La norma ISO/IEC 27037

Guidelines for identification, collection, acquisition and preservation of digital evidence

Alessandro Guarino
Digital Forensics Alumni
www.perfezionisti.it

Milano, 10 Novembre 2011

La norma nella serie 27000

Si colloca tra quelle "meno note"
È ancora in fase di sviluppo
(prevista al momento la pubblicazione nel 2012)

E' (sarà) una "linea guida"
non verificabile o certificabile

Iter di approvazione: a che punto siamo

- ✔ Preliminary stage
- ✔ Proposal stage
- ✔ Preparatory stage (WDs - working drafts)
- ✔ **Commitee stage (CDs - commitee drafts)**
- ✗ **Enquiry stage (DIS - draft international standard) 31/10/11**
- ✗ Approval stage (FDIS - final draft international standard)
- ✗ Publication stage
- ✗ (periodical review, withdrawal)

Iter di approvazione: a che punto siamo

Il 31 Ottobre è stata pubblicata la prima bozza "definitiva" (DIS)

In votazione fino al 31 Marzo 2012

Ambito di applicazione

Fasi di lavoro:

Fornisce linee guida per specifiche attività nella gestione (handling) delle evidenze digitali.

Da subito definisce le fasi:
Identificazione
Raccolta (*collection*)
Acquisizione
"Conservazione" (*preservation*).

Ambito di applicazione

La norma non riguarda quindi le fasi di analisi, presentazione, eliminazione (*disposal*).

Ambito di applicazione

Giurisdizioni

Nessun riferimento a particolari giurisdizioni ma uno degli obiettivi è facilitare l'interscambio di evidenze (potenziali) tra giurisdizioni diverse.

Applicabile a contesti aziendali e processuali.

Ambito di applicazione

Tecnico

Esplicito elenco di dispositivi/circostanze/tipologie di evidenze a cui si applica: dispositivi di storage ottici e magnetici, telefoni, PDA (esistono ancora?) e schede di memoria, dispositivi di navigazione, fotocamere e videocamere digitali, postazioni di lavoro connesse in rete, reti basate su TCP/IP e altri protocolli digitali, sistemi di videosorveglianza.

Definizioni

***Digital evidence* / evidenze digitali:**

informazioni o dati memorizzati o trasmessi in forma binaria su cui si può fare affidamento (*may be relied upon*) come evidenza (mezzi di prova).

Definizioni

DEFR e DES

(forse quelle più importanti...)

First responder: persona che è autorizzata, addestrata e qualificata ad agire per prima sulla scena (incident scene) per eseguire la raccolta e l'acquisizione delle evidenze digitali (con la relativa responsabilità). E' prevista esplicitamente la possibilità che il DEFR non abbia le tre caratteristiche dette: in questo caso altre circostanza possono essere considerate, compresa la legge locale applicabile.

Definizioni

DES (Specialist):

oltre ad essere in grado di assolvere i compiti del DEFR, possiede "conoscenza specializzata" per gestire una "grande quantità" di tecnologie.

Definizioni

Ripetibilità e riproducibilità

(*repeatability / reproducibility*):

Definizioni

Ripetibilità: proprietà di una procedura condotta per ottenere gli stessi risultati sullo stesso ambiente di test

Riproducibilità: proprietà di una procedura per ottenere gli stessi risultati in un diverso ambiente di test (computer, hd, modalità di operazione etc.)

Domanda aperta. come si possono conciliare queste definizioni con il C.P.P. Italiano e la prassi?

Overview (principi generali)

- Procedere nella maniera meno intrusiva possibile
- Documentare i metodi applicati in dettaglio, specie se risulta necessario modificare le evidenze
- Per quanto praticamente possibile i metodi usati devono essere comprensibili e riproducibili da altro personale competente

Overview (principi generali)

- Rilevanza
- Affidabilità
- "Sufficienza" (*sufficiency*)

Overview (principi generali)

relevance / rilevanza

Occorre dimostrare che il materiale acquisito è rilevante ai fini dell'investigazione, cioè contiene informazioni utili ad assistere nell'investigazione, ed è stato giustificabile acquisirlo

Overview (principi generali)

reliability / affidabilità

i processi devono essere verificabili (*auditable*) e ripetibili (*repeatable*).

