ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

La gestione dell'Incidente Informatico in ambito aziendale

Paolo DAL CHECCO

Roma 28/01/2014

Agenda

- Presentazione relatore
- L'incidente informatico (RFC e ISO)
- La convenzione di Budapest
- Legge 48/2008
- D.lgs 231/2001
- La raccolta delle prove
- Strumenti
- Case Study
- Q&A
- Bibliografia & sitografia

Agenda

- Presentazione relatore
- L'incidente informatico (RFC e ISO)
- La convenzione di Budapest
- Legge 48/2008
- D.lgs 231/2001
- La raccolta delle prove
- Strumenti
- Case Study
- Q&A
- Bibliografia & sitografia

Presentazione relatore

Paolo Dal Checco

- PhD in Informatica @unito, gruppo Computer & Network Security
- Consulente Informatico Forense per Procure, Tribunali, Avvocati, Aziende e privati
- Consulenza su sicurezza e prevenzione dei reati informatici Ex. Art. 231/2001
- Co-titolare, insieme a Giuseppe Dezzani, dello Studio “Digital Forensics Bureau”
- Socio IISFA, CLUSIT, AIP
- DEFT Developer tra i fondatori della DEFT Association

Agenda

- Presentazione relatore
- L'incidente informatico (RFC e ISO)
- La convenzione di Budapest
- Legge 48/2008
- D.lgs 231/2001
- La raccolta delle prove
- Strumenti
- Case Study
- Q&A
- Bibliografia & sitografia

L’incidente informatico secondo le RFC

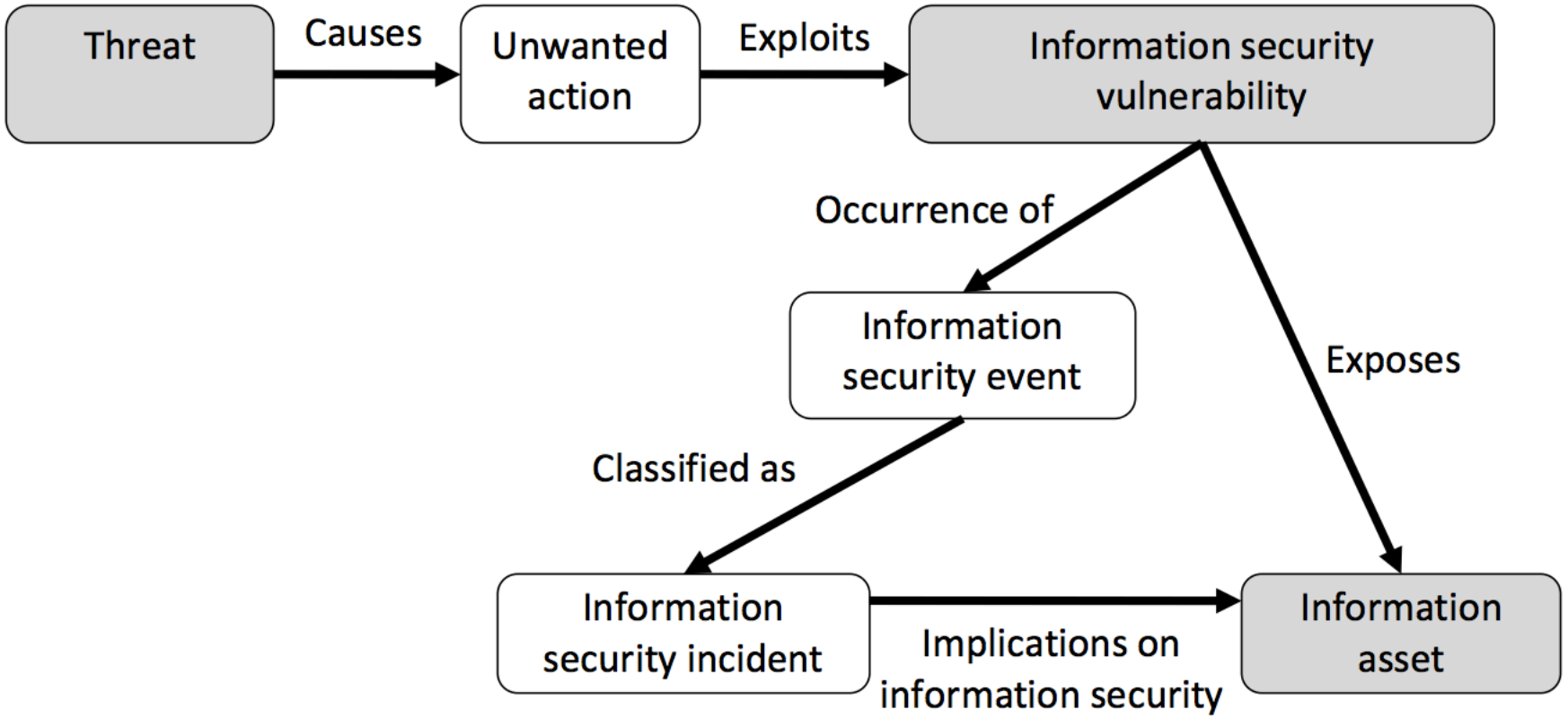
- RFC 2350: “Expectations for Computer Security Incident Response”
- Un evento che compromette aspetti della sicurezza dei computer e delle reti, con almeno uno dei seguenti fattori:
  - perdita di confidenzialità delle informazioni
  - compromissione dell’integrità delle informazioni
  - interruzione di servizio
  - utilizzo inappropriato di servizi, sistemi, informazioni
  - danneggiamento di sistemi

- Emerge l’mportanza del CSIRT “Computer Security Incident Response Team” (RFC 2828)

L’incidente informatico secondo ISO/IEC: ISO 27035

- “Information security incident management”
- Linee guida che forniscono approccio per rilevare, documentare e valutare, rispondere e gestire gli Incidenti Informatici;
- Descrizione di processi, routine che dovrebbero essere utilizzate da chi fornisce servizi di gestione degli incidenti informatici.

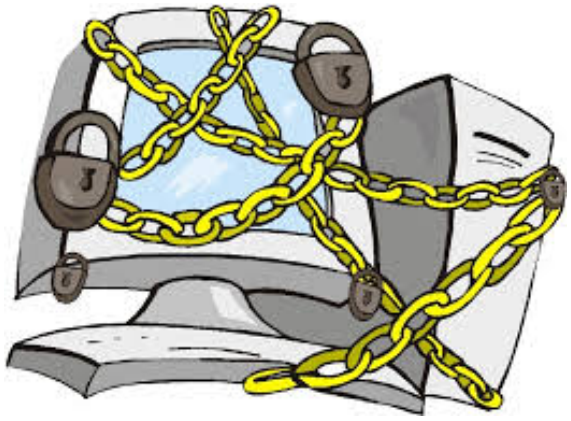
L’incidente informatico secondo ISO/IEC: ISO 27035



The shaded objects are pre-existing, affected by the unshaded objects in the chain that results in an information security incident.

