La perizia informatica: la gestione del rischio nel contenzioso Ict

Roberto Bello è stato perito estimatore e Ctu (codice 7890) presso il Tribunale di Milano per il software. Consulente per la preparazione del Dps (Documento programmatico sulla sicurezza). Esperto nel settore delle applicazioni e dell'ambiente *open source*. Socio fondatore dell'Associazione Italiana Professionale di Informatica e *Ict Strategist* del ClubTi di Milano.

Premessa

Il documento contiene consigli pratici per chi volesse intraprendere la professione di Ctu (Consulente Tecnico di Ufficio) o di Ctp (Consulente Tecnico di Parte).
Contiene anche molti consigli legali, tecnici e di *buon senso informatico* utili a prevenire inutili e lunghi contenziosi.
L'esposizione dei temi trattati è volutamente semplice nei limiti consentiti dagli argomenti legali e informatici citati.
Le pagine sono il concentrato di quindici anni di esperienza presso il Tribunale di Milano sia come Ctu sia come Ctp.
La nuova edizione contiene nuovi capitoli dedicati all'*Analisi forense*, alla *Perizia giurata / asseverata* e a *La sicurezza informatica nelle Imprese e nella Pubblica Amministrazione - Regolamento interno per dipendenti e collaboratori*.

Prepararsi prima, per litigare meglio dopo

Molto spesso non ci si immagina di diventare protagonisti, come attori o convenuti, in cause legali per applicazioni Ict, dove una parte lamenta errori, disfunzioni, anomalie e carenze in un'applicazione, mentre l'altra si difende con considerazioni opposte tese a dimostrare le adeguate funzionalità e il rispetto di quanto contrattualmente pattuito.
Ipotizziamo che un'azienda voglia acquistare da una *software house* la licenza di uso di un applicativo gestionale e chieda poi delle personalizzazioni.
Molto probabilmente, il fornitore farà sottoscrivere al cliente un primo contratto relativo alla cessione della licenza d'uso nella sua forma standard con un'appendice ove si descrivono le modalità dei futuri aggiornamenti, indicando i canoni di manutenzione ordinaria.
Un ulteriore contratto, più o meno dettagliato, potrebbe essere sottoscritto per le personalizzazioni e dovrebbe contenere la descrizione delle personalizzazioni, i tempi di realizzazione, le risorse stimate (giorni uomo per tipologia professionale) e le date previste di rilascio delle diverse funzionalità aggiunte o da modificare.
Più frequentemente, il fornitore fa sottoscrivere una *paginetta* dove le parti prendono atto del valore in euro delle tariffe giornaliere delle figure professionali del

fornitore coinvolte nelle attività di personalizzazione.
La logica sottostante questa tipologia di accordi, consente al cliente di chiedere quello che vuole, al fornitore di *eseguire* poiché il cliente pagherà il tempo consumato, indipendentemente dal risultato.
Interventi inizialmente stimati dal cliente come facili e poco impegnativi risultano poi costosi e complicati per il fornitore.
Alle volte anche gli errori trovati dal cliente in parti standard dell'applicazione, per il fornitore sono la conseguenza delle personalizzazioni volute dal cliente e, a parere del fornitore, il costo della loro sistemazione deve essere a totale carico del cliente.
Così comincia l'intrecciarsi di telefonate, *email*, raccomandate, diffide ad adempiere, fino alla notifica a comparire davanti al Giudice per la costituzione in giudizio delle parti, ormai in aperta lite.

Il ruolo del Ctu

La causa inizia il suo iter e dopo alcuni anni di udienze consumate a esaminare carte, chiedere rinvii, eccepire vizi procedurali, ascoltare testimoni, il Giudice assegna un quesito (o dei quesiti) a un consulente tecnico d'ufficio (Ctu) che deve, in circa sessanta giorni, scoprire se l'applicazione di cinque anni prima funzionava o meno.
Ma in cinque anni quanta acqua è passata sotto i ponti della tecnologia?
Spesso i computer di allora non esistono più e neppure i programmi.
Oppure i programmi sono su un Cd del fornitore che giura contengano proprio i programmi di allora, mentre il Cd potrebbe essere stato confezionato il giorno precedente con una versione dell'applicazione abilmente aggiornata ed esente dai vizi lamentati ai tempi della costituzione della causa.
Peggio ancora quando l'applicazione riguarda un sito Web di tipo dinamico.
Il Ctu ha il dovere di effettuare una valutazione di tipo tecnico su archivi e sistemi Ict riferibili ai tempi di inizio della lite, archivi e sistemi che non possano essere contestati dai consulenti tecnici di parte (Ctp), perché ritenuti da questi ultimi non rappresentativi di quanto in contestazione.
Una massima della Corte di Cassazione Sezione Lavoro n. 2912 del 18 febbraio 2004 in relazione al valore probatorio di una pagina Web indica che *la copia di una pagina Web su supporto cartaceo ha valore probatorio solo se raccolta con le dovute garanzie per la rispondenza all'originale e riferibili a un momento ben individuato. Le informazioni tratte da una rete telematica sono per loro natura volatili e suscettibili di continua trasformazione*.
Gli archivi memorizzati su supporti magnetici sono, per loro natura, facilmente manipolabili; le versioni precedenti degli archivi scompaiono in modo totale e, a differenza di ciò che accade nel mondo del reale, non restano tracce della loro precedente identità.

Precauzioni necessarie

Per prepararsi al meglio, in vista di possibili liti future, occorre osservare delle precauzioni di tipo contrattuale e altre di tipo tecnico-organizzativo.
Sono molto importanti i contenuti del contratto iniziale di fornitura, soprattutto per

quanto riguarda il dettaglio delle personalizzazioni, i tempi di realizzazione e quelli di risposta, i risultati attesi, gli utenti che possono operare contemporaneamente sull'applicazione, la disponibilità del codice sorgente, i requisiti minimi di hardware e di software, gli obblighi e le penali in caso di malfunzionamento, le garanzie di operabilità su altri sistemi operativi, i livelli di addestramento richiesti agli utenti e quant'altro i soggetti contrattuali ritengano necessario per definire le prestazioni di una parte verso l'altra.
Sono, sicuramente, da evitare contratti per la personalizzazione di un'applicazione che tengano conto come termine di misura solo il tempo speso per realizzare quanto il cliente desidera: il fornitore sarebbe troppo tentato nel seguire i desideri più strani del cliente e destabilizzanti (per l'applicazione); interventi dannosi che comunque procurerebbero fatturato al fornitore senza alcuna sua responsabilità.
Nella mia esperienza di Ctu, ho verificato che l'aspetto contrattuale è preso in considerazione ma non con il dettaglio tecnico necessario a una futura perizia.
Nel corso della stipulazione, le parti dovrebbero procurarsi delle prove valide da utilizzare in caso di eventuale contenzioso.
Quando avviene la consegna dell'applicazione, ad esempio, è opportuno che cliente e fornitore diano atto dell'installazione avvenuta, apponendo anche la firma e la data di installazione (con pennarello a inchiostro indelebile) su copie identiche di Cd contenenti i programmi eseguibili, gli eventuali sorgenti, i manuali di installazione e di uso, le specifiche tecniche e così via.
Tali copie potranno servire in sede di contenzioso e la loro autenticità non potrà essere messa in dubbio, poiché registrate su supporti non alterabili, datati e sottoscritti da entrambe le parti.
Può succedere che il cliente lamenti poi errori e malfunzionamenti dell'applicazione che il fornitore non riconosce.
In questo caso, mancando la collaborazione, è opportuno rivolgersi a un perito, meglio se iscritto all'albo del Tribunale, e incaricarlo di una perizia giurata.
Svolto l'incarico, il perito prepara l'elaborato, allega ad esso il Cd (datato e firmato) contenente i programmi, i dati e quant'altro necessario per documentare gli errori riscontrati, si reca in Tribunale e giura di aver svolto la perizia presso il cliente nella data certa riportata nell'elaborato stesso.
Il documento peritale costituisce un altro esempio di prova precostituita.
Risultato analogo si otterrebbe depositando il Cd presso un notaio che, senza entrare nel merito tecnico del contenuto, potrebbe certificarne la data di deposito.
In alternativa alla Ctu sono disponibili altri procedimenti previsti dall'art. 696bis c.p.c. (ATP - Accertamento tecnico preventivo e CTP – Consulenza Tecnica Preventiva) che, con tempi molto rapidi, possono intervenire su sistemi, programmi e reti di comunicazione ancora attuali ed operativi.
Il consiglio principale, comunque, resta quello di andare in causa solo se si è in grado di produrre prove tecniche sicure e non contestabili, a meno che il fine effettivo sia di tirare per le lunghe il procedimento, usando i tempi della giustizia per non pagare. E' una circostanza che purtroppo spesso si verifica.

La figura del Ctu nel contenzioso Ict

Ruolo, responsabilità e funzioni

Una figura professionale poco nota fra le molte presenti e conosciute nel settore dell'Ict è quella del consulente tecnico di ufficio (Ctu) che interviene in cause legali a seguito di liti per carenze o disservizi nel campo del software, dell'hardware e delle telecomunicazioni.
Diventare Ctu può essere un obiettivo professionale gratificante, che il responsabile dei sistemi informativi potrebbe perseguire per utilizzare, valorizzandola, l'esperienza acquisita in azienda.

L'iter iniziale

Nell'iter di causa, una delle parti può ritenere necessario chiedere al Giudice una consulenza tecnica d'ufficio per accertare eventuali vizi, difetti, errori, anomalie e quant'altro di non funzionante o di non funzionale in relazione al prodotto/servizio oggetto di causa.
Le parti possono proporre al Giudice delle ipotesi di quesiti ai quali il futuro Ctu dovrà rispondere.
Il Giudice sceglie il possibile Ctu consultando la lista presente nell'albo del Tribunale nella sezione di competenza (informatica).
Il futuro Ctu viene convocato in Tribunale dove, alla presenza dei legali delle parti e del Giudice, dopo aver letto gli atti di causa, accetta l'incarico e presta giuramento di adempiere con professionalità e onestà all'incarico ricevuto.
A questo punto, il Giudice, con l'eventuale aiuto dei legali e del Ctu, formula i quesiti tecnici ai quali il Ctu stesso dovrà rispondere nel suo elaborato finale.
Viene, poi, fissata la data e il luogo della prima riunione di apertura della consulenza tecnica, il Giudice fissa il termine massimo per il deposito dell'elaborato della consulenza tecnica presso la cancelleria del Tribunale (di norma 60/90 giorni) e l'eventuale anticipo in euro che le parti dovranno liquidare al Ctu come fondo spese (di norma ripartito equamente).
Per l'ATP (Accertamento Tecnico Preventivo) e per la CTP (Consulenza Tecnica Preventiva) il Giudice può fissare altri termini intermedi.
I legali possono nominare dei Ctp (consulenti tecnici di parte) che dovranno collaborare con il Ctu nelle verifiche tecniche per dare risposta ai quesiti posti dal Giudice (naturalmente, tenendo ben in mente gli interessi di parte).

Il percorso della consulenza

Nella prima riunione, il Ctu e i Ctp, dopo aver letto i quesiti posti dal Giudice, concordano le modalità e i tempi di svolgimento della consulenza tecnica.
In particolare, evidenziano gli *oggetti* da sottoporre a ispezione tecnica e il loro residuo *valore probatorio*, considerando la facilità di modifica dei dati informatici ed evidenziando gli strumenti, i fatti e le circostanze non più riproducibili.
Dalla data della prima riunione decorrono i termini per la consegna dell'elaborato finale in cancelleria da parte del Ctu, il quale, al termine dell'incontro redige una relazione sui fatti e sulle considerazioni di maggior rilievo.

Anche i Ctp possono verbalizzare dichiarazioni personali di precisazione o di disaccordo.
Il Ctu e i Ctp potranno raccogliere dati e documentazione riferibili ai quesiti posti e relativi a circostanze coeve alle situazioni che hanno portato le parti in lite; molto spesso il Giudice dà anche facoltà al Ctu di sentire persone terze e di attingere a fonti estranee alle parti in causa, nel caso ciò possa essere di aiuto all'evasione dei quesiti.
Il Ctu convoca riunioni periodiche alle quali possono partecipare i legali e anche i rappresentanti delle parti in causa, senza che i legali e le parti in lite arrechino turbative al normale svolgimento della consulenza tecnica.
La sede nella quale si svolge la consulenza tecnica ha la stessa valenza di un'aula di Tribunale, anche nel caso fosse in realtà l'ufficio di una delle due aziende in lite, perché il Ctu rappresenta il Giudice ovunque si svolgano le attività della Ctu.
Il Ctu deve garantire il contraddittorio fra i Ctp e verbalizzare le loro opinioni, rimandando all'elaborato finale ogni sua considerazione.
In occasione delle riunioni di consulenza tecnica si esaminano i documenti raccolti, se ne verifica l'attendibilità e la pertinenza e si procede alla verifica tecnica delle ipotesi del Ctu e dei Ctp sugli oggetti del contendere, sempre con l'obiettivo di rispondere ai quesiti del Giudice.
I documenti discussi, verificati, convalidati, rifiutati, accettati sono sottoscritti dal Ctu e dai Ctp e essi faranno parte degli allegati all'elaborato finale.
Eventuali archivi digitali sono riprodotti su copie identiche di cd rom, sottoscritte e rese disponibili al Ctu e ai Ctp.
Al termine di ogni riunione si redige un verbale, sottoscritto, che sarà poi allegato all'elaborato finale del Ctu.
Avendo trovato esaurienti risposte a tutti i quesiti posti, oppure constatata l'impossibilità di completare il compito assegnato, il Ctu dichiara chiusa la consulenza tecnica, predisponendosi alla redazione dell'elaborato finale.
Altre volte, prepara una bozza che invia ai Ctp, attendendo da essi commenti in risposta, che possono servire per comporre l'elaborato finale.

Le conclusioni finali

L'elaborato finale deve essere chiaro, circostanziato, documentato, di facile lettura e non eccessivamente tecnologico.
Il Ctu, infatti, deve sempre ricordarsi che il Giudice non è un informatico,
Il Ctu deve essere in grado di spiegare con semplicità gli aspetti tecnici, apportatori di conseguenze benefiche o dannose che siano pertinenti e collegati ai quesiti posti.
Il testo finale si articola in diverse parti: la prima pagina con riferimento agli estremi di causa, poi l'indice dell'intero elaborato, seguito dall'oggetto della consulenza tecnica di ufficio con riportati i quesiti posti dal Giudice.
Poi si indica la cronistoria dello svolgimento delle operazioni peritali con i riferimenti ai verbali delle riunioni effettuate e le considerazioni del Ctu in relazione ai quesiti posti con il dettaglio delle conclusioni raggiunte.
Sono inoltre indicati gli eventuali commenti alle relazioni presentate dai Ctp e le conclusioni contenenti le risposte sintetiche del Ctu ai quesiti posti dal Giudice.

Infine, è la volta di tutti gli allegati dei verbali delle riunioni effettuate e dei documenti raccolti da Ctu e Ctp, sia in forma cartacea sia in forma digitale.
Le conclusioni del Ctu sono, di norma, accolte e condivise dal Giudice che ha comunque la facoltà di dissentire motivando per iscritto il suo diverso parere.
All'elaborato finale viene allegata una proposta di parcella, con indicazione delle spese sostenute e degli onorari richiesti.
Il Giudice la valuterà per poi liquidarla mettendola a carico delle parti in solido (formula più frequente) oppure solo di una parte.
La parcella, a questo punto, assume la caratteristica di titolo di credito esecutivo.
Purtroppo i guadagni sono modesti, poiché normalmente non superano la metà di quelli di un'equivalente attività svolta nel privato.

