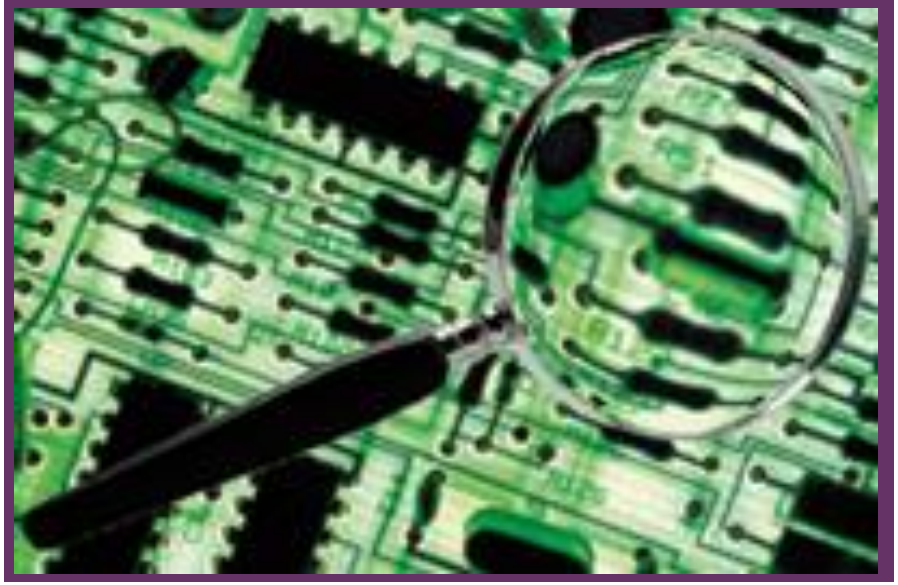



# Electronic Evidence Guide

## Guida alla prova digitale

Una guida di base per agenti di polizia, pubblici ministeri e giudici (versione 1.0)

*DFA Open Day,* Università degli Studi di Milano, 5 giugno 2014

# Chi siamo

- **Mattia Epifani**
  - Digital Forensics Analyst
  - Partner @ Reality Net
  - Vice presidente @ **DFA**, Fellow @ **TLC**
  - Email: *mattia.epifani@realitynet.it*

- **Donato La Muscatella**
  - Avvocato
  - Ricercatore indipendente (*Ciberspazio e Diritto*, *Rivista Penale ed altre*)
  - Socio @ **DFA**, Member @ **TLC**
  - Email: *donato.lamuscatella@hotmail.it*

# Agenda

- Introduzione e genesi del progetto
- Metodologia di traduzione
- Timeline
- Struttura del documento
- Pregi e limiti
- Statistiche di accesso

# Introduzione

- Sviluppata nell'ambito del progetto congiunto CyberCrime@IPA del Consiglio d'Europa e dell'Unione Europea
- "Field guide" per forze dell'ordine e autorità giudiziaria
- Attività partita nel febbraio 2012, la pubblicazione della prima versione risale al Marzo 2013
- Distribuita gratuitamente previa richiesta della password di accesso

# Introduzione

- http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp


# Metodologia di traduzione

- In Italia, primo "avvistamento" della EEG a DEFTCon 2013
- 8 Maggio 2013, primo DFA Open Day
- L'idea alla base è stata quella di costruire un gruppo di «traduttori», composti da tecnici, legali e LE
- Il testo è stato suddiviso in sezioni e sono stati assegnati 2 o 3 traduttori per ciascuna sezione (corrispondenti con uno o più capitoli)
- I traduttori producono la prima versione
- Viene composto un gruppo di «reviewers» per verificare e uniformare la traduzione

# Timeline

- 8 Maggio 2013 - annuncio all'Open Day di DFA
- 27 Maggio 2013 – richiesta candidature per l'attività
- 29 Maggio 2013 – chiusura candidature e nomina di 2 responsabili
- 31 Maggio 2013 – il testo viene "rivelato"

- 17 giugno 2013 – prima "conf. call" organizzativa
- 29 giugno 2013 – assegnazione delle parti da tradurre

- 5 luglio 2013 – VIA!
- 26 luglio 2013 – seconda "conf. call" solo per i "legal"

# Timeline

- agosto 2013 – lavoro di traduzione
- settembre 2013 – consegna delle parti
- 31 ottobre 2013 – Draft v.1
- 17 novembre 2013 – terza "conf. call" istituzione gruppi di revisione
- 21 novembre 2013 – rilascio della Draft v.2
- 19 dicembre 2013 – rilascio della Draft v.3
- 16 gennaio 2014 – "conf. call" dei revisori
- 10 febbraio 2014 – "Final Draft"
- 24 febbraio 2014 – quarta "conf. call" – next steps
- 7 marzo 2014 – Approvazione COE !
- 29 marzo 2014 – rilascio EEG ITA V.1 Ufficiale