L’incidente informatico secondo ISO/IEC: ISO 27037

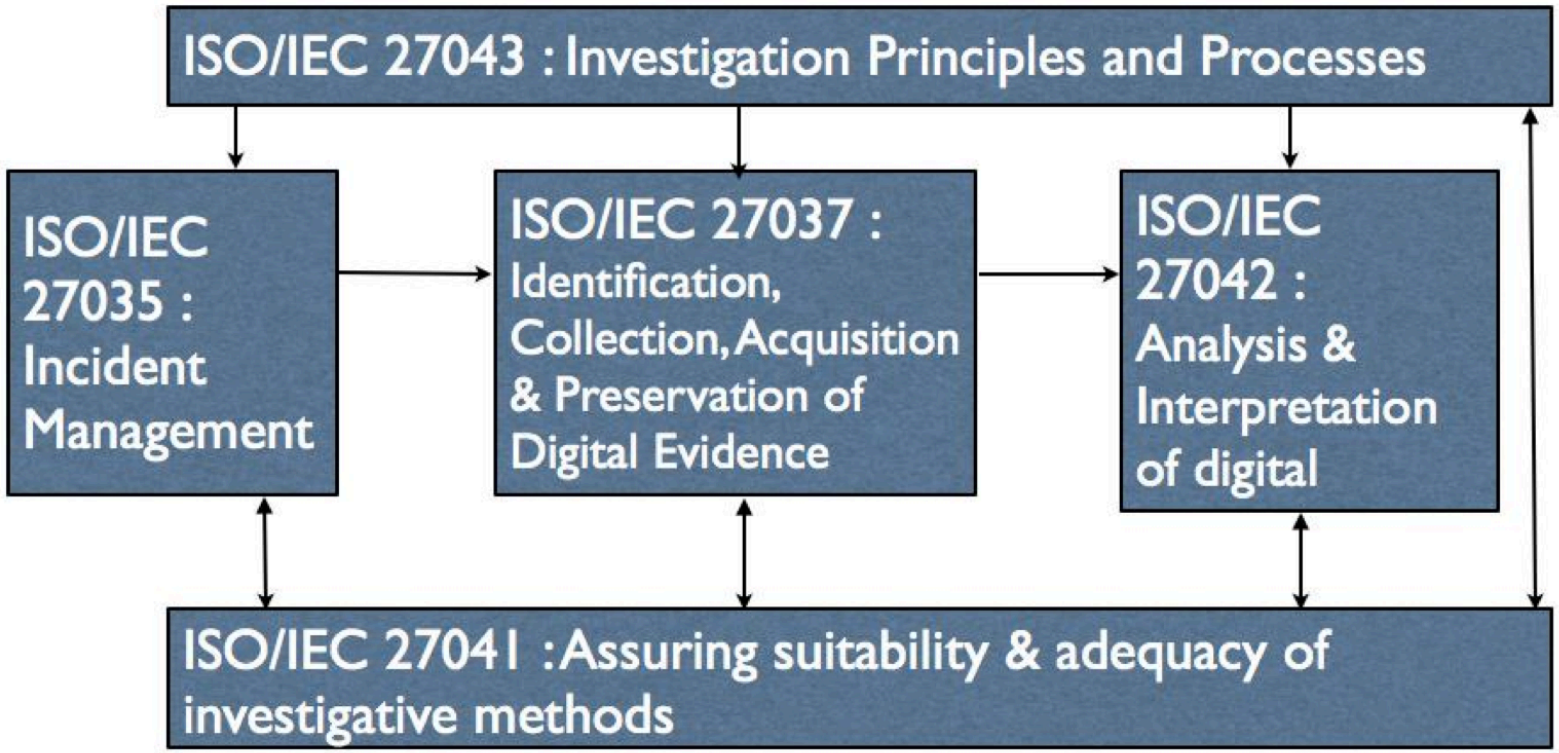
- “Guidelines for identification, collection, acquisition and preservation of digital evidence”
- Linee guida che riprendono la RFC 3227.
- Fasi di identificazione, raccolta, acquisizione e conservazione delle evidenze digitali
- Nasce la figura professionale del DEFR (Digital Evidence First Responder)
- Acquisizione dei reperti di particolare interesse probatorio.
- Attenzione all’integrità delle informazioni così ottenute
- Catena di custodia, ripetibilità, riproducibilità



L’incidente informatico secondo ISO/IEC: ISO 27041/2/3

- “iso 27041: Guidance on assuring suitability and adequacy of incident investigation methods (2013-03-22)
- iso 27042: Guidelines for the analysis and interpretation of digital evidence (2013-03-22)
- iso 27043: Incident investigation principles and processes (2013-03-22)

L’incidente informatico secondo ISO/IEC



Agenda

- Presentazione relatore
- L'incidente informatico (RFC e ISO)
- La convenzione di Budapest
- Legge 48/2008
- D.lgs 231/2001
- La raccolta delle prove
- Strumenti
- Case Study
- Q&A
- Bibliografia & sitografia

La Convenzione di Budapest

- La Convenzione è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche, e tratta in particolare le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete. Contiene inoltre una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati.
- Il suo obiettivo principale, enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro la cibercriminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale.

La Convenzione di Budapest

Situazione in data del : 25/1/2014

Stati membri del Consiglio d'Europa

	Firma	Ratifica	Entrata in vigore	Rinv.	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra	23/4/2013									
Armenia	23/11/2001	12/10/2006	1/2/2007				X			
Austria	23/11/2001	13/6/2012	1/10/2012		X	X	X			
Azerbaijan	30/6/2008	15/3/2010	1/7/2010		X	X	X	X		
Belgio	23/11/2001	20/8/2012	1/12/2012		X	X	X			
Bosnia e Erzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Cipro	23/11/2001	19/1/2005	1/5/2005				X			
Croazia	23/11/2001	17/10/2002	1/7/2004				X			
Danimarca	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Ex-Repubblica Jugoslava di Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Finlandia	23/11/2001	24/5/2007	1/9/2007		X	X	X			
Francia	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia	1/4/2008	6/6/2012	1/10/2012			X				
Germania	23/11/2001	9/3/2009	1/7/2009		X	X	X			
Gran Bretagna	23/11/2001	25/5/2011	1/9/2011		X		X			
Grecia	23/11/2001									
Irlanda	28/2/2002									
Islanda	30/11/2001	29/1/2007	1/5/2007		X		X			
Italia	23/11/2001	5/6/2008	1/10/2008				X			

http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ITA&NT=185

La Convenzione di Budapest

Italia	23/11/2001	5/6/2008	1/10/2008				X	
Lettonia	5/5/2004	14/2/2007	1/6/2007		X		X	
Liechtenstein	17/11/2008							
Lituania	23/6/2003	18/3/2004	1/7/2004		X	X	X	
Lussemburgo	28/1/2003							
Malta	17/1/2002	12/4/2012	1/8/2012			X		
Moldavia	23/11/2001	12/5/2009	1/9/2009			X	X	X
Monaco	2/5/2013							
Montenegro	7/4/2005	3/3/2010	1/7/2010	55	X		X	
Norvegia	23/11/2001	30/6/2006	1/10/2006		X	X	X	
Paesi Bassi	23/11/2001	16/11/2006	1/3/2007				X	X
Polonia	23/11/2001							
Portogallo	23/11/2001	24/3/2010	1/7/2010			X	X	
Repubblica Ceca	9/2/2005	22/8/2013	1/12/2013		X	X	X	
Repubblica Slovacca	4/2/2005	8/1/2008	1/5/2008		X	X	X	
Romania	23/11/2001	12/5/2004	1/9/2004				X	
Russia								
San Marino								
Serbia	7/4/2005	14/4/2009	1/8/2009	55			X	
Slovenia	24/7/2002	8/9/2004	1/1/2005				X	
Spagna	23/11/2001	3/6/2010	1/10/2010			X	X	
Svezia	23/11/2001							
Svizzera	23/11/2001	21/9/2011	1/1/2012		X	X	X	
Turchia	10/11/2010							
Ucraina	23/11/2001	10/3/2006	1/7/2006		X		X	
Ungheria	23/11/2001	4/12/2003	1/7/2004		X	X	X	

http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ITA&NT=185

La Convenzione di Budapest

Non membri del Consiglio d'Europa

	Firma	Ratifica	Entrata in vigore	Rinv.	R.	D.	A.	T.	C.	O.
Argentina										
Australia		30/11/2012 a	1/3/2013		X		X			
Canada	23/11/2001									
Cile										
Colombia										
Costa Rica										
Filippine										
Giappone	23/11/2001	3/7/2012	1/11/2012		X	X	X			
Israele										
Marocco										
Mauritius		15/11/2013 a	1/3/2014				X			
Messico										
Panama										
Repubblica Dominicana		7/2/2013 a	1/6/2013			X	X			
Senegal										
Stati-Uniti d'America	23/11/2001	29/9/2006	1/1/2007		X	X	X			
Sud Africa	23/11/2001									

Numero totale di firme non seguite da ratifiche :	11
Numero totale di ratifiche/adesioni :	41

Rinvii :
(55) Date of signature by the state union of Serbia and Montenegro.
a.: Adesione - s.: Firma senza riserva di ratifica - su.: Successione - r.: Firma "ad referendum".
R.: Riserve - D.: Dichiarazioni - A.: Autorità - T.: Applicazione Territoriale - C.: Comunicazione - O.: Obiezione.

http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ITA&NT=185

Agenda

- Presentazione relatore
- L'incidente informatico (RFC e ISO)
- La convenzione di Budapest
- Legge 48/2008
- D.lgs 231/2001
- La raccolta delle prove
- Strumenti
- Case Study
- Q&A
- Bibliografia & sitografia

Legge 48/2008

- Legge 18 marzo 2008, n. 48
- "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno"
- pubblicata nella Gazzetta Ufficiale n. 80 del 4 aprile 2008 Supplemento ordinario n. 79
- Importante per le modifiche introdotte nel Codice di Procedura Penale

Legge 48/2008

- Art. 244 CPP “Casi e forme delle ispezioni”
- «L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica (359), anche in relazione a sistemi informatici o telematici, adottando **misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l’alterazione**».