Come si diventa Consulente tecnico del Giudice

Diventare Ctu (Consulente tecnico d'ufficio del Giudice) può essere un obiettivo professionale gratificante, che il responsabile dei sistemi informativi potrebbe perseguire per utilizzare, valorizzandola, l'esperienza acquisita in azienda.
La professionalità maturata sugli aspetti prettamente tecnologici deve però essere completata con le conoscenze di tipo legale indispensabili per svolgere adeguatamente i compiti richiesti a un Ctu.
Un amico avvocato oppure la conoscenza di un Ctu saranno utili per apprendere come muoversi fra le aule di udienza e le cancellerie, come comportarsi con i Ctp (Consulenti tecnici di parte), le parti in lite, i legali e il Giudice, come redarre l'elaborato finale e come calcolare i compensi da proporre al Giudice per la liquidazione.
Un aspetto molto delicato è riferibile agli atteggiamenti e ai comportamenti che il Ctu deve intrattenere con i Ctp garantendo imparzialità e facilitando, al tempo stesso, il contraddittorio fra le diverse posizioni e valutazioni tecniche dei Ctp fra di loro avversi.
Il Ctu è, praticamente, la mente tecnica del Giudice e deve agire tecnicamente con giustizia.
Deve sempre ricordare che anche il più piccolo errore di atteggiamento o comportamento potrebbe poi essere preso a pretesto da un legale di parte per chiedere al Giudice la censura di tutto il suo operato, vanificando la consistenza e la validità degli accertamenti tecnici effettuati.

La fase preparatoria

Sono disponibili alcuni testi di tipo pratico di ausilio a chi voglia intraprendere la professione di perito estimatore e di Ctu/Ctp.
Le case editrici di riferimento sono quelle che hanno collane di pubblicazioni in area giuridica, come avviene per Giuffrè Editore, Etas, Il Sole 24 Ore.
Nei loro libri si trovano i riferimenti alla legislazione in vigore, i formulari di uso più frequente, i casi tipo, le modalità di intervento, risposte ai quesiti principali, tabelle per il calcolo dei compensi e quant'altro sia utile all'esercizio della professione di Ctu nei diversi settori tecnici di specializzazione.
Esistono anche associazioni che offrono formazione e addestramento ai futuri periti

estimatori e Ctu, furbescamente proponendosi come certificatori.
Meglio evitare questi tranelli.
Sono solo due le commissioni che valutano e certificano: quella della Camera di Commercio e quella del Tribunale competente.
Dal punto di vista tecnico, un Ctu di contenzioso nell'Ict potrebbe essere nominato dal Giudice per intervenire in problemi di software applicativo, funzionamento di siti Web, software di sistema, reti di computer, sistemi di trasmissione dati, malfunzionamenti di hardware, violazione della privacy dei dati, truffe in Rete e altri reati informatici.
È improbabile trovare in una persona competenze adeguate per far fronte ad accertamenti tecnici in tutti i settori indicati.
Diventa allora importante che il futuro Ctu sappia dove cercare e, soprattutto, cosa cercare di utile alla consulenza tecnica di ufficio: la ricerca su Internet è una fonte inesauribile di conoscenza.
Gli stessi Ctp possono essere utilizzati dal Ctu, sempre nel rispetto del contraddittorio fra le parti, per acquisire quelle conoscenze tecniche di dettaglio che il Ctu potrebbe non possedere.
Alle volte il Giudice autorizza il Ctu, su sua richiesta, a reperire notizie e conoscenze anche presso terzi.

La procedura da seguire

Si diventa Ctu seguendo una procedura molto simile in tutti i tribunali italiani.
La procedura in vigore presso il Tribunale di Milano (Ufficio Volontaria Giurisdizione e Consulenti Tecnici, presso il palazzo di Giustizia) prevede che possano essere iscritti nell'albo dei consulenti tecnici del Giudice chi sia in possesso della cittadinanza italiana o di uno stato UE mediante domanda al Presidente del Tribunale di Milano, nella cui circoscrizione l'aspirante risiede, contenente la dichiarazione di iscrizione all'albo professionale, l'indicazione della *categoria* e della o delle *specialità*.
La domanda deve essere compilata in carta libera ed essere corredata da marca da 14,62 euro, curriculum vitae firmato, fotocopia di documento di identità, documenti vari per dimostrare la capacità tecnica e l'esperienza professionale acquisita (titoli scolastici, attestazioni di terzi, perizie effettuate, pubblicazioni e così via) e versamento della somma di 168,00 euro sul c/c 8003 (intestato all'Agenzia delle Entrate, Centro Operativo di Pescara, tasse e concessioni governative).
Il certificato generale del casellario giudiziario sarà acquisito d'ufficio.
Per coloro che fanno parte di categorie che non sono organizzate in ordini o collegi professionali e quindi non sono provviste di albi professionali (come è il caso dell'Ict), è necessario allegare un certificato di iscrizione nell'Albo dei Periti e degli Esperti, tenuto dalla Camera di Commercio (per Milano è la categoria XXV Funzioni Varie sub Sistemi informativi per la gestione aziendale, via Meravigli 9/B) in carta bollata da 14,62 euro (o, in alternativa, la dichiarazione sostitutiva di certificazione ai sensi dell'articolo 46 DPR 445/2000).
All'indirizzo http://www.mi.camcom.it sono indicati i requisiti di carattere personale, morale e professionale, oltre alla documentazione da produrre.

L’iscrizione all’albo della Camera di Commercio è subordinata al parere favorevole di un’apposita commissione di valutazione.
Una volta iscritti all’albo della Camera di Commercio, è possibile presentare la domanda di iscrizione nell’albo dei consulenti tecnici di ufficio del Tribunale.
Anche in questo caso, però, l’iscrizione è subordinata al parere favorevole di un’altra commissione di valutazione interna al Tribunale, che si riunisce circa due volte all’anno.
Ottenuta l’iscrizione all’albo del Tribunale, è consigliabile compilare un proprio profilo professionale e farne delle fotocopie da consegnare alle cancellerie delle sezioni dove è probabile sorgano necessità di nominare un Ctu esperto in Ict, pregando i cancellieri di inoltrarle ai giudici: è un’attività di tipo promozionale che può dare buoni frutti.

La perizia tecnica preventiva: prevenire per non litigare

E' buon senso diffuso rivolgersi agli esperti prima di avventurarsi in imprese rischiose o dall'esito incerto.
Così prima di andare *sotto i ferri*, facciamo tutte le analisi cliniche del caso; prima di intraprendere un lungo viaggio, facciamo controllare l'auto, studiamo i percorsi, ci documentiamo sugli usi, costumi e malattie endemiche dei luoghi che visiteremo.
In molte altre circostanze, pensiamo prima di decidere e di agire.
In sintesi, sapendoci ignoranti, raccogliamo informazioni utili per evitare pericolosi salti nel vuoto.
Non in modo analogo avviene quando un cliente inesperto e sprovveduto decide di acquistare un programma o un sistema ICT.
Spesso la regola è andare allo sbaraglio: si decide fidandosi della pubblicità, della presunta esperienza informatica del figlio della segretaria, delle argomentazioni commerciali (e fumose) del venditore appena uscito dal corso di formazione alla vendita.
Altre volte il cliente non ha la struttura organizzativa e le potenzialità per installare e poi utilizzare il programma applicativo e le attrezzature che il venditore propone.
Nella mia esperienza di Ctu, ho dovuto esaminare, a distanza di anni progetti ICT che non dovevano neppure iniziare.
Tutte le informazioni per sconsigliarne lo sviluppo, erano disponibili prima ancora che il progetto partisse.
Dopo anni di danni reclamati e non ammessi, di scambio di raccomandate, di ingiunzioni ad adempiere, di memorie di avvocati, di udienze, di testimonianze contestate, finalmente il Ctu nominato dal Giudice evidenzia che il progetto era viziato fin dall'origine, perché destinato a sicuro insuccesso e, nell'interesse di entrambe le parti, non doveva iniziare.

Come ci si dovrebbe comportare?

Prendere coscienza che i prodotti e le applicazioni ICT sono come le medicine che dovrebbero essere assunte solo dietro prescrizione medica.

Un'applicazione ICT idonea e perfetta per un cliente, potrebbe essere inadeguata, costosa e pericolosa per un altro.
Come per l'assunzione di medicine inadeguate, si scoprono i danni quando è trascorso troppo tempo e si è passati, senza giudizio, da medicina a medicina (e da applicazione ICT ad applicazione ICT), aggiungendo ulteriori problemi a quelli già presenti.
Con utili e salutari diffidenze ben stampate nella mente, cliente e fornitore dovrebbero accordarsi nel definire gli obiettivi del progetto e nel dettagliare le risorse ICT che si intendono destinare al progetto comune.
Dovrebbero nominare un perito, esperto in materia, che al di sopra delle parti, possa esaminare la struttura organizzativa e le potenzialità del cliente e dall'altra parte le caratteristiche e le potenzialità delle risorse ICT proposte dal fornitore.
Il perito nominato dalle parti non deve avere alcuna possibilità di proporsi o di proporre altri fornitori in grado di fornire quelle soluzioni ICT che, a suo avviso, potrebbero meglio realizzare gli obiettivi del cliente.
Escludendo a priori al perito ogni possibilità di lucrare sulle carenze della soluzione proposta dal fornitore, sarebbe un'ulteriore garanzia dell'imparzialità del perito, imparzialità che dovrebbe essere data per scontata se il perito è iscritto all'albo dei periti estimatori del Tribunale.
E' una proposta semplice e facilmente percorribile; richiede solo la volontà delle parti di prevenire prima, invece di litigare poi.
Basta che cliente e fornitore, con scrittura privata, si accordino sulla scelta del perito imponendogli i doveri appena richiamati e comportandosi poi con lo stesso in modo conforme alle regole pattuite.
La soluzione non è nuova in assoluto, ma è nuova nel settore dell'ICT.
In realtà quanto suggerito è alle volte formalmente prescritto nelle forniture alla Pubblica Amministrazione e nei progetti ICT con finanziamento agevolato.

L'analisi forense

La Computer Forensics (Informatica e analisi forense) è la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico per essere valutato in un processo giuridico e studia, ai fini probatori, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici (Wikipedia).
L'Informatica e analisi forense può anche definirsi come *la disciplina che studia l'insieme delle attività rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova*.
Di solito l'analisi forense entra in gioco quando un computer è stato posto sotto sequestro dall'autorità giudiziaria per ipotesi di reato commessi con il suo uso oppure nella convinzione della possibilità che nei suoi archivi vi siano prove documentali utili alle indagini.
Nell'analisi forense sono di indubbio rilievo le componenti tecnologiche e professionali di conoscenza di computer, reti informatiche, sistemi di archiviazione, sistemi operativi, programmi applicativi, programmi di utilità, sistemi di duplicazione

non invasivi degli archivi e quant'altro necessario per scoprire i particolari più reconditi e nascosti in grado di avvalorare o smentire le ipotesi investigative.
Gli specialisti di analisi forense devono anche possedere le conoscenze giuridiche necessarie per garantire che l'acquisizione delle prove, la loro conservazione e la loro possibile ripetibilità siano attività svolte nel rispetto della legge e dei legittimi diritti delle parti (accusa e difesa).
I reati per i quali potrebbe essere necessario ricorrere ad un'analisi forense sono:

- accesso non autorizzato ad un sistema informatico
- uso per scopo personale delle attrezzature informatiche del datore di lavoro
- detenzione abusiva e diffusione di codici di accesso (*password*)
- diffusione di virus o di programmi atti a danneggiare un sistema informatico
- intercettazioni o blocchi di comunicazioni informatiche
- *de-compilazione* / apertura non autorizzata di programmi coperti da diritto di autore
- decriptazione di dati
- frode informatica
- distruzione di dati o accesso abusivo ai sistemi informatici
- alterazione di dati od uso improprio di programmi
- invio di posta *spazzatura*
- uso improprio della posta elettronica
- frodi alle assicurazioni
- concorrenza sleale
- diffusione e detenzione di immagini pedo-pornografiche
- Ingiurie, minacce, diffamazione
- violazioni del diritto di autore
- riciclaggio di denaro e reati tributari
- furto di identità e truffe
- violazione della *privacy*
- diffamazione di persone, di aziende, di marchi
- contraffazione di marchi e di siti web
- spionaggio industriale
- diffusione abusiva di documenti riservati

L'analisi forense ha fra gli obiettivi principali:

- acquisire le prove nel rispettto delle procedure e delle regole di ammissibilità senza alterare o modificare il sistema informatico su cui si trovano
- garantire che le prove acquisite sul supporto di copia siano identiche a quelle originarie
- analizzare i dati raccolti sul supporto di copia senza apportare modifiche o alterazioni
- identificare il supporto di copia ai fini della sua conservazione ed eventuali successivi riesami

Un'analisi forense è svolta seguendo un iter che prevede sei fasi:

- **identificazione**
- **acquisizione**

- **conservazione**
- **analisi**
- **valutazione**
- **presentazione**

Identificazione

L'analisi forense normalmente interviene su un computer (o sistema informatico) già sottosto a sequestro giudiziale.
E' compito del Giudice autorizzare l'analista forense di svolgere la perizia indicando i punti da esaminare e soprattutto i quesiti ai quali dare risposta.
L'analista forense, per prima cosa, deve verificare che il computer (o sistema informatico) si presenti nello stesso stato di quello documentato nel provvedimento di sequestro e che non vi siano segni di rimozione degli eventuali sigilli apposti in occasione del sequestro; nel caso di manomissione dei sigilli, l'analista forense ha il dovere di verbalizzare la circostanza, sigillare nuovamente il computer ed informare il Giudice che deciderà come procedere.
Nella prima fase di **identificazione** l'analista forense cercherà di isolare i computer, i supporti di memorizzazione, i documenti e quant'altro a priori potrebbe contenere elementi utili per la formazione delle prove.
L'ambiente dovrà essere isolato per evitare che persone non autorizzate possano inquinare le prove in acquisizione.
E' opportuno descrivere accuratamente l'ambiente realizzando fotografie e filmati da produrre unitamente alla futura documentazione della perizia.
E' utile ricercare fra i documenti eventuali annotazioni di password utili per semplificare l'accesso al computer e alla rete, nel caso ciò sia indispensabile.
Per il computer è necessario identificare il disco fisso (*hard disk*) indicandone:

- la marca
- il modello
- i dati tecnici
- il numero di serie (*serial number*)
- versione del *firmware*
- la configurazione (cilindri, testine, settori, tracce, ecc.)

Analoghe annotazioni devono essere effettuate per tutti gli altri supporti di memorizzazione dei dati (dischi esterni, *tape backup*, chiavette usb, cd e dvd, *memory / sim card*, ecc.)