# Struttura del Documento

- 278 pagine, 12 Capitoli, 9 Appendici
- Suddivisa in 5 macro aree "logiche"
- Definizioni e Concetti Base
  1. Introduzione
  2. Fonti di Prova
- Individuazione e repertamento della prova
  3. Perquisizione e sequestro
  4. Acquisizione elementi di prova da Internet
  5. Dati in possesso di terze parti

# Fonti di prova

Articolo 1 – Definizioni

Ai fini della presente Convenzione:

a. "sistema informatico" indica qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati;

b "dati informatici" indica qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione;

Questa definizione include tablet, smartphone ed altri dispositivi descritti in seguito.

**Esempi di sistemi informatici**

Desktp/Tower [1]

Portatile [2]

Mainframe [3]

*Fonti delle immagini:*

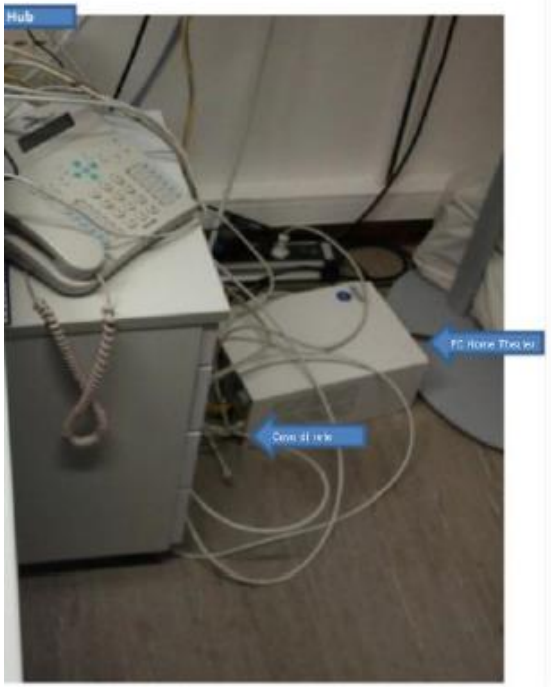
*[1] computershopper.com/var/ezwebin_site/storage/images/desktops/product-profile/superior-699-pc-model-6173/38202-1-eng-US/superior-699-pc-model-61731_product_review_thumb.jpg*

*[2] expresscomputing.info/siteimages/laptop1.jpg*

*[3] prepare.icttrends.com/images/2012/06/mainframe-computer.jpg*

# Perquisizione e sequestro

**Fotografie d'insieme:**

# Perquisizione e sequestro

Caine Live-CD con WinTaylor, Nanni Bassetti e altri, http://www.caine-live.net/



DEFT Live-CD di Stefano Fratepietro e altri, http://www.deftlinux.net/


# Acquisizione elementi di prova da Internet

### 4.3 Le fonti di informazioni in rete

Si possono trovare in rete (online) una grande mole di fonti di informazione che potrebbero essere impiegate in ogni fase dell'indagine. In questo paragrafo andremo ad individuare le fonti online più comuni con cui sarà necessario confrontarci nel prossimo futuro e quali tipologie di elementi di prova possono essere rese disponibili presso ciascuna di esse.

| Fonte | Esempi di elementi di prova |
|---|---|
| **Siti web** | ➢ codice sorgente<br>➢ commenti nel codice<br>➢ campi nascosti<br>➢ riferimenti a siti esterni<br>➢ pubblicità online<br>➢ codici di autenticazione di dominio<br>➢ codici WebSense/AdSense/SearchSense<br>➢ metadati (ad es. data di creazione / ultima modifica)<br>➢ versione precedente presso archive.org |
| **Siti di Social Network** | ➢ codice sorgente<br>➢ codici identificativi (ID) interni<br>➢ sottosistema di chat<br>➢ codici WebSense/AdSense/SearchSense<br>➢ metadati (ad es. data di creazione / ultima modifica) |
| **Siti di Blog** | ➢ codici identificativi (ID) interni (blogID, userID, threadID…)<br>➢ codici di autenticazione di dominio<br>➢ mash-up – Twitter<br>➢ mash-up – Facebook<br>➢ mash-up – Picasa /Flikr<br>➢ mash-up – URL-Shorteners<br>➢ codici WebSense/AdSense/SearchSense<br>➢ metadati (ad es. data di creazione / ultima modifica) |

# Dati in possesso di terze parti

## 5 Dati in possesso di terze parti

Non è sempre possibile accedere fisicamente o da remoto a dei dispositivi per la ricerca di informazioni utilizzabili come fonti di prova digitale, come descritto nei capitoli 3 e 4. Per esempio, nel caso si debba accedere a dati memorizzati in infrastrutture estese e complesse come quelle di un Internet service provider di grandi dimensioni, l'impresa per l'analista potrebbe essere tutto fuor che semplice. Anzi, spesso la cooperazione con la parte terza può essere l'unica soluzione per trovare un accordo che consenta l'accesso alle evidenze necessarie.

