Modalità di intervento del Consulente Tecnico

Osservatorio CSIG di Reggio Calabria

Corso di Alta Formazione in Diritto dell'Informatica
IV edizione

Il consulente tecnico

Il Consulente Tecnico può raccogliere elementi ed informazioni utili per predisporre la perizia richiesta, limitatamente ad elementi rigorosamente tecnici della consulenza ed indicare nella perizia le fonti d'informazione, limitandosi a compiere gli accertamenti richiesti dal giudice/parte, deve evitare di assumere elementi che potrebbero configurarsi quali prove testimoniali o interrogatori formali.

Il Consulente Tecnico è abilitato ad assumere informazioni da terzi e ad acquisire, anche di sua iniziativa, ogni elemento necessario per rispondere ai quesiti, sempre per fatti accessori e rientranti nell'ambito tecnico della consulenza.

Le caratteristiche

L'attività di consulente tecnico deve essere improntata:

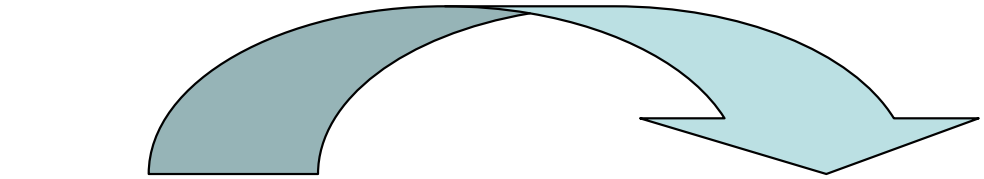
- *ad estremo rigore tecnico*
- *grande professionalità*
- *correttezza deontologica*

Le competenze

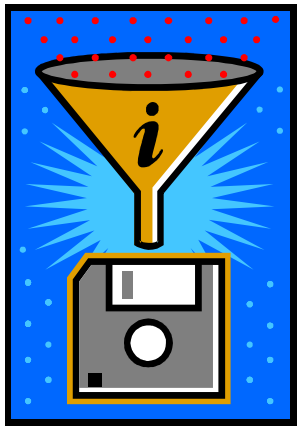
Conoscenza approfondita dei principali:

- *Componenti hardware*
- *Sistemi operativi*
- *File system*
- *Formati di file*
- *Tecnologie di comunicazione*
- *Protocolli di comunicazione*
- *Protocolli applicativi*
- *Tool di monitoring e hacking*
- *Aspetti giuridici legati alla forensics*

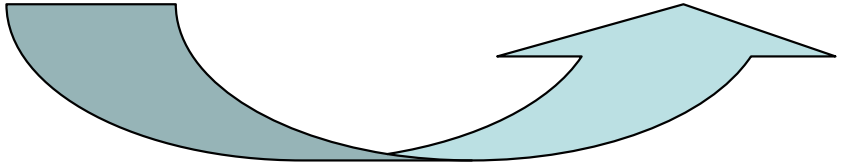
Digitalizzazione



La decodifica è un'interpretazione dell'elaborazione compiuta dalla macchina è mediata da componenti software



Qualsiasi informazione può essere codificata con un numero opportuno di bit



Digital Evidence

Digital Evidence *(traccia digitale)*

"Qualsiasi informazione, con valore probatorio, che sia o memorizzata o trasmessa in un formato digitale" [Scientific Working Group on Digital Evidence, 1998].

Digital Forensics

"Processo costituito dall'insieme di misure di carattere legislativo, organizzativo e tecnologico, tese ad analizzare dati e/o informazioni trattati in formato digitale"

Valore probatorio

Il valore probatorio di una traccia digitale dipenderà da:

- **Autenticità** - *Il dato proviene dalla fonte informativa presunta?*
- **Integrità** - *Il dato è conservato inalterato?*
- **Veracità** - *Il dato è interpretato in maniera corretta?*
- **Completezza** - *Sono stati raccolti tutti i dati relativi all'informazione rilevante?*
- **Legalità** - *Il dato è stato raccolto secondo le disposizioni della legge?*

