ISO IEC 27037/2012

Uno standard internazionale contenente linee guida per identificazione, raccolta, acquisizione e conservazione di evidente digitali

Michele Ferrazzano

ISO

- International Organization for Standardization
- La più importante organizzazione a livello mondiale per la definizione di norme tecniche
- Fondata il 23 febbraio 1947, quartier generale a Ginevra
- Membri dell'ISO sono gli organismi nazionali di standardizzazione di 162 Paesi del mondo
- ISO coopera strettamente con IEC, responsabile per la standardizzazione degli equipaggiamenti elettrici

IEC

- International Electrotechnical Commission
- Organizzazione internazionale per la definizione di standard in materia di elettricità, elettronica e tecnologie correlate
- Fondata nel 1906; ed inizialmente aveva sede a Londra; nel 1948 ha spostato la sua sede a Ginevra. Ad essa attualmente partecipano più di 60 paesi.
- Molti dei suoi standard sono definiti in collaborazione con ISO
- La commissione è formata da rappresentanti di enti di standardizzazione nazionali riconosciuti

ISO/IEC 27037/2012

- Information technology
  - Security techniques
    - **Guidelines for identification, collection, acquisition, and preservation of digital evidence**

ISO/IEC 27037/2012
Altri standard di riferimento

- ISO/TR 15801:2009
  - Document management - Information stored electronically - Recommendations for trustworthiness and reliability
- ISO/IEC 17020:2012
  - Conformity assessment - Requirements for the operation of various types of bodies performing inspection
- ISO/IEC 17025:2005
  - General requirements for the competence of testing and calibration laboratories
- ISO/IEC 27000:2012
  - Information technology - Security techniques - Information security management systems - Overview and vocabulary

ISO/IEC 27037/2012
Altri standard di riferimento (DRAFT)

- ISO/IEC 27041 – Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence (DRAFT)
- ISO/IEC 27042 – Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence (DRAFT)
- ISO/IEC 27043 – Information technology – Security techniques – Digital evidence investigation principles and processes (DRAFT)

ISO/IEC 27037/2012
Di cosa si occupa

- Trattamento del reperto informatico
- Definizione linee guida nelle fasi di
  - Identificazione (ispezione)
  - Raccolta (sequestro)
  - Acquisizione (sequestro virtuale)
  - Conservazione (conservazione e sigillo)
- Integrità della prova informatica e metodologia al fine di rendere ammissibile la prova in giudizio
  - Per prova informatica si fa riferimento a dati già in formato digitale
    - Esclusi quindi dati in formato analogico convertiti in formato digitale

ISO/IEC 27037/2012
Di cosa si occupa

- Per ogni fase
  - Documentazione (logging)
  - Tracciabilità (chain of custody)
  - Priorità di intervento (plan)
  - Imballaggio dei reperti (protection)
  - Trasporto dei reperti (real/virtual)
  - Ruoli nel passaggio dei reperti (who & why)

ISO/IEC 27037/2012
Di cosa non si occupa

- Aspetti legali
  - È internazionale, non legata ad un singolo ordinamento
- Analisi
- Strumenti tecnici
- Redazione di report e presentazione
- Trattamento di dati analogici

ISO/IEC 27037/2012
Persone che trattano reperti informatici

- Digital evidence first responders (*DEFRs*)
  - Operatore che si approccia per primo ai sistemi (supporti di memorizzazione e dati) di potenziale interesse
  - Deve avere adeguata esperienza e competenze
  - Può avvalersi di collaboratori

ISO/IEC 27037/2012
Persone che trattano reperti informatici e precauzioni

- Il DEFR deve mettere in sicurezza e proteggere il luogo appena possibile
  - Mettere in sicurezza e controllare l'area che contiene dispositivi di memorizzazione digitale
  - Individuare il responsabile dell'area
  - Allontanare le persone dai dispositivi digitali e dall'alimentazione elettrica
  - Documentare tutti quelli che sono autorizzati ad accedere all'area
    - E chi potesse avere moventi
  - Non mutare lo stato delle apparecchiature
    - Se acceso non spegnere, se spento non accendere
  - Documentare la scena, componenti, cavi
    - Fotografie, video, disegni, schemi
  - Individuare note, appunti, diari, fogli, manuali
    - Ricerca password, PIN

ISO/IEC 27037/2012
Persone che trattano reperti informatici

- Digital evidence specialists (*DESs*)
  - Operatore esperto di evidenze informatiche
- Incident response specialists
  - Operatore che si occupa del primo intervento post incidente informatico
    - In Italia spesso coincide (ahimè) con l'amministratore di sistema
- Forensic laboratory managers
  - Operatore responsabile di laboratorio informatico