Ottenere dati in possesso di terze parti è, quindi, una soluzione diversa per mettere in sicurezza evidenze digitali rispetto ad un'analisi specialistica dei dati ed alla loro salvaguardia descritte nei capitoli 3 e 4. Invece, l'indagine farà affidamento sulle terze parti proprietarie dei dati, quali i fornitori di servizi di hosting, allo scopo di ottenere evidenze digitali (electronic evidence), come file di log e dati di registrazione dei servizi. Il punto 5.1 si occuperà di come ottenere i dati dalle terze parti.

Nel 5.2 verrà discusso un secondo modo di usare dati detenuti da terze parti e riguarda la raccolta di evidenze digitali indiziarie che consentano alle forze dell'ordine o a un analista di capire che è stato commesso un crimine informatico e, conseguentemente, di iniziare un'indagine. Internet è un luogo vasto, utilizzato da miliardi di utenti, soggetti a diverse giurisdizioni e può essere difficile, se non impossibile, per un numero ristretto di analisti, monitorare tutte le informazioni diffuse su Internet. Inoltre, mentre alcune parti della rete sono pienamente accessibili da tutti gli utenti, altre parti sono ad accesso condizionato e le comunicazioni private, come quelle che avvengono tramite account di posta elettronica, account di social network, server e siti web che richiedono la registrazione delle utenze per l'accesso, non sono pubblicamente accessibili.

# Dati in possesso di terze parti

Council of Europe

Directorate of Communication

The Council in brief | Human Rights | Democracy | Rule of Law | Organisation | 47 Countries | Topics | Newsroom

LOGIN | PRINT | WORD | SEND | BOOKMARK | LANGUAGE | HELP

Comunicato stampa - 687(2008)

**Proteggere i diritti umani su Internet – Il Consiglio d'Europa presenta delle linee guida in cooperazione con i fornitori di giochi on line e servizi Internet**

Strasburgo, 03.10.2008 - In data 3 ottobre, il Consiglio d'Europa ha presentato, in stretta cooperazione con designer, editori europei di giochi on line e fornitori di servizi Internet, una doppia serie di linee guida che mirano a promuovere il rispetto della privacy, la sicurezza e la libertà d'espressione degli internauti che, per esempio, navigano sul web, comunicano attraverso e-mail, partecipano a chat o blog o che si dilettano con giochi on line.

La Federazione europea del software interattivo (ISFE) e l'Associazione europea degli Internet provider (EuroISPA), desiderosi di promuovere la sensibilizzazione per i diritti umani e di rafforzare la fiducia nei confronti di Internet, hanno collaborato con il Consiglio d'Europa – la cui missione è quella di proteggere tali diritti in Europa – per elaborare una doppia serie di linee guida a favore dei propri rispettivi settori. Tali linee guida, basate su delle regole di autodisciplina o su progetti esistenti, offrono agli operatori coinvolti dei consigli semplici e pratici sulle modalità per rendere Internet uno spazio aperto e sicuro per gli utenti in cui sia garantito il loro diritto di navigare, giocare e creare.

Le linee guida destinate ai fornitori di giochi on line sottintendono l'importanza di una sensibilizzazione all'utilizzo adeguato dei giochi, tenuto conto della necessità di garantire la libertà d'espressione e la protezione degli utenti, in particolare dei bambini, contro contenuti indesiderati, violenti o razzisti. Queste raccomandano, inoltre, di applicare ai giochi dei sistemi di valutazione e di certificazione indipendenti come il PEGI (Informazione paneuropea sui giochi online) o PEGI Online e di informare gli internauti ed i genitori sui pericoli che possono contenere i giochi on line – un loro utilizzo eccessivo, intimidazioni o molestie, uso abusivo di dati a carattere personale, ecc.

Le linee guida per i fornitori di servizi Internet – che forniscono accesso ad Internet, contenuti, *hosting* e servizi come la posta elettronica, le chat o i blog – raccomandano a questi ultimi di vegliare affinché gli utenti che entrano nel mondo di Internet siano informati sui rischi per la loro privacy, la sicurezza e la libertà d'espressione.

