

TECNICHE DI MICROACQUISIZIONE PROBATORIA DIGITALE IN AMBITO CIVILE



Il progetto mira a illustrare agli studenti, previa disamina del quadro normativo di riferimento, le principali procedure tecniche in vivo per lo svolgimento a fini forensi di attività di ricerca, acquisizione/estrazione, analisi/conservazione e presentazione di dati da dispositivi digitali.

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 dispositivi 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 della necessità di osservare le precauzioni sanitarie anti COVID-19,

- le attività verranno svolte dai relatori al tavolo, verranno riprese e proiettate su uno schermo e commentate in diretta;
- le esercitazioni non potranno essere effettuate in gruppi ma individualmente.

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; "Informatica forense", del cui modulo al Master in Diritto delle Nuove Tecnologie CIRSIFID-ALMA HUMAN AI è anche responsabile; "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 CIRSIFID-ALMA HUMAN AI dell'Università di Bologna *Alma Mater Studiorum*.

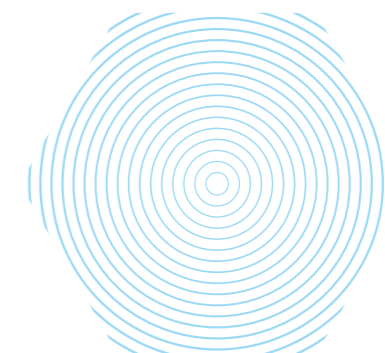
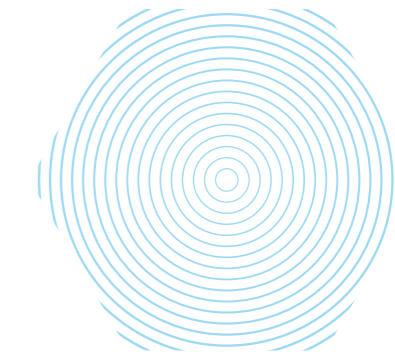
È Vice Ispettore della Polizia di Stato, per la quale ha svolto numerosi incarichi di indagine ad oggetto informatico, ed è Consulente Tecnico di diverse Procure della Repubblica italiana.

LUCA MERCURIALI

Perito industriale, è titolare di un laboratorio di informatica forense di Cesena. Consulente Tecnico di Digital Forensics per privati e società. Svolge abitualmente la propria attività come ausiliario di Polizia Giudiziaria per diverse Forze di Polizia ed è Consulente di Informatica forense per varie Procure della Repubblica italiana, tra le quali quelle di Ravenna, Rimini, Forlì, Bologna, Lecce; è stato Consulente Tecnico d'Ufficio e Perito per i Tribunali di Forlì, Ravenna e Bologna.



1222-2022
800
ANNI



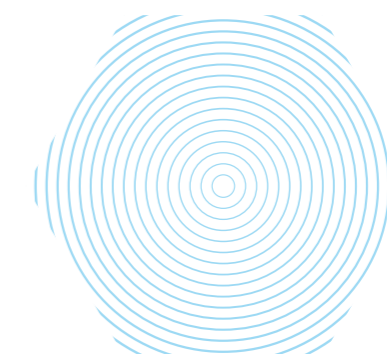
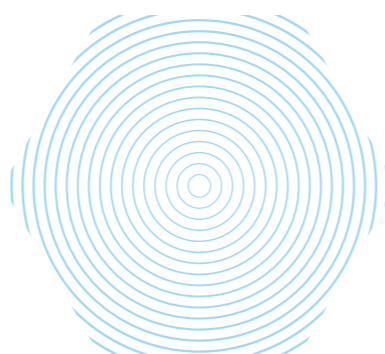
Progetto finanziato dall'Università degli Studi di Padova nell'ambito "Progetti innovativi di studentesse e studenti finalizzati al miglioramento della didattica" – bando 2020

Docente Referente:
Prof.ssa Elisa de Belvis

È previsto il rilascio di un attestato di frequenza

40 partecipanti

L'iscrizione è obbligatoria:
plt.dirprivatocritica@unipd.it



04 GIORNO
MAG 01

AULA EF2
COMPLESSO EX FIAT
Via Venezia 13
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 chip da 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 GIORNO
MAG 02

AULA EF2
COMPLESSO EX FIAT
Via Venezia 13
10:30
14:30

MOBILE FORENSICS: L'ACQUISIZIONE DATI DIGITALI DAI DISPOSITIVI 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 GIORNO
MAG 03

AULA EF2
COMPLESSO EX FIAT
Via Venezia 13
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 forense di dati contenuti in uno spazio Cloud
- Ricerca e acquisizione 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 GIORNO
MAG 04

AULA EF2
COMPLESSO EX FIAT
Via Venezia 13
10:30
14:30

I METADATI DEL TRAFFICO TELEFONICO ED ESERCITAZIONE

Illustrazione 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 tabulati telefonici e dati
- Acquisizione e analisi di file di log e dati di tracciamento
- Car forensics (mediante banco di simulazione parte elettronica di un'autovettura)
- Acquisizione dati da una Digital Diesel Elettronic
- Esempio di esperimento giudiziale
- Confronto tra dati investigativi e dati tecnici

ESERCITAZIONE PRATICA DEGLI STUDENTI

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

STRUMENTI:

PC (dello studente)
Connessione Internet (aula)
FTK da installare (i relatori indicheranno il link per il download)
Chiavetta USB con 4 file da acquisire, analizzare e presentare (i relatori forniranno a ciascuno studente una chiavetta USB con 4 file preinstallati).