DIGITAL E MOBILE FORENSICS

Acquisizione della prova digitale; procedure tecniche e panorama legislativo.

DIGITAL Forensics: Analisi forense delle evidenze digitali

- **INCIDENT RESPONSE:** si occupa di fornire una risposta veloce e efficace ad una criticità, limitando i danni nel breve periodo.

- **DIGITAL FORENSICS:** cerca di ricostruire la catena di eventi che porta alla criticità, cercando di dettagliarne lo svolgimento e di individuarne gli attori.

Nel nostro caso… Dottrina atta all'analisi, conservazione, preservazione e protezione di dati presenti in dispositivi informatici in modo che possano assumere un valore giuridico.

Con chi si lavora:

- **PRIVATI**: consulenze tecniche di parte

- **PUBBLICO**: consulenze tecniche d’ufficio, perizie per il giudice, ausiliari di polizia giudiziaria.

Caratteristiche e modalità di nomina e di intervento

- **Consulente tecnico di parte:** nominato dalle parti
- **Consulente tecnico del pubblico ministero:** nominato dal Pubblico Ministero, risponde a specifico quesito; condivide parte degli obblighi del CTU e del perito del giudice (obbligo di prestare l'opera, non deve trovarsi in condizioni di incompatibilità).
- **CTU, Perito del giudice:** super partes, vincolato (obbligo di prestare l'opera, non deve trovarsi in condizioni di incompatibilità, obbligo di ricercare la verità), .
- **Ausiliario di Polizia Giudiziaria:** persona tecnicamente competente, nominata e guidata dalla Polizia Giudiziaria per compiere attività di specifico profilo tecnico.

Tipologie di reati sui quali si interviene

- Pedopornografia
- Omicidio
- Spaccio
- Reati Finanziari (corruzione/concussione, etc…)
- Falsificazione documenti
- **Accesso abusivo a sistema informatico (art. 635 ter c.p.)**
- **Danneggiamento di sistemi informatici (art. 635 bis c.p.)**

Convenzione di Budapest 2001 sul Cybercrime ratificata con legge 48/2008

Norma e prevede una fattispecie di reati a sfondo informatico ben definita; proprio in base ad essa, diventa indispensabile creare degli strumenti giuridici per la tutela della prova informatica in sede di indagini e processuale.

Best-practices (ISO/IEC 27037)

- Documentazione di ogni azione al fine di mantenere la CATENA DI CUSTODIA

Obiettivo: documentare l'integrità dei dati acquisiti e l'integrità del reperto analizzato

Tipologie di accertamento tecnico

- **Accertamenti tecnici ripetibili (art. 359 c.p.p.)**

- **Accertamenti tecnici non ripetibili (art. 360 c.p.p.)**

Cosa succede quando bussano alla porta:

- 6 del mattino… DRIINN …“Buongiorno, siamo la Polizia… Apra!”
- “Staccah, Staccah!”
- Notifica degli atti.
- Mettere in sicurezza le evidenze.
- Dump della RAM? Una chimera…
- Controllo orario da Bios.
- Inventario delle evidence.
- **Copia forense dei dispositivi.**

Copie forensi (1)

- Copia bit-to-bit della memoria di massa (dove possibile).
- Calcolo dell'Hash (in doppio formato, solitamente MD5 e SHA1, per evitare collision) .
- Formati più utilizzati:
  - **Advanced Forensics Format** (AFF) → .aff
  - **RAW** → .dd
  - **Expert Witness Format** [EWF] → .E**
  - **EnCase** → .Ex**

Copie forensi (2)

Modalità di realizzazione della copia:

- Duplicatori forensi.

- Distribuzioni Linux Forensic-oriented, writeblocker e software di imaging.

