



IISFA ITALIAN CHAPTER CORSO INTENSIVO DI COMPUTER & MOBILE FORENSICS

Milano : 23, 24, 25 Febbraio 2010

Roma : 20, 21, 22 Ottobre 2010

Durata : 3 giorni (24 ore di formazione)

ASPETTI TEORICI E LEGALI

Primo giorno, 9.00 – 11.00 (2 ore)

Relatori : GERARDO COSTABILE - DAVIDE D'AGOSTINO

1. Information Forensics nel panorama giuridico internazionale ed italiano: le varie definizioni
2. Sequestro, Ispezione e incidente probatorio nell'informatica forense.
3. Computer Forensics alla luce della Legge 18 marzo 2008, n. 48 di ratifica ed esecuzione della Convenzione di Budapest sulla criminalità informatica.
4. Modalità di acquisizione dei dati su hard disk
5. Le linee guida internazionali e le differenze con il comparto italiano: IACIS guidelines
6. La Chain of Custody
7. Le prove atipiche e la Computer Forensics
8. Acquisizione delle fonti di prova digitale sul web
9. Incidente informatico aziendale: modalità di formazione delle prove
10. Log files e accountability: l'uso della firma digitale
11. Consulente, Perito, CTP e CTU: differenze
12. I quesiti al consulente in Information Forensics
13. Cenni sulle modifiche legislative in studio
14. Cenni all'Information Intelligence e motori semantici
15. Case study italiani: caso Vierika, Fineco, Chieti ecc.

ASPETTI TECNICI BASE

Primo giorno, 11.00 – 13.00 (2 ore)

Relatori : MASSIMILIANO GRAZIANI – GIUSEPPE MAZZARACO

1. Hash: Md5, Sha1 e altri algoritmi
2. Collisioni degli hash, utilizzo del doppio algoritmo e verifica del disco in porzioni DD
3. Blocchi hardware e software in scrittura
4. Acquisizione di un hard disk (sia con software che con sistemi hardware)
5. La copia di cortesia in modalità Clever Copy (cosa è e come si realizza)
6. L'importanza dei riferimenti temporali, i metadati: esercizio pratico
7. Realizzare una Timeline e rappresentarla in modo pratico nella relazione
8. La relazione delle attività di Computer Forensics
9. Importanza della Chain of Custody: un modello pratico
10. Questa sezione comprende un pen drive USB con il materiale didattico.



TEORIA E PRATICA TECNICA

Primo giorno, 14.00 – 18.00 (4 ore)

Relatori : MASSIMILIANO GRAZIANI – GIUSEPPE MAZZARACO

1. Case study: metodologia e processi in alcuni casi reali
2. Progettare un laboratorio di information forensics
3. Utilizzo di alcuni software di acquisizione ed analisi forense
4. Come gestire le situazioni critiche ed impreviste
5. Il corredo minimo del Consulente Tecnico
6. Riepilogo delle Best Practices
7. Un caso con FTK
8. Un caso con ENCASE
9. Network Forensics con Silent Runner
10. Questa sezione comprende uno o più supporti ottici con il materiale didattico

TEORIA E PRATICA TECNICA

Secondo giorno, 9.00 – 11.00 (2 ore)

Relatore : ANDREA GHIRARDINI

1. Information forensics con Linux
2. Motivazioni della scelta
3. Linux: installazione e live cd
4. Tecniche di duplicazione di RAM: copia via firewire, guillotine, congelamento
5. Tecniche di copia dei dischi: copia in locale, su disco esterno, via rete
6. Acquisizione di sistemi RAID
7. Problematiche relative alle SAN
8. Boot con sistemi Linux Live-CD e l'uso di software come "dd", "dcfldd" e varianti
9. Accortezze da tenere e pregi delle distribuzioni live per la forensics
10. Sessione specifica Filesystem
11. FAT: Il filesystem dei sistemi Microsoft dal DOS sino a oggi
12. NTFS: File system avanzato derivato da HPFS usato dalla famiglia NT, 2k e Vista
13. ext2/3/4: File system classico di Linux
14. reiserfs: File system journaled usato in Linux
15. UFS: Per i sistemi BSD o ZFS: Sun Microsystem
16. OpenAFS, dal lato dell'analisi
17. Cenni su computer forensics su media non tradizionali, ipod, ps3, psp in particolare



