Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Programma prima giornata, 18 febbraio 2019

"Introduzione alla Digital Forensics"

Docente: **Nanni Bassetti**

Parte prima

- Panoramica sulle Best Practices
- Non modificare la prova
- Analisi live e post (i perchè, pro e contro)
- Identicità della prova

Parte seconda

- Hash, cosa sono, collision e pre-image attack
- Catena custodia, nella teoria e nella realtà
- Ripetibilità delle operazioni
- Write blocker

Parte terza

- Gli strumenti della Computer Forensics – open source vs commerciale
- Le quattro fasi (Identificazione, acquisizione, analisi, reporting) in pratica.

Parte quarta

- CAINE forensic GNU/Linux distro per la digital forensics
- Cenni sulla legge 48/2008

Via Aurelio Carrante, 1/F
70124 Bari - ITALY
T. +39.080.2229894 F. +39.080.2229886
E-mail: gruppo@ugolopez.it

Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Il docente

Nanni Bassetti è Laureato in Scienze dell'Informazione a Bari ed è libero professionista specializzato in informatica forense. Ha collaborato come free-lance con molte riviste informatiche nazionali e internazionali e come docente per molti corsi presso enti, scuole e università, ha inoltre scritto articoli divulgativi di programmazione, web usability, sicurezza informatica e digital forensics.

Ha lavorato come ausiliario di Polizia Giudiziaria e per alcune Procure della Repubblica oltre che come CTU/CTP per molte analisi forensi informatiche civili e penali. Iscritto all'albo dei C.T.U. presso il Tribunale di Bari, è consulente di parte civile per alcuni casi di risonanza nazionale. Fondatore di CFI – Computer Forensics Italy – la più grande community di computer forensics italiana e segretario di ONIF (Osservatorio Nazionale Informatica Forense).

Project manager di Caine Linux Live Distro forense. Curatore del sito Scripts4cf dedicato a software per la computer forensics. Ha pubblicato "Internet Web Security – tutta la verità sulla sicurezza del web" nel 2004 con la Duke Editrice e il libro "Indagini Digitali". Fa parte del Comitato di Redazione della rivista "Sicurezza e Giustizia", su cui ha pubblicato diversi articoli.

Via Aurelio Carrante, 1/F
70124 Bari - ITALY
T. +39.080.2229894 F. +39.080.2229886
E-mail: gruppo@ugolopez.it

Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Programma seconda giornata, 19 febbraio 2019

"La Perizia Informatica con casi reali

Analisi con Ufed ed Axiom"

Docente: **Michele Vitiello**

- Il Consulente Informatico Forense
- Il Consulente Tecnico D'Ufficio – CTU
- Il Consulente Tecnico di Parte - CTP
- Il Consulente Tecnico del Pubblico Ministero – CTPM
- L'ausiliario di Polizia Giudiziaria
- Il Perito del Giudice
- Perquisizione Informatica
- Ispezione Informatica
- Acquisizione E-mail dal Cloud
- Copia Forense di memorie di massa
- Copie Forensi di dispositivi mobili
- Corretta modalità di produzione in giudizio di dati contenuti in dispositivi mobili
- Casi reali di redazione di Perizie Informatiche

Cenni alla modalità di lettura della memoria di dispositivi mobili

- Fisica
- File System
- Logica
- Estrazione dati SIM Card
- Estrazione dati Schede SD

Via Aurelio Carrante, 1/F
70124 Bari - ITALY
T. +39.080.2229894 F. +39.080.2229886
E-mail: gruppo@ugolopez.it

Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

- Dispositivi bloccati o danneggiati
- Recupero codice di sblocco
- Passware
- UFED Unlock tool
- Tecnica Chip-off
- Dettagli sui Sistemi Operativi
- Android
- ADB
- Procedura di root
- Custom recovery
- iOS
- Elcomsoft Cloud
- Windows Phone
- Analisi dei dump

Generazione dei report con UFED ed AXIOM nei vari formati

- Report in formato PDF
- Report in UFED Reader
- Come effettuare ricerche
- Come impostare filtri
- Creare e gestire i tag
- Creare report filtrati

Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Il docente

Socio fondatore ONIF, **Michele Vitiello** si è laureato in Ingegneria delle Telecomunicazioni presso l'Università di Pisa, si è perfezionato post Laurea presso l'Università di Milano in Computer Forensics e Investigazioni Digitali.

