✓PROCESSO PENALE E CRIMINALITÀ INFORMATICA:

✓UNA NUOVA REALTÀ DOPO LA CONVENZIONE DI BUDAPEST

CENTRO STUDI INTERDIPARTIMENTALE
SULLA CRIMINALITÀ INFORMATICA
http://csici.unipmn.it

✓Polizia Postale
✓e delle Comunicazioni
✓Torino

“LE PROSPETTIVE DELL’INVESTIGATORE”

16 settembre 2009
Alessandria

LEGGE 48/2008

Il dato normativo di riferimento è rappresentato dalla legge 48/2008 che ha ratificato la Convenzione di Budapest del 2001 sulla criminalità informatica.

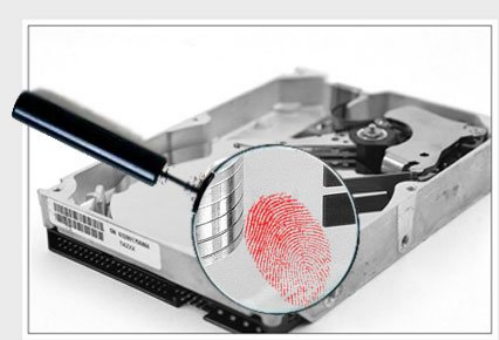
Sotto il profilo puramente operativo,le modifiche che sono state apportate al codice di procedura penale hanno come comune denominatore l'intento di introdurre procedure finalizzate ad ottenere **la c.d. evidenza informatica**, mediante l'adozione di misure tecniche dirette ad assicurare la **CONSERVAZIONE** dei dati originali e la **NON ALTERABILITA'** degli stessi.

EVIDENZA DIGITALE

L'**evidenza digitale** è un'informazione probante archiviata o trasmessa in formato digitale che difesa o accusa possono usare in un processo.

Essa è una sequenza di Bit che rivela un significato logico solo in seguito ad un corretto processo di decodifica.

EVIDENZA DIGITALE



- CONFORMITÀ DEI DATI ACQUISITI
- IMMODIFICABILITÀ
- RIPETIBILITÀ DEGLI ACCERTAMENTI

RICERCA FONTE DI PROVA

PROBLEMI DI RINVENIMENTO DELLE TRACCE INFORMATICHE

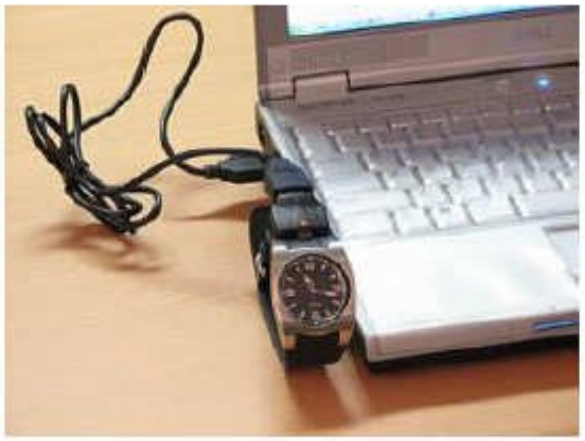
- Oltre ai noti supporti di archiviazione, hard disk, cd-rom, dvd, pen-drive, smart card, telefonini, macchine fotografiche digitali, acc.ecc. esistono sul mercato una serie infinita di manufatti che offrono una capacità di storage elevatissima e questi, come ovvio sono facilmente occultabili.

- Le informazioni ricercate possono essere, attraverso adeguati software, rese trasparenti e quindi non visibili, (es. steganografia, crittografia ecc.)

OCCULTABILITA’

OCCULTABILITA’

OCCULTABILITA’



OCCULTABILITA'

OCCULTABILITA’

RICERCA FONTE DI PROVA

ISOLAMENTO DELLA SCENA DEL CRIMINE
(fisico)

- Individuare le apparecchiature accese
- Tenere le persone lontane dagli apparati, dalle prese di corrente, dalle connessioni dati
- Non dovrà spegnere le apparecchiature accese prima di essere certo di poterlo fare (sui problemi connessi allo spegnimento torneremo successivamente)
- Non dovrà accendere apparecchiature spente

RICERCA FONTE DI PROVA

ISOLAMENTO DELLA SCENA DEL CRIMINE (logico)

- Se c'è un modem non connesso, converrà scollegarlo
- Se c'è attività sarà necessario scollegare i cavi solo dopo gli opportuni accertamenti da parte di personale specializzato
- Attenzione ai dispositivi wireless
- Rimuovere le batterie dei dispositivi mobili
- Occorrerà staccare i cavi dal lato del PC e non da quello delle prese

