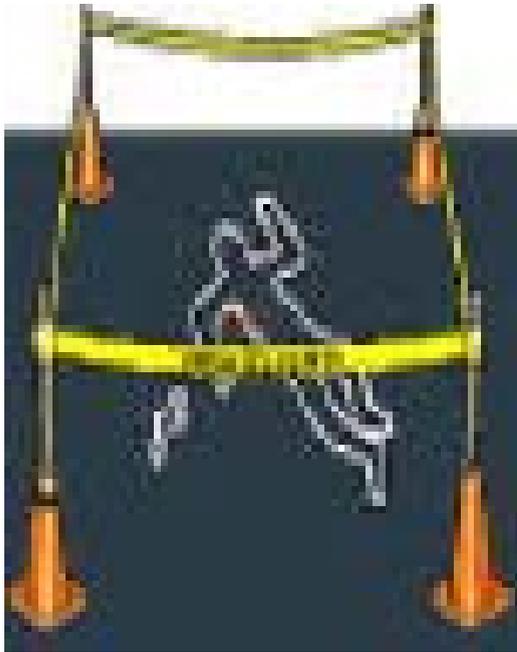


L'informatica Forense: profili critici della prova informatica

30 maggio 2011

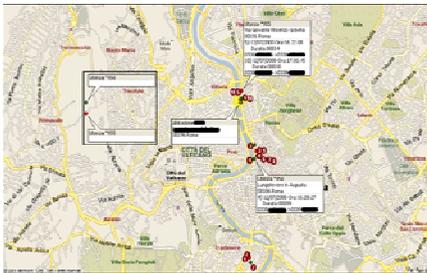


volatilità - modificabilità – alterabilità



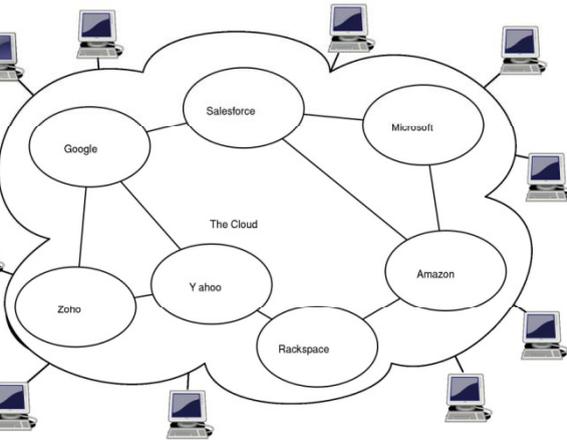
sulla scena
del crimine

sarà
possibile
individuare



Comune	Cella Inizio	Cella Fine	Indirizzo Cella Fine	Comune	Cella Fine	IMSI Chiamante	IMSI Chiamato
ROMA	22288	3003108871	VIA DELLA VENEZIA GIULIA 131 00177	ROMA	22288	████████████████████	22288 ████████████████████
ROMA	22288	3003009524	VIA DEGLI APUANI 4 00185	ROMA	22288	████████████████████	22288 ████████████████████

Nuove Reti e nuovi strumenti



Legge n. 48 del 2008

Ratifica della convenzione di Budapest 2001

Perquisizioni su sistemi informatici

Sequestri (supporti, dati, informazioni)

Acquisizioni

Ispezioni

”...adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali ed ad impedirne l’alterazione....”.

Le disposizioni processuali sul cybercrime introdotte dalla legge
18 marzo 2008, n. 48

**Art. 244 c.p.p. - Casi e forme delle ispezioni . (l., n. 48
del 2008)**

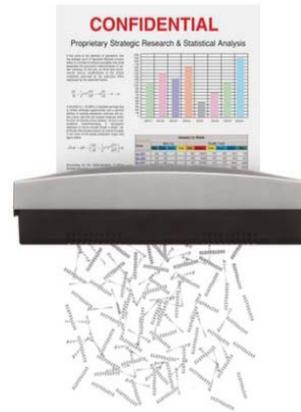
Art. 247 c.p.p. Casi e forme delle perquisizioni