Uno dei principali obiettivi è quello di completare il lavoro già avviato dagli operatori per proteggere i bambini contro i contenuti nocivi o illegali o altri pericoli come l'adescamento per fini sessuali (grooming). Le linee guida riguardano anche i rischi per l'integrità dei dati, come i virus e i *worm*, e per la privacy, come la raccolta dei dati a carattere personale senza il consenso dell'utente.

"Con tali linee guida, il Consiglio d'Europa aggiunge un nuovo aspetto alla promozione dei diritti umani considerati da un punto di vista differente. Siamo effettivamente convinti che ogni attore della società - ivi compreso il settore privato - abbia un ruolo da svolgere nella sua sfera d'attività. Non si tratta di creare dei testi giuridici, ma di aiutare le imprese a promuovere tali diritti nella quotidianità", ha dichiarato Jan Kleijssen, direttore delle

Attività normative del Consiglio d'Europa.

Da sei anni, il dispositivo di autodisciplina PEGI ha raggiunto il suo obiettivo fondamentale che è quello di fornire ai genitori europei delle raccomandazioni concernenti il carattere più o meno appropriato del contenuto dei giochi per i minori. Il sostegno fornito, per questa nuova iniziativa, dall'Organizzazione europea di difesa dei diritti umani costituisce allo stesso tempo un riconoscimento della nostra azione ed un invito a migliorare ancora il dispositivo PEGI", ha sottolineato Patrice Chazerand, segretario generale dell'ISFE – organizzazione che rappresenta gli interessi del settore dei giochi on line in 31 paesi europei.

"La difesa dei diritti umani è sempre stata una preoccupazione di primo piano per l'EurpISPA. Siamo perfettamente coscienti che Internet sollevi delle problematiche particolarmente complesse concernenti la protezione dei diritti fondamentali degli utenti. È per questa ragione che continueremo a vegliare affinché i consumatori dispongano di informazioni qualitativamente elevate, ribadendo con forza che i fornitori di servizi Internet non devono subire costrizioni eccessive da parte dei poteri pubblici né che i diritti dei consumatori siano indeboliti da una sovrabbondanza di informazioni o da un'ingerenza sproporzionata nella loro privacy", ha dichiarato il professore Micheal Rotert, vice presidente dell'EuroISPA. L'Associazione rappresenta circa un migliaio di fornitori di servizi Internet in Europa (fornitori di accesso ad Internet e ad altri servizi quali richieste, contenuti e hosting).

Linee guida per i fornitori di giochi on line
Linee guida per i fornitori di servizi Internet

**Contatti**

**Consiglio d'Europa**, Jaime Rodríguez, addetto stampa, Tel.: +33 (0) 689 99 50 42, jaime.rodriguez@coe.int
www.coe.int
**ISFE**, Patrice Chazerand, segretario generale, Tel.: +32 (0) 2 502 88 73, patrice.chazerand@isfe.eu
http://isfe.eu
**EuroISPA,** Joe Mcnamee, responsabile degli Affari pubblici, Tel.: +32 2 503 2265, joe@euroispa.org www.euroispa.org

**Divisione della Stampa del Consiglio d'Europa**
Tel: +33 (0)3 88 41 25 60
Fax:+33 (0)3 88 41 39 11
pressunit@coe.int
www.coe.int/press

Top

Activities | Press Multimedia | Useful links | Contact us

Disclaimer · © Council of Europe 2014 · © photo credit · Webmaster | close | Print | RSS | SHARE

EuroISPA

COUNCIL OF EUROPE | CONSEIL DE L'EUROPE

**Human rights guidelines for Internet service providers**

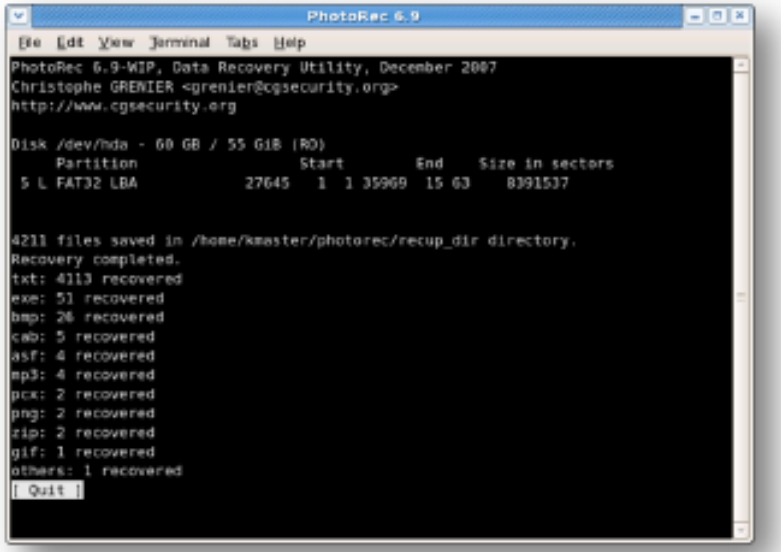
Developed by the Council of Europe
in co-operation with
the European Internet Services Providers Association
(EuroISPA)