ANALISI AMBIENTALE

MOTIVAZIONI

- Descrizione dell'ambiente per ciò che concerne l'esistenza di libri di testo su argomenti informatici, titoli di studio o di frequenza di corsi informatici posseduti dall'indagato ecc.ecc.
- Il soggetto che effettua l'indagine sui supporti sequestrati difficilmente avrà avuto modo di partecipare alla relativa fase della perquisizione
- L'art.27 Costituzione sancisce il carattere personale della responsabilità penale. Conoscere quindi chi, con ogni probabilità, aveva la disponibilità dei supporti risulta di primaria importanza, per una corretta attribuzione di responsabilità

ANALISI O ISPEZIONE SUL POSTO

PRO

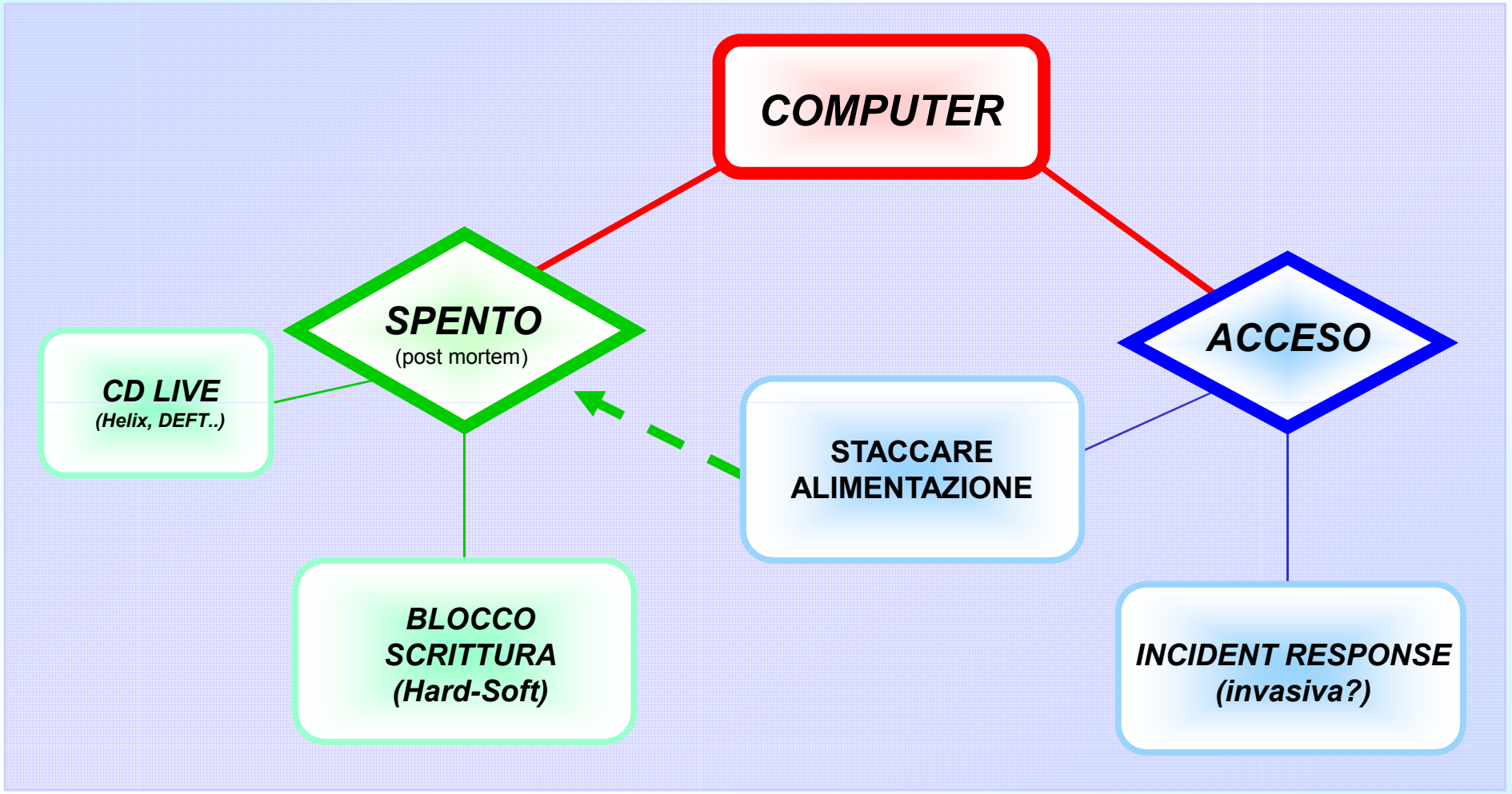
- Consente di eseguire un triage su quanto disponibile al fine di evitare"saccheggi" indiscriminati e di individuare subito responsabilità in ambienti condivisi.
- E' necessaria laddove il sistema non è fisicamente rimovibile ovvero sono rimuovibili solo i dischi, ma ciò potrebbe non bastare
- Ovvero quando non è possibile sequestrare tutti i sistemi ma occorre individuare solo quelli rilevanti ed ancora quando occorra solo acquisire i dati, senza porre sotto sequestro l'hardware.