Componente della Commissione Ingegneria Forense dell'Ordine degli Ingegneri della provincia di Brescia, è iscritto all'Albo dei Periti n° 110 e all' Albo dei CTU n° 844 del Tribunale di Brescia; opera altresì come Consulente Tecnico di Parte, Ausiliario di Polizia Giudiziaria e Consulente Tecnico della Procura della Repubblica.

I servizi di Consulenza Informatica Forense, si rivolgono a Privati, Aziende, altri Consulenti, Studi Legali, Procure e Forze dell'Ordine in tutti i Tribunali d' Italia.

È membro dell'IISFA (International Information Systems Forensics Association) e di DFA (Digital Forensics Alumni).

È il titolare dell'omonimo Studio di Ingegneria Informatica Forense, con sede principale a Brescia: insieme con il suo team effettua Consulenza Tecnica e Corsi di Formazione in Computer Forensics e Investigazioni Digitali, Perizie Informatiche, Foniche, Video/Fotografiche, Trascrizione Intercettazioni e Telecomunicazioni.

Lo studio da alcuni anni ha esteso la propria attività in partnership con il Centro Recupero Dati da qualsiasi supporto di memoria.

Lo studio ha una sede anche a Milano ed è operativo direttamente e con una rete di collaboratori su tutto il territorio nazionale.

Via Aurelio Carrante, 1/F
70124 Bari - ITALY
T. +39.080.2229894 F. +39.080.2229886
E-mail: gruppo@ugolopez.it

Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Programma terza giornata, 20 febbraio 2019

"Analisi Forense di Foto e Video Digitali"

Docente: **Massimo Iuliani**

Introduzione

Quando i contenuti multimediali (immagini digitali, flussi video, tracce audio) diventano possibili fonti di prova, la loro corretta analisi permette l'accesso a molteplici informazioni relative al dato digitale e al suo contenuto semantico.

Seguire un'appropriata metodologia per l'investigazione digitale consente di conoscere la storia del contenuto multimediale: attraverso l'applicazione di tecnologie di Multimedia Forensics è possibile risalire al dispositivo di acquisizione, conoscere la data e il luogo di acquisizione, verificare l'autenticità del dato digitale e determinare eventuali falsificazioni, migliorare l'intelligibilità del contenuto ed estrarre importati informazioni semantiche.

Dettaglio argomenti

- Il dato digitale come possibile fonte di prova: integrità e autenticità
- La catena di custodia di foto e video digitali
- Metodologia per l'investigazione digitale dei contenuti multimediali
- Analisi dei metadati e del formato dei dati
- Analisi audio-visuale
- Identificazione del dispositivo sorgente
- Verifica autenticità
- Miglioramento e analisi dei contenuti
- Sessione pratica: estrazione e analisi metadati; identificazione del dispositivo sorgente; verifica di autenticità; miglioramento e analisi dei contenuti

Via Aurelio Carrante, 1/F
70124 Bari - ITALY
T. +39.080.2229894 F. +39.080.2229886
E-mail: gruppo@ugolopez.it

Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Il docente

Massimo Iuliani lavora come consulente tecnico al FORLAB, il Laboratorio di Multimedia Forensics (www.forlab.org) del PIN s.c.r.l. - Servizi didattici e scientifici per l'Università di Firenze. Le sue attività principali riguardano la formazione delle Forze dell'Ordine e di operatori forensi e la consulenza per l'analisi di contenuti multimediali (immagini digitali, tracce audio e sequenze video) per scopi forensi.

In parallelo lavora come assistente alla ricerca nel campo della elaborazione delle immagini per la sicurezza e applicazioni forensi, presso il Dipartimento di Ingegneria dell'Informazione dell'Università degli Studi di Firenze.

Dal 2012, come responsabile tecnico del FORLAB ha completato indagini forensi di numerosi contenuti audiovisivi, che coprono una vasta gamma di casi, tra i quali: la verifica dell'autenticità di documenti scansionati; la verifica dell'autenticità di immagini e video digitali; la sincronizzazione tra le registrazioni audio e video provenienti da sorgenti indipendenti; il miglioramento intelligibilità di file audio da registrazioni e intercettazioni ambientali; la datazione di immagini digitali provenienti da dispositivi sequestrati; la verifica dell'integrità di registrazioni audio; estrazione di misure fotogrammetriche da sequenze video di sorveglianza.