CASE STUDY DI INFORMATION FORENSICS

Secondo giorno, 11.00 – 13.00 (2 ore)

Relatore : ANDREA GHIRARDINI

1. Esame del layout del disco: Si mostrerà come controllare la veridicità della partition table e verificare che non vi siano zone non assegnate dello stesso. Si tratteranno i sistemi di indirizzamento CHS e LBA, ma anche sistemi di protezione come HBA o full disk encryption.
2. Gestione a più livelli: Sarà mostrato quando effettuare una analisi a livello di raw device, di slack space e di file filesystem. In tutti i casi saranno esaminati i pro e i contro delle singole scelte.
3. Esame del file system: Si esamineranno sia software forensi dotati di GUI sia i tool specifici per i più noti filesystem oltre, naturalmente, alle utility che compongono lo Sleuth Kit e i normali comandi unix, sistemi di recupero dati, sistemi di analisi a basso livello, file carver.
4. Raw Device Slack Space, Swap e Hibernation: Si mostreranno le tecniche di file carving per recuperare i dati dove fallisca l'analisi a livello di file system. Si mostrerà l'uso di editor esadecimale per l'esame del disco a basso livello.
5. Comandi linux e programmi specialistici: Si mostrerà come usare comandi specifici per trovare le informazioni necessarie ed estrapolarle dal contesto.

ADVANCED FORENSICS

Secondo giorno, 14.00 – 18.00 (4 ore)

Relatore : ANDREA GHIRARDINI

1. Virtualizzazione:

- Virtualizzatori presenti sul mercato e particolarità
- Vmware Server
- Vmware ESX/ESXi
- Virtual Box
- Linux world (Qemu/KVM/XEN)
- Mac
- Fusion
- Parallels
- Gestione e uso delle macchine virtuali nell'analisi forensi
- Macchine virtuali e analisi forense
- Quando sono necessarie
- Trasformazione di immagini dd/raw in macchine virtuali
- Particolarità, dischi immutabili/indipendenti, snapshot
- Reti virtuali per la gestione dei malware

2. Log analysis:

- Raccolta e gestione
- Sistemi di analisi
- Sawmill
- Sed/awk/strings/perl e molti tool interessanti e sottovalutati
- Correlazione



LIVE FORENSICS

Terzo giorno, 09.00 – 11.00 (2 ore)

Relatore : DAVIDE GABRINI

1. On-site forensics: interventi su sistemi live e accertamenti d'urgenza.
2. Modalità operative durante gli interventi sul posto
3. Identificazione dei supporti durante le perquisizioni
4. Analisi live e post-mortem a confronto
5. Live forensics: best practices
6. Acquisizione di memorie volatili e accertamenti urgenti
7. Strumenti disponibili per sistemi Windows e Linux
8. Simulazione di intervento durante una perquisizione domiciliare
9. Windows Forensic Environment
10. Creazione di un live CD forense basato su Windows

ANTIFORENSICS

Terzo giorno, 11.00 – 13.00 (2 ore)

Relatore : DAVIDE GABRINI

1. Tecniche di anti-forensics e loro contenimento
2. Tecniche di distruzione dei dati
3. Tecniche di occultamento
4. Tecniche di falsificazione delle digital evidence
5. Altre tecniche di elusione
6. Contromisure e mitigazione delle tecniche discusse
7. Individuazione e analisi del malware

APPROFONDIMENTI - WINDOWS FORENSICS E FILE DI REGISTRO

Terzo Giorno, 14.00 – 16.00 (2 ore)

Relatore : LITIANO PICCIN

1. Strumenti di analisi a confronto: Encase - FTK (1.x/2.x/3.x) - X-WAYS
3. Windows REGISTRY: dove reperire le informazioni.