# Struttura del Documento

- Analisi e Presentazione
  6. Analisi
  7. Preparazione e Presentazione della Prova
- Norme, Ruoli e Scenari
  8. Giurisdizione
  9. Osservazioni specifiche in rapporto ai ruoli
- Riferimenti e Scenari
  10. Casi reali
  11. Glossario
  12. Informazioni Aggiuntive
- Appendici

# Analisi

Si possono ricostruire i file cancellati anche quando il file system non ha più alcun riferimento ad essi esaminando sul dispositivo di memorizzazione tutti i settori che il file system ha catalogato come disponibili e verificando se in tali settori siano in realtà presenti dei dati. Esiste un gran numero di strumenti software per recuperare i file cancellati, ad esempio i tool gratuiti TestDisk e PhotoRec di CGsecurity, che funzionano su un'ampia varietà di sistemi operativi e file system.



# Preparazione e presentazione della prova

## 7 Preparazione e presentazione della prova

### 7.1 L'uso della prova digitale nei procedimenti giudiziari

Questo paragrafo integra il punto 1.6 nella quale sono trattati i principi della prova digitale.

L'utilizzo della prova digitale è cresciuto nel corso degli ultimi anni dal momento in cui i Tribunali hanno ammesso questo tipo di prova sotto forma di e-mail, fotografie digitali, file di log inerenti transazioni bancarie, documenti di elaborazione di testi, messaggi istantanei, fogli elettronici, cronologia del browser Internet, database, contenuto della memoria del computer, backup del computer, schermate del computer, video digitali e contenuti audio – ognuno dei quali rappresenta un dato digitale.

Un dispositivo digitale utilizzato per commettere un reato dovrebbe essere preservato proprio come si farebbe con qualsiasi altro tipo di prova materiale ritrovata sulla scena del crimine, perché tutti questi dispositivi rappresentano prove materiali. Come per le impronte digitali e la prova del DNA, la prova digitale è fragile e facilmente cancellabile o alterabile qualora non siano adottate le opportune precauzioni. Nei primi casi in cui è stata utilizzata la prova digitale, gli agenti delle forze dell'Ordine, ancora non adeguatamente formati, accendevano i computer per ricercare le prove ancor prima di sottoporli ad un'analisi forense.

# Giurisdizione

## 8 Giurisdizione

### 8.1 La dimensione internazionale del crimine informatico

Il mondo della rete si potrebbe definire un enorme parco giochi per i criminali. Ogni giorno, migliaia di minori e adulti di tutto il mondo subiscono danni derivanti dall'uso improprio di Internet; molte persone innocenti vengono truffate e i criminali commettono i reati più gravi spostandosi tra le varie giurisdizioni. Per questa ragione, è importante facilitare gli accordi internazionali tra le Autorità inquirenti. Un ruolo importante nell'attività delle forze di polizia e dei Pubblici Ministeri è rappresentata proprio dalla mutua assistenza giudiziaria e dall'estradizione. I Pubblici Ministeri lavorano in contatto con inquirenti e Pubblici Ministeri di altri Paesi per portare avanti le indagini e l'azione penale. La cooperazione internazionale nell'attività investigativa dei crimini informatici non potrà mai essere incentivata abbastanza.

Le indagini transnazionali hanno a che fare principalmente con una questione fondamentale: la circostanza per la quale un agente di polizia può legalmente investigare al di fuori del proprio Paese (compresa l'acquisizione delle prove memorizzate nel "cloud", che possono essere ovunque), soprattutto se l'agente ha necessità di agire con urgenza. È importante sapere se è possibile ottenere e raccogliere le prove digitali conservate al di fuori dei confini nazionali, specialmente se queste prove sono presumibilmente destinate a scomparire.

# Osservazioni specifiche in rapporto ai ruoli

## 9 Osservazioni specifiche in rapporto ai ruoli

- Gestione delle indagini
- Catena di custodia
- Esame delle fonti di prova (tecniche di laboratorio)
- Impatto sui soggetti delle ricerche (ad esempio per le reti di società)
- Considerazioni sulla tutela della *privacy*, proporzionalità e profili collaterali

### 9.1 Le forze di polizia e le diverse autorità investigative

Non c'è alcun bisogno di presentare informazioni destinate a questo specifico ruolo, visto che tutte le considerazioni che andrebbero incluse in questo paragrafo sono già state trattate nei capitoli precedenti.