ISO/IEC 27037/2012
Dispositivi di memorizzazione che contengono dati

- Dispositivi di memorizzazione utilizzati nei computer quali dischi rigidi, floppy disk, supporti ottici, supporti magneto-ottici e altri dispositivi con funzioni simili
- Telefoni cellulari, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards, sistemi di navigazione mobile (GPS)
- Fotocamere e videocamere (incluse quelle a circuito chiuso)
- Computer con connessione di rete
- Reti basate sul protocollo TCP/IP e su altri protocolli
- Altri dispositivi assimilabili a quelli sopra definiti

La lista è indicativa e non esaustiva

Glossario

- Dispositivo digitale
  - Apparato elettronico usato per processare o memorizzare dati digitali
- Dispositivo di memorizzazione di dati digitali
  - Dispositivo che è in grado di memorizzare dati digitali
    - *[ISO/IEC 10027:1990]*
- Periferica
  - Dispositivo che, connesso ad un dispositivo digitale, ne estende le funzionalità

Glossario

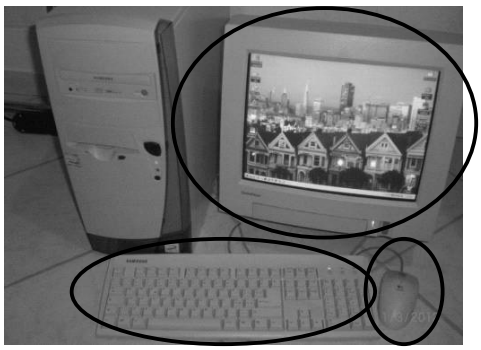
Dispositivo digitale *vs.* Dispositivo di memorizzazione di dati digitali *vs.* periferica

Glossario

Dispositivo digitale *vs.* Dispositivo di memorizzazione di dati digitali *vs.* periferica

Glossario

Dispositivo digitale *vs.* Dispositivo di memorizzazione di dati digitali *vs.* periferica



Glossario

- Spazio allocato
  - Area di un dispositivo di memoria che è utilizzata per memorizzare dati, inclusi metadati
- Spazio non allocato
  - Area di un dispositivo di memoria che non è allocato dal sistema operativo ed è a disposizione per memorizzare dati, inclusi metadati
- Manca definizione di **Slack space**
  - Area (compresa tra l'ultimo bit e la fine del settore) non utilizzata dal file che ha allocato lo spazio per ultimo

Glossario
Spazio allocato *vs.* non allocato (*vs.* slack)

01001010011	11101010101	01010100111	10010000110	

O più comunemente…

01001010011
11101010101
01010100111
10010000110

Glossario
Spazio allocato *vs.* non allocato (*vs.* slack)

Promessi sposi.txt	1	0
Il Cinque Maggio.txt	7	1
Divina commedia.txt	1	1

Nel mezzo del cammin di nostra vita

Ei fu. Siccome immobile, dato il mortal sospiro

1	**Nel mezz**	**1**	**2**
2	**o del ca**	**1**	**3**
3	**mmin di**	**1**	**4**
4	**nostra v**	**1**	**5**
5	**itaX a m**	**1**	**/**
5	**ezzogior**	**0**	**6**
6	**noX**	**0**	**/**
7	Ei fu. S	1	8
8	iccome i	1	9
9	mmobile,	1	10
10	dato il	1	11
11	mortal	1	12
12	sospiroX	1	/
13		0	/
14		0	/
15		0	/
16		0	/

Glossario
Spazio allocato *vs.* non allocato (*vs.* slack)

Promessi sposi.txt	1	0
Il Cinque Maggio.txt	7	1
Divina commedia.txt	1	1

Nel mezzo del cammin di nostra vita

Ei fu. Siccome immobile, dato il mortal sospiro

1	**Nel mezz**	**1**	**2**
2	**o del ca**	**1**	**3**
3	**mmin di**	**1**	**4**
4	**nostra v**	**1**	**5**
5	**itaX a m**	**1**	**/**
5	**ezzogior**	**0**	**6**
6	**noX**	**0**	**/**
7	Ei fu. S	1	8
8	iccome i	1	9
9	mmobile,	1	10
10	dato il	1	11
11	mortal	1	12
12	sospiroX	1	/
13		0	/
14		0	/
15		0	/
16		0	/

Spazio allocato

Glossario
Spazio allocato *vs.* non allocato (*vs.* slack)

Promessi sposi.txt	1	0
Il Cinque Maggio.txt	7	1
Divina commedia.txt	1	1

Nel mezzo del cammin di nostra vita

Ei fu. Siccome immobile, dato il mortal sospiro

1	**Nel mezz**	**1**	**2**
2	**o del ca**	**1**	**3**
3	**mmin di**	**1**	**4**
4	**nostra v**	**1**	**5**
5	**itaX a m**	**1**	**/**
5	**ezzogior**	**0**	**6**
6	**noX**	**0**	**/**
7	Ei fu. S	1	8
8	iccome i	1	9
9	mmobile,	1	10
10	dato il	1	11
11	mortal	1	12
12	sospiroX	1	/
13		0	/
14		0	/
15		0	/
16		0	/