Acquisizione

La fase di **acquisizione** ha l'obiettivo di raccogliere prove che siano:

- legalmente ammissibili
- direttamente riferibili all'oggetto dell'analisi
- ripetibili nel tempo
- attribuibili a persone e/o a circostanze
- dettagliate e non generiche
- convincenti anche per persone non esperte di informatica (Giudici ed

avvocati)
Le prove sono *legalmente ammissibili* se sono raccolte nel rispetto delle formalità richieste dalla legge (autorizzazione del Giudice inquirente, presenza del perito di parte, verbalizzazioni, depositi in cancelleria entro i termini stabiliti, ecc.)
Le prove devono essere *direttamente riferibili all'oggetto dell'analisi*; eventuali considerazioni del tutto estranee all'oggetto della perizia potrebbero renderla totalmente nulla.
Le prove acquisite sono *ripetibili nel tempo* se a distanza di anni posso, partendo dal computer sequestrato, ottenere delle nuove prove del tutto identiche a quelle già depositate; da ciò deriva che unitamente alle prove l'analista forense deve depositare anche i programmi che sono serviti per ottenere le *copie conformi*.
Quando l'analisi riguarda ipotesi di reato, le prove dovrebbero avere la caratteristica di essere *attribuibili a persone e/o a circostanze* raccogliendo dati sugli utenti del computer, password usate, date e ore di creazione / modifica / lettura degli archivi, *log* (cronistoria) di sistema e di navigazione in internet.
Bastano due esempi per dimostrare quanto spesso sia molto difficile attribuire ad una persona un reato informatico:
1) se trovo in un computer di uso individuale delle immagini penalmente rilevanti e se in tale computer non sono installati adeguati programmi atti ad impedire intrusioni dall'esterno, il computer potrebbe essere diventato un involontario automa al servizio del pirata informatico che si è mascherato usando l'identità del computer in analisi
2) se dall'analisi dei *log* (cronistoria) di sistema o di navigazione in internet trovo che per certo periodo di tempo l'utente ha usato il suo computer individuale, non è detto che la stessa persona non sia stata in altri luoghi a commettere reati: infatti si possono programmare degli *script* che in automatico aprono, leggono e scrivono archivi o navigano in internet.
Le prove devono essere *dettagliate e non generiche* con il grado di dettaglio richiesto dalla natura dei quesiti e dalla complessità del caso in esame.
E' preferibile che il perito dichiari che la prova non può essere fornita, indicandone i motivi, evitando di produrre inutili prove generiche.
Le prove devono essere *convincenti anche per persone non esperte di informatica*, evitando il ricorso alla sola terminologia informatica; i termini tecnici, se non esprimibili in italiano, devono essere spiegati usando paragoni, esemplificazioni e descrizioni articolate.
La fase di acquisizione è sicuramente la più importante dal punto di vista informatico, perché la raccolta dei dati deve avvenire assolutamente senza modificare gli archivi presenti sul computer o sui computer della rete.
Nella fase di acquisizione occorre perseguire l'obiettivo della preservazione definibile come quell'*insieme di procedure tecniche e procedurali volte a garantire la non alterazione della prova, quale insieme di dati digitali*.
A tale scopo si usano dei programmi specifici, quasi tutti in ambiente Linux, che sono in grado di *montare* e di accedere ai dischi da analizzare in modalità di *sola lettura*, garantendo così la conservazione dell'integrità dei dischi in esame.
Per acquisire dei dati da un computer occorre effettuare una *copia bit per bit* (copia fotografica) dell’intero supporto digitale, verificando l’integrità della copia con

funzioni di *hash* per generare un codice alfanumerico lungo molti caratteri.
Una funzione di *hash* è una funzione *one way* (mono direzionale) che, dato un testo di partenza di lunghezza arbitraria, fornisce un codice *hash* di lunghezza fissa; una piccola variazione nel testo di partenza si traduce in una grande variazione del codice *hash* risultante .
Il codice *hash* di un archivio (o di un intero disco) è diverso da quello di qualsiasi altro archivio che non sia completamente identico a quello di partenza: i due archivi possono essere uguali nella dimensione e anche nei caratteri contenuti ma se i caratteri sono messi in una diversa disposizione in uno dei due archivi, i codici *hash* saranno diversi.
L'ottenimento di due codici *hash* uguali è la prova che la copia è identica all'originale di partenza.
Per eccesso di scrupolo, si potrebbe ricalcolare il codice *hash* dell'archivio (o disco) originale verificando, per la perdurante uguaglianza del codice *hash*, che l'originale non ha subito alcuna modifica durante l'operazione di copia.
In aggiunta ai programmi specifici per l'acquisizione delle copie conformi dei supporti digitali si deve fare uso di procedure per:

- la documentazione degli spostamenti subiti dalla prova (*tracciabilità*)
- la duplicazione della copia conforme da trasmettere alla parte inquisita
- la redazione dei verbali (verbali di sequestro, di consegna, di affidamento, di deposito presso l'*Ufficio prove di reato*)
- la preparazione della documentazione relativa alla *catena di custodia*
- le registrazioni delle attività svolte sulla prova

Conservazione

Nella fase di **conservazione** l'analista forense garantisce la corretta gestione degli elementi di prova acquisiti, il loro trasporto, deposito e archiviazione per evitare che gli stessi siano modificati mettendo in discussione la loro integrità.
E' importante garantire la tracciabilità degli spostamenti delle prove (sequestro, acquisizione, estrazione e analisi dei dati, successivi riesami) e di tutte le attività svolte sulla prova.
Risulta utile ricorrere a strumenti di firma digitale, di *codici hash*, di crittografia anche abbinati alla redazione di verbali, fotografie e filmati che documentino la vita e la custodia delle prove acquisite.
La documentazione contenuta nella *catena di custodia* deve permettere di garantire che non si siano prodotte alterazioni ai dati acquisiti dal momento dell'inizio dell'analisi forense al momento del dibattimento in aula e per tutte le altre fasi dell'iter processuale.
In particolare per ogni prova acquisita si deve indicare nella *catena di custodia*:

- i dati identificativi della prova (data, ora, numero di protocollo, analista, ecc.)
- l'archivio di memorizzazione, la dimensione, il luogo di custodia, il *codice hash*, ecc.
- le persone che hanno avuto accesso alla prova (data ed autorizzazione)
- le operazioni effettuate sulla prova (tipo, persona, data, verifica del *codice hash*, ecc.)

Persone non autorizzate non devono avere accesso alle prove acquisite, perché non solo bisogna proteggere l'integrità della prova ma anche evitare che mancando idonei sistemi di custodia, la validità delle prove acquisite siano contestate in sede di dibattimento processuale.
Occorre documentare ogni attività con verbali esaurienti e dettagliati indicando le evidenze scoperte, gli strumenti informatici utilizzati (quale programma, con riferimento alla versione), le procedure usate con riferimenti alle motivazioni per il loro uso e del tempo impiegato.
La *catena di custodia* deve documentare che l'integrità dei dati è stata preservata e non c'è stata alcuna modifica delle prove acquisite.
L'autenticità delle prove può essere dimostrata facendo riferimento e utilizzando programmi di utilità specifici per l'analisi forense ritenuti oggettivamente idonei a raccogliere le prove senza modificare o in qualche modo turbare i contenuti del computer.
Esistono programmi applicativi per l'analisi forense sia di tipo commerciale (Encase, Helix, FTK, X-Way Forensic, ecc.) sia di tipo *open source* e gratuiti (Caine, BackTrack, Deftv, Snarl, ecc.); per alcuni di quelli *open source* sono presentate delle immagini nelle pagine che seguono.
Poiché è importante che le procedure usate siano ripetibili da parte di terze parti anche a distanza dei molti anni di durata dei processi, è opportuno fare copia dei programmi utilizzati per l'acquisizione delle prove.

Analisi

La fase di **analisi** deve essere svolta tenendo conto dei quesiti del Giudice esaminando ad esempio, se necessario:

- archivi di sistema
- archivi di registro e di cronologia (*log*)
- archivi dell'utente, documenti di ufficio, posta elettronica, testi, immagini, audio, video, ecc..
- archivi protetti da password
- *metadati* inclusi negli archivi multimediali (ultimo accesso, ultima modifica, software, copyright, fotocamera, valori di esposizione, ecc.)
- cronologia delle navigazioni in Internet
- elenco (e spesso anche il contenuto) degli archivi stampati con indicazione della stampante usata
- elenco degli archivi che sono stati creati, modificati, cancellati da un certo utente
- spazio non allocato dei dischi
- spazio destinato alla cache di navigazione e agli archivi temporanei
- archivi cancellati e partizioni nascoste
- archivi criptati (testi che possono diventare leggibili utilizzando un cifrario di decodifica)
- presenza di virus, di *trojan* e di altri programmi (*script*) malevoli
- presenza di programmi (*script*) di attivazione di una rete di computer (*botnet*) collegati ad Internet facenti parte di un insieme di computer controllato da un'unica entità, il *botmaster*; circostanza che può essere causata da falle

nella sicurezza o nella mancanza di attenzione da parte dell'utente e dell'amministratore di sistema, per cui i computer vengono infettati da virus informatici o *trojan* i quali consentono ai loro creatori di controllare il sistema da remoto. I controllori della *botnet* possono in questo modo sfruttare i sistemi compromessi per scagliare attacchi distribuiti del tipo *negazione del servizio* (*denial of service DDoS*) contro qualsiasi altro sistema in rete oppure compiere altre operazioni illecite; i computer che compongono la *botnet* sono chiamati *bot* (da roBOT) o zombie

- archivi steganografati (messaggi nascosti nei testi con l'uso di chiavi); steganografia è una parola di origine greca che significa *scrittura nascosta*; è una tecnica che consente di nascondere dei messaggi testuali all'interno di un file immagine; la steganografia utilizza l'algoritmo *LSB* (*Least Significant Bit*), che cerca i bit dei colori meno significativi e li sostituisce con i dati da nascondere (ad esempio un archivio di testo) cercando di non modificare visibilmente l'immagine originale; l'algoritmo LSB richiede un contenitore (l'immagine), un dato da nascondere (ad esempio un archivio di testo) ed una password per cifrare il messaggio

Valutazione

Nella fase di **valutazione** dei dati della prova è necessario creare delle relazioni tra gli stessi, al fine di ricostruire eventi compatibili nel tempo e mutuamente probatori .
E' opportuno elencare gli elementi della prova in una tabella cronologica (*Timeline Activity Table*) tenendo conto della data e dell'ora di creazione / modifica / accesso riferibili agli archivi contenenti informazioni significative per l'analisi forense.
Nella fase di valutazione è opportuno che l'analista forense confronti i dati raccolti con i quesiti del Giudice o con gli obiettivi dell'incarico per:

- scartare i dati e le informazioni non pertinenti
- rivedere i dati raccolti in fase di analisi per arricchire la prova di altri elementi probatori
- se necessario chiedere al Giudice un ampliamento del campo di analisi

Presentazione

La relazione di **presentazione** dei risultati deve essere redatta in forma comprensibile , perché i destinatari (giudici e avvocati) non hanno di solito conoscenze informatiche approfondite; di contro le loro conoscenze legali potrebbero consentir loro di sostenere la nullità, per vizio di forma, della relazione finale dell'analisi forense.
Infatti la relazione dell'analista forense è di solito esaminata dal tecnico e dal legale della controparte; essi possono opporsi alle conclusioni dell'analisi forense sia dal punto di vista tecnico sia dal punto di vista legale.
In genere la presentazione dovrebbe essere:

- semplice
- chiara
- completa
- professionale

- documentata
- condivisibile, perché completa, professionale e documentata

Programmi e sistemi per l'analisi forense

In generale i programmi per l'analisi forense hanno le seguenti caratteristiche:

- copie *fotografiche* dei dischi / partizioni a basso livello (copia *bit per bit*)
- ricerche veloci sull'intero disco (non solo all'interno degli archivi attivi ma anche sulla superficie non ancora utilizzata)
- ricerche per stringhe, recupero degli archivi incompleti, cronologie delle attività (*timeline*)
- accesso a diverse strutture di archivi (*file system*)
- *carving* per risalire al nome dell'archivio partendo dal numero di settore
- scelta di modi diversi di presentazione dei risultati delle prove raccolte
- analisi dei dati secondo varie modalità di codifica (per esempio ASCII ed esadecimale),
- recupero automatico di eventuali archivi solo *logicamente* cancellati,
- generazione di *codici hash* per il controllo di integrità
- *editor* di archivi di testo
- *editor* di immagini
- analisi dei registri di Windows
- analisi dei *metadati* degli archivi multimediali
- programmi di crittografia
- programmi di compressione e decompressione dei dati
- programmi di steganografia
- analisi del traffico di rete / Internet

Nelle pagine che seguono sono riprodotte le schermate di quattro programmi gratuiti utili per l'analisi forense: DEFT, BackTrack, CAINE, Clonezilla.

DEFT – funzionalità

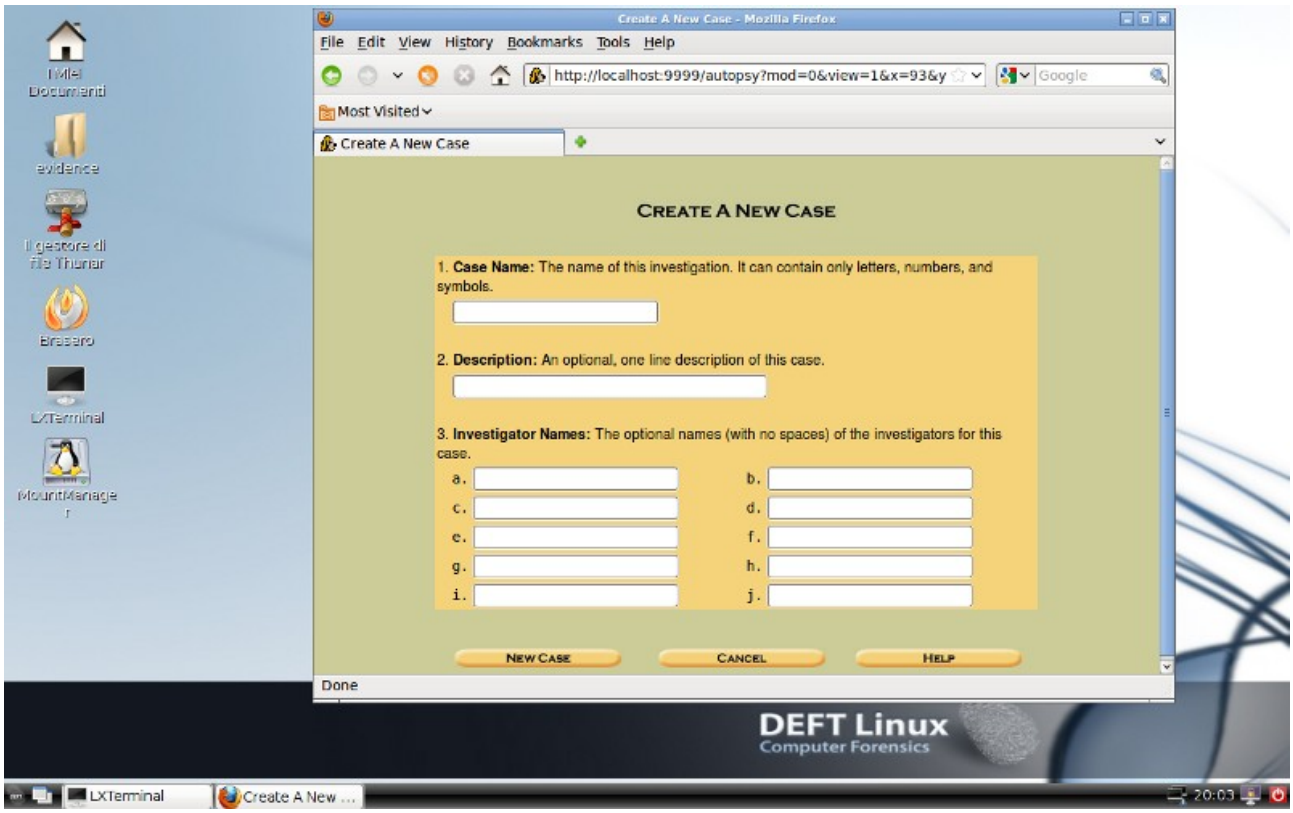
DEFT è una distribuzione italiana basata su Xubuntu (Linux), utilizzabile per:

- acquisire le immagini di dischi e partizioni
- acquisire anche le memorie che danno errori di lettura del supporto
- calcolare i *codici hash*
- ricercare i contenuti negli archivi
- recuperare gli archivi cancellati ricercando *header* e *footer* (testata e piede degli archivi)
- gestire le attività di analisi e di pre-analisi
- recuperare i dati (testi, immagini, musica, ecc.)
- gestire le intercettazioni telematiche
- scoprire le password
- individuare i programmi malevoli e intrusivi (*malware* e *rootkit*)
- autopsy - archiviazione di casi per l'investigazione con funzioni di ricerca e di documentazione cronologica
- acquisire il traffico telematico su rete IP
- Xplico - analisi del traffico telematico

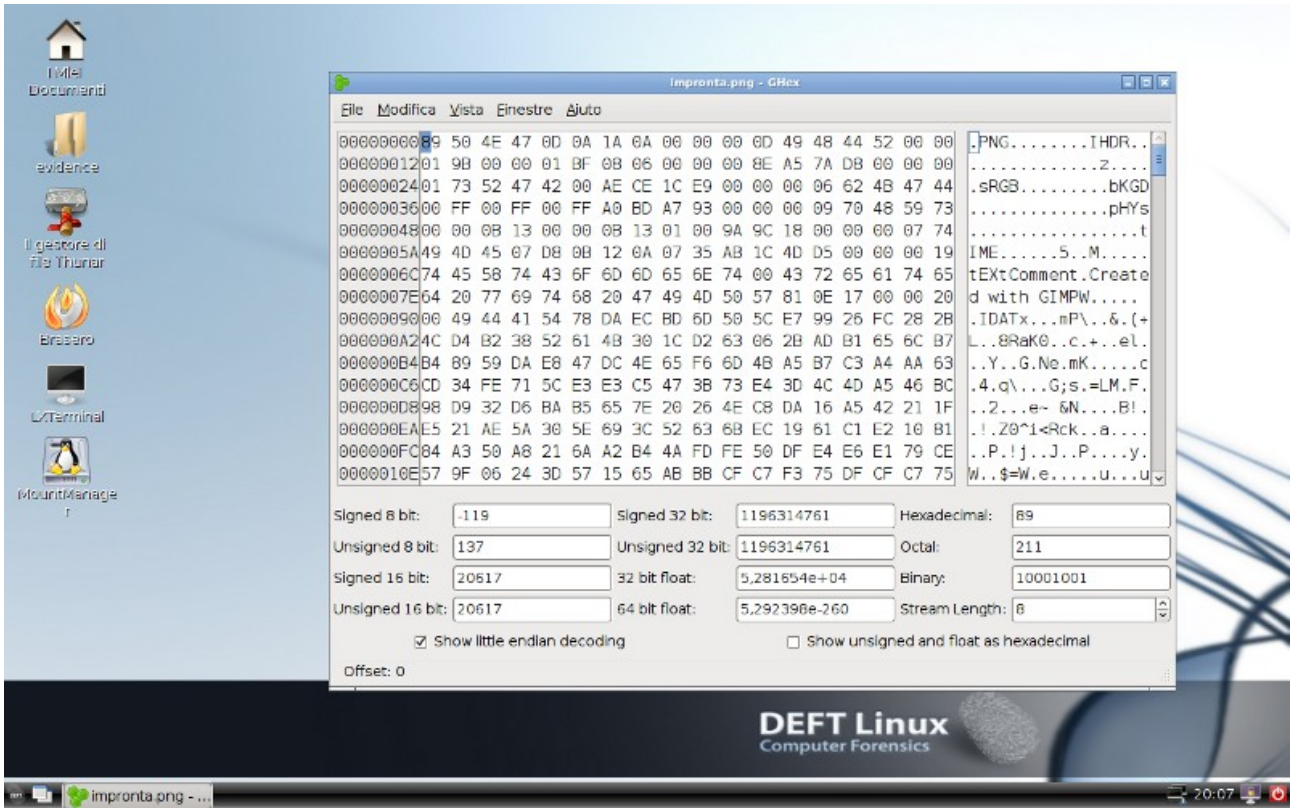
Di seguito sono riportate alcune immagini delle schermate di DEFT, programma gratuito.

