REGIONE CARABINIERI PIEMONTE E VALLE D'AOSTA
Comando Provinciale di Torino
Reparto Operativo – Sezione Investigazioni Scientifiche

Repertamento di materiale informatico

9. Il repertamento di materiale informatico.

a. Generalità;

b. Repertamento.

9. Il repertamento di materiale informatico.
a. Generalità.

Il termine Informatica Forense (I.F.) sta ad indicare quella parte delle scienze forensi che si occupa di determinare prove utilizzabili in ambito legale a partire da sistemi elettronici computerizzati in cui vengono memorizzate informazioni. La I.F. rientra nel più ampio campo della Telematica Forense (T.F.), la quale raccoglie, nel suo campo di analisi, anche i sistemi di telecomunicazione digitali ed analogici (GSM, telefonia fissa, etc.).

9. Il repertamento di materiale informatico.
a. Generalità.

La I.F. è lo strumento principale nella lotta al crimine informatico che può essere definito come un **atto criminale** per il quale:

l'utilizzo dell'elaboratore è essenziale per il compimento del crimine;

un elaboratore, non essenziale per la consumazione del crimine, è utilizzato invece per memorizzare o trasmettere informazioni riguardanti il crimine.

9. Il repertamento di materiale informatico.
a. Generalità.

I **crimini informatici principali** includono truffe su carte di credito, truffe su trasferimenti elettronici di fondi, distribuzione di pedopornografia via Internet, inserimenti illeciti e propagazione di virus.

Crimini per i quali un elaboratore **non è essenziale** includono, ad esempio, omicidi, truffa, furto, falsificazioni, etc.. L'elaboratore non è essenziale per l'esecuzione dei crimini suddetti ma può essere connesso ad essi (ad esempio per coordinare azioni criminose) oppure può contenere informazioni necessarie per risalire agli autori del crimine.

9. Il repertamento di materiale informatico.
b. Repertamento.

L'ambito limitato cui si fa riferimento riguarda il personal computer con le sue periferiche standard: stampanti, scanner, monitor, mouse, tastiera ed alcuni dispositivi di memoria di massa: floppy disk (FD), compact disk (CD), "chiavette elettroniche", e varie tipologie di nastri magnetici.

L'imperativo nelle operazioni di repertamento ed analisi dei dati è il seguente: **nemmeno un bit del contenuto stabile di memoria del sistema repertato deve essere modificato durante l'accertamento**.

9. Il repertamento di materiale informatico. b. Repertamento.

I due concetti più importanti trattati dall'investigazione informatica forense sono quelli relativi a:

integrità probatoria, che richiede che il materiale esaminato non venga modificato in nessun modo, ciò che si esamina deve essere una esatta copia dell'originale;

continuità probatoria, la continuità probatoria richiede che tutte le azioni, gli strumenti e le procedure coinvolti nell'investigazione siano registrati formalmente.

9. Il repertamento di materiale informatico. b. Repertamento.

Da un punto di vista concettuale esistono due livelli di repertamento di un sistema informatico:

repertamento dell'oggetto;

repertamento dei dati che in ambito forense internazionale viene identificato con il termine "*data analysis" o analisi dei dati*.

9. Il repertamento di materiale informatico.
b. Repertamento.

Generalmente il repertamento fisico anticipa quello dei dati ma si noti che questa tende a non essere più una regola. Si stanno infatti diffondendo rapidamente sistemi portatili di repertamento dati che consentono di registrare il contenuto dati di un PC senza necessariamente prelevarlo e trasportarlo in un laboratorio specializzato.

Nel repertamento fisico si deve identificare l'elaboratore e tutte le periferiche hardware: tastiera, monitor, stampanti ed altro ancora. La regola generale è prendere possesso di tutto l'hardware incluse le periferiche.

9. Il repertamento di materiale informatico.
b. Repertamento.

L'hardware, una volta sequestrato, deve essere collocato in un posto sicuro dove può essere riassemblato e preparato per la copia prima di iniziare l'esame. **In nessuna circostanza si dovrà tentare di esaminare il contenuto di una macchina direttamente sul posto.**

Non attivare computer sequestrati o sospetti al fine di controllarli preliminarmente perché si potrebbero inavvertitamente cancellare dei dati costituenti prove legali.