Spazio non allocato

Glossario
Spazio allocato *vs.* non allocato (*vs.* slack)

Promessi sposi.txt	1	0
Il Cinque Maggio.txt	7	1
Divina commedia.txt	1	1

Nel mezzo del cammin di nostra vita

Ei fu. Siccome immobile, dato il mortal sospiro

1	**Nel mezz**	**1**	**2**
2	**o del ca**	**1**	**3**
3	**mmin di**	**1**	**4**
4	**nostra v**	**1**	**5**
5	**itaX a m**	**1**	**/**
5	**ezzogior**	**0**	**6**
6	**noX**	**0**	**/**
7	Ei fu. S	1	8
8	iccome i	1	9
9	mmobile,	1	10
10	dato il	1	11
11	mortal	1	12
12	sospiroX	1	/
13		0	/
14		0	/
15		0	/
16		0	/

Slack space

Glossario

- Prova digitale
  - Informazione o dato, memorizzato o trasmesso in formato binario, che può essere utilizzato come prova
- Copia di prova digitale
  - Copia di prova digitale che può essere prodotta per mantenere l'affidabilità della prova, includendo sia la prova digitale che la procedura di verifica

Glossario

- Dato volatile
  - Dato facilmente soggetto a modifica. Una variazione può essere dovuta ad assenza di corrente o ad interventi di campi magnetici, a cambi di stato del sistema
    - Es.: dati contenuti in RAM
- Alterazione
  - Modifica del valore di potenziali evidenze digitali che ne riduce l'eventuale valore probatorio
- Distruzione di prova
  - Modifica volontaria del valore di potenziali evidenze digitali che ne riduce l'eventuale valore probatorio

Glossario

- Ripetibilità
  - Proprietà di un processo che produce lo stesso risultato partendo dallo stesso ambiente di partenza
- Riproducibilità
  - Proprietà di un processo che produce lo stesso risultato da ambienti di test differenti

Glossario

- Digital Evidence First Responder (DEFR)
  - Persona che è autorizzata, preparata e qualificata per operare per primo sulla scena del crimine al fine di raccogliere e acquisire prove digitali con il compito di imballare e conservare la prova
- Digital Evidence Specialist (DES)
  - Persona che può svolgere i compiti di un DEFR e ha conoscenze, competenze e capacità specialistiche per gestire una vasta gamma di questioni tecniche (ad esempio, acquisizioni in rete, sistemi operativi…)

Glossario

- Identificazione
  - Processo di ricerca, ricognizione e documentazione di potenziali prove digitali
- Raccolta
  - Processo di raccolta di dispositivi fisici che contengono potenziali prove in formato digitale
- Acquisizione
  - Processo di creazione di una copia di dati
  - Il prodotto del processo di acquisizione è una potenziale copia prova digitale

Glossario

- Conservazione
  - Processo di mantenimento e salvaguardia dell'integrità e delle condizioni originarie della potenziale prova informatica
- Deposito per la conservazione delle prove
  - Ambiente sicuro in cui prove raccolte o acquisite sono conservate
  - I supporti non devono essere esposti a campi magnetici, polvere, vibrazioni o altri elementi ambientali (ad esempio temperatura o umidità) che possono danneggiare i potenziali elementi di prova

Glossario

- Valore di hash
  - Stringa di bit che è prodotta in output da una funziona hash
  - *[ISO/IEC 10118-1:2000]*
- Validazione
  - Conferma, attraverso una prova, che i requisiti preposti sono stati soddisfatti
  - *[ISO/IEC 27004:2009]*
- Funzione di verifica
  - Funzione usata per verificare che due insieme di dati sono identici. Il processo di verifica è tipicamente implementato usando una funzione hash (come MD5, SHA1…)

Acronimi

- **AVI**: Audio Video Interleave
- **CCTV**: Closed Circuit Television
- **CD**: Compact Disk
- **DNA**: Deoxyribonucleic Acid
- **DEFR**: Digitai Evidence First Responder
- **DES**: Digitai Evidence Specialist
- **DVD**: Digitai VideoNersatile Disk
- **ESN**: Electronic Serial Number
- **GPS**: Global Positioning System
- **GSM**: Global System for Mobile Communication
- **IMEI**: International Mobile Equipment Identity
- **IP**: Internet Protocol
- **ISIRT**: Information Security Incident Response Team
- **LAN**: Local Area Network
- **MD5**: Message-Digest Algorithm 5
- **MP3**: MPEG Audio Layer 3
- **MPEG**: Moving Picture Experts Group
- **NAS**: Network Attached Storage
- PDA: Personal Digitai Assistant
- **PED**: Personal Electronic Device
- **PUK**: PIN Unlock Key
- **RAID**: Redundant Array of Independent Disks
- **RAM**: Random Access Memory
- **RFID**: Radio Frequency Identification
- **SAN**: Storage Area Network
- **SHA**: Secure Hash Algorithm
- **SIM**: Subscriber Identity Module
- **USB**: Universal Serial Bus
- **UPS**: Uninterruptible Power Supply
- **USIM**: Universal Subscriber Identity Module
- **uv**: Ultraviolet
- **WiFi**: Wireless Fidelity