Legge 48/2008

- Art. 247 CPP “Casi e forme delle perquisizioni”
- «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, **ancorché 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**».

Legge 48/2008

- Art. 254-bis: Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni)

- 1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che **la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità**. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali. (l., n. 48 del 2008)

Legge 48/2008

- Art. 259 CPP “Custodia delle cose sequestrate”
- «Quando la custodia riguarda dati, informazioni o programmi informatici, il **custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria**».

Legge 48/2008

- Art. 260 “Apposizione dei sigilli alle cose sequestrate. Cose deperibili”
- «anche di carattere elettronico o informatico»
- «Quando si tratta di dati, di informazioni o di programmi informatici, **la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità**; in tali casi, **la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria**»

Legge 48/2008

- Art. 352 Perquisizioni
- 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. (l., n. 48 del 2008)

Legge 48/2008

- Art. 354 - Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro
- 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 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 [253, 356; disp. att. 113] [1]. (l., n. 48 del 2008)

Agenda

- Presentazione relatore
- L'incidente informatico (RFC e ISO)
- La convenzione di Budapest
- Legge 48/2008
- D.lgs 231/2001
- La raccolta delle prove
- Strumenti
- Case Study
- Q&A
- Bibliografia & sitografia

D.Lgs 231/2001

- Responsabilità amministrativa delle società e degli enti,
- Prevede il modello di organizzazione e gestione" o "**Modello ex D.Lgs. n. 231/2001”** che è un atto privato adottato da una persona giuridica, o associazione priva di personalità giuridica, volto a prevenire la responsabilità penale derivante dal D.lgs 8 giugno 2001 n. 231.
- Estende alle persone giuridiche la responsabilità per reati commessi in Italia ed all’estero da persone fisiche che operano per la società per **alcuni reati commessi nell'interesse o a vantaggio degli stessi**
- Non è obbligatorio dotarsi di un Modello Organizzativo (MOG), ma l'organizzazione non risponde del reato se dimostra di avere adottato ed efficacemente attuato un modello organizzativo idoneo a prevenire la commissione di tali illeciti

D.Lgs 231/2001

- Secondo il D.Lgs. n. 231/2001, la società è responsabile per i reati commessi nel suo interesse o a suo vantaggio:
  - da "**persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione** dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dell'ente stesso" (cosiddetti soggetti in posizione apicale o apicali);
  - da **persone sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione apicale** (cosiddetti soggetti sottoposti all'altrui direzione);
- La società non risponde, per espressa previsione legislativa (art. 5, comma 2, D.Lgs. n. 231/2001), se le persone indicate hanno agito nell'interesse esclusivo proprio o di terzi.

D.Lgs 231/2001

- L'art. 6 del D. Lgs. n. 231/2001 prevede che la società possa essere esonerata dalla responsabilità conseguente alla commissione dei reati indicati se prova che:

  - a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, **modelli di organizzazione e di gestione idonei a prevenire reati della specie di quelli verificatisi**;
  - b) il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei modelli nonché di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo, il cosiddetto **organismo di vigilanza**;
  - c) le persone fisiche **hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione**;
  - d) **non vi sia stata omessa o insufficiente vigilanza** da parte dell'organismo di cui alla precedente lettera b).

D.Lgs 231/2001

- Le sanzioni previste dalla legge a carico della società consistono in:
  - sanzione pecuniaria, applicata secondo quote;
  - interdizione dall'esercizio dell'attività (anche in via definitiva, art. 16 D.lgs 231/2001)
  - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito,
  - divieto di contrattare con la Pubblica Amministrazione;
  - esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli concessi;
  - divieto di pubblicizzare beni o servizi;
  - confisca del prezzo o del profitto che la società ha tratto dal reato (e sequestro conservativo, in sede cautelare);
  - pubblicazione della sentenza di condanna, che può essere disposta in caso di applicazione di una sanzione interdittiva.
  - commissariamento dell'ente

D.Lgs 231/2001

- Trai i reati identificati dal legislatore possiamo elencarne alcuni:

  - Indebita percezione di erogazioni pubbliche;
  - Truffa ai danni dello Stato o di altro Ente Pubblico;
  - Illegale ripartizione degli utili;
  - Falsità nelle comunicazioni sociali;
  - Operazioni in pregiudizio dei creditori;
  - Formazione fittizia del capitale;
  - Indebita influenza nell'assemblea;
  - Ostacolo all'esercizio della funzione di pubblica vigilanza;
  - Aggiotaggio;
  - Frode informatica a danno dello Stato o di altro Ente Pubblico;
  - Corruzione e Concussione;
  - Reati in tema di erogazioni pubbliche;
  - Reati contro la personalità individuale

D.Lgs 231/2001

- In particolare, per i reati informatici:
  - Attentato a impianti di pubblica utilità compreso il danneggiamento (Art. 420 c.p.)
  - falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.);
  - accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
  - detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);
  - diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
  - intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);

D.Lgs 231/2001

- In particolare, per i reati informatici (continua da slide precedente):
  - installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 615-quinquies c.p.);
  - danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
  - danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
  - danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
  - danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
  - frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)
  - Falsità di documenti informatici (art. 491 bis c.p.)

D.Lgs 231/2001

- Adempiere agli obblighi legislativi che ne derivano richiede, tra l'altro, di:
  - adottare, prima della commissione del fatto, modelli organizzativi e gestionali idonei a prevenire reati;
  - costituire un organismo dell'ente con compito di vigilare efficacemente sul funzionamento e sull'osservanza di modelli e curare il loro aggiornamento;
  - definire i modelli di organizzazione e gestione;
  - essere in grado di evitare la commissione del reato se non mediante l'elusione fraudolenta dei modelli stessi;
  - individuare le attività nel cui ambito possono essere commessi tali reati;
  - prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
  - individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di reati

D.Lgs 231/2001

- Soppressione dei Reati di Privacy
- In data 11/10/2013 è stato abrogato l'intero comma 2 dell'Art. 9 del D.lgs 231/2001 che era stato ampliato lo scorso 14/08/2013 eliminando 5 reati:

    - **i delitti sulla privacy**, ovvero i reati di trattamento illecito dei dati personali, falsità nelle dichiarazioni e notificazioni al Garante e inosservanza dei provvedimenti del Garante
    - la **frode informatica con sostituzione dell'identità digitale**
    - l'**indebito utilizzo, falsificazione, alterazione e ricettazione di carte di credito**

- Confindustria aveva infatti sollevato i propri dubbi in merito ai costi di un aggiornamento e implementazione da parte delle aziende già a poche settimane dall'aggiunta dei reati.
- Inoltre, la mancata correzione degli stessi modelli avrebbe previsto, in caso di eventuali illeciti dei vertici delle società per uno dei delitti previsti in materia di privacy, una sanzione tra i 200 e i 700 mila euro

D.Lgs 231/2001

- Alcune note sulla data retention e l'importanza dei log file.
- Il Garante per la Privacy indica la durata di retention:
    - 6 mesi per accessi amministrativi [doc. web n. 1577499 G. Privacy]
    - 12 mesi per accessi a posta elettronica
    - 24 mesi per telefonia
- Necessità di archiviazione sicura e policy di accesso
- Attenzione alla quantità di informazioni archiviate

D.Lgs 231/2001

A: a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, è consentito al fornitore, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale (art. 123, comma 2 DLGV 196/03).

B: per finalità di accertamento e repressione dei reati (art 132, comma 1 DLGV 196/03).

C: per esclusive finalità di accertamento e repressione dei delitti di cui all'art. 407, comma 2, lettera a) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici (art. 132, comma 2 DLGV 196/03).

D: debbono essere conservati fino a quella data dai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, fatte salve le disposizioni vigenti che prevedono un periodo di conservazione ulteriore. I dati del traffico conservati oltre i limiti previsti dall'art. 132 del decreto legislativo 30 giugno 2003, n. 196, possono essere utilizzati esclusivamente per le finalità del decreto-legge, salvo l'esercizio dell'azione penale per i reati comunque perseguibili (Art. 6. Nuove norme sui dati del traffico telefonico e telematico legge 31 luglio 2005 n. 155 (Pisanu), comma 1come modificato dal decreto "mille proroghe" n. 248 del 31.12.2007).