Copie forensi (3)

- Duplicatori Forensi

PREGI	DIFETTI
Velocità, frustano i transfer-rate al massimo	Più duplicazioni in parallelo
Write blocker sulla sorgente di default	Costo elevato

Copie Forensi (4)

- Distro Linux e Software di Imaging

PREGI	DIFETTI
Molte copie in parallelo (dipende dal computer)	Necessità di un writeblocker hardware o software
Software open source	velocità
	Vi servono un sacco di dischi esterni

Fase di analisi

- Estrazione dei file presenti
- Recupero dei file cancellati (carving)
- Analisi delle mail e del traffico su Internet
- Analisi del registro di sistema (e dei LOG)
- Analisi delle azioni avvenute sul dispositivo
  (timeline - supertimeline)
- Analisi mobile
- Analisi mirate in base alle richieste dell'A.G./P.G.

Estrazione dei dati presenti

- Navigazione all'interno dell'albero del file system dell'immagine forense in modalità **read/only** alla ricerca dei file d'interesse

- I dati vengono filtrati per estensione per escludere tutta la parte non di interesse (file di sistema).

Recupero dati cancellati (Carving)

- Dati recuperati tramite la ricostruzione di versioni di MFT precedenti a quella presente.

- RAW: recupero tramite marker distintivi del tipo di files, può coinvolgere anche lo spazio non allocato del disco.

Traffico Web e Posta elettronica

- Parsing delle cache del browser
- Recupero delle password memorizzate
- Recupero delle ricerche effettuate sui motori di ricerca
- Interpretazione dei messaggi di posta in base al formato (.pst, .dbx, .eml, .msg, Thunderbird) e recupero di eventuale posta cancellata ove possibile

Eventi di sistema

- Analisi dei files di registro
- Eventi di sistema (accensione/spegnimento, log-in utenti etc…)
- Elenco utenti e sessioni
- .lnk files
- Shellbags (analisi dei puntatori alle cartelle e ai files di explorer)
- Prefetch (analisi dei processi eseguiti sul sistema)
- Dispositivi collegati

Timeline e Supertimeline

- Timeline: analisi delle date di creazione/ultima modifica/ultimo accesso relative ai soli files presenti sul sistema.

- Super Timeline: analisi delle date di creazione/ultima modifica/ultimo accesso relative ai files presenti sul sistema e degli eventi di sistema.

Analisi a richesta

- Metadati
- Alterazione immagini
- Virtualizzazione di ambienti software specifici
- Virtualizzazione di intere reti per simulare il funzionamento di servizi
- Miglioramento video
- Tracking e ricostruzioni facciali in 3D

Mobile Forensics

- ARGH!!!
- Tutt’altro che scienza esatta…
- OS in continua evoluzione
- Cifratura/codici di blocco
- Necessità sempre maggiore di operare ex art. 360 c.p.p.

Principali ostacoli

- Consegna di reperti con una catena di custodia non adeguata.
- Necessità di restituire dati consultabili a prova di utente.
- Necessità di fornire spiegazioni assolutamente basilari a persone tecnicamente meno competenti che riguardano argomenti tecnicamente complessi.
- BI.A.PO.D. (Big Amount of Porn Data).

Dubbi operativi

- Ruolo dei legali nell’ambito di perquisizione e opposizione tecnica.

- È possibile effettuare le copie in loco, senza necessità di sequestrare tutto?
- Extraterritorialità ed estensione del domicilio fisico (mail su server all’estero e cloud.
- Detenzione e trattamento di dati delicati e copia indiscriminata della totalità dei supporti.

CONCLUSIONI...

Quindi, se proprio volete, la ricetta giusta è...

- **Fatene una, fatela grossa, fatela in live e, soprattutto, fatela dal wifi di un kebab!**

Software utili

Imaging:

- guymager
- dd
- dd rescue
- dclfdd
- cyclone
- FTK Imager (AccessData)
- mount
- xmount
- ewfmount

recupero / estrazione:

- binwalk
- foremost
- photorec
- scalpel

Ambienti di analisi/web:

- Sleuthkit con Autopsy
- bulk extractor

Posta

- undbx
- readpst

Timeline:

- log2timeline

Metadati e img:

- exiftools
- jpegsnoop
- steghide