Requisiti per la gestione della prova digitale Requisiti generali

- Pertinenza
  - Serve per incolpare (o discolpare)
  - Dimostrare che il materiale è rilevante, cioè che contiene dati utili e che pertanto esiste una buona ragione per acquisirli
- Affidabilità
  - Assicurarsi che la prova digitale sia genuina
  - Tutti i processi eseguiti devono essere ben documentati e, se possibile, ripetibili. Il risultato dovrebbe essere riproducibile
- Sufficienza
  - Il DEFR deve valutare quanto materiale deve essere raccolto e le procedure da utilizzare
  - Il materiale può essere copiato o acquisito (preso)
  - Non è detto che sia sempre necessario acquisire una copia completa
    - Valutare in base al caso (interessa la figura del DEFR)
    - Può dipende dalla legislazione nazionale

Requisiti per la gestione della prova digitale Aspetti chiave

- Verificabilità
  - Un terzo deve essere in grado di valutare le attività svolte dal DEFR e dal DES
    - Possibile se esiste documentazione delle azioni svolte
    - Valutare metodo scientifico, tecniche e procedure seguite
  - DEFR e DES devono essere in grado di giustificare le azioni svolte
- Ripetibilità
  - Le operazioni sono ripetibili sempre usando le stesse procedure, lo stesso metodo, gli stessi strumenti, sotto le stesse condizioni
- Riproducibilità
  - Le operazioni sono ripetibili sempre usando lo stesso metodo, strumenti diversi, sotto condizioni diverse
- Giustificabilità
  - Dimostrare che le scelte adoperate erano le migliori possibili

Processo di gestione della prova digitale Aspetti chiave

- La ISO/IEC 27037:2012 si limita alle fasi iniziali del processo di gestione della prova informatica
  - Non arriva all'analisi
- La prova digitale è per sua natura fragile
  - Può subire alterazioni naturali, colpose o dolose
- 4 fasi
  - Identificazione
  - Raccolta
  - Acquisizione
  - Conservazione

Processo di gestione della prova digitale Fasi

- Identificazione
  - La prova informatica si presenta in forma fisica e logica
    - Device
    - Rappresentazione
  - Ricerca dei device che possono contenere dati rilevanti
    - Priorità ai dati volatili
    - Considerare dispositivi di difficile identificazione
      - Geografica
        - Es.: Cloud computing, SAN
      - Dimensioni
        - Es.: miniSD

Processo di gestione della prova digitale Fasi

- Si considera computer un dispositivo digitale standalone che riceve, processa e memorizza dati e produce risultati
  - Non connesso in rete
  - Ci possono essere periferiche connesse
- Se il computer ha un'interfaccia di rete, anche se non è connesso in rete al momento dell'intervento, bisogna individuare eventuale sistemi con cui può aver comunicato

Processo di gestione della prova digitale
Fasi

- La scena del crimine può contenere diversi tipi di dispositivi di memorizzazione
  - Hard disk, hard disk esterni, floppy disk
  - Memorie flash, memory card, CD, DVD, Blu-ray
- Il DEFR deve
  - Documentare marca, tipo, s/n di ogni supporto
  - Identificare tutti i computer e le periferiche e il loro stato
    - Se acceso, documentare cosa si vede a schermo
      - Fotografia, video, scrivere a verbale
  - Recuperare i cavi di alimentazione dei dispositivi che usano batterie
  - Utilizzare un rilevatore di segnali wireless per eventuali sistemi non visibili
  - Considerare anche evidenze non digitali e/o fornite a voce

Processo di gestione della prova digitale
Fasi

- In sede di raccolta o acquisizione bisogna considerare alcuni fattori
  - Volatilità
  - Esistenza di cifratura a livello di supporto o di partizione
  - Criticità del sistema
  - Requisiti legali
  - Risorse
    - Disponibilità di storage, tempo, disponibilità di personale

Processo di gestione della prova digitale
Fasi

- Raccolta
  - Device vengono rimossi dalla posizione originaria e trasportati in laboratorio per acquisizione e analisi
    - Talvolta rimuovere un supporto può essere pericoloso
  - Il device può trovarsi in due situazioni
    - Acceso o spento
      - Approcci diversi, tool diversi
  - DEFR e DES devono utilizzare il metodo migliore sulla base di situazione, costi, tempi
    - Tutto da documentare
  - Raccogliere anche gli accessori

Processo di gestione della prova digitale
Fasi

- Acquisizione
  - Creazione di una copia forense e documentazione di metodo, strumenti, attività
    - Supporto, partizione, gruppo di file
      - Acquisendo solo un gruppo di file si perdono alcuni dati
        - Es.: spazio non allocato, file cancellati, slack space
    - Apportare meno alterazioni possibili
      - Tendere a non modificare alcun bit
      - Documentare eventuali alterazioni e giustificare
      - Es.: sistema in esecuzione, settori danneggiati, tempo insufficiente