DEFT – home page

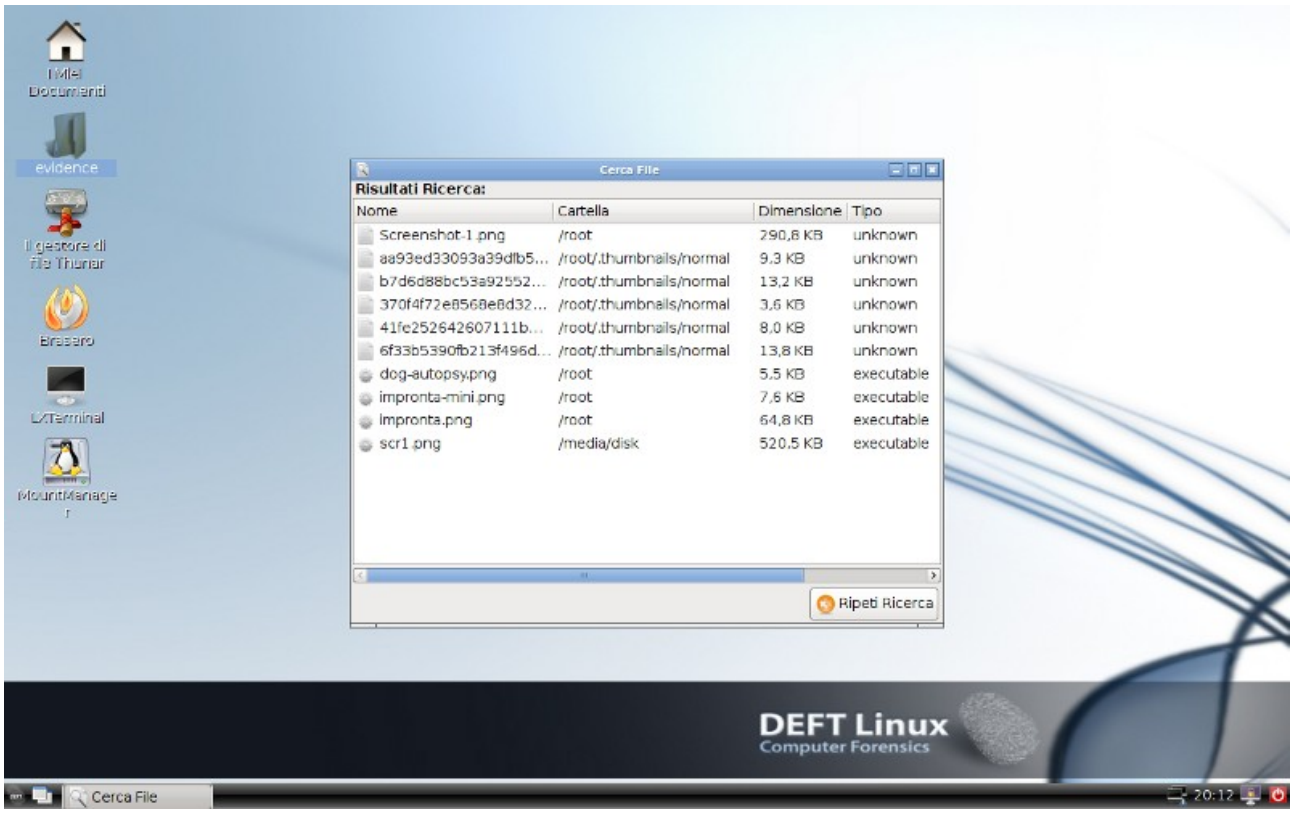
DEFT – creare un nuovo caso



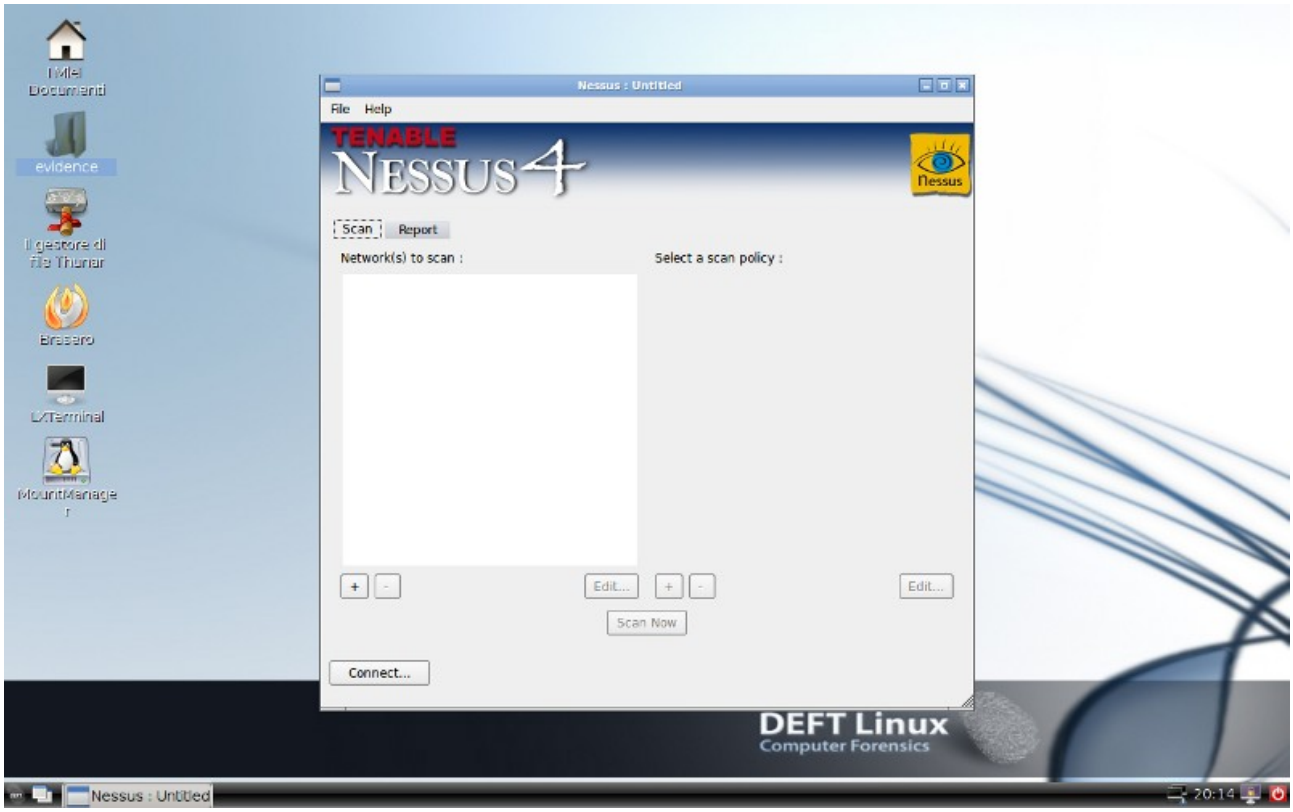
DEFT – esaminare dettagliatamente un archivio