Da dicembre 2017 è socio ordinario dell'**Osservatorio Nazionale di Informatica Forense** (ONIF) attraverso il quale è in contatto con esperti di tutte le diramazioni della Digital Forensics.

Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Programma quarta giornata, 21 febbraio 2019

"Analisi delle celle e tabulati"

Docente: **Paolo Reale**

1. INTRODUZIONE ALLA RETE GSM

- Cenni storici
- Schema della rete GSM
- Mobile Station
- Configurazione e copertura delle celle
- Procedure e caratteristiche reti 2G, 3G e 4G

2. ANALISI DEI TABULATI TELEFONICI

- Richiami sulla normativa per la conservazione dei dati
- La direttiva 2006/24/CE
- Come si legge un tabulato telefonico
- Le caratteristiche dei tabulati dei principali operatori
- Gli strumenti per l'analisi automatica

3. ANALISI DELLE LOCALIZZAZIONI

- Premesse generali sull'analisi delle celle telefoniche
- Le mappe di copertura radioelettrica
- Le misure sul campo
- Strumenti di misura e di analisi
- Le ipotesi di localizzazione

Via Aurelio Carrante, 1/F
70124 Bari - ITALY
T. +39.080.2229894 F. +39.080.2229886
E-mail: gruppo@ugolopez.it

Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Il docente

Paolo Reale si è laureato nel 1994 in Ingegneria Elettronica presso l'Università di Pisa con il massimo dei voti, con una tesi in Robotica pubblicata nel 1995 al simposio INRIA/IEEE sulle tecnologie emergenti.

Ha proseguito il percorso formativo nell'ambito delle FFAA, come Ufficiale nell'Arma delle Trasmissioni, e successivamente presso la Scuola Superiore G. Reiss Romoli de L'Aquila.

Ha operato inizialmente nell'industria, seguendo lo sviluppo della produzione di dispositivi elettronici a microprocessore, proseguendo con le attività di project management, e assumendo ruoli di livello manageriale, per l'ingegnerizzazione di processi e sistemi di controllo per le grandi aziende di ICT, con particolare attenzione alle tematiche di tutela delle informazioni aziendali, della security e della privacy. Su queste tematiche ha anche dedicato un iter di approfondimento specifico con il corso di alta formazione per DPO, organizzato dal CNF e dal CNI con il patrocinio del Garante per la protezione dei dati personali.

Esercita da anni l'attività di Consulente, al servizio di Aziende e Privati, della Polizia Giudiziaria e del Giudice (Consulenze d'Ufficio), mettendo a disposizione l'esperienza e le competenze acquisite nell'ambito delle telecomunicazioni, dell'informatica e più in generale dei sistemi di Information and Communication Technology. Tra gli incarichi affidati e svolti si contano casi di particolare rilevanza, anche mediatica.

Da giugno 2017 è professore straordinario per l'insegnamento di "Informatica di base e metodologia di acquisizione delle prove" nell'ambito del corso di laurea triennale di "Diritto dell'impresa, del lavoro e delle nuove tecnologie" dell'Università Telematica UNINETTUNO. Partecipa come Key note speaker a conferenze internazionali su temi legati alle telecomunicazioni e all'Informatica Forense (digital forensics, computer forensics, mobile forensics), presta docenze presso Organizzazioni, Ordini e Università: si citano in particolare i moduli di "Digital Forensics" presso l'Università LIUC, per il Master in Criminologia Sociale dell'Università di Pisa e per la Cattedra di Criminologia dell'Università di Tor Vergata (Roma), per il Master di I livello "Il consulente tecnico del tribunale nel contenzioso civile e penale" all'Università degli studi Internazionali di Roma. Collabora con la trasmissione TV di Rete4 "Quarto Grado", come consulente di 'informatica forense' in studio.

Via Aurelio Carrante, 1/F
70124 Bari - ITALY
T. +39.080.2229894 F. +39.080.2229886
E-mail: gruppo@ugolopez.it

Fa parte del Comitato di Redazione della rivista 'Sicurezza e Giustizia', per la quale pubblica articoli sui temi di digital forensics. Scrive anche sulla rivista "Quarto Grado magazine" edito da L'Ego Editore. E' membro del comitato scientifico dell'evento "Treviso Forensics 2018" patrocinato dal CNI, dal CNF e dall'Università di Padova.