***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***

(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 immutabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali. (l., n. 48 del 2008)

0.000	1.11	02/00/00	Misc	0.000
0.000	1.11	03/00/00	Misc	0.000
0.000	1.11	04/00/00	Misc	0.000
0.000	1.11	05/00/00	Misc	0.000
0.000	1.11	06/00/00	Misc	0.000
0.000	1.11	07/00/00	Misc	0.000
0.000	1.11	08/00/00	Misc	0.000
0.000	1.11	09/00/00	Misc	0.000
0.000	1.11	10/00/00	Misc	0.000
0.000	1.11	11/00/00	Misc	0.000
0.000	1.11	12/00/00	Misc	0.000
0.000	1.11	13/00/00	Misc	0.000
0.000	1.11	14/00/00	Misc	0.000
0.000	1.11	15/00/00	Misc	0.000
0.000	1.11	16/00/00	Misc	0.000
0.000	1.11	17/00/00	Misc	0.000
0.000	1.11	18/00/00	Misc	0.000
0.000	1.11	19/00/00	Misc	0.000
0.000	1.11	20/00/00	Misc	0.000
0.000	1.11	21/00/00	Misc	0.000
0.000	1.11	22/00/00	Misc	0.000
0.000	1.11	23/00/00	Misc	0.000
0.000	1.11	24/00/00	Misc	0.000
0.000	1.11	25/00/00	Misc	0.000
0.000	1.11	26/00/00	Misc	0.000
0.000	1.11	27/00/00	Misc	0.000
0.000	1.11	28/00/00	Misc	0.000
0.000	1.11	29/00/00	Misc	0.000
0.000	1.11	30/00/00	Misc	0.000
0.000	1.11	31/00/00	Misc	0.000
0.000	1.11	32/00/00	Misc	0.000
0.000	1.11	33/00/00	Misc	0.000
0.000	1.11	34/00/00	Misc	0.000
0.000	1.11	35/00/00	Misc	0.000
0.000	1.11	36/00/00	Misc	0.000
0.000	1.11	37/00/00	Misc	0.000
0.000	1.11	38/00/00	Misc	0.000
0.000	1.11	39/00/00	Misc	0.000
0.000	1.11	40/00/00	Misc	0.000
0.000	1.11	41/00/00	Misc	0.000
0.000	1.11	42/00/00	Misc	0.000
0.000	1.11	43/00/00	Misc	0.000
0.000	1.11	44/00/00	Misc	0.000
0.000	1.11	45/00/00	Misc	0.000
0.000	1.11	46/00/00	Misc	0.000
0.000	1.11	47/00/00	Misc	0.000
0.000	1.11	48/00/00	Misc	0.000
0.000	1.11	49/00/00	Misc	0.000
0.000	1.11	50/00/00	Misc	0.000
0.000	1.11	51/00/00	Misc	0.000
0.000	1.11	52/00/00	Misc	0.000
0.000	1.11	53/00/00	Misc	0.000
0.000	1.11	54/00/00	Misc	0.000
0.000	1.11	55/00/00	Misc	0.000
0.000	1.11	56/00/00	Misc	0.000
0.000	1.11	57/00/00	Misc	0.000
0.000	1.11	58/00/00	Misc	0.000
0.000	1.11	59/00/00	Misc	0.000
0.000	1.11	60/00/00	Misc	0.000
0.000	1.11	61/00/00	Misc	0.000
0.000	1.11	62/00/00	Misc	0.000
0.000	1.11	63/00/00	Misc	0.000
0.000	1.11	64/00/00	Misc	0.000
0.000	1.11	65/00/00	Misc	0.000
0.000	1.11	66/00/00	Misc	0.000
0.000	1.11	67/00/00	Misc	0.000
0.000	1.11	68/00/00	Misc	0.000
0.000	1.11	69/00/00	Misc	0.000
0.000	1.11	70/00/00	Misc	0.000
0.000	1.11	71/00/00	Misc	0.000
0.000	1.11	72/00/00	Misc	0.000
0.000	1.11	73/00/00	Misc	0.000
0.000	1.11	74/00/00	Misc	0.000
0.000	1.11	75/00/00	Misc	0.000
0.000	1.11	76/00/00	Misc	0.000
0.000	1.11	77/00/00	Misc	0.000
0.000	1.11	78/00/00	Misc	0.000
0.000	1.11	79/00/00	Misc	0.000
0.000	1.11	80/00/00	Misc	0.000
0.000	1.11	81/00/00	Misc	0.000
0.000	1.11	82/00/00	Misc	0.000
0.000	1.11	83/00/00	Misc	0.000
0.000	1.11	84/00/00	Misc	0.000
0.000	1.11	85/00/00	Misc	0.000
0.000	1.11	86/00/00	Misc	0.000
0.000	1.11	87/00/00	Misc	0.000
0.000	1.11	88/00/00	Misc	0.000
0.000	1.11	89/00/00	Misc	0.000
0.000	1.11	90/00/00	Misc	0.000
0.000	1.11	91/00/00	Misc	0.000
0.000	1.11	92/00/00	Misc	0.000
0.000	1.11	93/00/00	Misc	0.000
0.000	1.11	94/00/00	Misc	0.000
0.000	1.11	95/00/00	Misc	0.000
0.000	1.11	96/00/00	Misc	0.000
0.000	1.11	97/00/00	Misc	0.000
0.000	1.11	98/00/00	Misc	0.000
0.000	1.11	99/00/00	Misc	0.000
0.000	1.11	00/00/00	Misc	0.000



