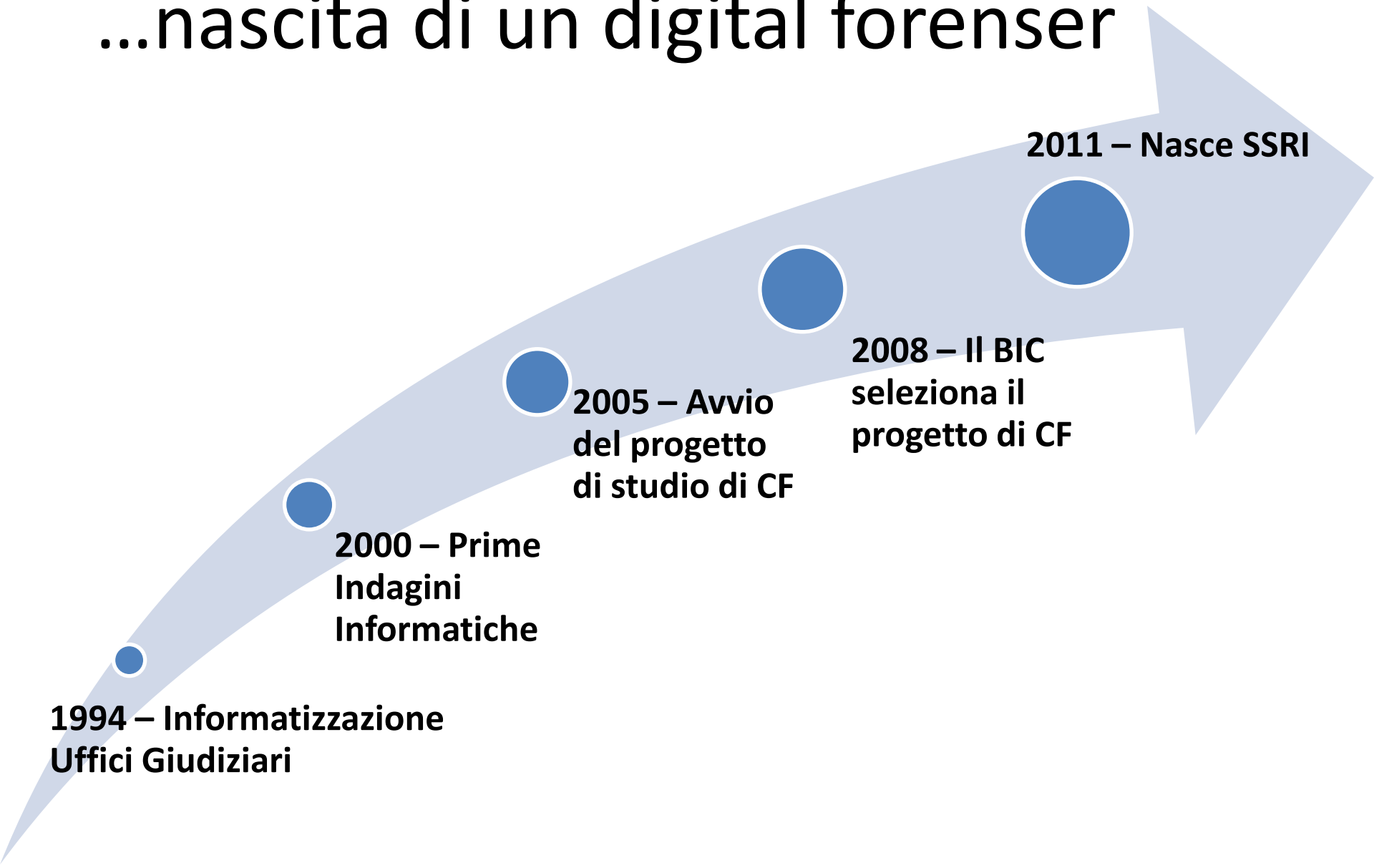
INTRODUZIONE ALLA COMPUTER FORENSICS

Inquadramento dello scenario di riferimento tecnico normativo e descrizione dei punti cardine dell'attività del computer forenser

Lorenzo Laurato

UNIVERSITA' DEGLI STUDI DI NAPOLI FEDERICO II

…nascita di un digital forenser



Cosa è la Digital Forensics?

l'insieme di metodologie scientificamente provate finalizzate alla ricostruzione di eventi che coinvolgono direttamente o indirettamente un supporto digitale

Metodologie

- Identificazione
- Raccolta
- Validazione
- Preservazione
- Analisi
- Interpretazione
- Documentazione
- Presentazione

Reato Informatico

- In ambito penale la definizione si è evoluta nel tempo:
- *Illecito che richiede conoscenze di informatica per la sua realizzazione*
- *Illecito che comporta il coinvolgimento di un qualunque tipo di elaboratore*
- **Illecito nel quale il computer interviene come strumento o come oggetto**