### 9.2 Il pubblico ministero

#### 9.2.1 La gestione delle indagini

Investigatori, rappresentanti dell'accusa e della difesa, giudici e giurie hanno tutti necessità di comprendere l'informatica e le nuove tecnologie. I casi possono risolversi in un nulla di fatto se la pubblica accusa non è in grado di identificare le questioni che devono essere chiarite nel processo

# Casi

## 10 Casi

### 10.1 Cause penali

#### 10.1.1 Ammissibilità dell'elaborazione di un computer come prova.

*R v Wood (Stanley William) (1983) 76 Cr. App. R. 23*

In questo caso alcune tipologie di metalli lavorati vennero rubati durante la fase di trasferimento dalla società di lavorazione e metalli dello stesso tipo furono rinvenuti in possesso del signor Wood. Il sig. Wood fu accusato di aver dirottato i metalli rubati. Al fine di provare che i metalli che il sig. Wood aveva trasportato facessero parte del lotto rubato, la documentazione in possesso della società di lavorazione consisteva in copie di calcoli ricavate da stampe eseguite al computer, successivamente distrutte, relative alla composizione chimica del lotto fornite dai chimici, i quali avevano eseguito un'analisi elaborata che richiedeva calcoli complessi effettuati da un programmatore utilizzando un computer.

I risultati furono confrontati per provare che i metalli trasportati e quelli conservati del lotto rubato avessero la stessa composizione. In questo processo il sig. Wood si oppose all'ammissione delle stampe come prova. Il giudice di prima istanza rigettò questa obiezione e la prova testimoniale, diversamente non contestata dall'appellante, fu fornita dai chimici e dal programmatore (i custodi della documentazione) e il sig. Wood fu condannato.

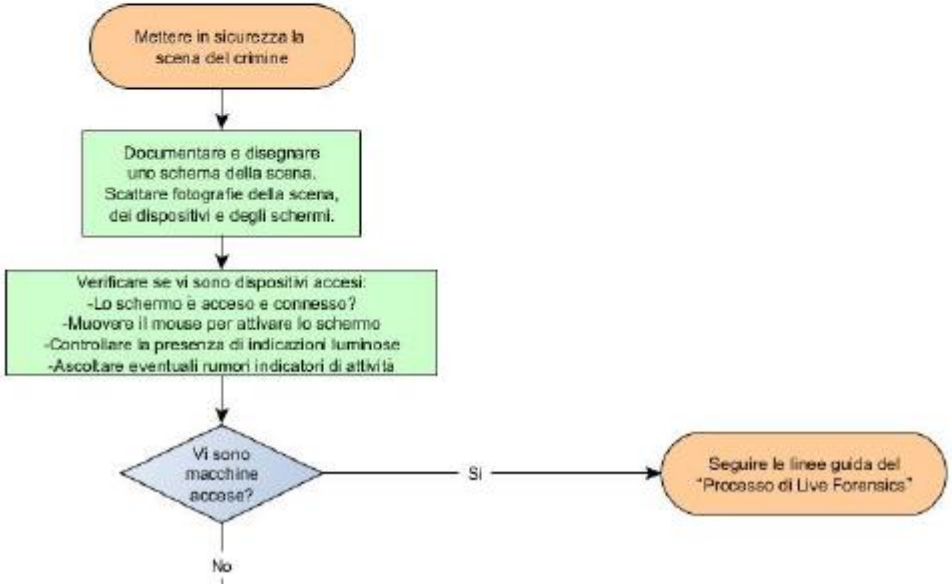
# Appendici

Fondato
dall'Unione Europea

Realizzato
dal Consiglio d'Europa

## Guida alla prova digitale

**Processo di ricerca e acquisizione per Forze dell'Ordine**



# Appendici

Fondato
dall'Unione Europea

Realizzato
dal Consiglio d'Europa

**Guida alla prova digitale**

## REGISTRO DELLA CATENA DI CUSTODIA

**Caso di riferimento……..……..**

**Registro ……... di ……...**

# Appendici

Fondato
dall'Unione Europea

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Realizzato
dal Consiglio d'Europa

## INFORMAZIONI GENERALI

| | |
|---|---|
| **Dispositivi rinvenuti sul posto** | ..... |
| **Computer da tavolo (numero)** | ..... |
| **Computer portatili (es. notebook. Laptop, etc...) (numero)** | ..... |
| **Computer in rete** | **Postazioni di lavoro** ..... **Server** ..... |
| **Altro** | |