- ***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)***

NO alle “perquisizioni” occulte !

- **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)*

Le prime pronunce della Cassazione

- **Cass.** 12 dicembre 2008-13 marzo 2009 n. 11135, **B.**
- **Cass. n.** 11503 del 16/03/2009, **Dell'Av.**
- **Cass. n.** 11863 del 18/03/2009, **Ammu.**
- **Cass. n.** 14511 del 02/04/2009. **Stab.**
- **Cass.** n. 2388, 19.1.2010, **Pirr.**
- **Cass. n.** 16556 del 29/04/2010 sul **cd captatore informatico**

La Cassazione e il suo rapporto con l'hashing

Cass. 12 dicembre 2008-13 marzo 2009 n. 11135, B.

L'esperibilità delle procedure di hashing, ossia delle tecniche volte a verificare l'integrità e la conformità all'originale del dato informatico sequestrato e conservato in copia su un apposito supporto (nella specie Cd-Rom), è una questione di merito, potendosi in sede di legittimità **esclusivamente delibare se gli accorgimenti adottati dalla polizia giudiziaria delegata siano o meno idonei in astratto a tutelare le finalità indicate dal legislatore** negli articoli 247, comma 1-bis, e 354, comma 2, del C.p.p. per come modificati dalla legge 48/2008 di ratifica della Convenzione del Consiglio d'Europa sul cybercrime.

La Cassazione e la lettura “post factum” del PC. Ripetibilità.

Sez. 1, **Sentenza** n. 11503 del 25/02/2009,
cc. (dep. 16/03/2009) Dell'Av.

Ipotesi di analisi/lettura del PC in assenza dei difensori in assenza di una accertata alterazione del disco informatico, tra l'altro appartenente ad un terzo soggetto.

Non dà luogo ad accertamento tecnico irripetibile la lettura dell' "hard disk" di un computer sequestrato, che è attività di polizia giudiziaria volta, anche con urgenza, all'assicurazione delle fonti di prova. E' quindi ripetibile.

La Cassazione e l'estrazione dei dati da parte di personale esperto

- *Sez. 1, **Sentenza n. 11863 del 26/02/2009***
Cc. (dep. 18/03/2009), **Amm.**
- L'estrazione dei dati contenuti in un supporto informatico, se eseguita da personale esperto in grado di evitare la perdita dei medesimi dati, costituisce un accertamento tecnico ripetibile.

