TECNICHE DI MICROACQUISIZIONE PROBATORIA DIGITALE IN AMBITO CIVILE

Il progetto mira a illustrare in vivo agli studenti, previa disamina del quadro normativo di riferimento, le principali procedure tecniche per lo svolgimento di attività di ricerca, acquisizione/estrazione, analisi/conservazione e presentazione di dati da dispositivi digitali a fini forensi.
La programmazione degli incontri segue una precisa scansione che, muovendo dalle tecniche più elementari, si sviluppa progressivamente fino a considerare quelle più complesse. In ogni giornata è previsto l'utilizzo di tecnologie *hardware* e *software* che verranno impiegate secondo le procedure tecniche normalmente utilizzate nei più avanzati laboratori di *digital forensics*.
Al termine del ciclo di seminari, gli studenti verranno coinvolti attivamente ed invitati a svolgere, con la strumentazione che verrà loro indicata e/o fornita, l'attività di acquisizione, copia, analisi e presentazione di file digitali da un dispositivo passivo.

04.05.2021
10.30 – 14.30
Computer forensics delle memorie passive

11.05.2021
10.30 – 14.30
Mobile forensics: l'acquisizione dati digitali dai dispostivi mobili

18.05.2021
10.30 – 14.30
Network e cloud forensics: l'acquisizione di dati digitali via Internet

25.05.2021
10.30 – 14.30
I metadati del traffico telefonico ed esercitazione

In considerazione dell'emergenza sanitaria, gli incontri si svolgeranno online mediante la piattaforma Zoom.

RELATORI

AVV. ANTONIO GAMMAROTA, PH.D.
Avvocato libero professionista, Cassazionista, Dottore di ricerca in Diritto delle Nuove Tecnologie, è professore a contratto dell'Università di Bologna *Alma Mater Studiorum* in "Fondamenti giuridici dell'informatica forense", nel Corso di Informatica forense, DSG; in "Informatica forense", del cui modulo è anche responsabile al Master in Diritto delle Nuove Tecnologie CIRSFID-ALMA HUMAN AI; in "Aspetti giuridici dell'Informatica forense", nel Dipartimento di Medicina Specialistica, Diagnostica e Sperimentale.

DOTT. ULRICO BARDARI, PH.D
Dottore di ricerca e cultore di Informatica giuridica al CIRSFID-ALMA HUMAN AI dell' Università di Bologna *Alma Mater Studiorum*.
E' Consulente Tecnico in materia informatica per diverse Procure della Repubblica italiane.
È Vice Ispettore della Polizia di Stato.

PER. IND. LUCA MERCURIALI
Titolare di un laboratorio di informatica forense a Cesena, svolge l'attività di Consulente Tecnico di Digital Forensics per privati e società, nonchè di ausiliario di Polizia Giudiziaria per diverse Forze di Polizia. E' stato Consulente Tecnico d'Ufficio e Perito per i Tribunali di Forlì, Ravenna e Bologna ed è Consulente di Informatica forense per varie Procure della Repubblica italiane, tra le quali quelle di Ravenna, Rimini, Forlì, Bologna, Lecce.

Progetto finanziato dall'Università degli Studi di Padova nell'ambito **"Progetti innovativi di studentesse e studenti finalizzati al miglioramento della didattica"** – bando 2020

Direttore Scientifico e Docente Referente:
Prof. Elisa de Belvis

È previsto il rilascio di un attestato di frequenza

40 partecipanti
L'iscrizione è obbligatoria:
plt.dirprivatocritica@unipd.it
Sarà seguito l'ordine cronologico di iscrizione

04 MAG GIORNO 01

10:30
14:30

COMPUTER FORENSICS DELLE MEMORIE PASSIVE

Attività basilari di computer forensics relative a dati digitali archiviati in memorie passive e dispositivi stand alone.

- **INDIVIDUAZIONE -** La ricerca dei dati; tipologie di dispositivi
- **ACQUISIZIONE** DI DATI DIGITALI DA ALCUNI TIPI DI MEMORIE PASSIVE – HDD; SSD; NAND FLASH micro SD e da chip con tecnica "chip-off"
- **CONSERVAZIONE -** Hash, firma digitale e marca temporale; Dati originari, originali, copie di dati per esame, catena di custodia
- **ANALISI -** Verifica hash; struttura di archiviazione in generale; struttura file (header, body, footer); metadati, la master file table e il calcolo di hash; tecniche di recupero dati raw e carving; timeline
- **PRESENTAZIONE DEI RISULTATI -** La relazione tecnica: struttura; premesse metodologiche; metodi di acquisizione e attività svolte; analisi e risultati; conclusioni

11 MAG GIORNO 02

10:30
14:30

MOBILE FORENSICS: L'ACQUISIZIONE DATI DIGITALI DAI DISPOSTIVI MOBILI

Attività di mobile forensics relative a dati archiviati in dispositivi digitali e in particolare negli *smartphone.*

- La ricerca dei dati
- Tipologie di dispositivi e sistemi operativi
- Tipologie di acquisizione
- Strumenti hardware e software
- Acquisizione di messaggistica istantanea
- Chip off: il recupero di dati digitali da memorie di cellulari inaccessibili
- Concetti base di crittografia
- Jailbreak e downgrade

18 MAG GIORNO 03

10:30
14:30

NETWORK E *CLOUD FORENSICS*: L'ACQUISIZIONE DI DATI DIGITALI VIA INTERNET

Attività di *network* e *cloud forensics* relative a dati digitali archiviati in sistemi distribuiti, *data center*, *cloud*.

- Acquisizione e analisi di email
- Acquisizione di pagine web
- Acquisizione di dati digitali da uno spazio Cloud
- Ricerca e acquisizione di documenti digitali in ambito aziendale
- Intercettazioni telematiche
- Trojan e captatore: tecniche e differenze
- Analisi di struttura file (header, body, footer); timeline; analisi dei protocolli

25 MAG GIORNO 04

10:30
14:30

ACQUISIZIONE DI DATI DIGITALI DI TRAFFICO TELEFONICO E DA AUTOMOBILI

Descrizione di schemi di reti mobili, modi e protocolli e conservazione dei dati di traffico telefonico con esemplificazione pratica mediante tabulati dei principali operatori telefonici nazionali.

- Analisi celle telefoniche
- Misurazioni strumentali
- Acquisizione e analisi di tabulati telefonici e dati
- Acquisizione e analisi di file di log e dati di tracciamento
- Car forensics e simulazione a banco dell'elettronica di un'autovettura
- Acquisizione dati da una Digital Diesel Elettronic
- L'esperimento giudiziale
- Dai dati tecnici ai dati investigativi

ESERCITAZIONE PRATICA DEGLI STUDENTI

Ogni studente, usando un software open source, dovrà svolgere autonomamente un'attività basilare di digital forensics per l'acquisizione, analisi e presentazione di dati da un dispositivo digitale passivo.

STRUMENTI:
PC
Connessione Internet
Software open source
File da acquisire, analizzare e presentare
Ai partecipanti sarà fornito il link per il download del software e sarà illustrata la procedura di installazione dei file oggetto di esercitazione