MOBILE FORENSICS

Terzo Giorno, 16.00 – 18.00 (2 ore)

Relatore : LITIANO PICCIN

1. Maneggiare e preservare i dispositivi mobili:
- FARADAYBAG, JAMMER, SIM CLONING
2. Strumenti usati per l'analisi dei dispositivi mobili:
- SOFTWARE: MOBILEEDIT/OXYGEN/DEVICE SEIZURE
3. Case Study "Forensics IPHONE"
4. JAILBREAK Copia fisica (realizzata e testata su firmware 3.0)



I RELATORI

Gerardo Costabile:

Responsabile della Sicurezza Logica (Tutela Aziendale) di Poste Italiane Spa, Presidente dell'Italian e dell'European Chapter e Vicepresidente dell'International Chapter dell'IISFA (International Information Systems Forensics Association – www.iisfa.it), no profit Association. Rappresenta altresì Poste Italiane Spa nel New York Electronic Crime Task Force (NYECTF) dell'United States Secret Service.

Member of “The International Association of Computer Investigative Specialists” (IACIS – www.cops.org), è stato per molti anni cybercop del Gruppo Repressione Frodi della Guardia di Finanza di Milano, occupandosi di indagini e “computer forensics” nel settore degli abusi tecnologici, nell'attività di contrasto al terrorismo, nazionale e internazionale, e nella formazione e cristallizzazione della c.d. “prova informatica”.

E' Certified Information Forensics Investigator (CIFI), Certified in the Governance of Enterprise IT (CGEIT) e AccessData Certified Examiner (ACE) riconosciute in ambito internazionale e conseguite rispettivamente presso l'IISFA International (www.iisfa.org), ISACA (www.isaca.org) ed AccessData.

Membro del Team che ha catturato 2 gruppi di hacker italiani che hanno attaccato computer della NASA e altre 1000 macchine governative e militari in tutto il mondo e gli unici 2 virus writer in Italia (Vierika e Zelig), uno dei quali definito dalle comunità scientifiche come il primo virus al mondo avente lo scopo di frodare soldi agli utenti con un ritmo di 1.200.000 euro al mese.

Membro dell'Antiphishing Working Group, ha partecipato alla prima indagine di phishing e cyberciclaggio in Italia (anno 2005), con arresti di cittadini dell'Est e con oltre 150 indagati.

Ha cooperato con Autorità governative, militari e di intelligence americane ed europee, quali ad esempio la NASA, l'US Army, l'US Navy, l'United States Secret Service e l'OLAF (Ufficio europeo per la lotta antifrode presso la Commissione Europea a Bruxelles) al fine di reprimere queste nuove forme di criminalità informatica transnazionale e frodi comunitarie.

Consulente tecnico per la Procura di Milano e Verona per attività di analisi forense sulle Digital Evidence e recupero di dati cancellati su Computer, Palmari e Mobile Phone Gsm e Umts, ha collaborato altresì con la DDA - Direzione Distrettuale Antimafia - e la DIA - Direzione Investigativa Antimafia - di Milano per attività coperte dal "Non Disclosure Agreement".

Cultore della materia presso l'Università La Sapienza di Roma (in informatica forense), docente presso il Consiglio Superiore della Magistratura e presso numerose Università, quali ad esempio quelle di Milano (Statale e Politecnico), Camerino, Roma (La Sapienza), Orvieto (Luiss), Potenza, European School of Economics (Milano) per master, cicli seminari, conferenze e lezioni agli studenti, con temi afferenti la Privacy, criminalità informatica, cybersecurity, cyberintelligence e computer forensics.

Ha collaborato e collabora altresì con riviste e pubblicazioni scientifiche, anche cartacee come ad esempio “Italiaoggi”, “Ciberspazio e Diritto”, il “Nuovo Diritto”, “Il diritto dell'informazione e dell'informatica”, con interventi sulla Privacy, sulla criminalità informatica, sull'analisi forense delle tracce informatiche e più in generale nel settore dell'informatica giuridica e giudiziaria.



Andrea Ghirardini:

Fondatore di Pila Security ora @PSS Srl, Computer Forensier per tutti i corpi di polizia italiani, lavora con oltre 50 Pubblici Ministeri e ha seguito oltre 300 casi che coinvolgono lotta alla criminalità organizzata ed eversiva, pedofilia, spaccio di droga, traffico d'armi, reati fiscali, omicidi e rapimenti. Relatore in numerose conferenze è anche l'autore del libro "Computer Forensics" edito da Apogeo, primo testo specifico pubblicato in Italia sull'argomento.