9. Il repertamento di materiale informatico.
b. Repertamento.

La prima operazione da compiere è la disattivazione del sistema. Questo perché l'unico stato dell'elaboratore che assicura la sua impossibilità di proteggersi o distruggere dati utili è proprio quello in cui il sistema non è alimentato elettricamente.

Disattivare un sistema, seconda del sistema operativo utilizzato, può voler dire o staccare semplicemente la spina di alimentazione o instaurare un processo di disattivazione dalla rete di computer cui si è connessi tramite comandi appropriati. Nel primo caso si può agire senza l'intervento del tecnico specializzato mentre nel secondo è necessario richiedere l'intervento del personale specializzato (tecnici del Ra.C.I.S. od altro consulente), impedendo, nel frattempo, al tecnico gestore del sistema di agire su di esso per qualsiasi motivo.

9. Il repertamento di materiale informatico.
b. Repertamento.

Durante le operazioni di repertamento è importante che vengano fatte delle fotografie del sistema da varie angolazioni per documentare la configurazione Hardware e le relative connessioni.

È inoltre importante inoltre etichettare ogni cavo di connessione ed ogni elemento hardware presente (stampanti, video, etc.) in modo da poterli facilmente riconnettere una volta che il computer debba essere riportato nelle condizioni originali in un luogo sicuro dove poi procedere all'accertamento tecnico.

9. Il repertamento di materiale informatico.
b. Repertamento.

Una volta smontato il sistema si deve aver cura di imballare le singole parti in contenitori che diano la sufficiente protezione meccanica può infatti capitare he tali parti siano soggette ad urti durante il viaggio fino al laboratorio, quindi si deve provvedere ad inserire nell'imballo del materiale plastico per assorbire gli urti o più semplicemente ed economicamente dei giornali accartocciati. Tali imballi potranno essere successivamente etichettati.

Per quello che riguarda i cavi di collegamento tra i vari dispositivi del sistema, si devono etichettare e porre in un imballo separato da quello della rispettiva parte collegata in maniera, da rendere difficile ad un inesperto la reinstallazione del sistema globale.

9. Il repertamento di materiale informatico.
b. Repertamento.

Dopo la disattivazione del sistema individuato è necessario raccogliere fisicamente tutti i supporti di memorizzazione presenti avendo cura di segnalare la loro posizione fisica (vicino al PC di lavoro, nel cassetto chiuso a chiave, etc.) Bisogna fare quindi attenzione a dischetti, CD, cassette di formato diverso da quelle musicali, nastri, hard disk staccati da PC, etc.

Dischetti, CD, cassette e nastri magnetici di vari formati sono una fonte di dati il più delle volte importantissima ai fini del repertamento; è quindi necessario soffermarsi accuratamente a catalogare ed etichettare tutto il materiale di questo tipo.

9. Il repertamento di materiale informatico.
b. Repertamento.

La data e l'ora associati ai file di un computer possono essere estremamente importanti dal punto di vista delle prove. Tuttavia soltanto l'accuratezza di questi dati è veramente importante. Se l'orologio (clock) del sistema presenta un errore (ad esempio legato all'ora solare) allora anche l'orario associato ai file rifletterà tale errore.

Per correggere queste imprecisioni, quindi, bisogna documentare l'orario e la data in cui si trova il sistema al momento in cui si entra in possesso del computer e fare in modo che il software di analisi dei dati modifichi tutte le date dei file da esaminare in base all'errore riscontrato. Si fa chiaramente l'ipotesi (mediamente valida) che tutti i file del PC repertato siano stati soggetti alla stessa modifica dell'orario; questo naturalmente non è sempre vero e tale fatto bisogna sia evidenziato nella relazione tecnica finale.

REGIONE CARABINIERI PIEMONTE E VALLE D'AOSTA
Comando Provinciale di Torino
Reparto Operativo -Sezione Investigazioni Scientifiche

Quesiti ?

Cap. Emilio Bosini
Reparto Operativo Carabinieri – Sezione Investigazioni Scientifiche
Via F.Valfré nr. 5/bis 10121 Torino
Tel 011/6887655 e-mail emilio.bosini@carabinieri.it