Il Processo di Analisi

- *Stu*
- *Ide*
- *Ac*
- *An*
- *Documenta*

- Allegati tecnici:
  - Catena d
  - Azioni int
  - Informaz
  - Doc
  - e la r
- Report
  - Rife
  - Dat
  - Dat
  - Lis
  - Ris

- Mettere in sicurezza la prova
- Documentare configurazioni HW
- r
- r
- P
- in
- p
- D
- p

- Predisposizione strumenti di analisi
- Estrazione informazioni fisiche
- Estrazione informazioni logiche
- Analisi:
  - finestra temporale di riferimento
  - dati nascosti o cancellati
  - file e applicazioni
  - utenti e permessi
- Ripetibilità dell'analisi
- Documentazione accurata delle fasi di analisi e delle procedure utilizzate

Computer Crime Scene

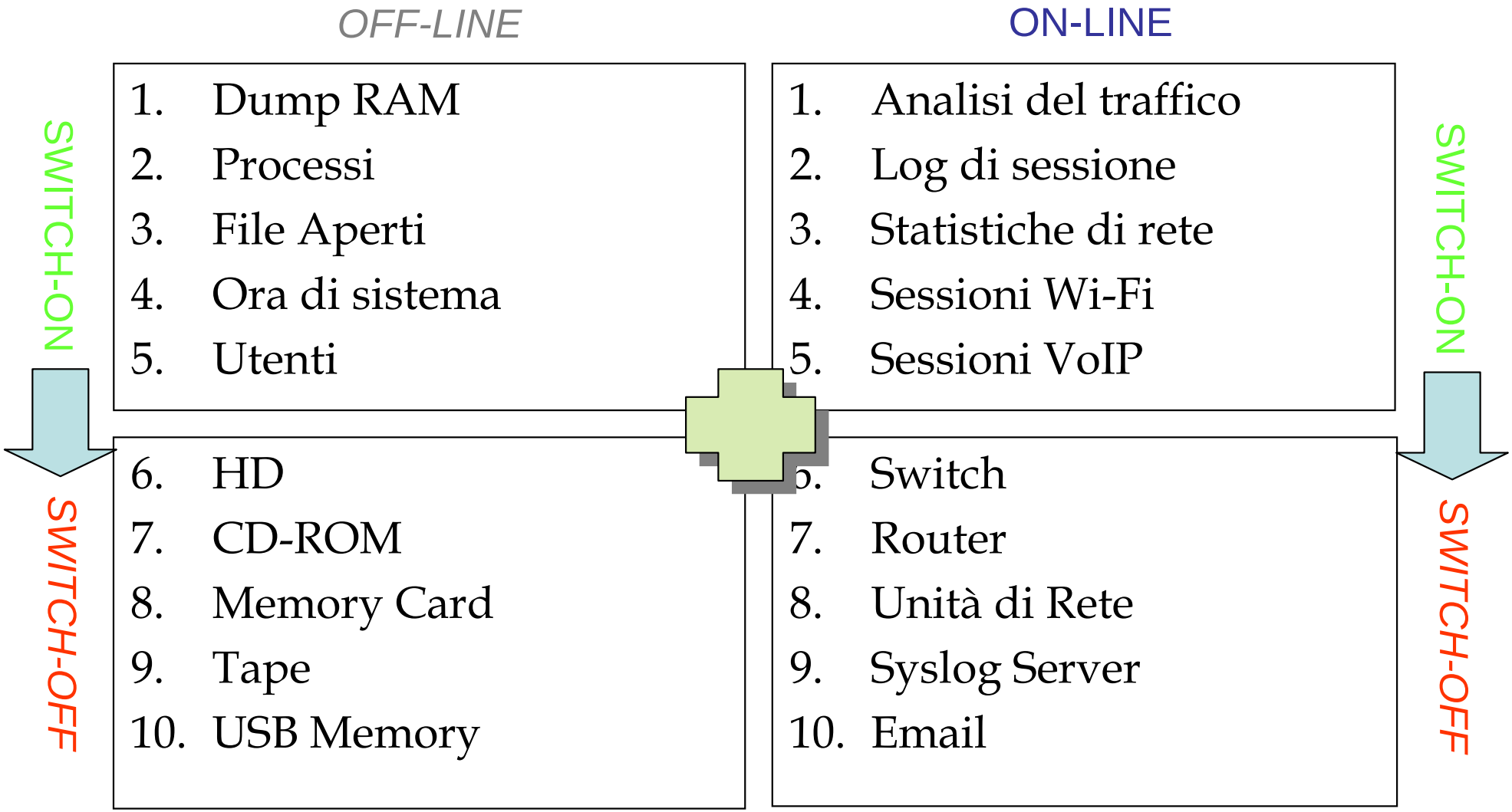
- Elaboratori e dispositivi elettronici
- Supporti di memorizzazione interni ed esterni (Pen drive, Lettori MP3, Memory Card, ecc.)
- Supporti rimovibili (CD-ROM, DVD, Floppy)
- Documentazione analog
  ecc.)
- Sistemi di comunicazion
  router, webcam)
- *… ma anche tutto il rest*
- Connessioni esterne