# Appendici

Fondato
dall'Unione Europea

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Realizzato
dal Consiglio d'Europa

| INFORMAZIONI SUL CASO | |
|---|---|
| ID Progetto (1) | |
| Progetto/Nome dell'indagine (2) | |
| Nome del custode (3) | |
| Responsabile progetto (5) | |

| INFORMAZIONI SUL SISTEMA DA ANALIZZARE | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Posizione del sistema (6) | | | | | | | | | | |
| Tipo di sistema (7) | ☐ | Desktop | ☐ | Laptop | ☐ | Server | ☐ | Altro: | | |
| Tipo di prova (8) | ☐ | Hard drive | ☐ | CD/DVD | ☐ | Floppy | ☐ | RAID | ☐ | Altro: |
| Stato del sistema (9) | ☐ | ON | ☐ | OFF | ☐ | Logged ON | ☐ | Altro: | | |
| BIOS Data/ora (10) | | | | | | | | | | |
| Data/ora corrente (11) | | | | | | | | | | |
| Numero totale di Hard Drive nel computer (12) | | | | | | | | | | |
| Hard Drive rimossi da (13): | | | | | | | | | | |
| Foto catturate (14) | SI | NO | Se non catturata indicare la ragione | | | | | | | |

# Considerazioni finali

- PUNTI DI FORZA

  - Utile e **comprensibile anche ai non "addetti ai lavori"**, potrebbe essere utilizzata per dimostrare l'ammissibilità e l'utilizzabilità della prova digitale (in applicazione dei canoni elaborati dalla giurisprudenza);
  - "Metalingua" tra tecnici e giuristi;
  - La possibilità, per chi avesse poca dimestichezza con le procedure di gestione/acquisizione della prova digitale, di avere un quadro completo dei passi da compiere, grazie ai processi inseriti nelle Appendici.

# Considerazioni finali

- PUNTI DEBOLI
  - Manca di un diretto riscontro con le norme processuali italiane (sebbene, in alcune parti, si sia cercato un raccordo, pur nel rispetto del testo originale).
  - Livello qualitativo della versione originale non troppo elevato, soprattutto dal punto di vista tecnico.

**CyberCrime@IPA**

EU/COE Joint Project on Regional Cooperation against Cybercrime

# Guida alla prova digitale

**Una guida di base per agenti di polizia, pubblici ministeri e giudici**

**Versione 1.0**

Data Protection and Cybercrime Division
Council of Europe
Strasbourg, France, 18 March 2013 - Restricted/not for publication

**www.coe.int/cybercrime**

Funded by the European Union and the Council of Europe

Implemented by the Council of Europe

# Modulo di richiesta per la "Guida alla Prova Digitale"

Attraverso questo modulo è possibile richiedere il link per il download della "Guida alla Prova Digitale", traduzione in italiano della "Electronic Evidence Guide" redatta nell'ambito del progetto congiunto CyberCrime@IPA del Consiglio d'Europa e dell'Unione europea.

La guida è stata tradotta da un team di volontari italiani che ha sottoposto la traduzione al Council of Europe ottenendo l'approvazione ufficiale. Per la distribuzione della guida viene richiesto l'inserimento di un indirizzo di posta elettronica valido, al quale verrà inviato il link per il download del PDF e la password per aprirlo, oltre a notifiche per futuri aggiornamenti del testo.

*Campo obbligatorio

**Nome** *
Inserisci il tuo nome e cognome

**Email** *
Inserisci il tuo indirizzo email

## Informativa

L'Associazione Digital Forensics Alumni (DFA) con sede legale in Via Spallanzani 16, 20129 Milano, C.F. 97643570159, e-mail info@perfezionisti.it, ("Titolare"), in qualità di Titolare del Trattamento effettuato sul sito www.perfezionisti.it ("Sito") e le Associazioni Tech and Law Center (TLC), con sede in Piazza San Pietro in Gessate 2, 20122 Milano, C.F. 97695650152, info@techandlaw.net e DEFT, con sede in Piazza dei Colori, 26, 40138 Bologna, C.F. 91350600374, info@deftlinux.net, in qualità di co-Titolari del trattamento dei dati, Ti informano che tratteranno i Tuoi dati personali al fine di (i) verificare i requisiti professionali per la concessione delle credenziali di accesso al documento "Guida alla Prova Digitale"; (ii) segnarTi eventi o workshop attinenti alla materia dell'informatica giuridica.