Reato Informatico

- Quelle appena esposte sono tuttavia definizioni troppo ampie che non riescono a delimitare correttamente quale condotta possa essere definita “reato informatico”.
- **A livello internazionale si è rinunciato a dare una vera e propria definizione di reato informatico.**
- **Si è preferito concordare una tipologia di comportamenti ai quali dare l’etichetta di reati informatici.**

Tipologie di reato

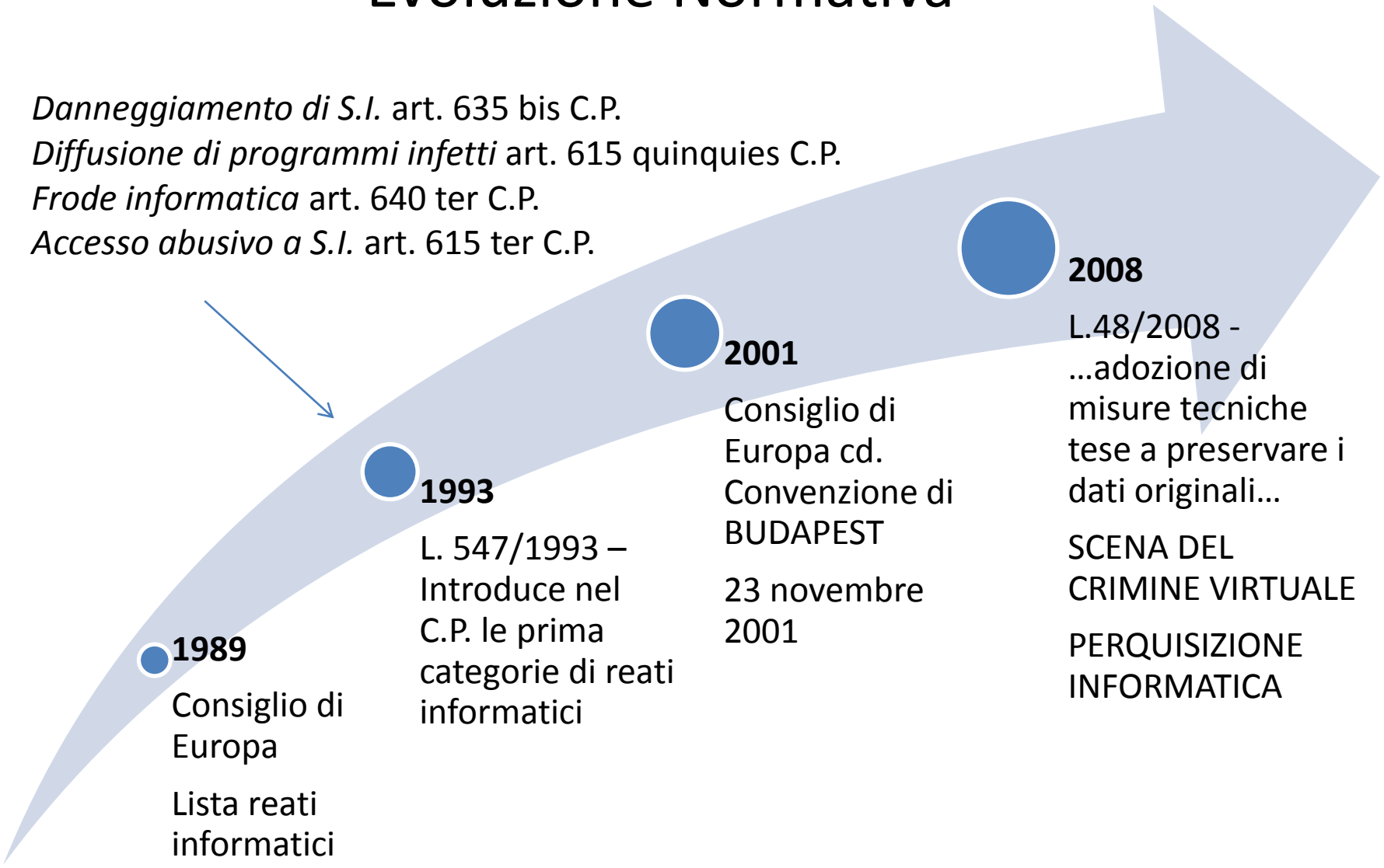
MANIPOLAZIONE DI DATI (frode informatica) a fine di LUCRO

SABOTAGGIO INFORMATICO

SPIONAGGIO INFORMATICO

Evoluzione Normativa

Danneggiamento di S.I. art. 635 bis C.P.
Diffusione di programmi infetti art. 615 quinquies C.P.
Frode informatica art. 640 ter C.P.
Accesso abusivo a S.I. art. 615 ter C.P.



