Prova di laboratorio

Disk e Network Forensics

Modalità di lavoro

- Prova individuale (2 max)
- Svolgimento in proprio (non in aula)
- Tempi di consegna max (circa una settimana)

- Verrà valutata anche la tempistica di consegna ()

Materiale su cui lavorare

- Scaricare il file zip disponibile all'url
  www.informaticaforense.it/esame-if-2011/prova_studenti.zip
- All'interno del file zippato sono presenti due file
  - Osama.E01, immagine di una chiavetta usb per la disk forensics
  - traffico.pcap, file di wireshark con traffico telematico intercettato

Disk forensics

- Vi viene fornita l'immagine della chiavetta usb sequestrata a Bin Laden
- Obiettivo
  - Trovare elementi utili a poter evitare un attentato
  - Produrre una relazione tecnica

Network forensics

- Vi viene fornito un file con traffico telematico intercettato
- Obiettivo
  - Documentare attività svolte
  - Ricostruire i file (es: le pagine web)
  - Produrre una relazione tecnica

Relazione

- Un esempio base di relazione vi viene reso disponibile all'url
  www.informaticaforense.it/esame-if-2011/esempio_relazione.zip
- Dovete documentare
  - Metodologie
  - Risultati
  - Conclusioni

Scadenze

- Consegna via mail (sebastiano.battiato@gmail.com) dei pdf della relazione tecnica.
- La mail dovrà riportare:
  - subject: [CF] Prova di Laboratorio
  - Corpo: Nome, Cognome e Matricola degli studenti (max 2 per relazione)
- Scadenza: Lunedì 16 Maggio – ore 12.00 AM