Processo di gestione della prova digitale
Fasi

- Conservazione
  - Proteggere integrità dei dati
    - Da alterazioni naturali, colpose o dolose
  - Normalmente, non dovrebbero esserci alterazioni
    - Utilizzare metodologia per dimostrare che non si sono verificate alterazioni
  - Proteggere anche la riservatezza dei dati
  - Utilizzare imballaggi opportuni
    - Es.: per i supporti magnetici, imballaggi antistatici
    - Non devono danneggiare il supporto

Processo di gestione della prova digitale
Fasi

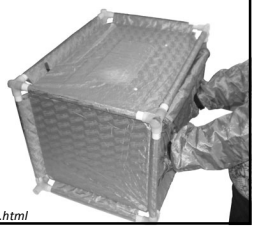
- Etichettare tutto
- Verificare che le batterie siano opportunamente caricate (e ricaricare), ove presenti
- Bloccare parti mobili
- Ridurre rischi in base alla natura del supporto
- Ridurre rischi dovuti al trasporto
- Preservare eventuali altri tracce
  - Es.: tracce biologiche
  - Utilizzare guanti puliti

Conservazione
ESD Bag

Conservazione
Patented Wireless StrongHold Bag

http://www.paraben.com/stronghold-bag.html

Conservazione
Tabletop StrongHold Tent



http://www.paraben.com/tabletop-stronghold.html

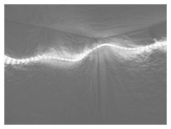
Conservazione
StrongHold Pouch

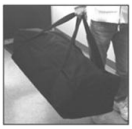
http://www.paraben.com/stronghold-pouch.html

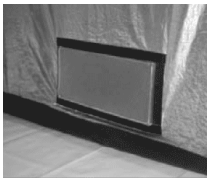
Conservazione
StrongHold Tent

http://www.paraben.com/stronghold-tent.html

Conservazione
StrongHold Tent





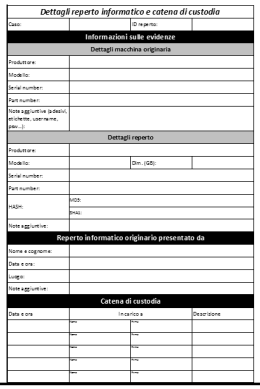


http://www.paraben.com/stronghold-tent.html

Processo di gestione della prova digitale
Catena di custodia

- Documentare movimenti e interazioni con la potenziale prova digitale
- Storia del supporto a partire dalla fase di raccolta
- Formato cartaceo o digitale
- Deve contenere
  - Identificativo unico dell'evidenza
  - Quando, dove, chi e perché ha avuto accesso all'evidenza
  - Documentare e giustificare ogni alterazione inevitabile, con il nome del responsabile

Processo di gestione della prova digitale
Catena di custodia



Dettagli reperto informatico e catena di custodia			
Caso:		ID reperto:	
Informazioni sulle evidenze			
Dettagli macchina originaria			
Produttore:			
Modello:			
Serial number:			
Part number:			
Note aggiuntive (adesivi, etichette, username, psw…):			
Dettagli reperto			
Produttore:			
Modello:		Dim. (GB):	
Serial number:			
Part number:			
HASH:	MD5:		
	SHA1:		
Note aggiuntive:			
Reperto informatico originario presentato da			
Nome e cognome:			
Data e ora:			
Luogo:			
Note aggiuntive:			
Catena di custodia			
Data e ora	Incarico a		Descrizione
	Nome	Firma	
	Nome	Firma	
	Nome	Firma	
	Nome	Firma	
	Nome	Firma	

Processo di gestione della prova digitale
Catena di custodia

Dettagli reperto informatico e catena di custodia			
Caso:		ID reperto:	
Informazioni sulle evidenze			
Dettagli macchina originaria			
Produttore:			
Modello:			
Serial number:			
Part number:			
Note aggiuntive (adesivi, etichette, username, psw…):			
Dettagli reperto			
Produttore:			
Modello:		Dim. (GB):	
Serial number:			
Part number:			
HASH:	MD5:		
	SHA1:		
Note aggiuntive:			

Processo di gestione della prova digitale
Catena di custodia

Reperto informatico originario presentato da			
Nome e cognome:			
Data e ora:			
Luogo:			
Note aggiuntive:			
Catena di custodia			
Data e ora	Incarico a		Descrizione
	Nome	Firma	
	Nome	Firma	
	Nome	Firma	
	Nome	Firma	
	Nome	Firma	

Briefing

- Capire cosa è accaduto
- Cosa cercare
- Cosa ci si aspetta di trovare e cosa ci si aspetta di non trovare
- Valutare aspetti di riservatezza
- Valutare precauzione per mantenere integrità dei dati