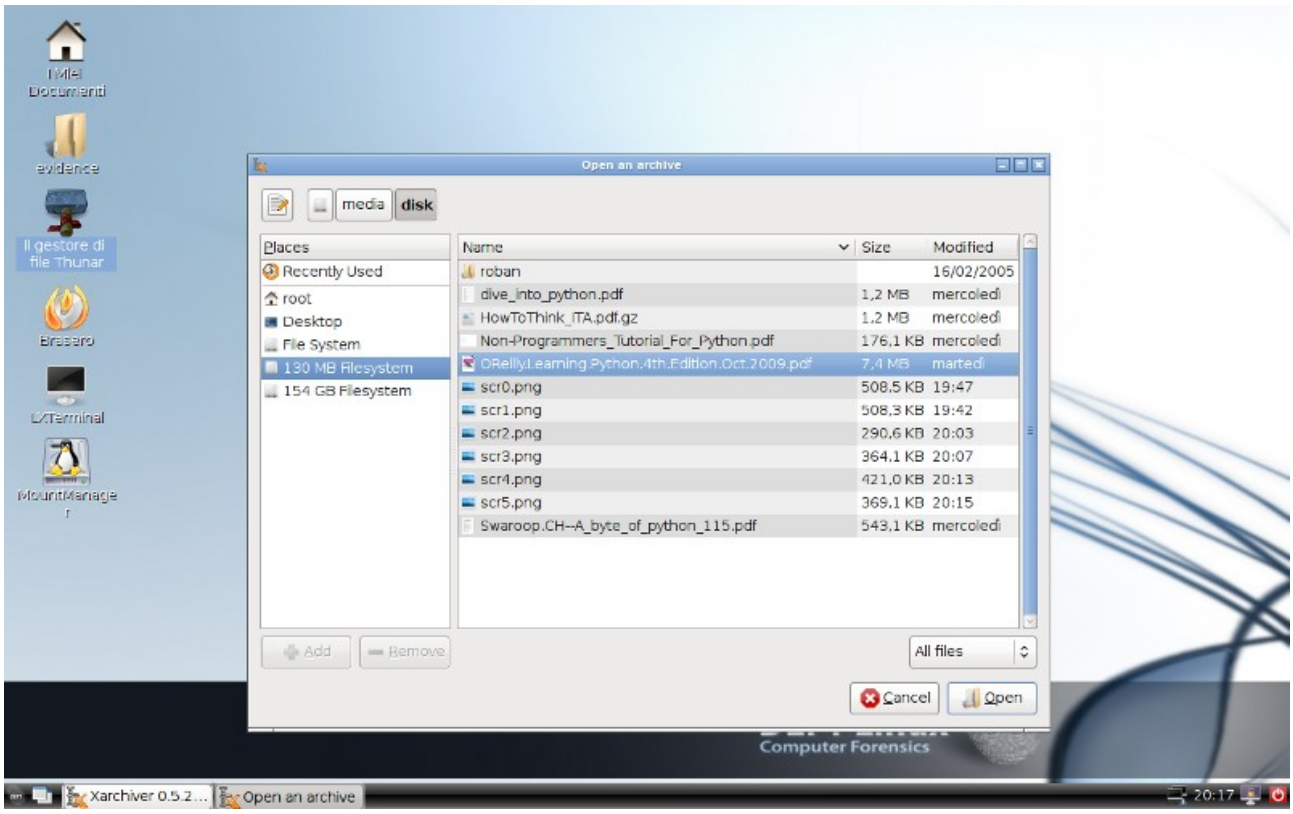
DEFT – ricerca di archivi



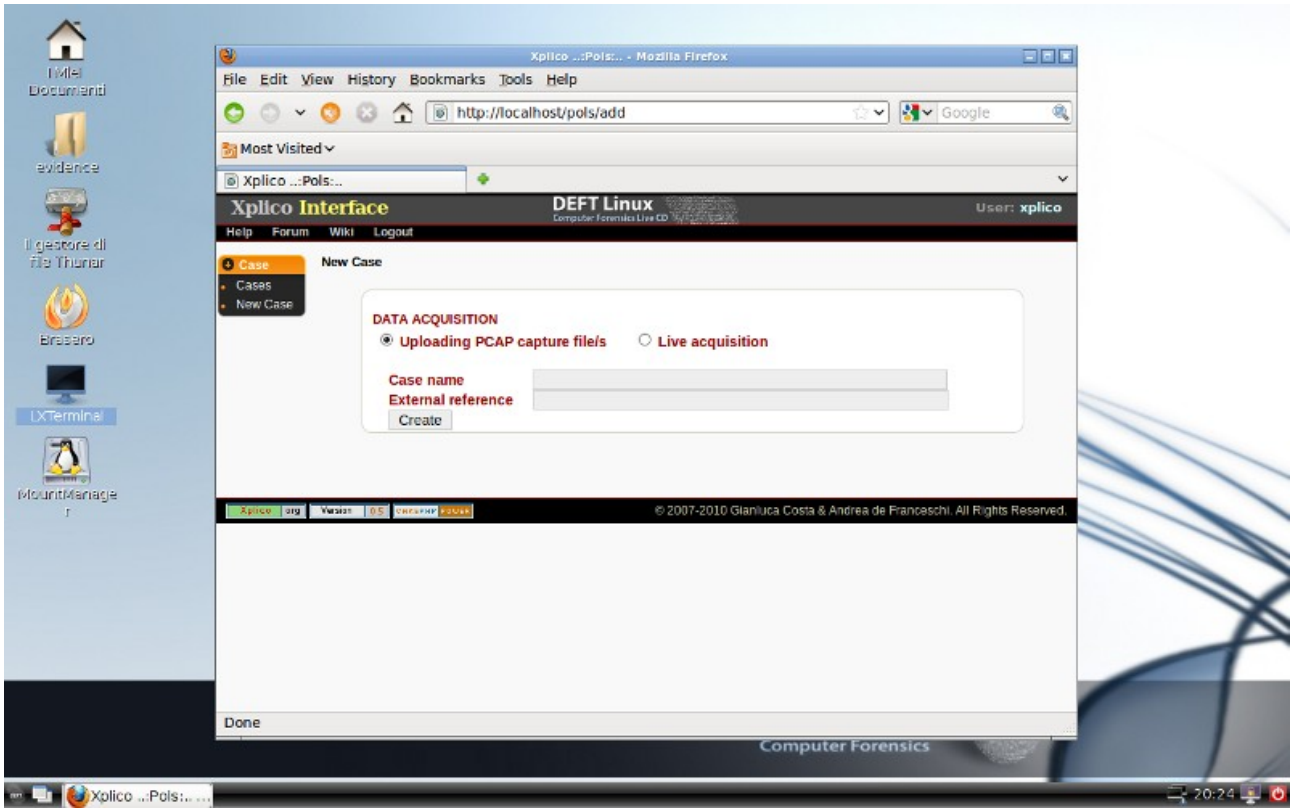
DEFT – esame del traffico di rete



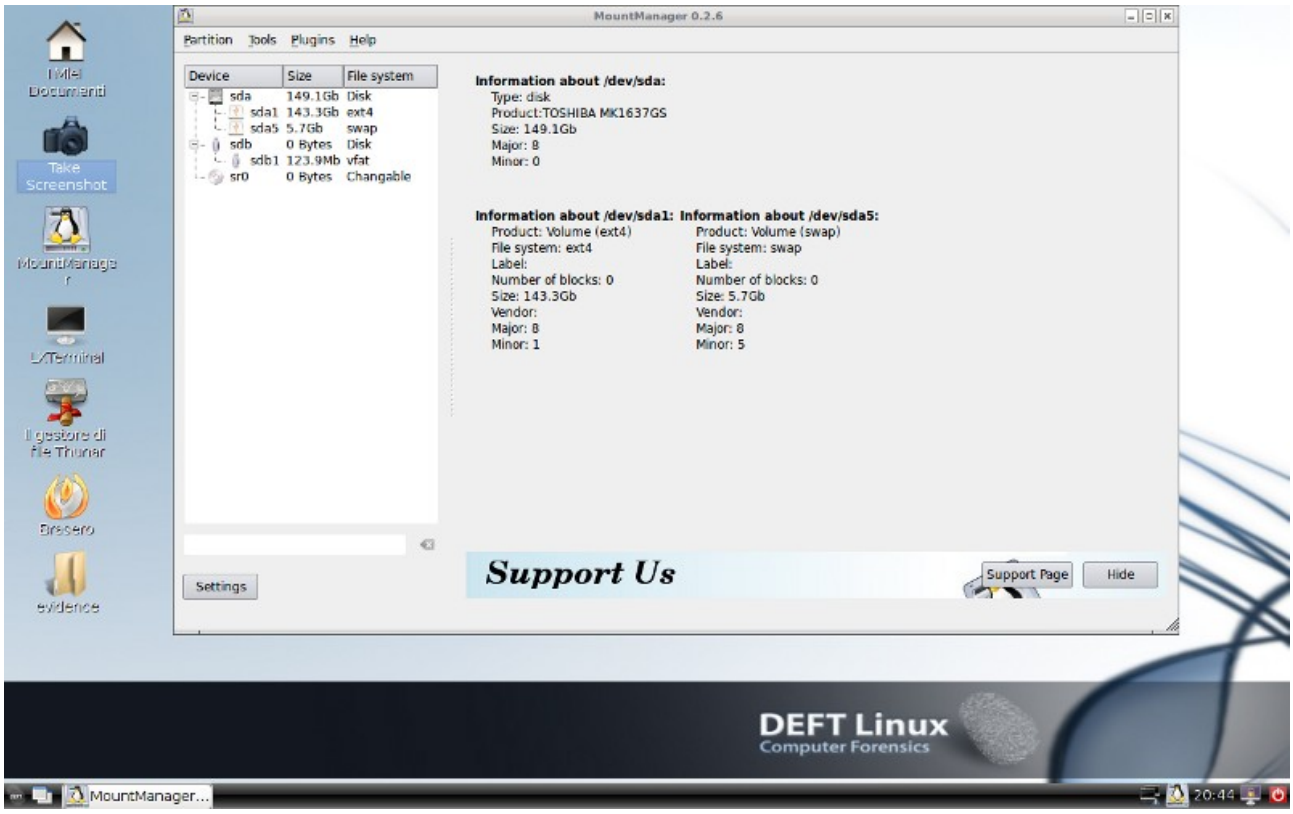
DEFT – date di modifiche sui dischi / archivi



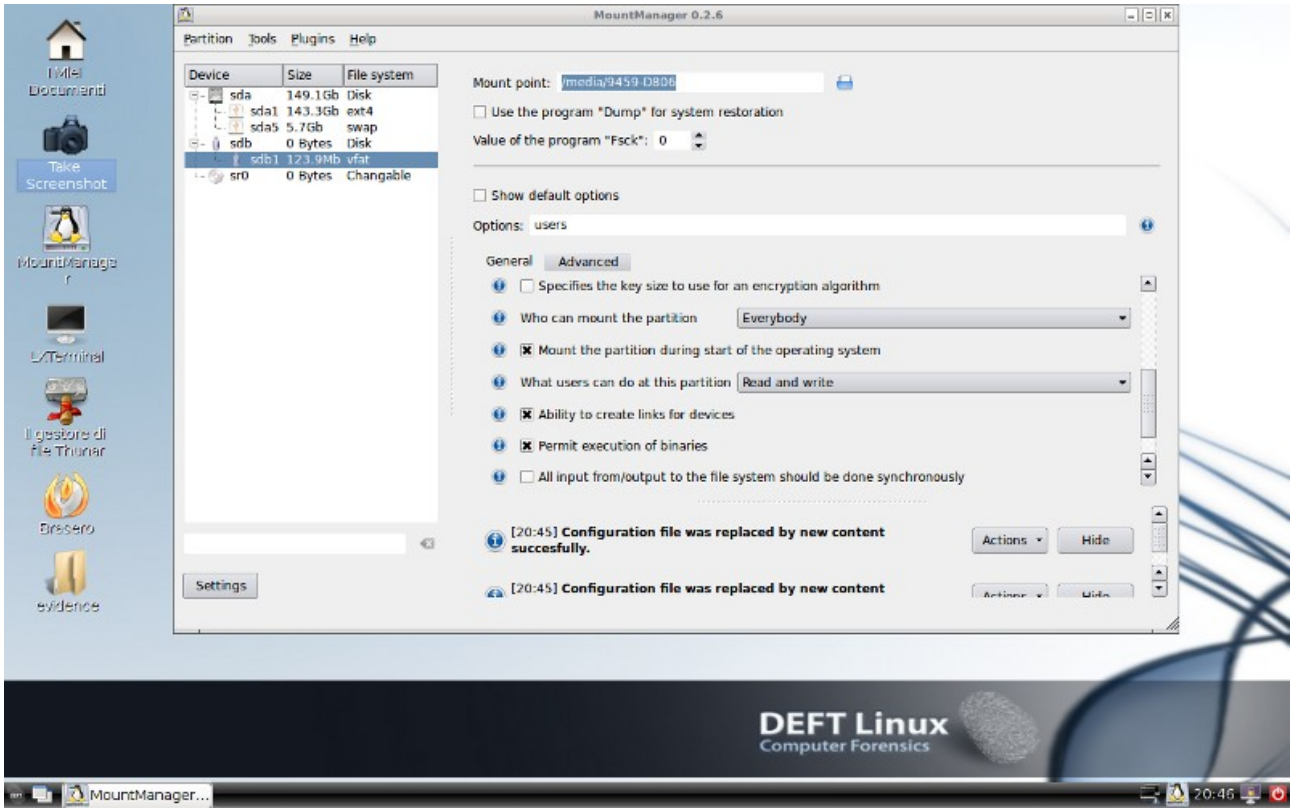
DEFT – programma Xplico



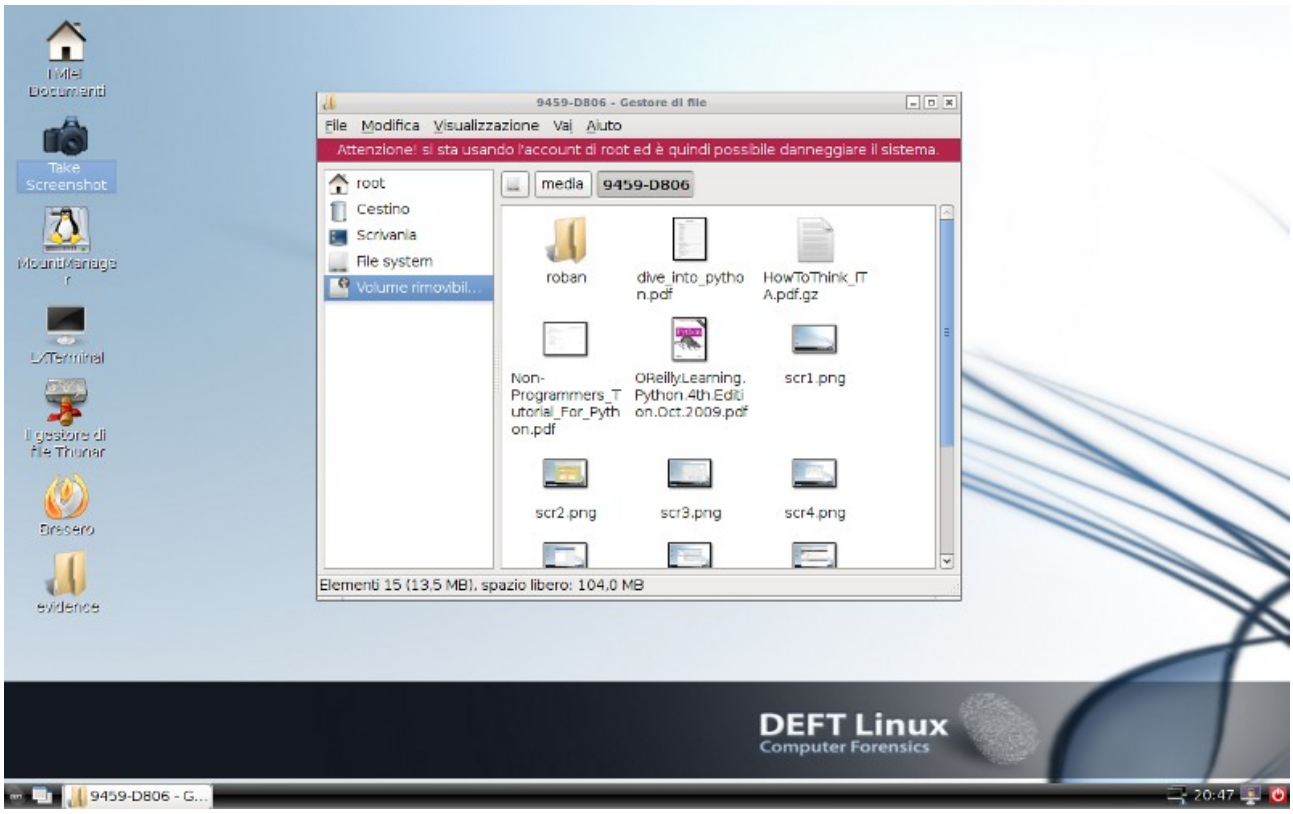
DEFT – informazioni sulle partizioni e sui dischi



DEFT – privilegi su partizioni e dischi



DEFT – gestione degli archivi



BackTrack – funzionalità

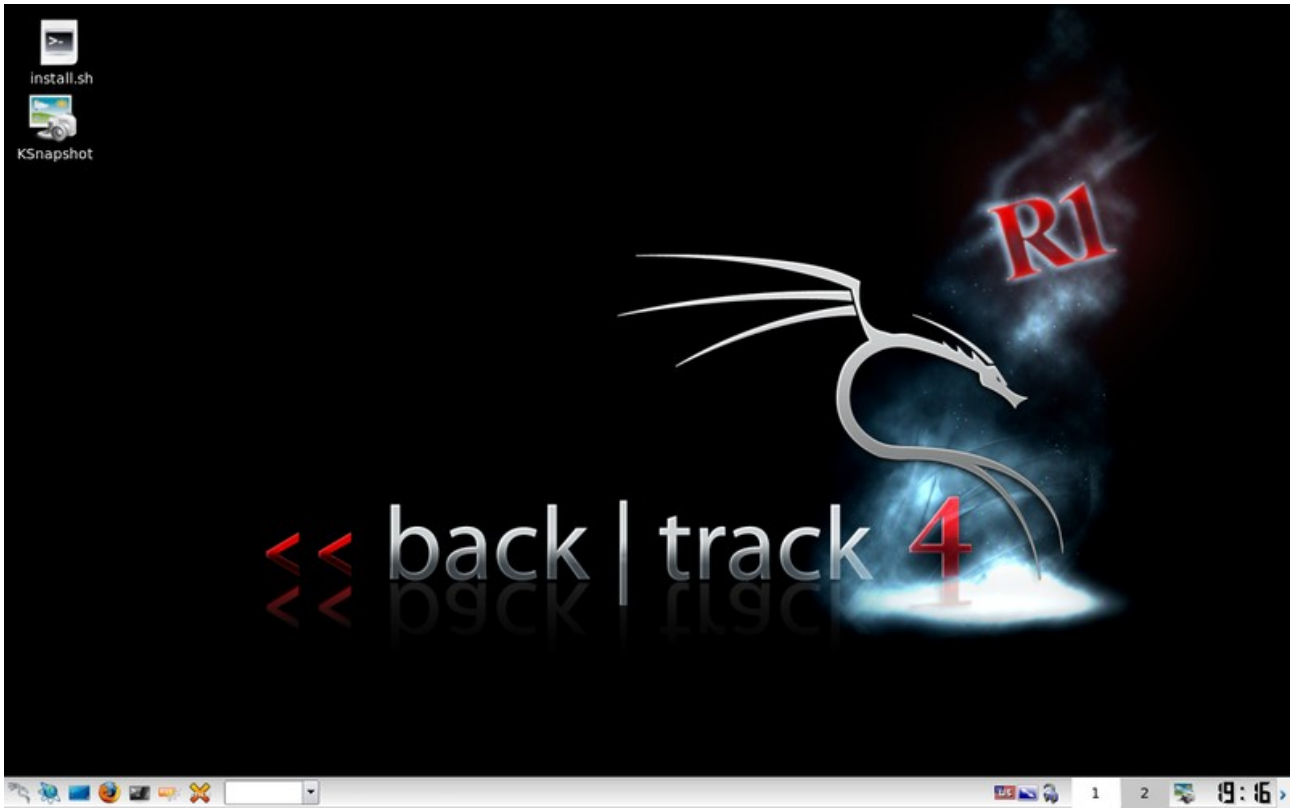
BackTrack rende disponibili più di 300 programmi / funzioni suddivisi in gruppi:

- Backtrack
  - Information Gathering
  - Network Mapping
  - Vulnerability Identification
  - Web Application Analysis
  - Radio Network Analysis
  - Penetration
  - Privilege Escalation
  - Maintaining Access
  - Digital Forensics
  - Reverse Engineering
  - Voice Over IP
  - Miscellaneous
- Internet
  - Ettercap
  - gFTP
  - Kopete - Instant Messenger
  - Liferea Feed Reader
  - Paterva Maltego CE
  - tpcat
  - Wicd Network Manager
  - Wireshark - Network Analyzer
  - Sun Java 6 Web Start
  - Konqueror - Web Browser
  - Lynx Web Browser
  - XChat IRC
  - Firefox Web Browser
- Services
  - BEEF
  - GPSD
  - HTTPD
  - Mysql
  - NETWORK
  - PCSCD
  - SNORT
  - SSH
  - TFTPD
  - VNC
- Wine
  - Programs