E: ai fini dello svolgimento delle investigazioni preventive previste dall'articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati (in conseguenza della ratifica italiana della convenzione sul Cyber Crime)

Agenda

- Presentazione relatore
- L'incidente informatico (RFC e ISO)
- La convenzione di Budapest
- Legge 48/2008
- D.lgs 231/2001
- La raccolta delle prove
- Strumenti
- Case Study
- Q&A
- Bibliografia & sitografia

La raccolta delle prove

- RFC 3227: “Guidelines for Evidence Collection and Archiving”
- Procedere metodicamente
- Catturare un’immagine completa del sistema
- Minimizzare le modifiche ai dati
- Isolare se necessario il sistema
- Prima si raccoglie, poi si analizza
- Procedere in ordine di volatilità
- Garantire la catena di custodia

La raccolta delle prove

- ISO 27037: ““Guidelines for identification, collection, acquisition and preservation of digital evidence”
- La ISO/IEC 27037:2012 si limita alle fasi iniziali del processo di gestione della prova informatica, non arriva all’analisi, non si occupa di aspetti legali, strumenti, reportistica, trattamento dei dati
- Si occupa di:
  - Trattamento del reperto informatico
  - Definizione linee guida nelle fasi di 1)Identificazione (ispezione), 2) Raccolta (sequestro), 3) Acquisizione (copia o sequestro virtuale), 4) Conservazione (conservazione e sigillo)
  - Integrità della prova informatica e metodologia al fine di rendere ammissibile la prova in giudizio

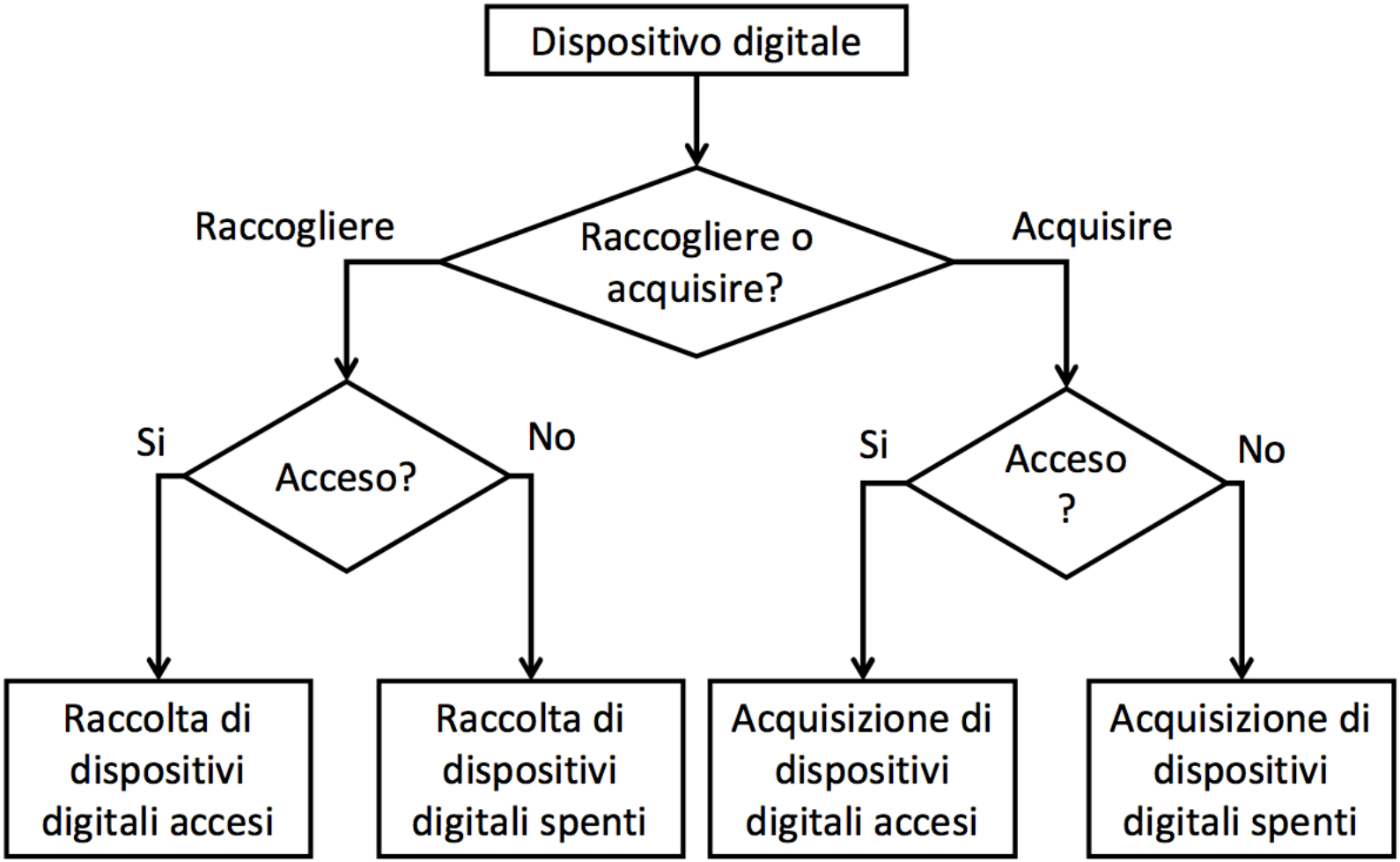
La raccolta delle prove: regole generali

- 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)

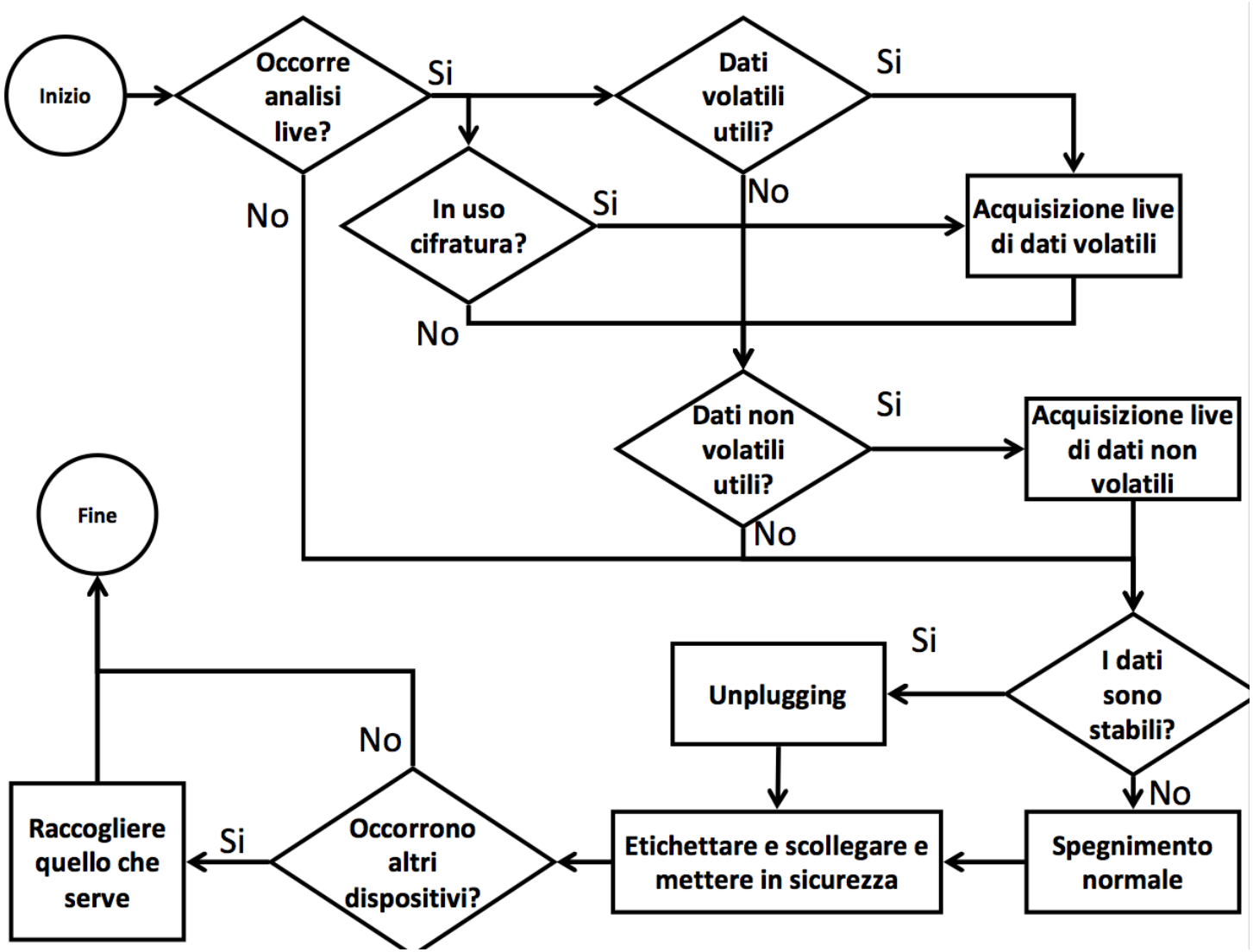
La raccolta delle prove: Identificazione