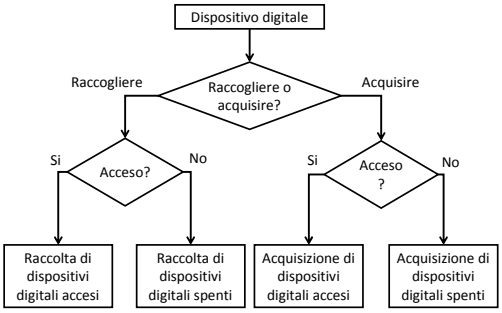
Briefing

- Tipo di incidente
- Data e ora
- Definire piano di investigazione
- Considerare dove e come l'evidenza digitale è memorizzata/trasportata
- Individuare eventuali tool specifici per le attività di acquisizione
- Definire strumenti necessari
- Disattivare comunicazioni via cavo e senza fili
- Assegnare compiti ai vari soggetti
  - Non accettare ausilio tecnico da non autorizzati
  - Utilizzare materiali opportuni per l'imballaggio

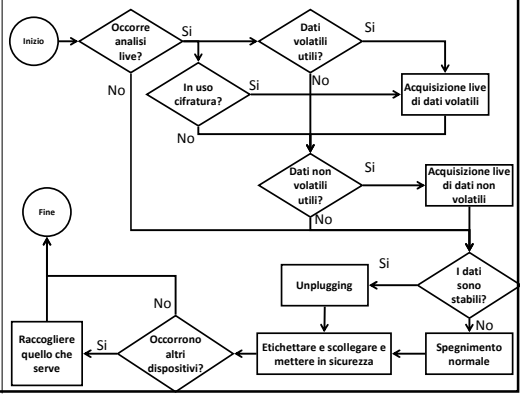
Precauzioni sulla scena del crimine
Valutazione dei rischi

- Scegliere bene tool e metodologie
  - Rischi non calcolati possono compromettere per sempre i dati
- Una valutazione dei rischi riduce al minimo gli errori
  - Che tipo di metodologia applicare per la raccolta e l'acquisizione?
  - Quali strumenti possono essere utili per l'attività?
  - Qual è il livello di volatilità dei dati?
  - I dati sono raggiungibili da remoto? Qual è il rischio di alterazione?
  - Cosa fare se gli strumenti non dovessero funzionare?
  - I dati potrebbero essere stati già compromessi?
  - È possibile che siano state previste bombe logiche per distruggere o nascondere dati?

Identificazione



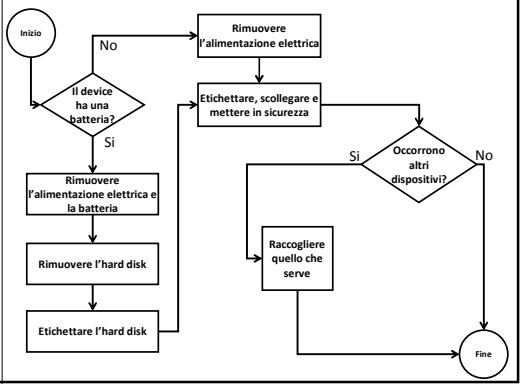
Dispositivi accessi



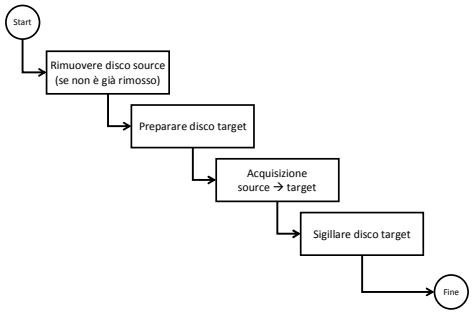
Linee guida per acquisizione di dispositivi di memorizzazione digitali – Stato: spento

- No dati volatili
- Procedura:
  - Assicurarsi che i dispositivi siano effettivamente spenti
  - Rimuovere il dispositivo di memorizzazione dal dispositivo spento (se non già rimosso)
    - Porre attenzione quando il dispositivo di memorizzazione viene rimosso: potrebbe essere confuso con altri o danneggiato
  - Etichettare il dispositivo di memorizzazione come "suspect"
  - Documentare tutti i dettagli
    - Produttore, modello, serial number, part number, dimensione
  - Acquisire e calcolare impronta hash

Dispositivi spenti



Acquisizione dispositivo spento



Situazioni critiche

- In alcuni casi, I dispositivi non possono essere spenti a causa della natura del sistema
  - Es.: data center che offrono servizi a terzi, sistemi di sorveglianza, sistemi medici, altri sistemi critici…
- Occorre prevedere particolari attenzioni
- É possibile procedere con
  - Acquisizione live
  - Acquisizione parziale