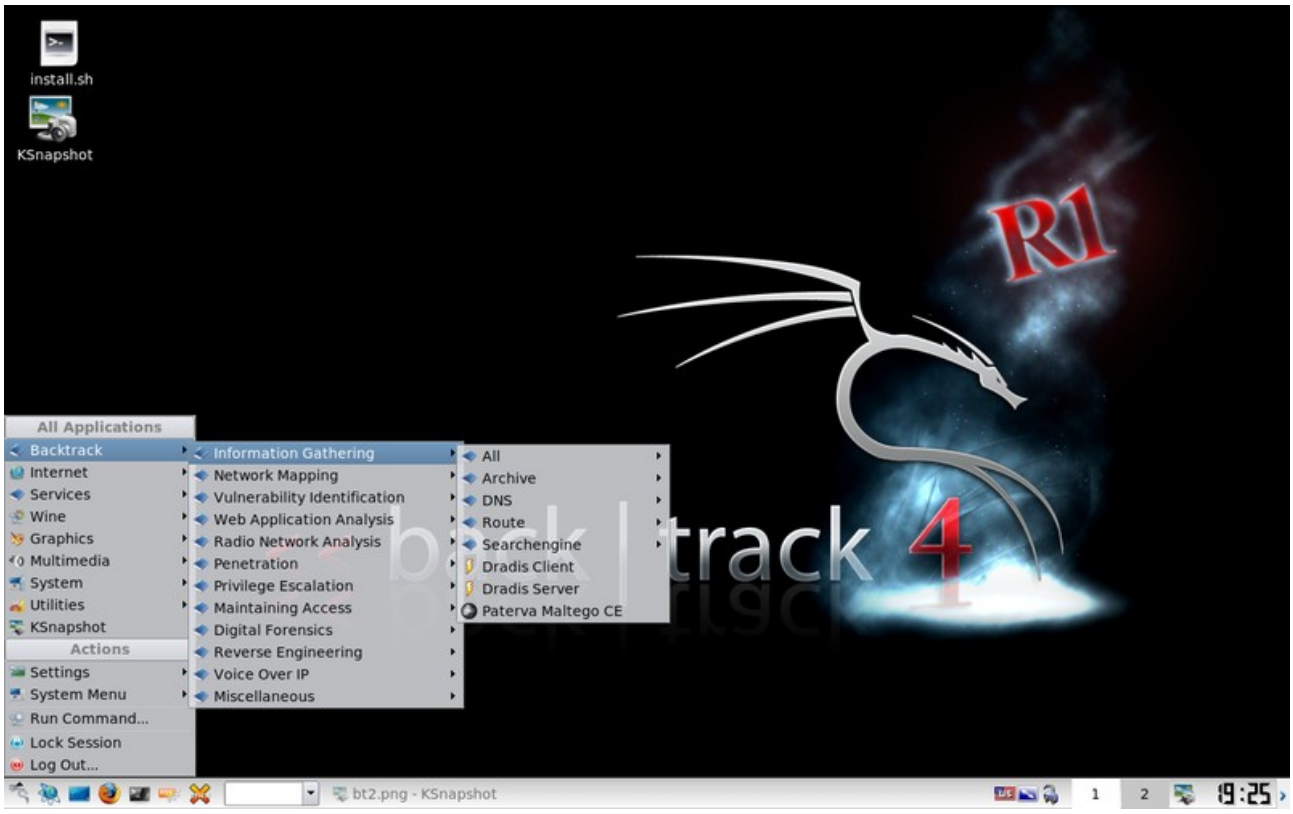
    - Browse C:\Drive
    - Configure Wine
    - Uninstall Wine Software
- System
    - Setting
    - Add/Remove Package Manager
    - Ettercap
    - Gentoo
    - kpowersafe - Battery Monitor
    - Partition Editor
    - Services
    - Shared Folders
    - Time and Date
    - Users and Groups
    - Yakuake
    - Software Sources
    - KinfoCenter - Info Center
    - KSysGuard - Performance Monitor
    - Konsole - Terminal Program
- Utilities
    - Ark - Archiving Tool
    - Emacs 21.4a (X11)
    - Gscriptor
    - KGpg - Encryption Tool
    - KjobViewer _ Print jobs
    - KRegExpEditor - Regular Expression Editor
    - kTip - Useful Tips
    - Terminator
    - Kate - Advanced Text Editor
- Settings
    - Control Center
    - Appearance & Themes
    - Desktop
    - Internet & Network
    - KDE Components
    - Peripherals
    - Regional & Accessibility
    - Security & Privacy
    - Sound & Multimedia
    - System Administration
- Altri programmi / funzioni

Di seguito sono riportate alcune immagini delle schermate di BackTrack, programma gratuito.

BackTrack – home page

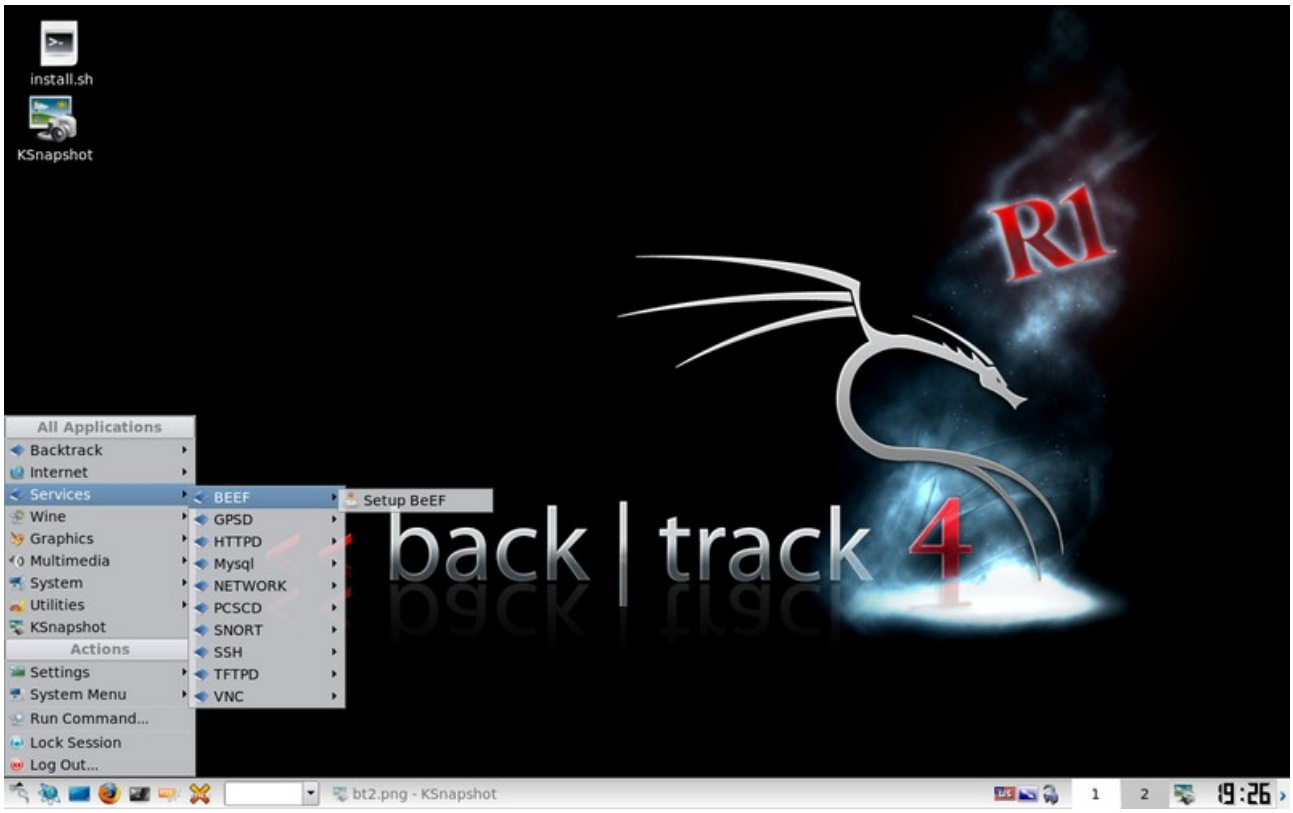


BackTrack – menu di BackTrack



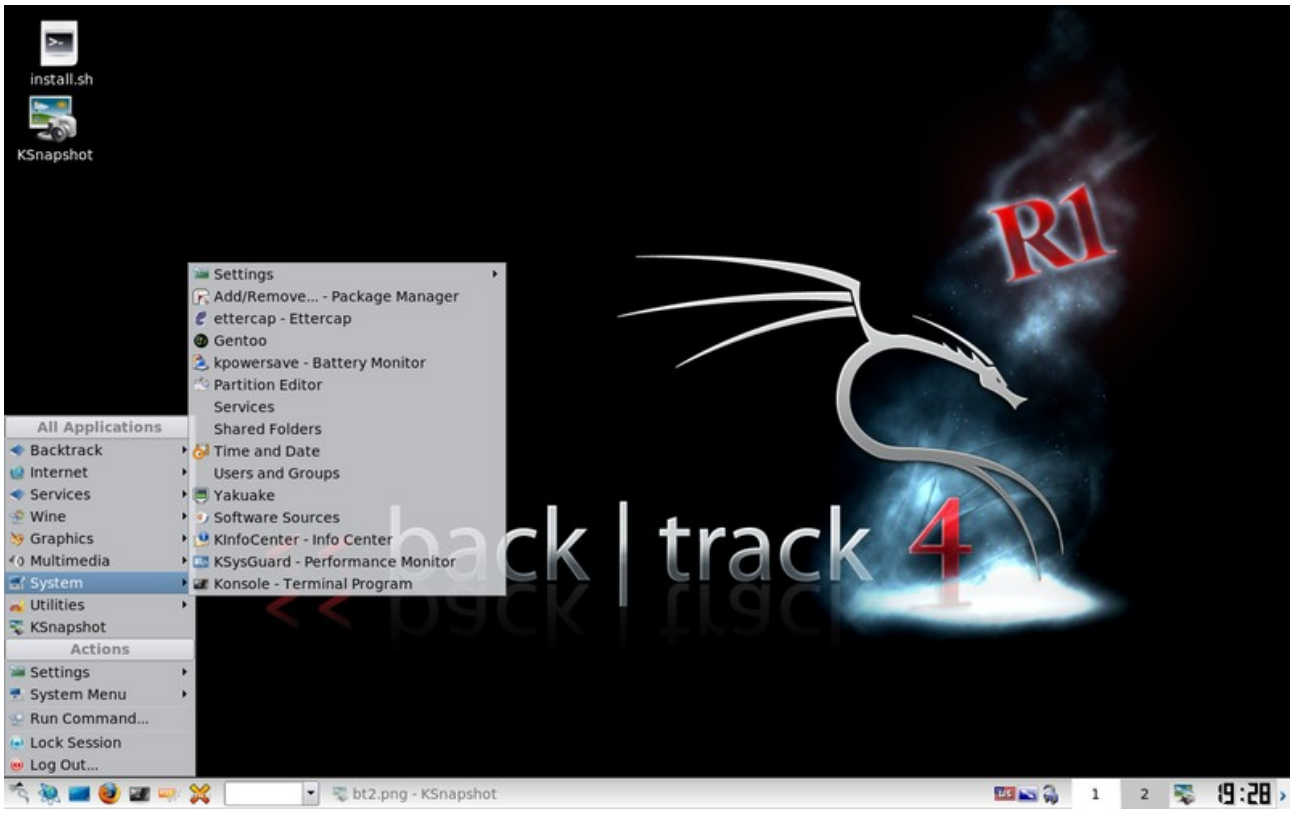
BackTrack – menu Internet

BackTrack – menu dei servizi



BackTrack – menu di wine

BackTrack – menu dei sistemi



BackTrack – menu delle utilità

BackTrack – menu della configurazione

CAINE – funzionalità

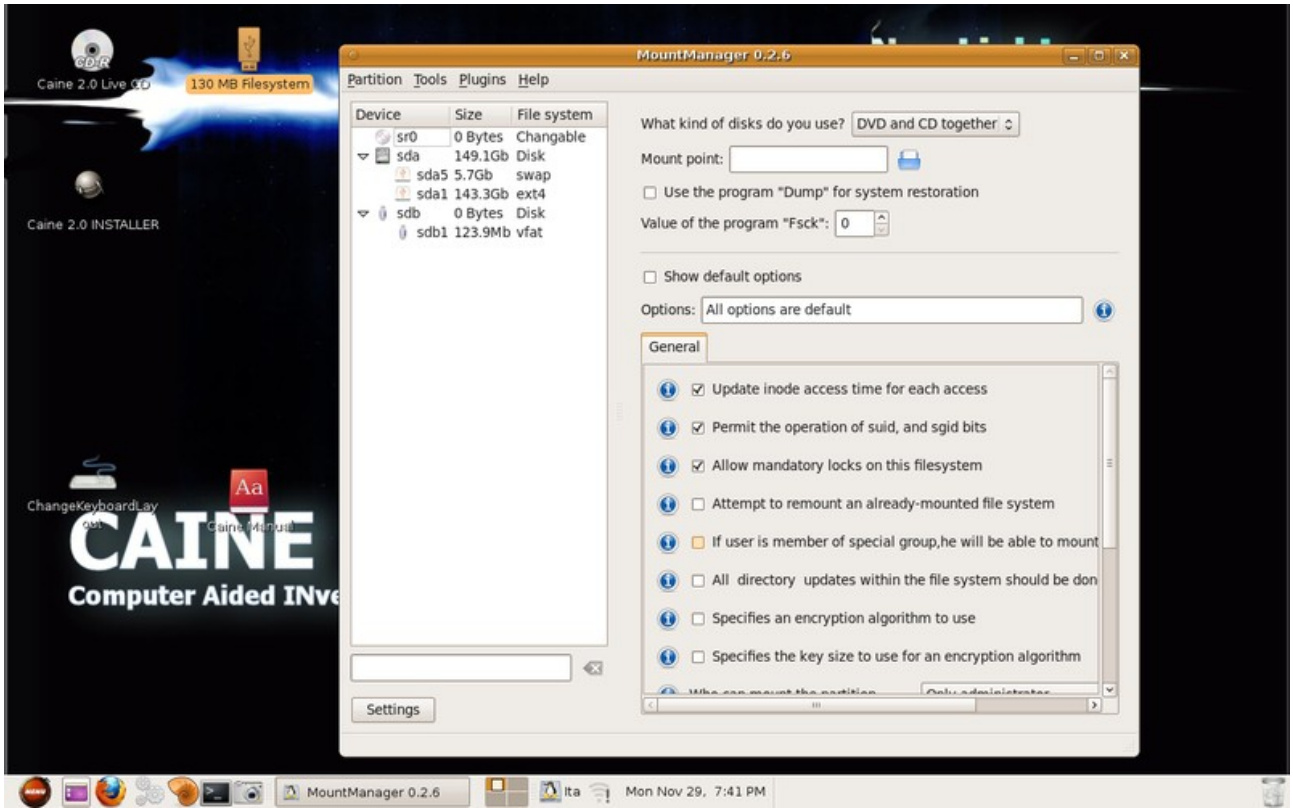
I programmi di utilità più importanti inclusi in CAINE sono:

- AIR (*Automated Image Restore*): programma sofisticato per la copia non invasiva di immagini di dischi e di partizioni e per l'eventuale successivo ripristino su altri supporti di memoria
- Autopsy: programma per eseguire analisi sugli archivi ed eventualmente recuperare quelli cancellati
- Exif: un programma che permette di estrarre i *metadati* EXIF dalle fotografie digitali
- Guymager: programma per la copia di immagini fedeli dei supporti digitali meno complesso rispetto ad AIR
- DvdDisaster: programma per il recupero di dati da supporti ottici danneggiati
- Wipe: programma per cancellare, con sovrascritture ripetute, gli archivi in modo che non siano più recuperabili
- Fundl: programma per il recupero rapido dei dati cancellati
- Ophcrack: violazione (*cracking)* delle password di Windows utilizzando le *rainbow tables*
- Stegbreak: estrazione dei dati nascosti in file JPG mediante steganografia
- GtkHash: calcolo del *codice hash* di un archivio mediante diversi algoritmi di calcolo
- Pasco: programma per l'analisi avanzata della *cache* (archivio temporaneo) di Internet Explorer
- Photorec: programma per il recupero degli archivi cancellati utilizzando tecniche di *data carving* ricercando *header e footer* (testata e piede degli archivi)

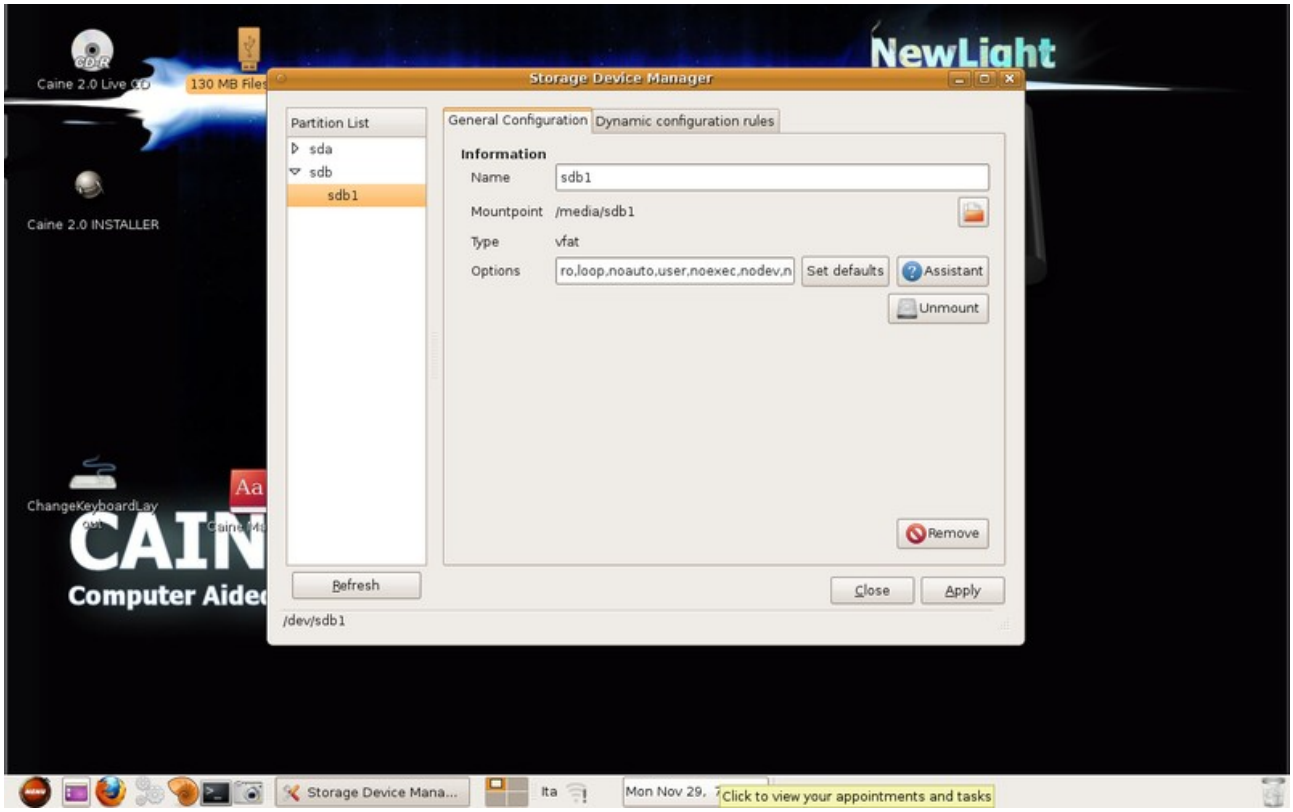
Di seguito sono riportate alcune immagini delle schermate di CAINE, programma gratuito.