Giuseppe Mazzaraco:

Membro di "The International Association of Computer Investigative Specialists" (IACIS - www.cops.org) e "Phishing Incident Reporting and Termination (PIRT) Squad" (www.castlecops.com), si occupa di indagini e "computer forensics" nel settore delle frodi e degli abusi tecnologici, nell'attività di contrasto al Phishing, nazionale e internazionale, e nella formazione e cristallizzazione della c.d. "prova informatica".

E' Certified Information Forensics Investigator (CIFI) e Certified Fraud Examiner (CFE) conseguita presso l' Association of Certified Fraud Examiner www.acfe.org, Certified in the Governance of Enterprise IT (CGEIT) conseguita presso l'organizzazione internazionale ISACA e AccesData Certified Examiner (ACE).

Consulente tecnico per le Procure Italiane per attività di analisi forense sulle Digital Evidence e recupero di dati cancellati su Computer, Palmari e Mobile Phone, ha collaborato altresì con la DDA - Direzione Distrettuale Antimafia - e la DIA - Direzione Investigativa Antimafia - di Milano per attività coperte dal "Non Disclosure Agreement".

Membro del Team che ha catturato 2 gruppi di hacker italiani che hanno attaccato computer della Nasa e altre 1000 macchine governative e militari in tutto il mondo e gli unici 2 virus writer in Italia (Vierika e Zelig), uno dei quali definito dalle comunità scientifiche come il primo worm al mondo avente lo scopo di frodare soldi agli utenti con un ritmo di 1.200.000 euro al mese.

Ha cooperato con Autorità Governative, militari e di intelligence americane ed europee, quali ad esempio la NASA, l'US Army, l'US Navy, l'United States Secret Service e l'OLAF (Ufficio europeo per la lotta antifrode presso la Commissione Europea a Bruxelles) al fine di reprimere queste nuove forme di criminalità Informatica transnazionale e frodi comunitarie.



Massimiliano Graziani:

Consulente in Computer Forensics presso la Procura della Repubblica di Roma e Latina, Aziende di Pubblica Amministrazione e Private.

Attualmente Senior Security Consultant in Visiant Security.

È Certified Information Forensics Investigator (CIFI), Certified Fraud Examiner (CFE) conseguita presso l'Association of Certified Fraud Examiner www.acfe.org, OSSTMM Security Professional Analyst (OPSA) presso ISECOM www.isecom.org e AccesData Certified Examiner (ACE).

Ha conseguito il Master in Information Security Management del Politecnico di Milano (CEFRIEL), dove ha ideato e sviluppato il project work "E-Forensics Best Practices" e conseguito la qualifica internazionale IQNet Information Security Manager.

Attivo ricercatore antivirus sin dal 1990 (primo test comparativo sugli antivirus pubblicato in Italia nel 1994), è socio fondatore di IISFA Italian Chapter, membro di ACFE, dell'OWASP Italian Chapter e socio del CLUSIT. E' relatore per varie Associazioni e Università in materia di Computer Forensics, in particolare è orientato alla condivisione dei casi pratici nell'ottica del miglioramento continuo.

Davide Gabrini:

Da oltre 10 anni si guadagna da vivere grazie ai reati informatici altrui, occupandosi del contrasto a crimini informatici in senso proprio, alla pedopornografia (anche attraverso operazioni sotto copertura), allo spionaggio civile, al terrorismo e ad altre attività delittuose che coinvolgono a vario titolo reperti o tracce di natura informatica.

Ha svolto consulenze tecniche e perizie per diverse Procure e Tribunali ed è stato relatore e docente presso numerosi convegni di settore e corsi universitari.

E' attualmente impiegato presso la Polizia delle Comunicazioni di Milano, dove si occupa prevalentemente di ricerca e sviluppo, Digital Forensics e formazione del personale; è inoltre docente di sicurezza delle reti e di computer forensics presso Corsisoftware srl.

Nel 2008, ha guidato il team di analisti che ha vinto la competizione nazionale "Cybercop" organizzata da IISFA.

Davide D'Agostino:

Maresciallo capo della Guardia di Finanza che si occupa da anni di cyber crime. Ha condotto e coordinato una delle prime indagini in ambito internazionale che ha portato all'arresto di 29 persone (tra l'Italia e la Romania) dedite ad attività di phishing ai danni di importanti istituti di credito nazionali. Si è occupato, in passato, anche di pedopornografia on line e Cyber bullismo.