Situazioni critiche
Acquisizione parziale

- Si procede ad un'acquisizione parziale quando intervengono particolari situazioni:
  - Il sistema da acquisire contiene troppi dati
    - Es.: Google server… ma anche "banali" DB server
  - Il sistema non può essere spento
  - Solo alcuni dati sono rilevanti
  - Solo alcuni dati possono essere acquisiti per vincoli legali
- Quando si procede ad un'acquisizione parziale, le attività devono includere (ma non sono limitate a):
  - Identificazione delle cartelle, file ed ogni altra proprietà o opzione rilevante
  - Acquisizione dei sopra indicati dati

Competenze degli operatori
Identificazione

- Identificare
  - Dati e informazioni utili per il proseguimento delle indagini
  - Strumenti per raccolta e acquisizione
  - Valutazione dei rischi
- Competenze
  - Utente e amministratore di vari tipi di dispositivi
  - Procedure di indagine sulla scena del crimine
  - Capacità di determinare lo stato del sistema
  - Conoscere sistemi e configurazione di log
    - Email, web, accessi, password…
  - Conoscere funzionamento dei dispositivi
  - Conoscere l'importanza dei dati volatili e non volatili
  - Comprensione dei diagrammi di rete
  - Comprendere le connessioni tra indirizzi IP e indirizzi MAC

Competenze degli operatori
Raccolta

- Identificare
  - Tool e procedure per imballaggio dei supporti, protezione da minacce ambientali
- Competenze
  - Raccolta in sicurezza di dati e dispositivi digitali
  - Definire il miglior metodo per la raccolta e la conservazione del maggior numero di informazioni
  - Definire documenti di catena di custodia
  - Interrogare persone che utilizzano i sistemi
  - Identificare e raccogliere tutti i dati e gli strumenti che possono tornare utili in fase di analisi
    - Password, dongle, metodologie…

Competenze degli operatori
Acquisizione

- Requisiti
  - Metodologie e strumenti per garantire ripetibilità, riproducibilità, integrità dei dati
  - Acquisire dati e applicare hash
- Competenze
  - Struttura dei file system (e RAID) dei vari sistemi operativi
  - Comprendere l'organizzazione dei dati nei supporti
    - File generati dal sistema, file generati dall'utente
  - Saper definire i requisiti di storage
  - Eseguire le operazioni tecniche di acquisizione
    - Dispositivi spenti, accesi, di rete; Contesti critici; Parziali; Generazione di impronte hash
  - Capire quanto incide una procedura di acquisizione rispetto ad un'altra

Competenze degli operatori
Conservazione

- Requisiti
  - Applicare e valutare requisiti per la conservazione
  - Mantenimento della catena di custodia
- Competenze
  - Impatto delle minacce ambientali
    - Umidità, temperatura…
  - Imballaggio e trasporto di dispositivi digitali

Quantificazione ed individuazione delle alterazioni dei dati nell'ambito di indagini di Informatica Forense

Michele Ferrazzano

Quello che accade nella pratica…

CORRIERE DELLA SERA

L' ULTIMA UDIENZA

Garlasco, l' arringa dei legali di Alberto: computer alterato, dovete assolverlo

VIGEVANO (Pavia) - Tanti indizi, sì. Ma nessuna prova. Nessun movente e niente arma del delitto. E poi troppi elementi trascurati nel corso delle indagini. «Alberto è innocente. Non ha ucciso lui Chiara Poggi la mattina del 13 agosto 2007, a Garlasco». Quindi, la via è obbligata: assoluzione, per non aver commesso il fatto. È il filo logico seguito dalla difesa di Alberto Stasi, il professor Angelo Giarda e i fratelli Giulio e Giuseppe Colli. Ieri le loro conclusioni davanti al giudice dell' udienza preliminare di Vigevano, Stefano Vitelli: dieci ore di arringa per convincere il gup che la mattina del delitto il biondino di Garlasco non massacrò la sua fidanzata ma rimase a casa sua a scrivere quattro pagine della tesi di laurea. La dimostrazione del suo alibi, ripetono da mesi i tre legali, è stata compromessa dall' alterazione dei dati del computer, aperto e consultato più volte dai carabinieri prima che fosse consegnato ai colleghi del Ris di Parma. Il perito del pubblico ministero Rosa

Quello che accade nella pratica…

- Poca attenzione degli operanti
- Si verificano alterazioni dei dati
- Si compromette l'utilizzabilità di una prova
  - A favore o contro l'indagato
  - A favore o contro terzi

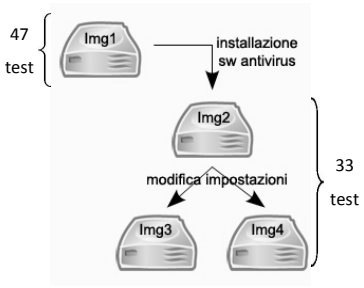
Studio sperimentale sull'alterazione dei reperti informatici

- Verificare
  - cosa accade in caso di utilizzo scorretto del reperto informatico
- Misurare
  - **quante e quali alterazioni si verificano**