- La prova informatica si presenta in forma fisica e logica
- 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
- 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

La raccolta delle prove: Identificazione



La raccolta delle prove: Identificazione



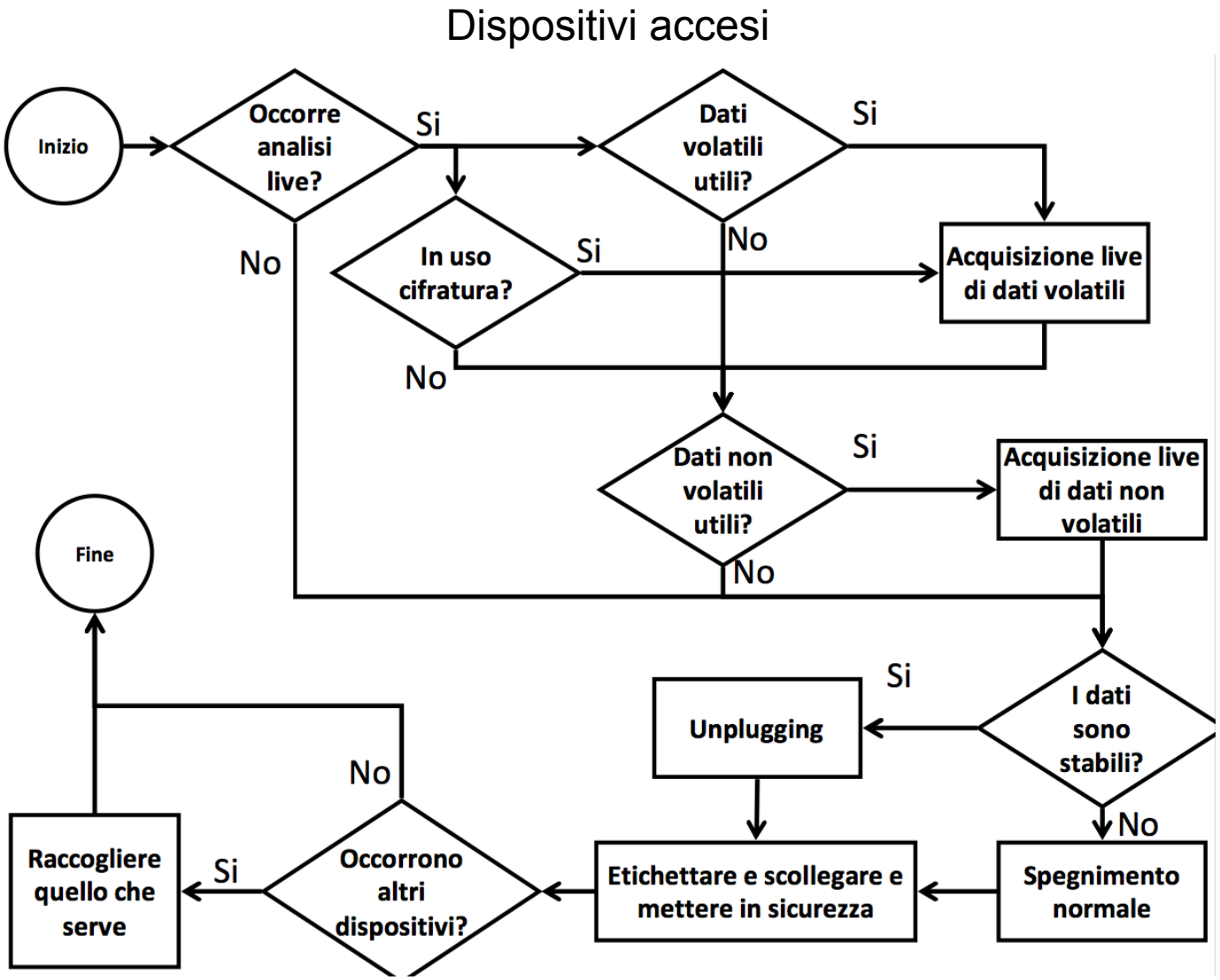
La raccolta delle prove: Raccolta

- I dispositivi 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 va documentato documentare
- Raccogliere anche gli accessori
- 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 disponibili (tempo, storage, personale)

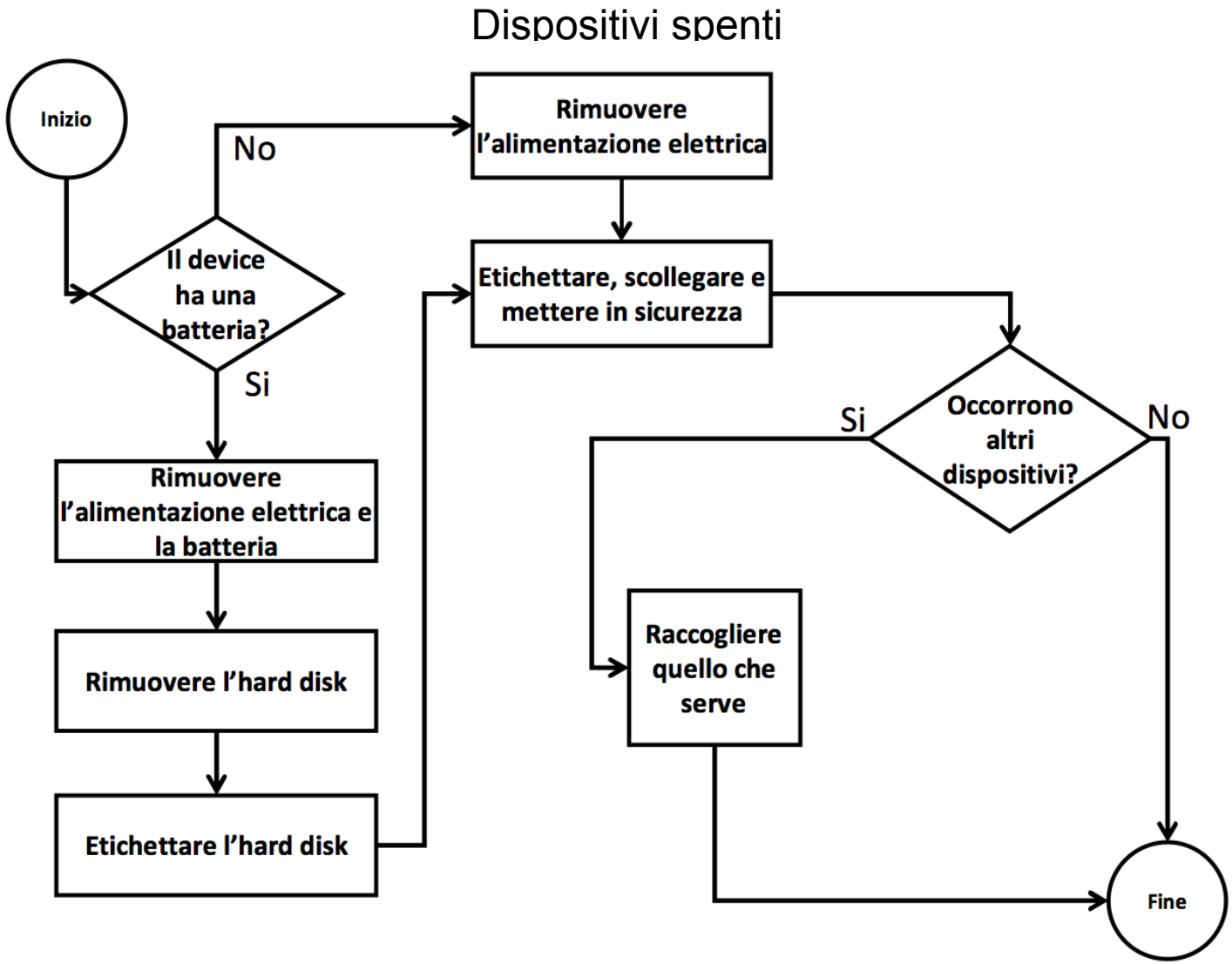
La raccolta delle prove: Acquisizione

- Creazione di una copia forense e documentazione di metodo, strumenti, attività
- Nel caso di dischi, è possibile acquisire il supporto, singole partizioni o gruppi di file
- Acquisendo solo un gruppo di file si perdono alcuni dati (spazio non allocato, file cancellati, slack space)
- Apportare meno alterazioni possibili (tendere a non modificare alcun bit)
- Documentare eventuali alterazioni e giustificare (sistema in esecuzione, settori danneggiati, tempo insufficiente)
- Può essere utile ma non indispensabile **fare wipe del disco destinazione**
- Originale e copia devono essere verificati tramite calcolo di codici hash che devono coincidere
- Se gli hash non coincidono (es. settori difettosi) descrivere e documentare il contesto e l'esito dei test