CAINE – home page

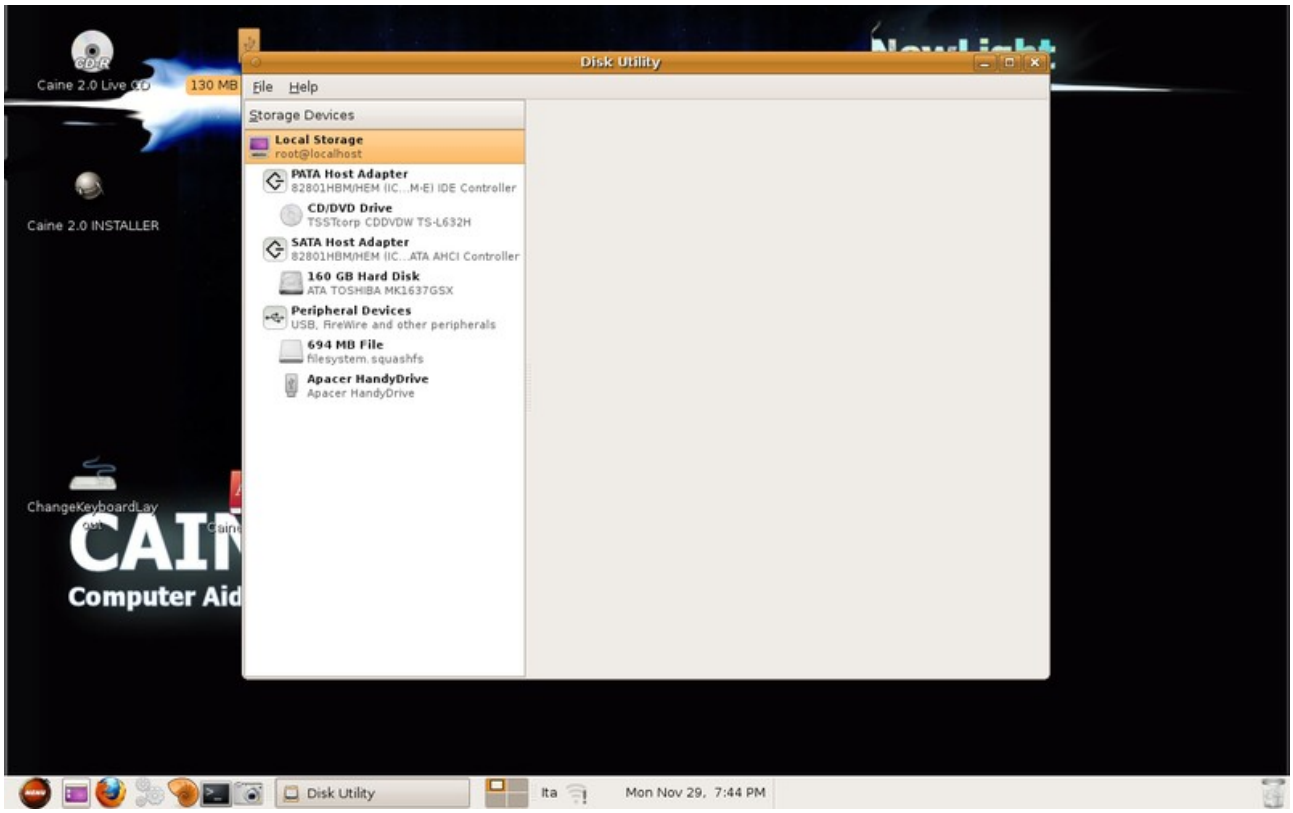
CAINE – mount manager



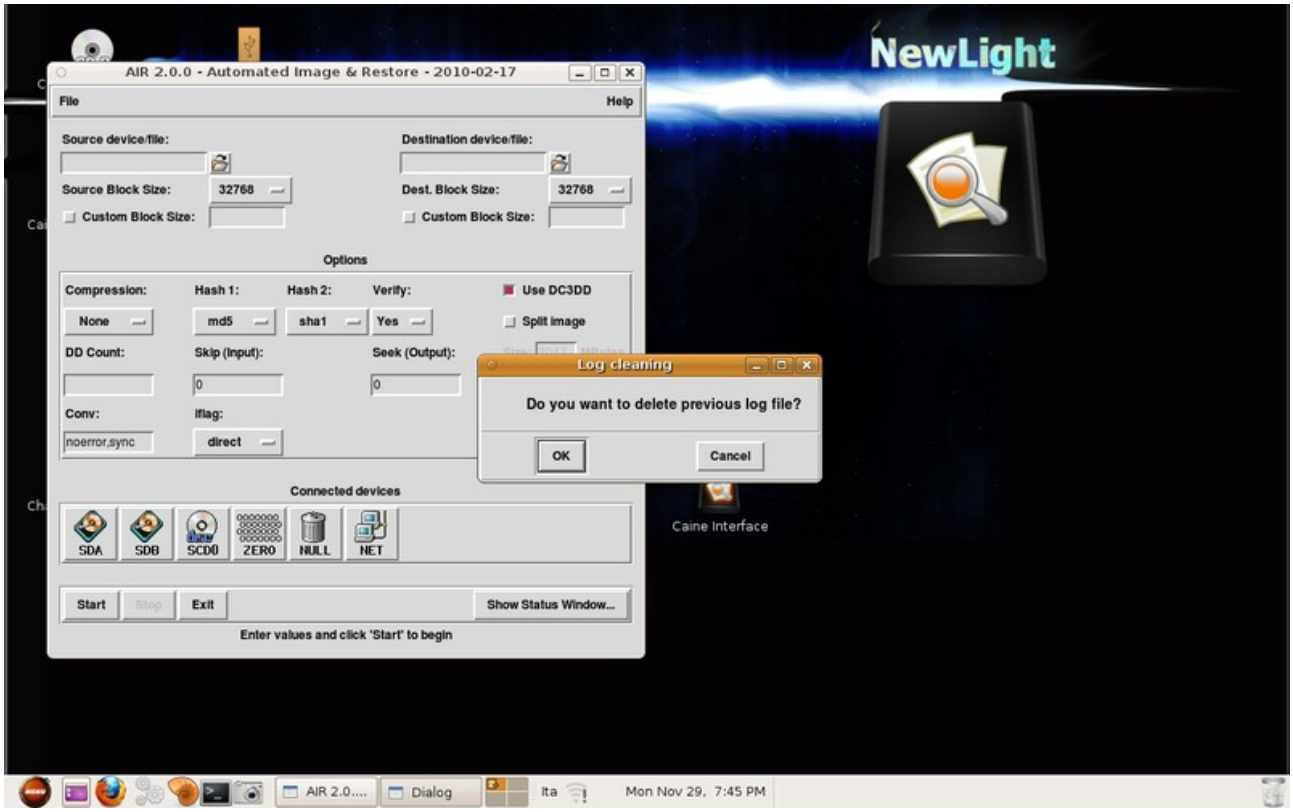
CAINE – gestore dei dischi



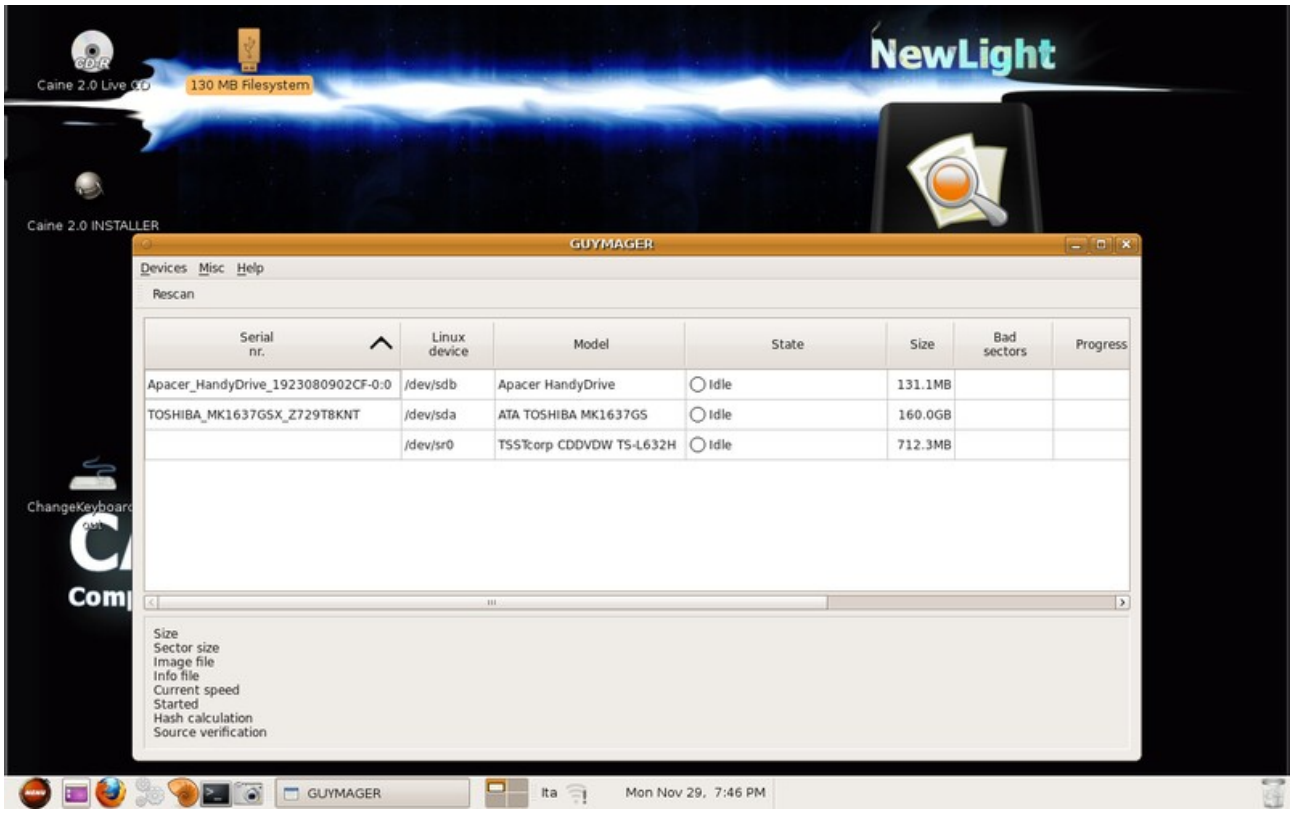
CAINE – utilità dei dischi



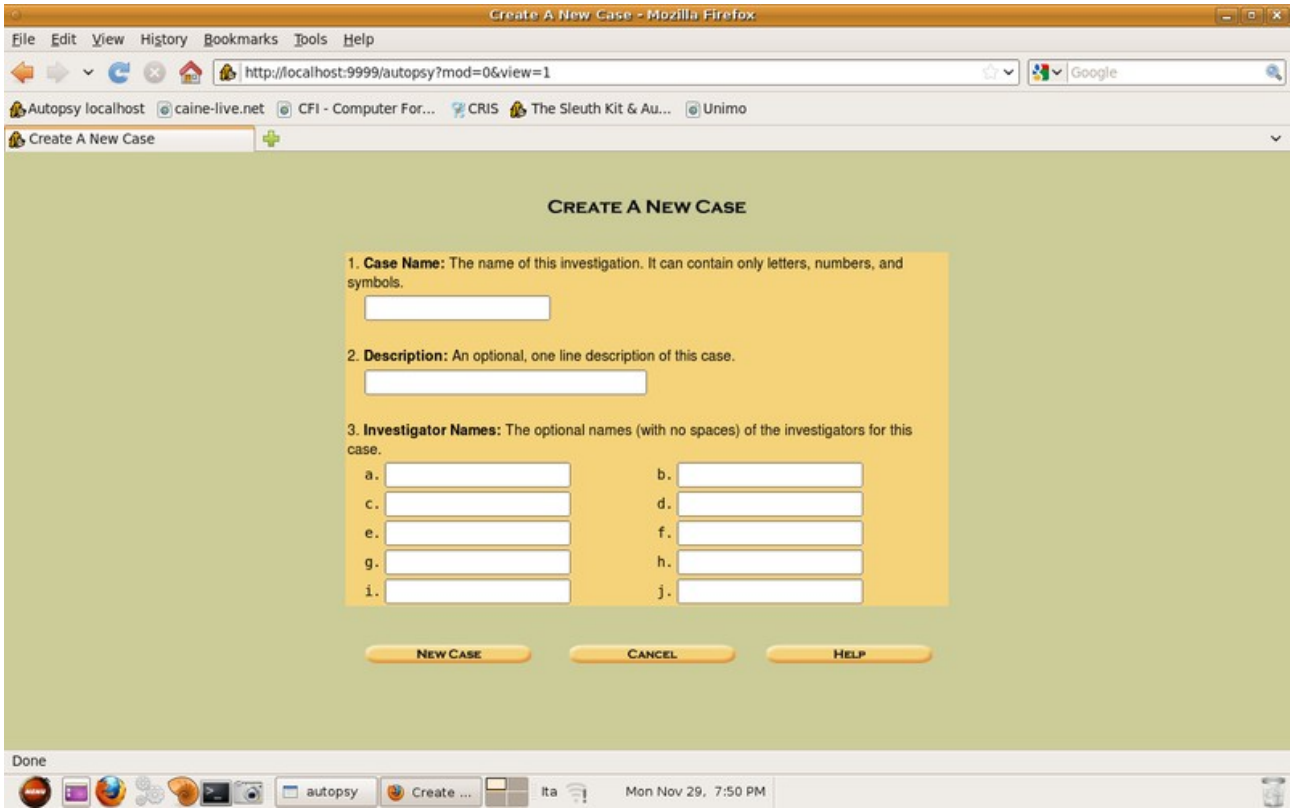
CAINE – AIR: copia automatica e ripristino