ANALISI O ISPEZIONE SUL POSTO

CONTRO

- Le condizioni operative non sono paragonabili a quelle di un laboratorio
- L'attrezzatura a disposizione non può che essere limitata
- Situazioni imprevedibili sono sempre in agguato
- Fattore tempo, che è forzatamente limitato.
- Responso incerto. Un'analisi eseguita in queste condizioni può dare riscontri solo in positivo infatti nella migliore delle ipotesi si può da subito confermare l'esistenza di un'evidence individuata ma non individuarla non ne conferma l'assenza con altrettanta certezza

POSSIBILITA' OPERATIVE



INCIDENT RESPONSE

PROBLEMATICHE

- Le modifiche apportate sono note?
- Sono documentabili?
- Intaccano significativamente il risultato dell'analisi?
- Ogni modifica distrugge qualcosa

SEQUESTRO

1) Porre sotto sequestro l'INTERO ELABORATORE

2) Porre sotto sequestro SOLTANTO GLI HARD-DISK

3) Porre sotto sequestro SOLO I DATI INERENTI L'INDAGINE (email, profili utente in file server, siti web remoti. Esempio di modalità: stampa di documenti, masterizzazione cdrom.)

SEQUESTRO DELL'INTERO ELABORATORE

PRO

- Utile in presenza di particolari configurazioni (vedi hard disk in raid o supporti con tecnologia SCSI, sistemi hardware complessi, sistemi NAS, dischi di difficile estrazione)
- L'intera macchina e supporti offre all'investigatore una completa visione riguardo l'utilizzo della stessa.

CONTRO

- Si possono sequestrare computer che non contengono informazioni attinenti le indagini o di proprietà di terzi soggetti;
- La persona coinvolta (parte lesa od indagato) si vede privare per lungo tempo di un oggetto a volte indispensabile.

SEQUESTRO DEI SOLI DISCHI

PRO

- Il sequestro dei soli hard disk permette di gestire in maniera più agevole la loro custodia.
- Permette all'indagato di poter usufruire del restante materiale.

CONTRO

- Questa operazione anche se all'apparenza banale, può causare la rottura dei supporti (scariche elettrostatiche, cadute e danneggiamenti accidentali).

SEQUESTRO DI ALCUNI DATI

PRO

- Si possono estrarre dei dati preservando dati non inerenti l'indagine, contenuti in sistemi relativi ad aziende o sistemi multiutente.

- Si possono sequestrare file contenuti in un server remoto, magari all'estero. (siti web)

CONTRO

- Non possiamo avere accesso al supporto originale nelle fasi processuali successive.

SEQUESTRO (1/3)

- Se si decide di sequestrare SOLTANTO L'HARD DISK di un sistema è necessario annotare *l'ora di sistema* e gli eventuali sfasamenti.
- Descrivere precisamente il materiale, annotare i seriali ed etichettare tutti i reperti (eventualmente anche cavi o connettori particolari)
- Ricercare eventuali annotazioni utili come account, password, indirizzi e-mail, url, soprattutto nell'ambiente prossimo alla postazione

SEQUESTRO (2/3)

- Verificare la presenza di CD, Floppy o schede di memoria inserite nei lettori.
- Sequestrare anche gli alimentatori e gli altri accessori (cd driver) necessari per la futura analisi.
- Eseguire, se possibile ed utile, rilievi fotografici
- Se il COMPUTER È ACCESO, annotare quali siano i programmi in esecuzione nonché eventuali informazioni ad essi connessi (pagine web attive, nickname, documenti aperti ecc.) scollegare la presa di corrente e procedere quindi come nel caso della macchina spenta.

SEQUESTRO (3/3)

- Nel caso di SEQUESTRO PARZIALE DI DATI, al fine di garantire la conformità in sede di acquisizione tra originale e dato sequestrato, sui file acquisiti può essere applicata una verifica Hash.

- La codifica di Hash è un algoritmo che, applicato ad una sequenza di byte, la elabora producendo un codice di dimensione fissa detto *digest*. Il metodo di elaborazione è tale che se anche solo un byte della sequenza cambiasse, il risultato dell'Hash sarebbe diverso.

CONCLUSIONI

EVOLUZIONE TECNOLOGICA

Esigenza di un aggiornamento costante del personale operante, per fronteggiare scenari sempre nuovi e diversi.

✓CONTATTI

VICE QUESTORE AGG.
D.ssa Assunta ESPOSITO

ASSISTENTE
Dott. Dario FUGALLI

POLIZIA DI STATO

COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI

"Piemonte e Valle d'Aosta"

Corso Tazzoli nr. 235 – 10135 Torino

0113014611 – fax 0113014670
poltel.to@poliziadistato.it