Overview (principi generali)

sufficiency / sufficienza

Il DEFR deve assicurare di aver raccolto abbastanza materiale per permettere una adeguata investigazione, giustificando eventualmente le procedure e le scelte fatte nella raccolta.

Quanto corente con l'ordinamento italiano?

La norma dice che non è sempre necessario per il DEFR acquisire tutto il materiale etc.

Overview (principi generali)

Validazione degli strumenti (tool) prima del loro uso

Il concetto di validazione è stato oggetto di molti commenti; in quest'ultimo CD è stato ancora modificato ma rimane molto poco definito:

- può essere condotta "internamente" o "esternamente"
- la documentazione deve essere disponibile (data set di test ? procedure ?)

Overview (principi generali)

Passi da compiere per la gestione delle evidenze (*handling steps*)

In generale va minimizzato l'accesso al dispositivo originale, documentato ogni cambiamento e ogni azione intrapresa, conformarsi alle norme locali in vigore e non effettuare nessuna azione al di là della proprie competenze.

Overview (principi generali)

Identificazione

- Ricerca, riconoscimento, documentazione di potenziali evidenze sulla scena
- id fisica dei supporti e dei dispositivi
- questa fase include il triage eventuale
- va considerata la volatilità delle potenziali evidenze nel definire le priorità e l'ordine di acquisizione
- attenzione alle evidenze "nascoste"

Overview (principi generali)

Raccolta / *Collection*

- decisione per l'acquisizione sul posto o la “raccolta” del dispositivo
- i dispositivi che possono contenere evidenze vengono spostati dalla scena al laboratorio, dopo essere stati inventariati, documentati e adeguatamente protetti

Overview (principi generali)

Acquisizione

Questo processo classicamente comporta la produzione di un'immagine se possibile identica di una potenziale evidenza, sempre documentando e giustificando i metodi usati.

I metodi possono variare a seconda della:
- tipologia di supporto o dispositivo
- situazione
- tempi e costi

Overview (principi generali)

l'originale e la copia devono essere "verificati" e originale e copia devono fornire la stessa verifica (*hash*, per esempio)

in alcuni casi questo non è possibile (settori danneggiati, dischi troppo grandi, altre difficoltà) ma in ogni caso il metodo va giustificato e documentato

Overview (principi generali)

Preservation / **Conservazione**

- Protezione dell'integrità delle evidenze in ogni momento
- Processo che inizia sulla scena e continua in ogni momento del ciclo di vita
- Obiettivo: proteggere da *spoliation* (deterioramento non intenzionale) e *tampering* (modifiche intenzionali)
- la confidenzialità delle evidenze deve essere assicurata in ogni momento

Overview (principi generali)

Componenti chiave della identificazione, raccolta, acquisizione e conservazione.

Catena di custodia
Sicurezza
Ruoli e responsabilità, competenze

Overview (principi generali)

Catena di custodia

"in ogni investigazione il DEFR dovrebbe essere in grado di rendere conto di ogni dato e dispositivo acquisito in ogni momento durante l'investigazione"

L'obiettivo sarà raggiunto tipicamente tracciando la storia di ogni "item" (oggetto, evidenza) dal momento in cui è stato acquisito o raccolto sulla scena fino al presente.

Catena di custodia (2)

Contenuto minimo dei record: ID, operatore che ha avuto accesso, chi ha prelevato l'evidenza, quando e perchè...

Overview (principi generali)

Sicurezza (safety) sulla scena

(dell'"incidente", non del crimine...)

