Programma Workshop Digital Forensics

25 novembre 2017

LABORATORIO

Esempio d'analisi live ed uso dei tools.
Simulazione di sopralluogo sulla scena criminis, col ritrovamento di un pendrive
sospetto.
Esempio attività su pc spento
La checklist delle operazioni da compiere.
Preview & acquisizione (imaging)
Attività d'analisi con i tools a disposizione.

ACQUISIZIONE

Acquisizione di un supporto tramite Linux su disco destinazione
Acquisizione di un supporto tramite Linux via rete
Acquisizione di un supporto tramite Windows con FTK Imager.

ANALISI

Il carving (Foremost, Photorec) e come risalire al nome file dal numero di settore.
Analisi tramite Autopsy e Sleuthkit su un supporto (browsing il filesystem, ricerca per stringhe, recupero dei file cancellati, ecc.)
Ricostruzione degli headers tramiter editor esadecimale.
Analisi dei registri di Windows.
Analisi dei metadati dei file multimediali.
Panoramica su altri tools.
Alcune tecniche di anti-forensics.
La virtualizzazione di un sistema (VirtualBox).

REPORTING

Esempio di una perizia demo.

Via Aurelio Carrante, 1/F
70124 BARI
Tel: 080-2229894 Fax: 080-2229886
E-mail: gruppo@ugolopez.it