La raccolta delle prove: Acquisizione

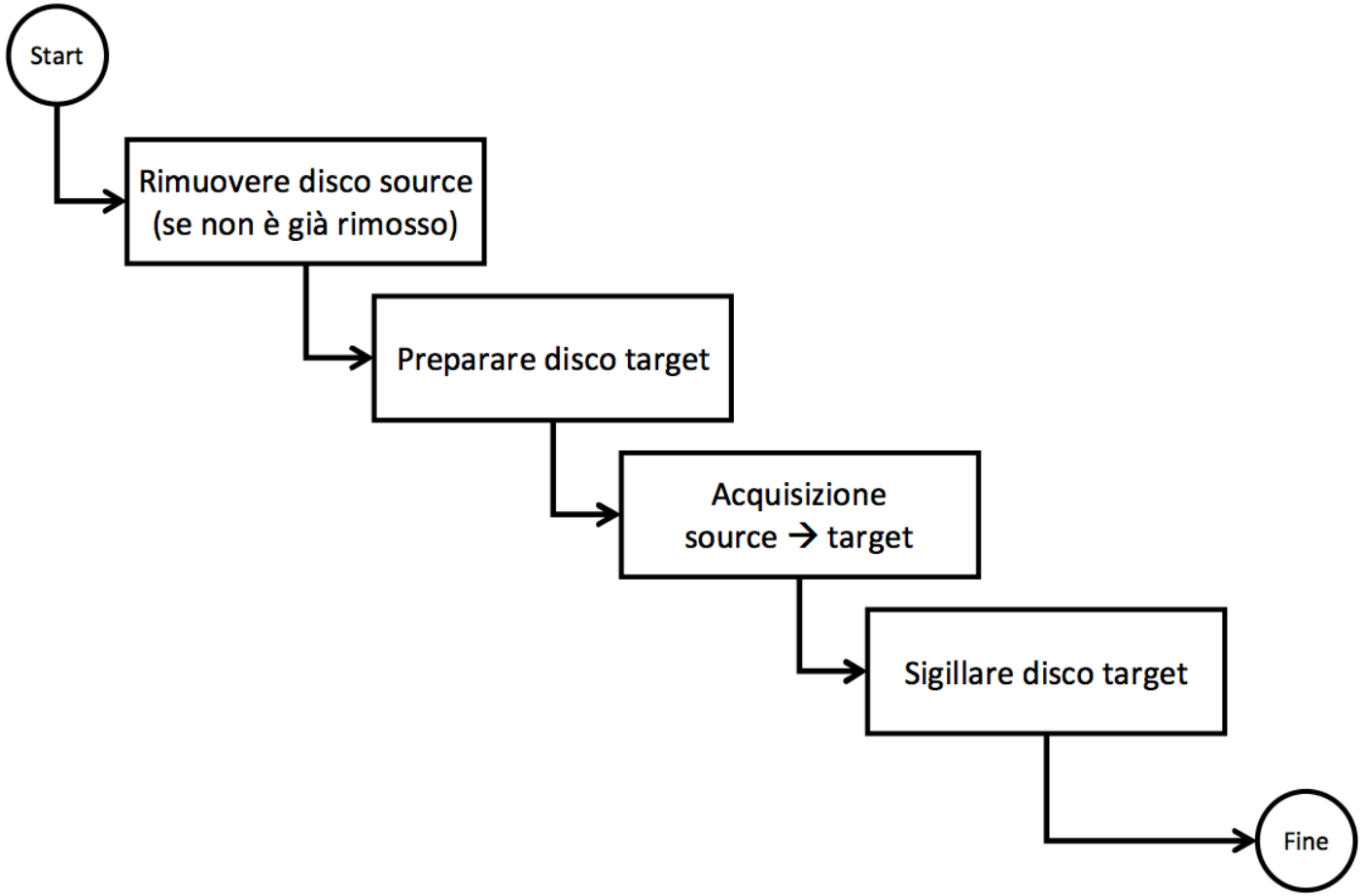


La raccolta delle prove: Acquisizione



La raccolta delle prove: Acquisizione

Dispositivi spenti



La raccolta delle prove: Acquisizione

- 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)
    - Non si riesce a rimuovere il disco o ad acquisirlo
    - 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 ed acquisizione delle cartelle, file ed altra proprietà od opzione rilevante.

La raccolta delle prove: Acquisizione

- 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

La raccolta delle prove: Conservazione

- Proteggere integrità dei dati da alterazioni naturali, colpose o dolose
- Utilizzare metodologia per dimostrare che non si sono verificate alterazioni
- Proteggere anche la riservatezza dei dati
- Descrivere la **catena di custodia**
- Utilizzare imballaggi opportuni (es. per i supporti magnetici, imballaggi antistatici) che non danneggino il supporto

La raccolta delle prove: I ruoli

- Definizione dei ruoli:

- 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...)

Agenda

- Presentazione relatore
- L'incidente informatico (RFC e ISO)
- La convenzione di Budapest
- Legge 48/2008
- D.lgs 231/2001
- La raccolta delle prove
- Strumenti
- Case Study
- Q&A
- Bibliografia & sitografia

Strumenti: Live CD

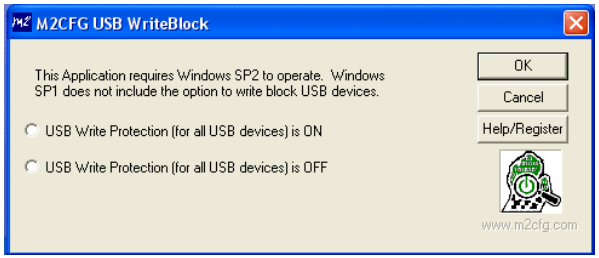
- Live CD/DVD/USB disponibili online gratuitamente e a pagamento
- DEFT, Caine, Helix, Paladin, Raptor (Linux) ma anche WinFE WinPE (Win)
- Cosa si può fare:
  - Preview
  - Copie forensi
  - Hash e verifica
  - Recupero ed estrazione dati
  - Ripristino di sistemi o accesso ai dati su disco
  - Analisi forensi (meglio versione installabile)

Strumenti: Write Blocker e Copiatori (HW)

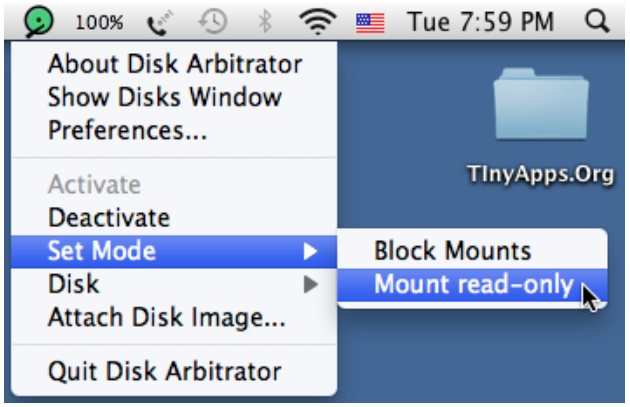
Strumenti: Write Blocker e Copiatori

- Linux (OS con modifiche su automount)

- Windows (chiave di registro - M2CFG)



- Mac OS (Disk Arbitrator)



Strumenti: Mobile Forensics

- Closed source
  - Cellebrite UFED, Micro Systemation XRY, Oxygen Forensics, Praben Device Seizure, Lantern, MOBILedit

- Open Source
  - Libimobiledevice
  - Adb
  - Iphone Backup Analyzer
  - Sqlite Browser

deft

SANTOKU

Strumenti: copie forensi

- Concetto di copia/acquisizione “forense”
- Formati (EWF, raw, split-raw, AFF, disk2disk)
- Hash e verifica
- Strumenti SW (dd/dcfldd, Guymager, FTK Imager, etc...) o HW
- Supporti difettosi: ddrescue, dd_rescue, dd_rhelp
- Apposizione data certa (firma digitale, PEC, asseverazione, poste)

- Apertura e montaggio:
  - Win: FTK Imager, Mount Image Pro, OS Mount
  - Linux: xmount, mount -o loop, Autopsy/TSK, FTK Imager
  - Mac: Disk Utility o “hdiutil mount image.dd” e/o xmount
  - FTK Imager (segue approfondimento)