Generale

Controllo dell'area, determinare il referente, allontanare le persone presenti se applicabile.

Del personale

la persona investigata è presente?
si può isolare la scena?
ci sono armi?
ci sono macchinari pericolosi, materiali pericolosi?.

Delle evidenze:

- Selezione dei tool e dei dispositivi di acquisizione
- Procedure in caso di danneggiamento delle evidenze

Overview (principi generali)

Ruoli e responsabilità, competenze

DEFR e DES: il DES fornisce conoscenze e skill specializzati ai first responder

DEFR e DES devono essere forniti delle minime competenze per gestire le evidenze (tecniche e anche legali/procedurali), addestrati nella gestione di dispositivi digitali che possono contenere evidenze, devono mantenere queste conoscenze nel tempo.

Overview (principi generali)

Reasonable care

- Evitare azioni che possano condurre a degradazione delle evidenze
- Opportunità: evitare azioni in alcune condizioni:
- Attenzione alla business continuity
- Dispositivi mission-critical device (ad esempio medicali...)
- Supporti molto grandi
- Presenza di dati di terze parti non coinvolte

Overview (principi generali)

Documentazione

- Documentazione di ogni passo compiuto
- Attenzione a timestamp e date
- Documentazione degli schermi e dell'esterno dei dispositivi
- Identificazione, numeri di serie e fotografie
- Organizzazione: comunicazione (briefing) dei "primi risponditori"
- Prioritizzazione (triage), raccolta e acquisizione

Conservazione

Scenari di applicazione

Istanze

(scenari di applicazione più dettagliati)

§ 7.1 - Computer (PC) e periferiche associate

§ 7.2 – Dispositivi connessi in rete

Scenari di applicazione - Computer

Prima scelta:

acquisizione o raccolta ?
poi: dispositivo acceso o spento ?

Questo porta a quattro procedure dettagliate

Scenari di applicazione - Computer

Procedure per la raccolta (*collection*)

Dispositivo acceso:

• considerare l'acquisizione logica quando sia sospettabile la presenza di dischi o partizioni crittografate
• la configurazione del device determina le procedure di shut down: con le procedure normali del SO oppure "staccando la spina" (dal dispositivo, non dal muro..)
• etichettare, sconnettere e mettere in sicurezza cavi e porte di I/O
• Inibire fisicamente l'interruttore di accensione

Opzionali: togliere batterie in caso di portatili
Togliere CD/DVD dal drive se presente

Scenari di applicazione - Computer

Raccolta - Dispositivo spento:

- Sconnettere cavi di alimentazione
- Etichettare, sconnettere e mettere in sicurezza cavi e porte di I/O
- Opzionali: se possibile rimuovere i dischi fissi, etichettarli e documentarli
- Togliere CD/DVD dal drive se presente

Scenari di applicazione - Computer

Acquisizione – dispositivo acceso

- Considerare la necessità di acquisire la memoria o l'opportunità di non spegnere il dispositivo
- Quindi alternativa: spegnere e acquisire le memorie di massa oppure prima effettuare l'acquisizione dei dati più “deperibili” (RAM)

Scenari di applicazione - Computer

Acquisizione – dispositivo spento

- La procedura consigliata consiste nel rimuovere le memorie di massa, e dopo avere preparato (eliminato tutti i dati presenti) il disco destinazione, creare una copia (*imaging*)

Scenari di applicazione – dispositivi in rete

"Dispositivi connessi in rete" (*Networked devices*)

Procedure e definizioni non completamente formalizzate come la precedente e anche un po' confusa nell'esposizione.

Scenari di applicazione – dispositivi in rete

Definizione di "networked devices":

"computer o altri dispositivi digitali che sono connessi ad una rete cablata o senza fili. Possono includere mainframe, server, desktop, access point, switch, hub, router, dispositivi mobili, PDA, sistemi CCTV e molti altri..:"

Definizione vaga se mai ce n'è una...