1989

Consiglio di Europa

Lista reati informatici

1993

L. 547/1993 – Introduce nel C.P. le prima categorie di reati informatici

2001

Consiglio di Europa cd. Convenzione di BUDAPEST

23 novembre 2001

2008

L.48/2008 - …adozione di misure tecniche tese a preservare i dati originali…

SCENA DEL CRIMINE VIRTUALE

PERQUISIZIONE INFORMATICA

L 48/2008 – Scena del Crimine

- **Art. 244 C.P.P. - Casi e forme delle ispezioni:**
  - 1. L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.
  - 2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica***, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.***

L 48/2008 – Scena del Crimine

- **Art. 247 C.C.P. - Casi e forme delle perquisizioni:**
  - 1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.
  - ***1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.***
  - 2. La perquisizione è disposta con decreto motivato.
  - 3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.

L 48/2008 – Scena del Crimine

- **Art. 352 C.P.P. - Perquisizioni:**
  - 1. Nella flagranza del reato o nel caso di evasione, gli ufficiali di polizia giudiziaria procedono a perquisizione personale o locale quando hanno fondato motivo di ritenere che sulla persona si trovino occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero che tali cose o tracce si trovino in un determinato luogo o che ivi si trovi la persona sottoposta alle indagini o l'evaso.
  - ***1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.***
  - 2. Quando si deve procedere alla esecuzione di un'ordinanza che dispone la custodia cautelare o di un ordine che dispone la carcerazione nei confronti di persona imputata o condannata per uno dei delitti previsti dall'articolo 380 ovvero al fermo di una persona indiziata di delitto, gli ufficiali di polizia giudiziaria possono altresì procedere a perquisizione personale o locale se ricorrono i presupposti indicati nel comma 1 e sussistono particolari motivi di urgenza che non consentono la emissione di un tempestivo decreto di perquisizione.
  - 3. La perquisizione domiciliare può essere eseguita anche fuori dei limiti temporali dell'articolo 251 quando il ritardo potrebbe pregiudicarne l'esito.
  - 4. La polizia giudiziaria trasmette senza ritardo, e comunque non oltre le quarantotto ore, al pubblico ministero del luogo dove la perquisizione è stata eseguita il verbale delle operazioni compiute. Il pubblico ministero, se ne ricorrono i presupposti, nelle quarantotto ore successive, convalida la perquisizione.

L 48/2008 – Scena del Crimine

- **Art. 354 C.C.P. - Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro:**
  - 1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.
  - 2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. ***In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.*** Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.
  - 3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale.

