IISFA ITALIAN CHAPTER
CORSO INTENSIVO DI COMPUTER & MOBILE FORENSICS
Roma 10-11-12 Novembre 2010

Durata : 3 giorni

COMPUTER FORENSICS
Primo giorno, 9.00 – 13.00 (4 ore)
Relatori : MATTIA EPIFANI – GIUSEPPE MAZZARACO

- Definizione di Computer Forensics
- Prova digitale
- Passi operativi in Computer Forensics:
  1. **Identificazione** (Hard disk e file system, SSD, NAS, floppy disk, ZIP/JAZ, CD/DVD, Usb, Memory Card, MP3, videocamere, fotocamere, ecc.)
  2. **Acquisizione** (best practises per computer acceso, best practises per computer spento, linee guida internazionali, copia forense, acquisizione hardware, acquisizione software, write blocker hardware e software, verifica dell'integrità, demo di acquisizione)
  3. **Conservazione** (catena di custodia, trasporto e conservazione delle prove)
  4. **Analisi** (toolkit forensi commerciale e opensource, data recovery, analisi dei principali sistemi operativi, registro di configurazione di Windows, navigazione su Internet, posta elettronica, cronologia chat e IM, documenti e metadati, thumbnails, P2P, registro eventi, volumi cifrati, ambienti virtuali, ecc.)
  5. **Valutazione e Presentazione**
- Il laboratorio forense

ASPETTI TECNICI PRATICI
Primo giorno, 14.00 – 18.00 (4 ore)
Relatori : MASSIMILIANO GRAZIANI – DAVIDE D'AGOSTINO

- Collisioni degli hash MD5 E SHA1
- Differenza tra dati e metadati, importanza dei riferimenti temporali
- Software e hardware per acquisizione forense, open source e freeware vs professional
- Hardware professionali in dotazione alle FF.OO.: il Logicube Dossier
- Hardware Tableau T35es, T4, T8 e accessori utili
- Cellebrite UFED per la Mobile Forensics
- Un caso veloce: dall'acquisizione all'analisi
- Case study: metodologia e processi in alcuni casi reali
- Progettare un laboratorio di information forensics in pratica
- I software di acquisizione ed analisi forense
- Un modello pratico della Chain of Custody
- Un modello pratico per la Relazione
- Come gestire le situazioni critiche ed impreviste
- Il corredo da campo, il minimo del Consulente Tecnico
- Riepilogo delle Best Practices

CASE STUDY DI INFORMATION FORENSICS
Secondo giorno, 09.00 – 13.00 (4 ore totali)
Relatore : DAVIDE GABRINI

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 disck encryption.
2. Gestione a più livelli: Sarà mostrato quando effettuare una analisi a livello di raw device, di slack space e di file filsystem. 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 esadecimali 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.

LIVE FORENSICS

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

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
Secondo Giorno, 14.00 – 18.00 (4 ore totali)
Relatore : LITIANO PICCIN

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

MOBILE FORENSICS

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

TEORIA E PRATICA TECNICA
Terzo 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

ADVANCED FORENSICS
Terzo giorno, 11.00 – 16.00 (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 analisys:

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

ESAME CIFI
Terzo giorno, 16.00 – 18.00 (2 ore)
Relatore: GIUSEPPE MAZZARACO

PREPARAZIONE ALL'ESAME E SESSIONE DI ESAME CIFI

Ai discenti sarà fornito il materiale del corso su supporto digitale USB

I RELATORI

Andrea Ghirardini:

Fondatore di Pila Security ora @PSS Srl, Computer Forenser 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), Certified in the Governance of Enterprise IT (CGEIT) 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). 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.
E' membro fondatore di IISFA Italian Chapter e dell'OWASP Italian Chapter.

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.

Massimiliano Graziani:

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

È Certified Information Forensics Investigator (CIFI), Certified Fraud Examiner (CFE), OSSTMM Security Professional Analyst (OPSA) 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.

E' membro fondatore di IISFA Italian Chapter e dell'OWASP Italian Chapter, membro di ACFE, e socio del CLUSIT. E' relatore per varie Associazioni e Università, docente presso la Scuola PT della Guardia di Finanza in materia di Computer Forensics.

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.

Mattia Epifani:

Socio della REALITY NET - System Solutions, azienda di consulenza informatica con sede a Genova, dove si occupa di informatica forense, networking, consulenza in materia di sicurezza informatica e formazione (networking, sicurezza, computer forensics, ethical hacking, sistemi operativi). Laureato in Informatica nel 2002 presso il Dipartimento di Informatica e Scienze dell'Informazione dell'Università degli Studi di Genova. Negli ultimi anni ha frequentato il Corso di Perfezionamento in Computer Forensics dell'Università Statale di Milano e ha conseguito certificazioni in materia (CIFI, CCE, CEH, CHFI, CEI, ACE, ECCE). Ha tenuto diversi seminari e corsi in materia e ha pubblicato alcuni articoli su libri e riviste.

INFORMAZIONI CORSO:

CREDITI CERTIFICAZIONE
Il corso è valido ai fini della certificazione CIFI

QUANDO e DOVE
A Roma il 10, 11 e 12 presso ELEA in Via Lucrezio Caro, 63

Dall'aeroporto di Fiumicino: treno navetta per Roma Termini; proseguire in Metropolitana (A).

Dalla stazione FS Termini: Metropolitana (A) direzione Battistini; scendere alla fermata LEPANTO. Proseguire lungo Via Cicerone e girare poi a sinistra verso Via Lucrezio Caro.

COSTO PER PARTECIPANTE:

€ 900,00 euro *– 1 giornata*
€ 1500,00 euro *– 2 giornate*
€ 1900,00 euro *– 3 giornate*
€ 250,00 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

MODALITÀ DI PAGAMENTO

Il pagamento può essere effettuato a mezzo bonifico bancario alle seguenti coordinate:

- ***Intestatario 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".

Oppure tramite il form di pagamento elettronico presente nel sito www.iisfa.it nella sezione ISCRIZIONE / PAGAMENTI.

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 e ove specificatamente richiesto applicando l'IVA normale.

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.

Variazione programma:
IISFA Italian Chapter si riserva il diritto di variare il programma del corso in qualsiasi momento.