A questo punto occorrerà utilizzare una metodologia "***restrittiva***".
Quale sono le informazioni strettamente necessarie all'indagine?
NETWORK FORENSIC

Strumenti

- Postazione di acquisizione ed analisi
- Adattatori Hardware
- Cavi ed Interfacce
- Software di Acquisizione Open Source
- Macchine Fotografica
- Guanti e Dispositivi Antistatici
- Cassetta degli Attrezzi, Torcia
- Carta e Penna *… e tanta pazienza*

Stato delle prove



Memorie di massa

Un esempio: acquisizione di dati su memoria di massa (hard disk) in un sistema spento.

Obiettivo: realizzazione di una copia-immagine del disco che risponda ai seguenti principi fondamentali:

- *Non alterare in alcun modo il reperto oggetto di prova*
- *Ottenere una raccolta completa di informazioni*
- *Avere informazioni e dati accurati*
- *Se possibile effettuare una seconda copia*

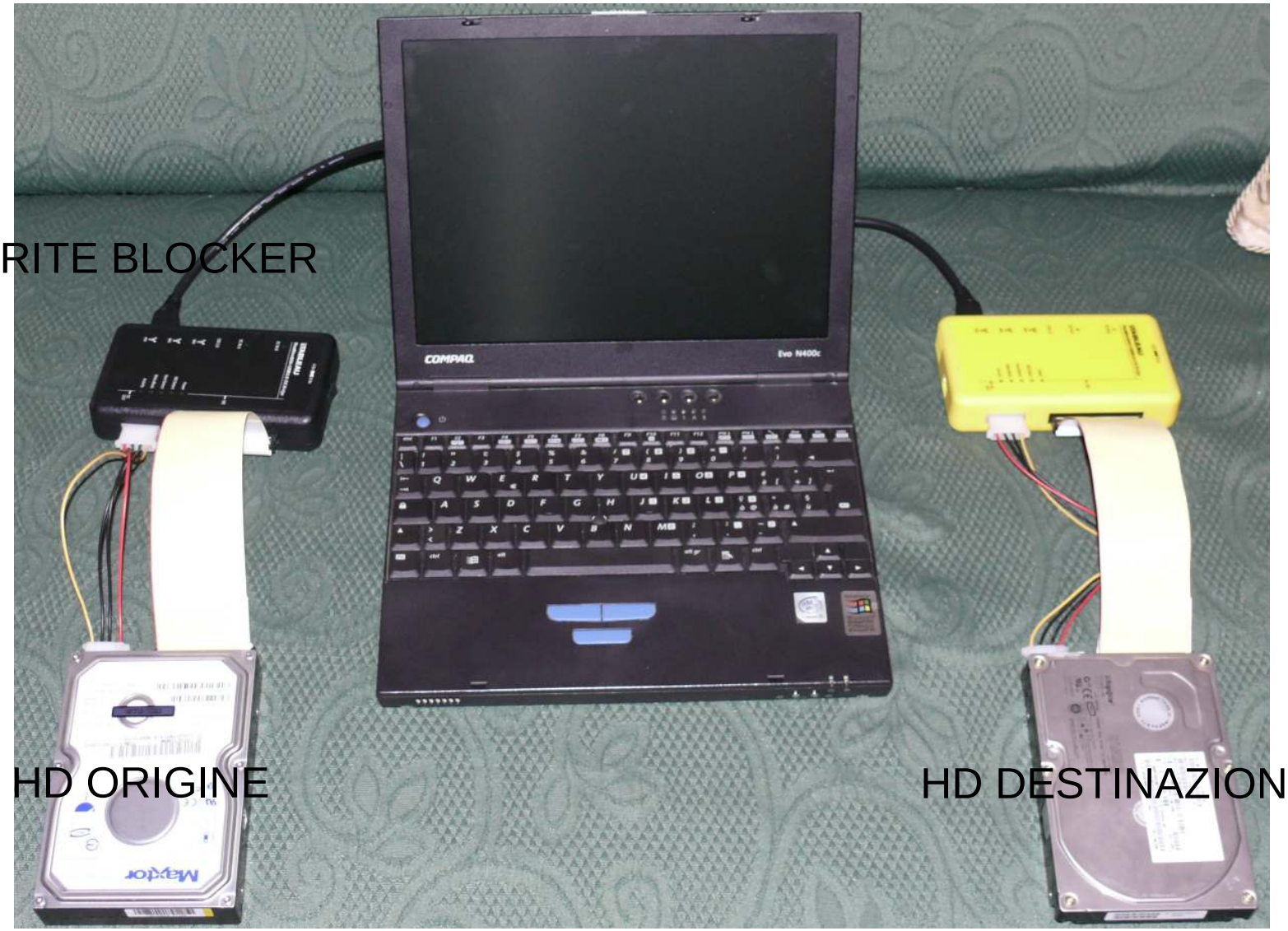
Passi successivi

Si prepara una piattaforma per il rilievo:

- Si documenta tutto l'hardware della macchina d'origine