# Dove reperire la versione Italiana

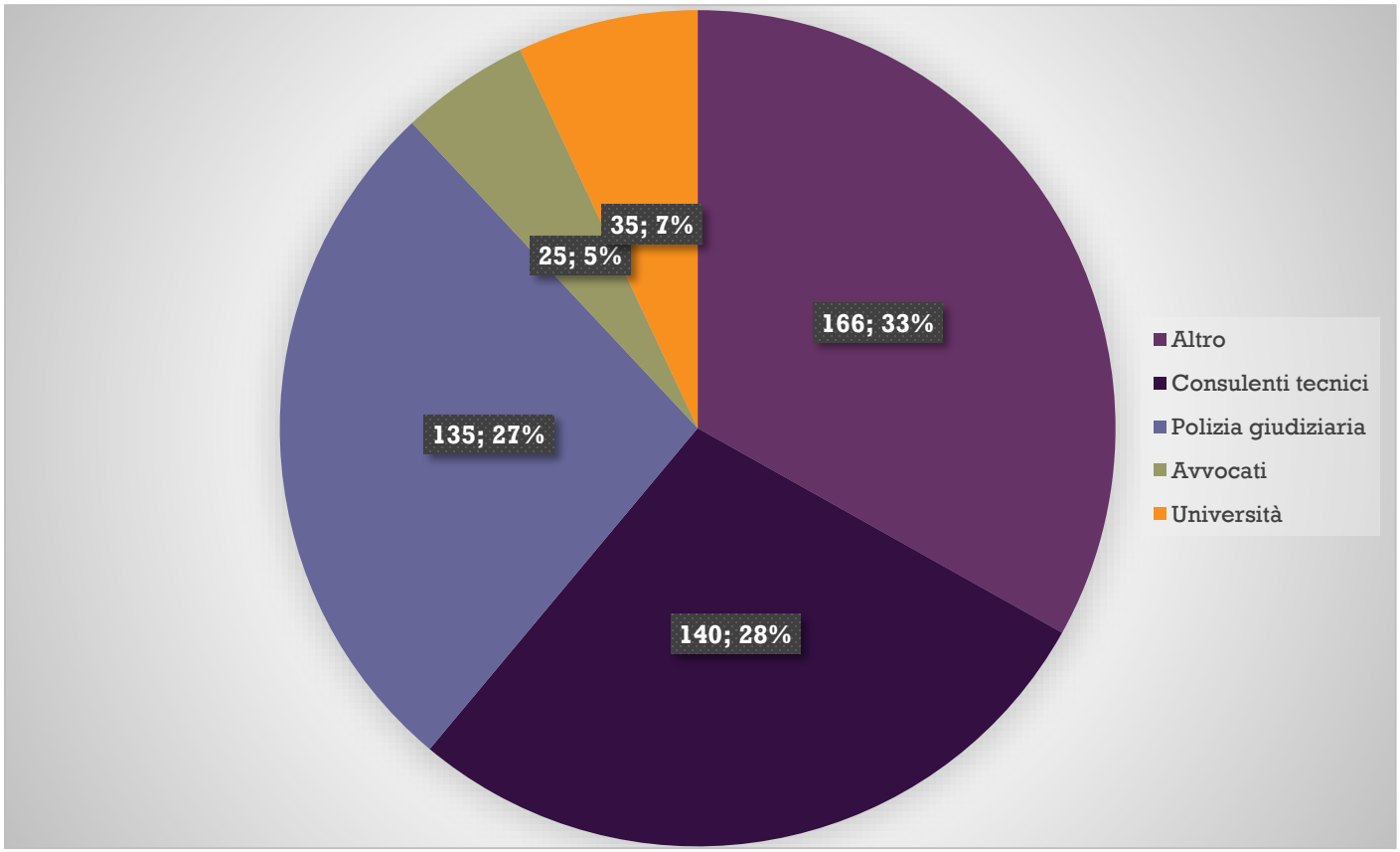
- A chi è rivolta?
- Compilare form con Nome, Cognome, indirizzo email valido

http://bit.ly/eeg-ita-form

- Per informazioni: info@perfezionisti.it

# Statistiche di download

- **501 download** "ufficiali" dal 11/4 al 31/5



# Ringraziamenti


- *Francesco* ***Acchiappati***
- *Ilaria* ***Bevilacqua***
- *Roberto* ***Bonalumi***
- *Francesca* ***Bosco***
- *Gianbattista* ***Causin***
- *Eleonora* ***Colombo***
- *Paolo* ***Dal Checco***
- *Ferdinando* ***Ditaranto***
- *Mattia* ***Epifani***
- *Fabio* ***Filippi***
- *Stefano* ***Fratepietro***
- *Nicoleta* ***Gherghina***
- *Donato* ***La Muscatella***
- *Angelo Osvaldo* ***Rovegno***
- *Giuseppe* ***Serafini***
- *Marco Carlo* ***Spada***
- *Pasquale* ***Stirparo***
- *Remo* ***Tantalo***
- *Riccardo* ***Trifonio***
- *Giuseppe* ***Vaciago***
- *Alessandro* ***Valerio***
- *Alberto* ***Vigano***
- *Lisa* ***Zinato***