Litiano Piccin:

Netapp e VmWare System Admin presso il Centro Servizi CSE di San Lazzario di Savena (BO).

Consulente Tecnico presso la Procura della Repubblica di Bolzano.

E' relatore per varie Associazioni e Università in materia di Computer Forensics.



INFORMAZIONI CORSO:

In via del tutto eccezionale, chi si iscriverà al corso potrà accedere all'esame di certificazione CIFI gratuitamente. Per informazioni e per accedere all'esame a fine corso contattare Giuseppe Mazzaraco all'indirizzo certification@iisfa.it

CREDITI CERTIFICAZIONE

Il corso è valido ai fini della certificazione CIFI

SEDI

Milano : 23, 24, 25 Febbraio 2010 - Corsi Software Via Desenzano, 14*

Roma : 20, 21, 22 Ottobre 2010 - Sede da definire, verrà comunicata in tempo utile.

COSTO PER PARTECIPANTE:

900 euro - 1 giornata

1500 euro - 2 giornate

1900 euro - 3 giornate

250 euro - *Voucher esame CIFI (gratuito per chi effettua il corso).*

All'importo deve essere aggiunta l'IVA del 20%

SCONTI PARTICOLARI

- 20% di sconto per i soci IISFA
- 10% di sconto per i soci Clusit, ICAA, ISACA e AIPSA

Se si richiede la fattura devono essere forniti i seguenti dati:

Dati di fatturazione		
AZIENDA		P. IVA:
		C.FISCALE:
INDIRIZZO (Via, Piazza, e numero)		
CITTA'	Prov.	CAP
E-mail Azienda		Tel. Azienda

* *E' possibile raggiungere la sede dalla fermata Bande Nere della linea Rossa (MM1).*

Nel primo caso procedere in direzione Nordovest verso Via Anguissola; dopo 200 metri svoltare a sinistra per via Desenzano. Nel secondo caso procedere per Viale Caterina da Forlì; dopo 200 metri svoltare a sinistra per rimanere sul Viale; successivamente svoltare a sinistra per via Desenzano.



MODALITÀ DI ISCRIZIONE E PAGAMENTO

Per iscriversi bisogna contattare l'organizzazione all'indirizzo **webmaster@iisfa.it** ed inviare i nominativi dei discenti, per confermare l'iscrizione si dovrà effettuare il pagamento prima dello svolgimento del corso, a mezzo bonifico bancario alle seguenti coordinate:

- **Intestataro del conto corrente** Banco Posta: Information Systems Forensics Association Italian Chapter
- **IBAN: IT98 I076 0103 2000 0008 3548 909**

Nella causale deve essere specificato quanto segue:

“partecipazione al corso IISFA del dd/mm/aaaa Nome e Cognome”.

La ricevuta di avvenuto pagamento dovrà essere inviata all'indirizzo di mail **secretary@iisfa.it** o al numero di fax 178 270 85 06 all'attenzione della Segreteria IISFA.

Il presente modulo è ordine formale e impegnativo di partecipazione al seminario; quindi dovrà pervenire presso ISFA Italian Chapter, anche via fax, entro e non oltre il decimo (10°) giorno precedente l'inizio del corso.

Ogni tipo di modifica andrà comunicata per iscritto, anche via fax.

La conferma di erogazione del seminario avverrà via e-mail da parte di ISFA Italian Chapter entro 5 giorni lavorativi prima della data di inizio dello stesso e conterrà tutte le informazioni relative alla sede in cui il seminario verrà svolto.

Fatturazione:

La fatturazione avverrà al ricevimento del pagamento.

Annullamento e mancata partecipazione.

L'iscrizione al seminario viene ritenuta definitiva al ricevimento del pagamento. Un'eventuale successiva comunicazione di annullamento della partecipazione del corso deve essere effettuata per iscritto e non oltre i 5 giorni lavorativi prima della data di inizio dello stesso. Oltre tale termine sarà trattenuta la quota di iscrizione.

Riserva per numero minimo:

IISFA Italian Chapter si riserva il diritto di cancellare il corso se i partecipanti iscritti non raggiungessero il numero sufficiente, dandone avviso sul sito www.IISFA.it o a mezzo e-mail. In questo caso la responsabilità di IISFA Italian Chapter sarà limitata alla restituzione dell'importo pagato.