
Corso di
Indagini Digitali Forensi
- Livello Base

INDAGINI DIGITALI FORENSI - LIVELLO BASE**1. PANORAMICA SULLE BEST PRACTICES COMPUTER FORENSICS;****1.1 – L'immodificabilità della fonte di prova ed il metodo scientifico;****1.1.1 Il sopralluogo informatico;****1.2 - Analisi live e post mortem (i perché, pro e contro);****1.3 - Identicità della prova;****1.3.1 - hash, cosa sono ed il problema della collisione;****1.3.2 - catena custodia;****1.3.3 - ripetibilità delle operazioni;****1.4 – Elementi di OSINT.****2. Gli strumenti della C.F. - open source e commerciale.****3. Write blocker ed hardware forense.****3. 1 Le quattro fasi (Identificazione, acquisizione, analisi, reporting) in pratica.****4. GNU/Linux per la C.F. (uso della distro C.A.I.N.E. <http://www.caine-live.net> live distro forense).****5. Cenni su casi reali.****6. Panoramica sulla mobile forensics: tecniche di acquisizione ed analisi sui cellulari/tablet.****7. Cenni sulla legge 48/2008, art. 359 e 360 c.p.p. e DPR 115/02.****8. Live analysis ed acquisizione su un sistema acceso.****9. Elementi di mobile forensics.****10. Il futuro della D.F. e cenni sull'Intelligenza Artificiale****11. I miti e le leggende.****12. CASI PRATICI, LABORATORIO LIVE CON ESERCIZI DI LABORATORIO**

come ad esempio:

- esercizi
- virtualizzazione di un sistema
- data carving
- esempio di memory forensics
- creazione di una timeline
- Analisi con Autopsy