Iscritto all'Albo degli Ingegneri della Provincia di Roma, da maggio 2013 è anche Presidente della Commissione Informatica e Telecomunicazioni dell'Ordine.

Nel 2014 ha fondato, insieme ad altri esperti del settore, l'Osservatorio Nazionale di Informatica Forense (ONIF). Da gennaio 2015 ne è anche il primo Presidente, confermato anche per il secondo triennio.

Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Programma quinta giornata, 22 febbraio 2019

"Mobile forensics: breve panoramica ed evoluzione della materia ad oggi"

Docente: **Luca Governatori**

Identificazione ed acquisizione delle device di tipo mobile

Strumenti commerciali per l'acquisizione

Estrazione Logica

Estrazione del File System

Estrazione Fisica

Advanced mobile forensics Metodologie e strumenti utilizzati

IOS / ANDROID / WINDOWS cenni sulle peculiarità dei sistemi operativi

DATA ANALYSIS:

Parsing 1: utilizzo degli strumenti commerciali

Parsing 2: utilizzo approfondito degli strumenti commerciali

Parsing 3: utilizzo di strumenti commerciali e revisione dei dati dalle app non supportate

Reportistica Vs. ricerca

Via Aurelio Carrante, 1/F
70124 Bari - ITALY
T. +39.080.2229894 F. +39.080.2229886
E-mail: gruppo@ugolopez.it

Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Il docente

Luca Governatori ha esperienza ultradecennale nell'ambito della mobile forensics, a partire dalla partnership commerciale con Cellebrite per il prodotto UFED fino a giungere alle consulenze specifiche sui dispositivi mobili.

Ha conseguito certificazioni Cellebrite nel 2011 e 2013. Amministratore della GovForensics s.r.l. società specializzata nelle tecniche di recupero dati dai dispositivi mobili.

Via Aurelio Carrante, 1/F
70124 Bari - ITALY
T. +39.080.2229894 F. +39.080.2229886
E-mail: gruppo@ugolopez.it

Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Programma sesta giornata, 23 febbraio 2019

"Penetration testing"

Docente: **Lorenzo Faletra**

ABSTRACT

Il corso ha l'obiettivo di formare i partecipanti sulle tecniche e le metodologie necessarie a condurre penetration tests e analisi della sicurezza di infrastrutture di rete. Durante lo svolgimento del corso verranno fornite nozioni di base per operare su sistemi Linux server, per effettuare scansioni di target, per saper affrontare il mondo della crittografia e per poter adoperare tecniche di attacco e di exfiltration, attraverso un approccio pratico.

PROGRAMMA

- Information gathering
  tecniche di acquisizione di dati da fonti aperte
- Scanning & enumerazione
  sniffing di rete con wireshark e tcpdump, scansione di porte con nmap
- Vulnerability assessment
  tools per il web application
- Exploitation
  metasploit framework e nozioni di base di exploitation
  backdoors con metasploit e weevely
- Maintaining access
  creazione di backdoor e canali di accesso persistenti
- Nuove tipologie di minaccia
  disamina di alcune nuove tecniche di attacco relative al mondo IoT e alle nuove tecnologie emergenti
- Cenni di reportistica
  come scrivere un report di successo

Via Aurelio Carrante, 1/F
70124 Bari - ITALY
T. +39.080.2229894 F. +39.080.2229886
E-mail: gruppo@ugolopez.it

Studio d'Ingegneria Informatica & Forense
Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Il docente

Lorenzo Faletra (Palermo, 1995), ricercatore e appassionato di cyber security nonché militante del software libero, è team leader e principale sviluppatore del sistema operativo di pentesting e privacy **Parrot Security** (www.parrotsec.org) e contributor di Caine e Debian pkg-security.

Ha lavorato come sysadmin, consulente e pentester freelance presso varie aziende sul territorio ed estere, e come docente per corsi di sicurezza informatica presso varie aziende ed enti di formazione.

Via Aurelio Carrante, 1/F
70124 Bari - ITALY
T. +39.080.2229894 F. +39.080.2229886
E-mail: gruppo@ugolopez.it