Strumenti: FTK Imager

- Sviluppato e distribuito gratuitamente da AccessData (FTK)
- Anche Portable (lite)
- Win - Mac - Linux (wine)
- Utile per acquisizioni ma anche elaborazioni o esame live/IR
- Accedendo al disco a livello raw può eseguire operazioni che il Sistema Opeartivo non lascerebbe fare (es. copia forense o accesso a locked files)
- Permette aprire e visionare il contenuto di immagini forensi, macchine virtuali, dispositivi collegati al PC
- Può fare mount di copie forensi:
    - Physical e/o Logical
    - Filesystem
    - Read only oppure read/write tramite cache su file
- Può generare dump della RAM
- Può essere usato per copie forensi di dispositivi ma anche acquisizioni di folder o file, tramite il formato (proprietario AccessData) di Logical Image ad1 (che produce file a01, a02, etc…)

Strumenti: Analisi e recupero dati

- Recupero dati tramite MFT e/o Carving
  - Windows: FTK-Imager, Recuva, R-Studio, Photorec, etc...
  - Linux: Photorec, Foremost, Scalpel, TSK

- Analisi ed estrazione dati:
  - TSK
  - Timeline/Supertimeline (TSK con fls, log2timeline, PLASO)
  - bulk_extractor
  - regripper/RegistryReport
  - antivirus/spyware
  - USNJRNL (journal parser di TZWorks o il parser in DEFT)
  - Browser History (log2timeline o vari tool)
  - Trash (rifiuti)
  - Shellbag/Jump List (TZWorks tools), USB Deview,

Strumenti: Virtualizzazione e Forensics

- Utilizzo, vantaggi e svantaggi
- Strumenti per generare disco virtuale:
    - Live View (mantiene dd)
    - Raw2Vmdk (mantiene dd)
    - VBoxManage (conversione raw->vmdk/vdi)
    - Xmount (conversione “virtuale” on the go)
- Per avviare il disco virtuale:
    - VMWare Player/Workstation/Fusion
    - VirtualBox
    - Qemu
- Attivazione Windows, problemi driver Win e OS X, BSOD
- Solzione: Opengates e openjobs
- Possibilità di usare live CD su immagine forense virtualizzata

Agenda

- Presentazione relatore
- L'incidente informatico (RFC e ISO)
- La convenzione di Budapest
- Legge 48/2008
- D.lgs 231/2001
- La raccolta delle prove
- Strumenti
- Case Study
- Q&A
- Bibliografia & sitografia

Case Study

- Un dipendente lascia l'azienda (o la sta per lasciare) e c'è il sospetto che abbia trafugato materiale riservato (progetti, elenco clienti, documenti, etc...) copiandolo su una sua chiavetta USB o inviandolo via email, anche cancellandolo dal PC aziendale e togliendolo quindi dalla disponibilità della società
- L'Avvocato e il Consulente Informatico vengono chiamati per far luce su quanto accaduto e valutare come procedere (eventualmente ricuperando i dati se di valore)

Case Study

- Cosa fare:
    - Cercare tracce di invio email o copia massiva su USB
    - Cercare file cancellati, valutarne il contenuto aziendale e quando possibile data di cancellazione (danneggiamento)
    - Valutare se c'è stato accesso abusivo
    - Cercare di dimostrare l'autore delle attività rilevate (incrociando anche bollature di ingresso e metadati digitali)
    - Cercare di dimostrare l'utilizzo delle informazioni sottratte (valutare IP email ricevute dai clienti, errori sul DB, etc...)

Case Study

- Cosa non fare:
  - Mancata copia forense (bitstream) dei supporti
  - Accensione e utilizzo del PC originale
  - Mancata conservazione dei supporti originali
  - Mancata apposizione di data certa
  - Monitoraggio del dipendente in tempo reale
  - Violazione Privacy
  - Errata repertazione (hash, sigilli, catena di conservazione)
  - Uso di strumenti di duplicazione inadeguati (es. Norton Ghost)
  - Utilizzo di strumenti di analisi o metodologie non adeguate (es. RegExp malformate)
  - Per l'Avvocato: non chiamare il CT all'ultimo momento

Case Study

- Per rilevare leak di informazioni tramite pendrive o dischi USB, eseguire una file activity timeline with daily summary (TSK/Autopsy)

fls -o 63 -r -m C: /dev/sda > c-timeline.body

mactime -y -m -d -i day c-timeline-daily.csv -z Europe/Rome -b c-timeline.body > c-timeline.csv

- Suite TSK, con fls creo file in formato bodyfile
- Converto il bodyfile in CSV
- Creo daily summary con attività giornaliera

Case Study

- Per rilevare leak di informazioni tramite pendrive o dischi USB, eseguire una file activity timeline with daily summary (TSK/Autopsy)
- Esempio: daily summary dal quale risulta attività massiva il 30 settembre e il 1 ottobre. Si andrà ad indagare in quei giorni per capire se sono state connesse periferiche USB, masterizzati CD, usata la rete, etc…

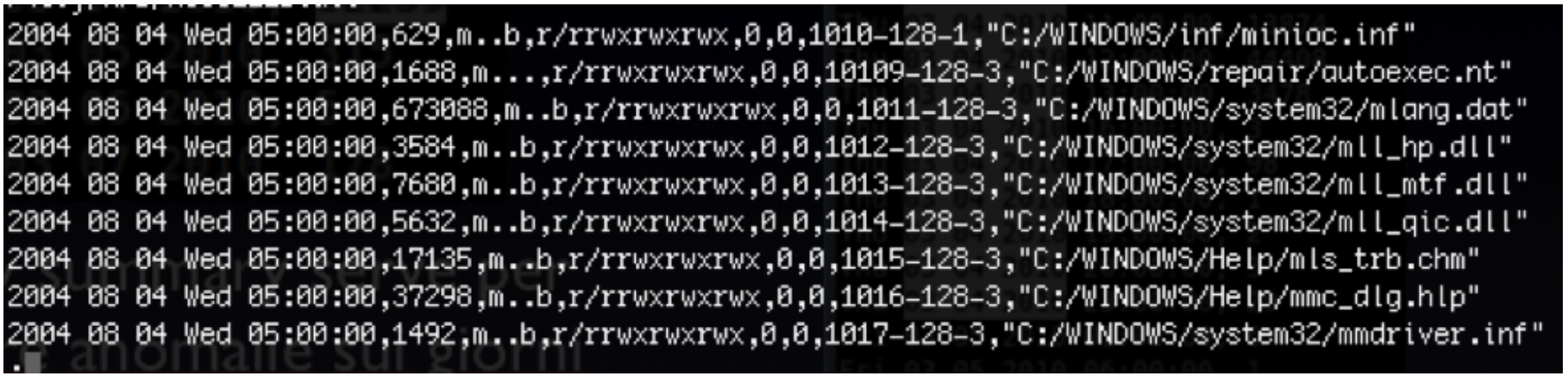
```
Tue 03 02 2010, 6616
Wed 03 03 2010, 3990
Thu 03 04 2010, 62239
Fri 03 05 2010, 315
Sat 03 06 2010, 5
Sun 03 07 2010, 178
```


```
Wed 03 03 2010 17:00:00, 63
Wed 03 03 2010 18:00:00, 94
Thu 03 04 2010 01:00:00, 2
Thu 03 04 2010 02:00:00, 1
Thu 03 04 2010 09:00:00, 294
Thu 03 04 2010 10:00:00, 46
Thu 03 04 2010 11:00:00, 13874
Thu 03 04 2010 12:00:00, 44408
Thu 03 04 2010 13:00:00, 3478
Thu 03 04 2010 16:00:00, 3
Thu 03 04 2010 17:00:00, 98
Thu 03 04 2010 18:00:00, 1
Thu 03 04 2010 19:00:00, 2
Thu 03 04 2010 20:00:00, 3
Thu 03 04 2010 23:00:00, 29
Fri 03 05 2010 01:00:00, 6
Fri 03 05 2010 06:00:00, 1
Fri 03 05 2010 08:00:00, 10
```