Modalità operative per l'analisi delle alterazioni

- Metodologia utilizzata per eseguire i test
  - Simulazione di semplici azioni (molto più semplici di quelle eseguite nella realtà) che un operatore inesperto/disattento potrebbe ragionevole provare
  - Utilizzo di una macchina virtuale con il sistema operativo più diffuso sul mercato alla data di esecuzione dei test
    - Microsoft Windows XP con SP 3
  - Ripetizione dei test partendo sempre dallo stesso stato di partenza
  - Utilizzo di una distribuzione live forense per analisi del disco

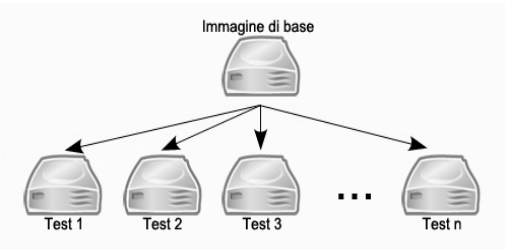
Simulazione ipotizzando diversi scenari



Simulazione ipotizzando diversi scenari

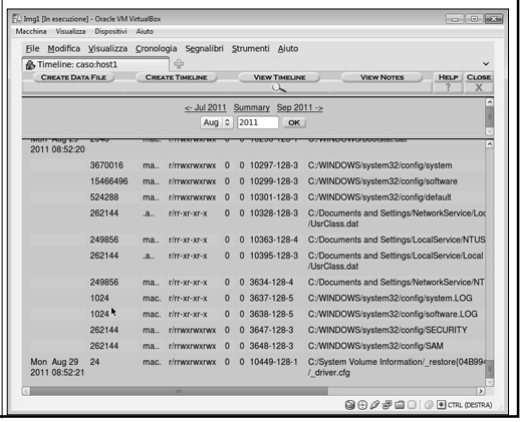
- Sistema operativo e software applicativi molto diffusi, con configurazioni di default
  - Microsoft Windows XP con SP3
  - Microsoft Office
  - OpenOffice
  - Acrobat Reader
- Varianti
  - Installazione di un antivirus
    - Avast Free Edition
  - Modifica di alcune impostazioni
- In totale 80 test eseguiti

Modalità operative



Un'immagine forense per ogni test per garantire l'indipendenza

Timeline e metadati

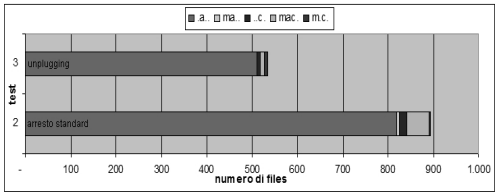


Timeline e metadati

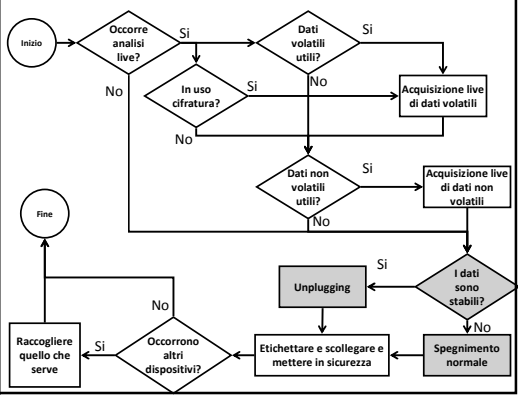
m "written"	Il file è stato modificato
a "accessed"	Il file è stato acceduto
c "changed"	I metadati del file (MFT) sono cambiati
b "created"	Il file è stato creato

- Alterazioni rilevate dopo una determinata data sul File System
- Calcolate le variazioni per tipologia di variazione e possibili combinazioni di esse

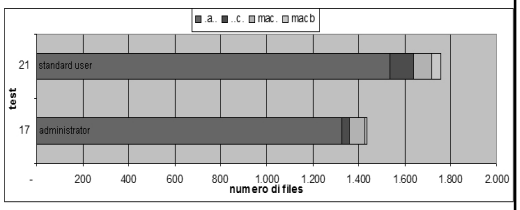
Unplugging *vs.* shutdown



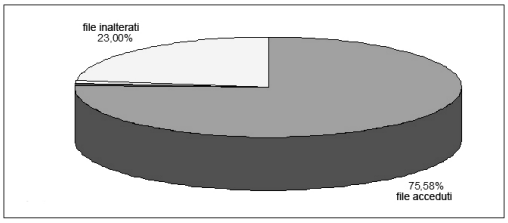
Vi ricordate?



Standard user *vs.* Admin user



Gli effetti dell'utilizzo della funzione "Cerca" di Windows



Conclusioni

- Il reperto informatico è estremamente delicato e i dati in esso contenuti sono estremamente volatili
  - Necessità di rigore scientifico nel trattamento di dati informatici
- Alcune operazioni portano un numero di alterazioni estremamente elevato
  - Almeno nelle date di accesso
    - Si perdono alibi
    - Si perde consapevolezza
    - Si perdono prove!