La Cassazione e la ripetibilità degli atti prelevati su PC

- Sez. 1, **Sentenza n. 14511 del 05/03/2009**
Cc. (dep. 02/04/2009) **imputato: S. Av.**
- Non rientra nel novero degli atti irripetibili l'attività di estrazione di copia di "file" da un computer oggetto di sequestro, dal momento che essa non comporta alcuna attività di carattere valutativo su base tecnico-scientifica, né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità d'informazioni identiche a quelle contenute nell'originale

3. Ciò posto, è da escludere che l'attività di estrazione di copia di "file" da un computer costituisca un atto irripetibile (nel senso in precedenza indicato), atteso che non comporta alcuna attività di carattere valutativo su base tecnico-scientifica né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità di informazioni identiche a quelle contenute nell'originale.

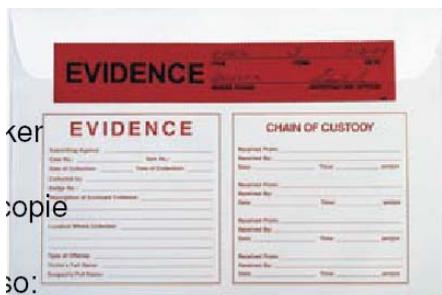
Lo stesso ricorrente, del resto, non ha in concreto allegato alcuna forma di distruzione o alterazione dei dati acquisiti, tale da confortare il suo assunto, ma si è limitato a prospettare ipoteticamente alcune situazioni potenziali che esulano dalla fattispecie sottoposta all'esame della Corte.

IN DIRITTO

Il quinto motivo è fondato e assorbe anche gli altri perché impone una rivalutazione del materiale sequestrato,

Il perito nominato dal tribunale ha rilevato, dandone altresì immediata comunicazione al tribunale, che il materiale che gli era stato consegnato era difforme quantitativamente da quanto

verbalizzato dalla Questura di Lecco ed ha precisato altresì che esso non era stato in alcun modo sigillato e che gli era stato consegnato in scatoloni di cartone aperti. A norma dell'articolo 260 c.p.p. le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario al quale vengono consegnate e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che vi assiste ovvero, in relazione alla natura delle cose, con altro mezzo idoneo ad indicare il vincolo imposto a fini di giustizia. La funzione dei sigilli serve a garantire la genuinità del sequestro. La mancata apposizione dei sigilli alla cosa sequestrata, per la tassatività delle nullità, non determina l'illegittimità del sequestro e non impedisce l'utilizzabilità della prova che dai reperti sia in seguito acquisita a condizione però che sia comunque certa l'identità della cosa sequestrata. Nella fattispecie, a seguito della comunicazione del consulente e dei rilievi del difensore, prima di utilizzare la perizia, si sarebbero dovuti svolgere accertamenti per stabilire se, nonostante la mancanza dei sigilli, dovessero escludersi ipotesi di manomissione o di confusione tra reperti. La questione,



La Cassazione sulla captazione occulta di dati da remoto

- Sez. 5, **Sentenza n. 16556 del 14/10/2009** Ud. (dep. 29/04/2010)
- È legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel "personal computer" in uso all'imputato e installato **presso un ufficio pubblico**, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati. (Nel caso di specie, l'attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull'"hard disk" del computer in uso all'imputato, aveva avuto ad oggetto non un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma "una relazione operativa tra microprocessore e video del sistema elettronico", ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer; la S.C. ha ritenuto corretta la qualificazione dell'attività di captazione in questione quale prova atipica, sottratta alla disciplina prescritta dagli artt. 266 ss. cod. proc. pen.).

Le indagini informatiche e l'acquisizione di elementi di prova digitali

- Assistenza passiva (aspettate che il PM finisca le indagini)
- Assistenza attiva – tempestività nell'esecuzione delle indagini difensive

Grazie per l'attenzione
Resto vostra disposizione per eventuali
domande

Avv. Stefano Aterno

www.studioaterno.it

s.aterno@studioaterno.it