Case Study

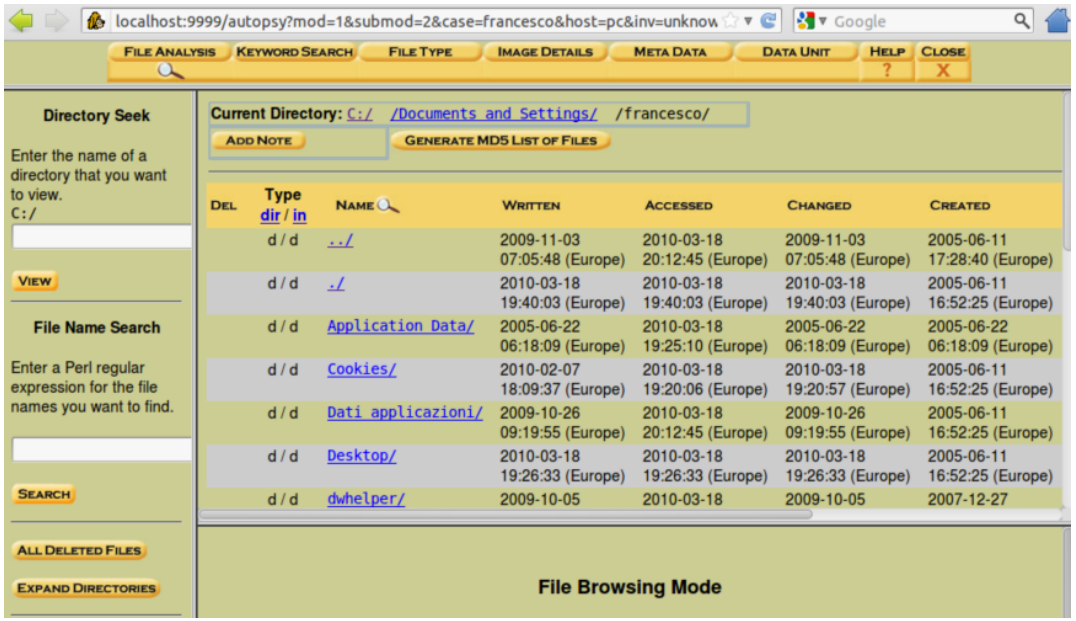
- Tramite i comandi fls e bodyfile Otteniamo (i dati provegono dall'$MFT) data di creazione/accesso/salvataggio/entry modified, dimensione, numero di inode e percorso sul filesystem quando disponibile

- Sappiamo se un file esisteva ma è stato cancellato e in tal caso anche se l'area disco è stata riscritta



Case Study

- Se non vogliamo usare linea di comando, c'è Autopsy (TSK GUI)
- Creo un caso, imposto timezone, inserisco immagini/dischi (/dev/sda)
- Utile per fare preview di file anche cancellati (ricavati da MFT table)
- Utile per fare keyword search su raw disk, estrazione stringhe, estrazione spazio non allocato, organizzazione file per tipo, ricupero di tutti i file cancellati (a livello MFT)
- Preview raw a livello di settore

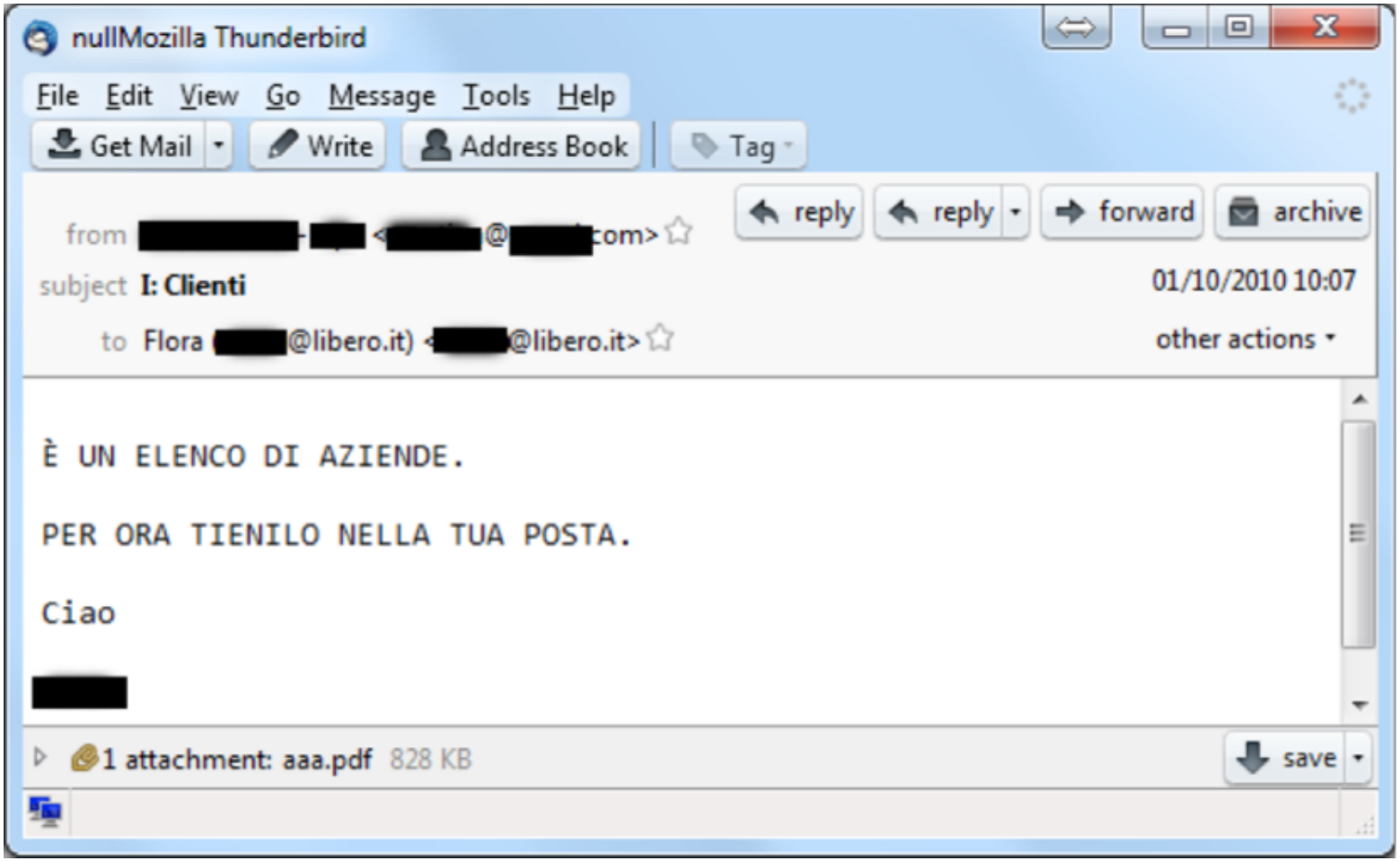


Case Study

- Per andare ancora oltre, aggiungiamo ai timestamp del filesystem anche i metadati contenuti nei file per creare la nostra linea temporale
- utilizzeremo il tool open source log2timeline, scritto in perl dal ricercatore Kristinn Gudjonsson, oppure PLASO, l'evoluzione di log2timeline
- framework composto da 4 moduli: front-end, librerie condivise, modulo input e modulo output
- Diversi plugin: browser history, registry, events, $MFT, exif, etc…
- l2t_process ordina e filtra i risultati di log2timeline
- Otterremo così un diario temporale di gran parte delle attività avvenute sul PC, compresi inserimenti di pendrive, login, avvio, stampa di file, etc…

Case Study

- Ma la realtà è molto più semplice dell'immaginazione…



Agenda

- Presentazione relatore
- L'incidente informatico (RFC e ISO)
- La convenzione di Budapest
- Legge 48/2008
- D.lgs 231/2001
- La raccolta delle prove
- Strumenti
- Case Study
- Q&A
- Bibliografia & sitografia

Q&A

Agenda

- Presentazione relatore
- L'incidente informatico (RFC e ISO)
- La convenzione di Budapest
- Legge 48/2008
- D.lgs 231/2001
- La raccolta delle prove
- Strumenti
- Case Study
- Q&A
- Bibliografia & sitografia

Bibliografia e Sitografia

- “Guide to Integrating Forensic Techniques into Incident Response” – NIST
- “Using Computer Forensics When Investigating System Attacks” – SANS
- “Investigazione Penale e Tecnologia Informatica”, Giuffré – Ziccardi

- RFC 2350, 2828, 3227 (http://tools.ietf.org)
- ISO/IEC 27041, 27042, 27043, 27035, 27037 (http://www.iso.org)
- http://it.wikipedia.org/wiki/Modello_di_organizzazione_e_gestione
- http://www.dmi.unict.it/~battiato/CF1213/Lezione02%20-%20ISO%20e%20misurazione%20alterazioni.pdf
- http://www.interlex.it/675/marcoccio7.htm

Contatti

- www.dalchecco.it /www.difob.it
- paolo@dalchecco.it / pdc@difob.it
- @forensico, @studiodifob

Grazie...