Scenari di applicazione – dispositivi in rete

Identificazione

Raccomandazioni specifiche per identificare i dispositivi: possono essere utili le caratteristiche fisiche, eventuali interfacce proprietarie, etichette presenti (IMEI), il reverse lookup del numero telefonico (per definire l'operatore di rete).

Scenari di applicazione – dispositivi in rete

- Ricerca sulla scena e documentazione
- Registrare tipo, marca, modello, numero di serie di ogni dispositivo (e degli oggetti associati: SIM, alimentatori, confezioni etc)
- Per i dispositivi tipo server che forniscono servizi di rete: identificare se possibile i servizi -> definire il livello di criticità e la conseguenze in caso di disconnessione della rete
- CCTV: annotare numero/tipo delle videocamere e quali stanno registrando; tipo e configurazione del videoserver.

Scenari di applicazione – dispositivi in rete

Raccolta, acquisizione e conservazione

Generale - aspetti da considerare:
i dispositivi possono avere molti modi di connessione: RF, Blootooth, IR, Touch screen
varietà di sistemi operativi e quindi di modalità di acquisizione
non introdurre dispositivi wireless sulla scena

Scenari di applicazione – dispositivi in rete

Collection

E' raccomandato isolare il dispositivo della rete (in accordo con le leggi vigenti).

Documentare tutti le connessioni

Se la collection precede l'acquisizione il dispositivo deve essere mantenuto alimentato...

Scenari di applicazione – dispositivi in rete

Acquisizione

- Prima di sconnettere il dispositivo della rete, effettuare l'acquisizione logica
- Tenere conto della possibilità di connessioni multiple
- Isolamento dalla rete: (jammer, area di lavoro schermata, use delle (U)SIM forensi)

Scenari di applicazione

Sistemi di videosorveglianza
(*Ancora definiti CCTV*)

• Determinare se la sequenza di interesse è stata effettivamente registrata
• Determinare la/le videocamere interessate
• Verificare i timestamp delle immagini
• Opzioni possibili:
•acquisire i file video copiandoli su DVD/BR
•acquisire i file su un disco esterno
•acquisire via rete
•(extrema ratio): acquisire utilizzando le opzioni del sistema (esportazione MP4 etc). E' probabile che i file vengano compressi e si perdano informazioni.

Commenti italiani e criticità

Ultimo meeting

Il paragrafo sulle procedure per l'acquisizione dei dispositivi in rete troppo ampio → chiesta la separazione del “mobile forensics”

		to contact a network.	
	We feel the need to move to a separate clause, detailing a different instance, the procedures for identification, collection, acquisition and preservation of evidence coming from mobile devices (e.g. cell phones and tablet PCs) from the 7.2 clause. Main reason is the very different nature of the items and the consequent different procedural needs when dealing with mobile devices as opposed to network servers for instance.	We propose to modify the structure of the document inserting a new 7.3 clause titled "Mobile devices" and moving current 7.3 clause to 7.4. Content currently present in clause 7.2 and pertaining to mobile devices should be deleted and moving to the new 7.3 clause, which will have a sub-structure mirroring the present 7.2 like this: 7.3 Mobile devices 7.3.1 Identification 7.3.1.1 Overview	Rejected – During a previous meeting, it was decided to combine the subclause on mobile devices with the subclause on networked devices. In the interest of publishing the standard as soon as possible, this restructuring would delay the process. It is suggested that a separate clause on mobile devices be planned for the first revision of this document.

Commenti italiani e criticità

Ultimo meeting

Molte modifiche editoriali → eliminata la parola “triage” e sostituita con “prioritization”

Criticità

Non copre l'analisi (ci sono comunque degli item proposti dagli inglesi)

Grazie!
Domande?

Digital Forensics Alumni
www.perfezionisti.it

StudioAG – ICT Consulting & Engineering
www.studioag.eu
www.studioag.pro