresa
Causale: Iscrizione Corso LUMSA in Diritto penale dell'informatica specificando nome e cognome iscritto;
- 500,00 euro da versare tramite bonifico bancario a favore di:
LUMSA – presso la Banca Monte dei Paschi di Siena Ag.
41 Cod **IBAN: IT 42 X 01030 03241 000000023140**
specificando nella causale nome e cognome e il titolo del corso.

Tutte le altre informazioni sono disponibili al sito www.apdi.it e www.lumsa.it (nell'area didattica - master e corsi di perfezionamento) <http://www.masterlumsa.it/corsi/corsi-formazione/diritto-penale-dellinformatica.html>

e scrivendo all'indirizzo email info@apdi.it

Direttore : Prof. Avv. Roberto Zannotti

Responsabile e coordinatore :

Avv. Stefano Aterno mobile : +39335 6795965 0632609427 s.aterno@studioaterno.it

Segreteria organizzativa del corso:

Avv. Clementina Arcuri mobile: +39349 2205355 segreteria@apdi.it