- Si scollega il disco
- Il disco viene collegato alla piattaforma *"write-blocker"*
- Si attiva il s.o. della piattaforma
- Si produce *"hash"* del disco (documentare programma)
- Si azzera il supporto di destinazione
- Si effettua la copia del device (documentare programma)
- Si produce *"hash"* della copia
- Si confrontano gli *"hash"*
- Documentare la presenza di errori
- Si rimonta il disco
- Si documenta la strumentazione HW e SW utilizzata
- Si aggiorna la catena di custodia

… si può passare alla fase di analisi

Postazione Forensic



Come rendere inattaccabili le indagini?

- Formazione e aggiornamento
- Verifiche incrociate e indipendenti
- Adesione a standard d'azione internazionali
- Scrupolosa reportistica
- Oggettività

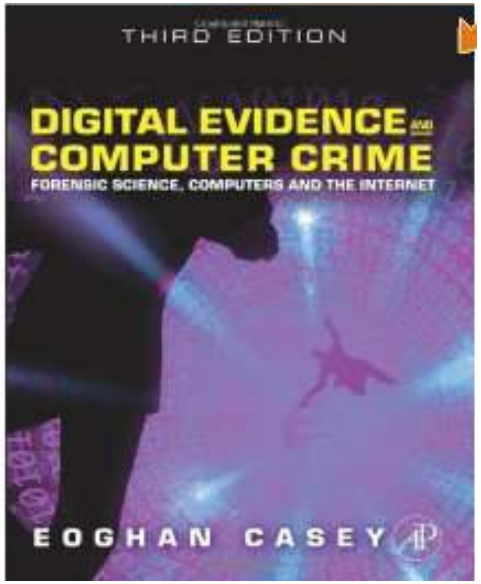
… modestia !

Per approfondimenti

Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet

Eoghan Casey BS MA

Academic Press;
3 edition (May 4, 2011)



Grazie.

www.vincenzocalabro.it