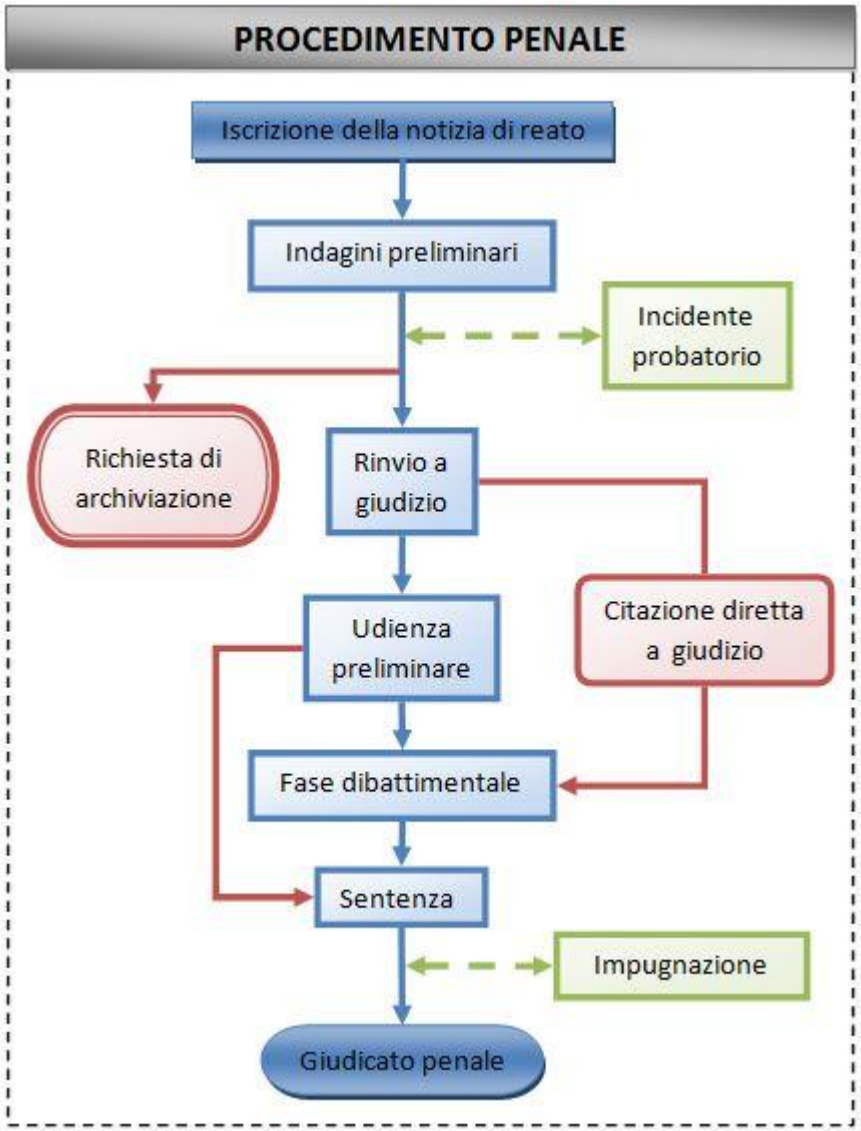
Procura della Repubblica

Il Pubblico Ministero Gestisce le Indagini ed ha il potere di esercitare l'azione penale

Tribunale

Il Giudice valuta le tesi accusatorie e difensive.

CONDANNA o ASSOLVE


PROCEDIMENTO PENALE
Iscrizione della notizia di reato
Indagini preliminari
Incidente probatorio
Richiesta di archiviazione
Rinvio a giudizio
Udienza preliminare
Citazione diretta a giudizio
Fase dibattimentale
Sentenza
Impugnazione
Giudicato penale

Computer Forensics

*“**L'informatica forense** (computer forensics) è la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico al fine di essere valutato in un processo giuridico e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici.” (Wikipedia)*

Computer Forensics: best practices

1 - Identificazione

2 - Acquisizione

3 - Analisi

4 - Refertazione

5 - Presentazione

1- Identificazione della “evidence”

- Specificità del reperto e pertinenza all’indagine
- Individuazione del supporto (magnetico, ottico, ecc)
- Rilievo fotografico e repertazione
- BIOS
- Sistema operativo e file system
- Eventuali condizioni speciali (cloud, ambienti virtuali…)

2 - Acquisizione del reperto

Sequestro fisico

- Prelievo del supporto di memoria e relativa verbalizzazione

Sequestro logico

- Produzione di una **copia forense** sul posto

2 - Copia Forense

- Deve essere eseguita "…adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione…" (L. 48/2008)

2 – Il Forenser deve:

- Rispettare la corretta procedura
- Impiegare strumentazione adeguata
- Gestire e documentare gli errori
- Verbalizzare e documentare le operazioni
- Sigillare elettronicamente la copia ottenuta mediante la computazione ed il confronto dell'algoritmo di hasing MD5 o SHA1 su originale e copia
- Settare in sola lettura le copie

GARANZIA DI RIPETIBILITA' DEI SUCCESSIVI ACCERTAMENTI CHE VERRANNO ESEGUITI SULLA COPIA FORENSE

3 – ANALISI

SEARCHING

PROFILING

Possibilmente sempre sulla Copia Forense

3 – Tecniche

Strumenti commerciali	Strumenti liberamente distribuiti

In alcuni casi può essere opportuno l’incrocio delle risultanze di entrambi gli strumenti

3 – Tecniche

- Data Mining
- Tracing
- Event Correlation
- Analisi Investigativa
- Analisi dei log
- Password Cracking (creazione di dizionari, brute force attacks…)
- Data Recovery
- Data Carving

4 - Refertazione

- Le risultanze dell'analisi di Computer Forensics sono rappresentate da un elaborato documentale, pertanto la sua redazione è di fondamentale rilievo.
- Andrà calibrato il dettaglio tecnico tenendo conto che i lettori designati saranno sia tecnici (CTU, CTP, Periti) sia Legali (magistrati, avvocati) sia Polizia Giudiziaria ed investigatori.

5 - Presentazione

- L’atto finale dell’attività del Computer Forenser si consuma nell’aula dibattimentale.
- Una rappresentazione teatrale dove il Computer forenser ha 3 obiettivi da conseguire.
- Guadagnare in poche battute credibilità professionale presso soggetti che si incontra per la prima volta
- Convincere il giudice della validità ed attendibilità delle conclusioni cui si è addivenuti
- Scoraggiare la controparte nell’avanzare eccezioni

Grazie per l’attenzione ed arrivederci al prossimo incontro.

Per qualsiasi necessità di chiarimento ed approfondimento potete contattarmi alla mia casella di posta personale.

lorenzo.laurato@gmail.com