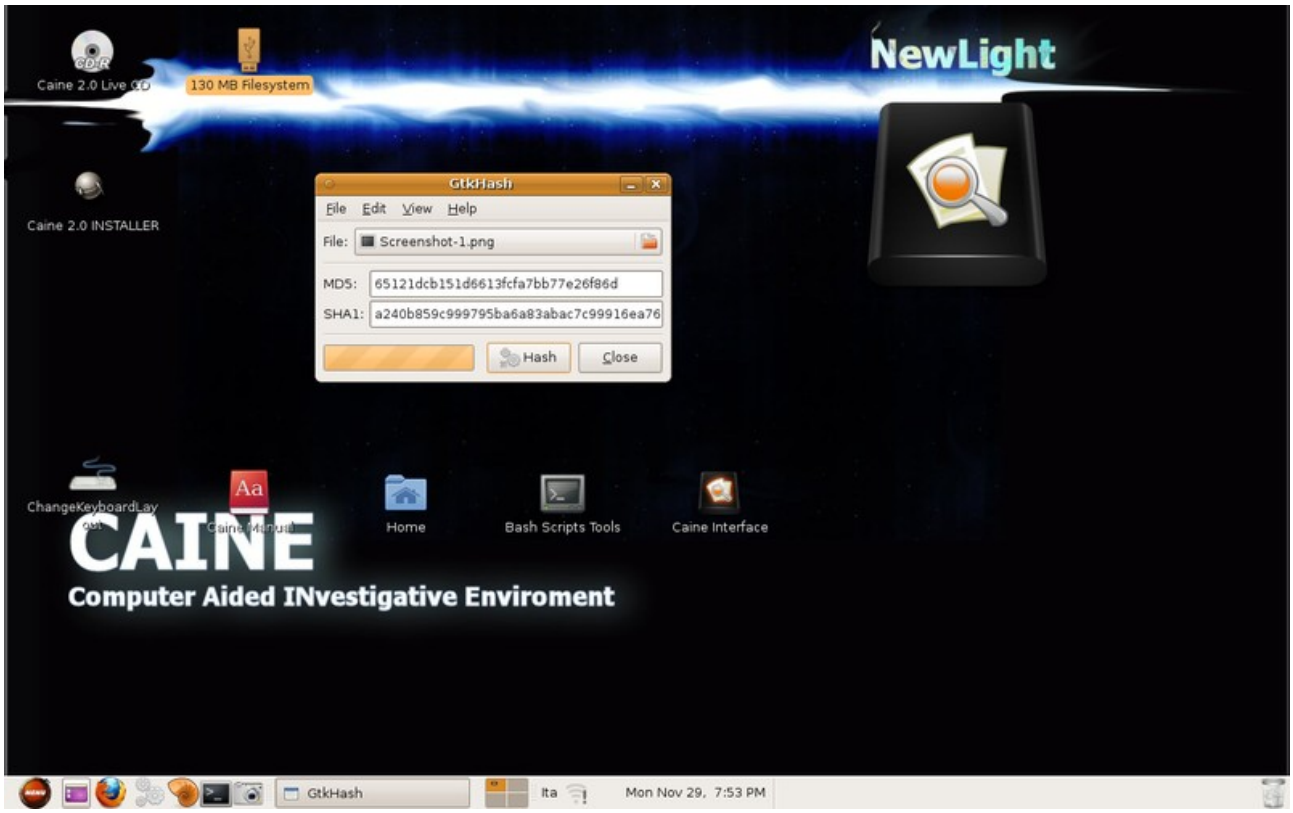
CAINE – caratteristiche dei dischi



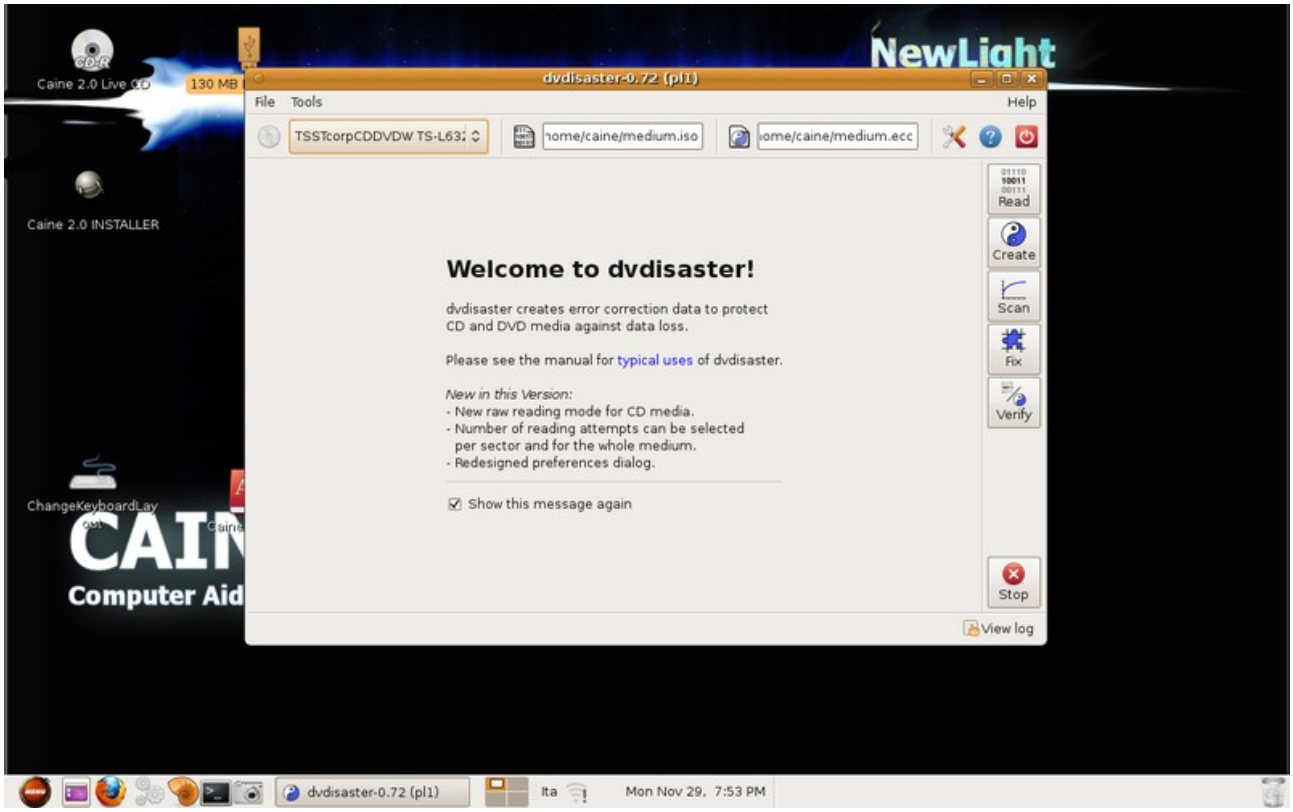
CAINE – creare un nuovo caso



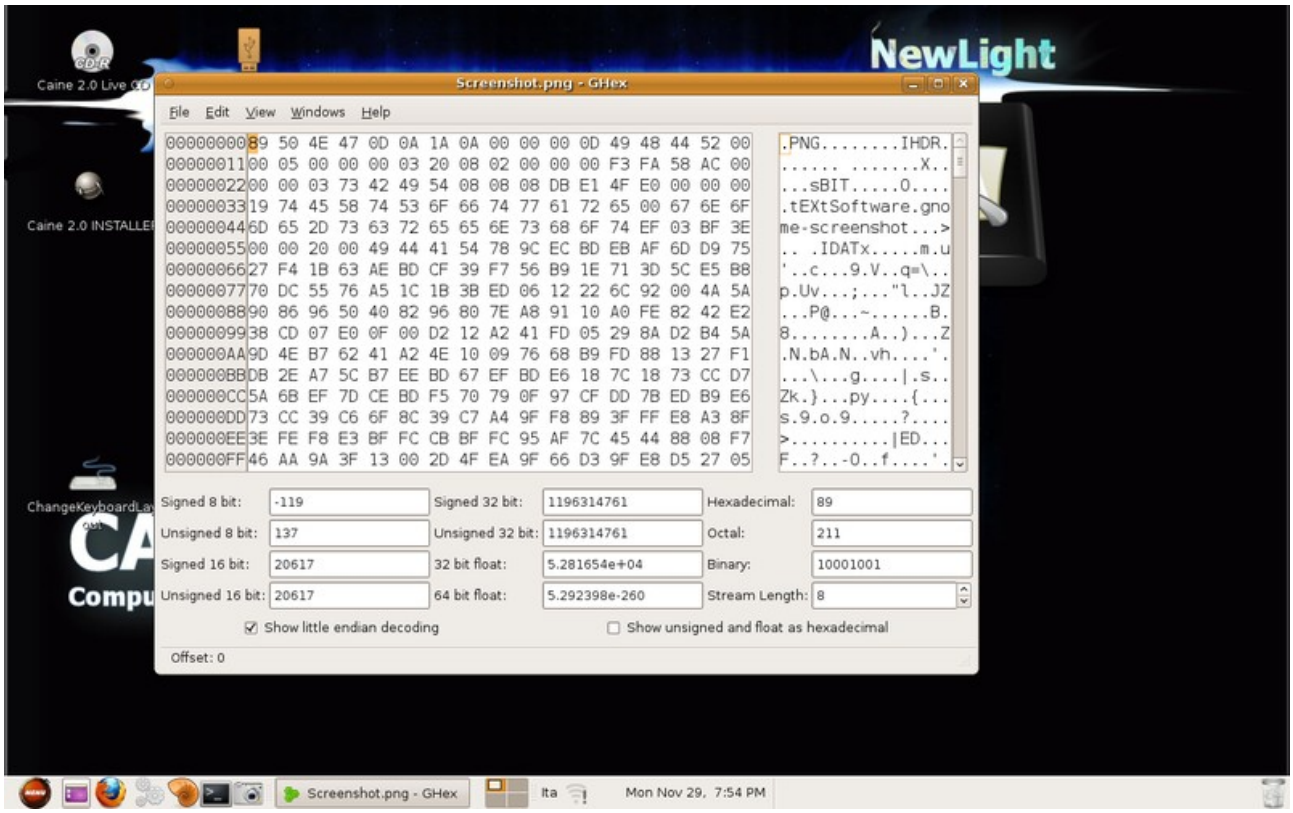
CAINE – calcolo dei codici hash



CAINE – dvdisaster: protezione contro la perdita dei dati

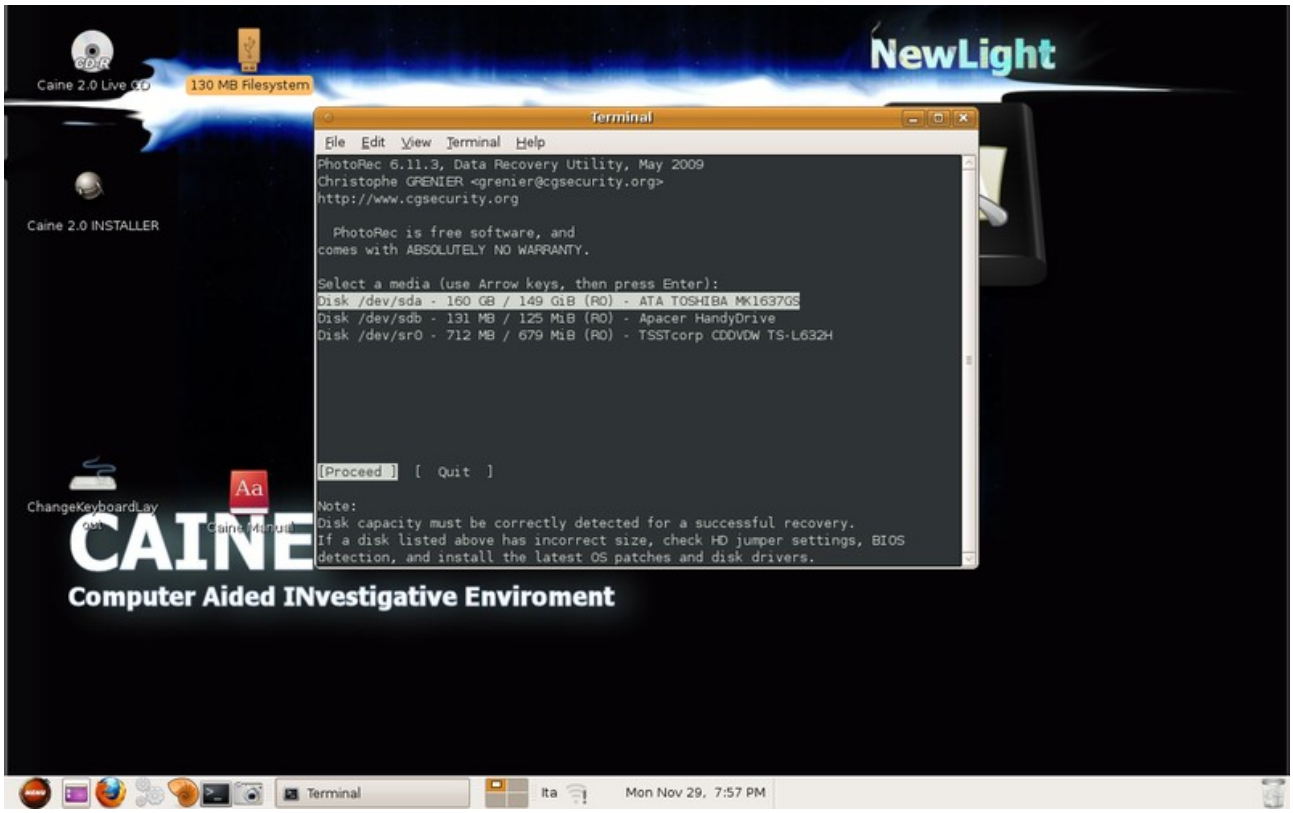


CAINE – esame dettagliato dell'archivio

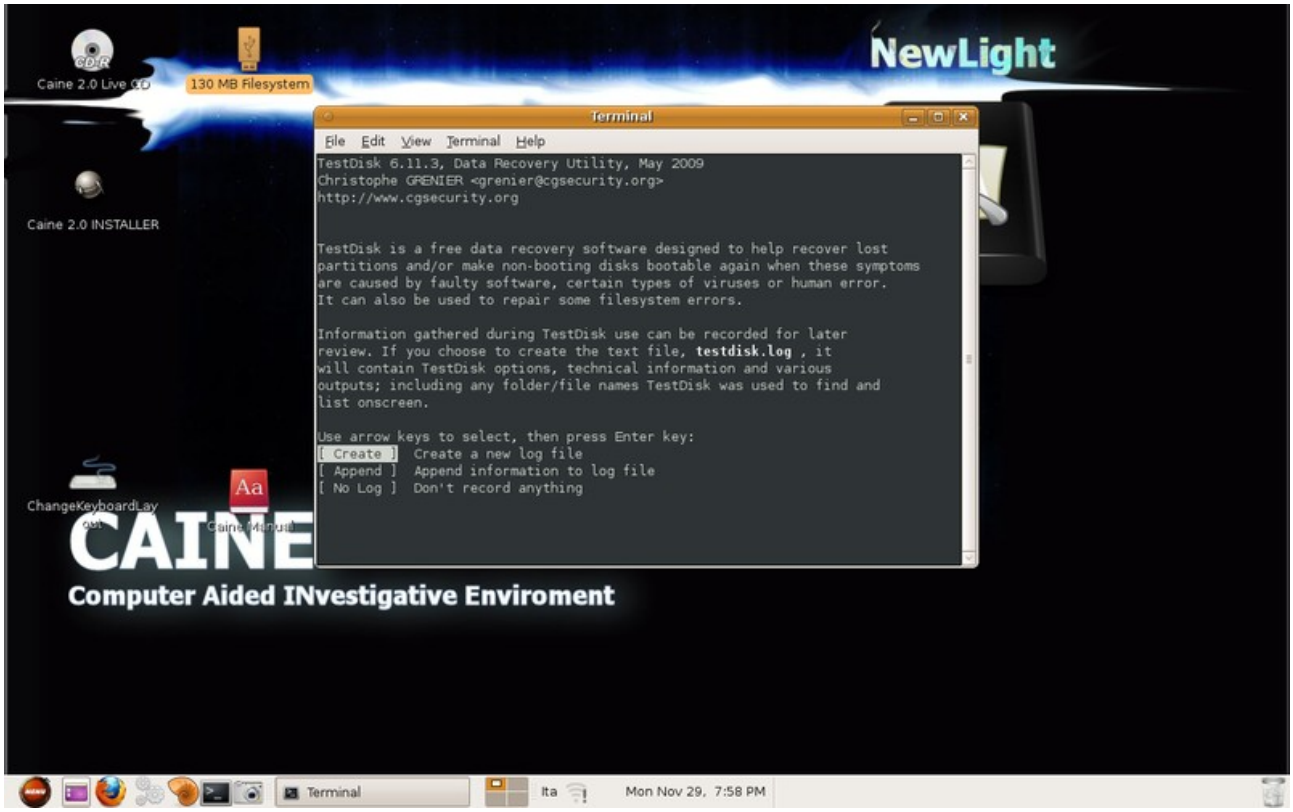


CAINE – ricerca di password

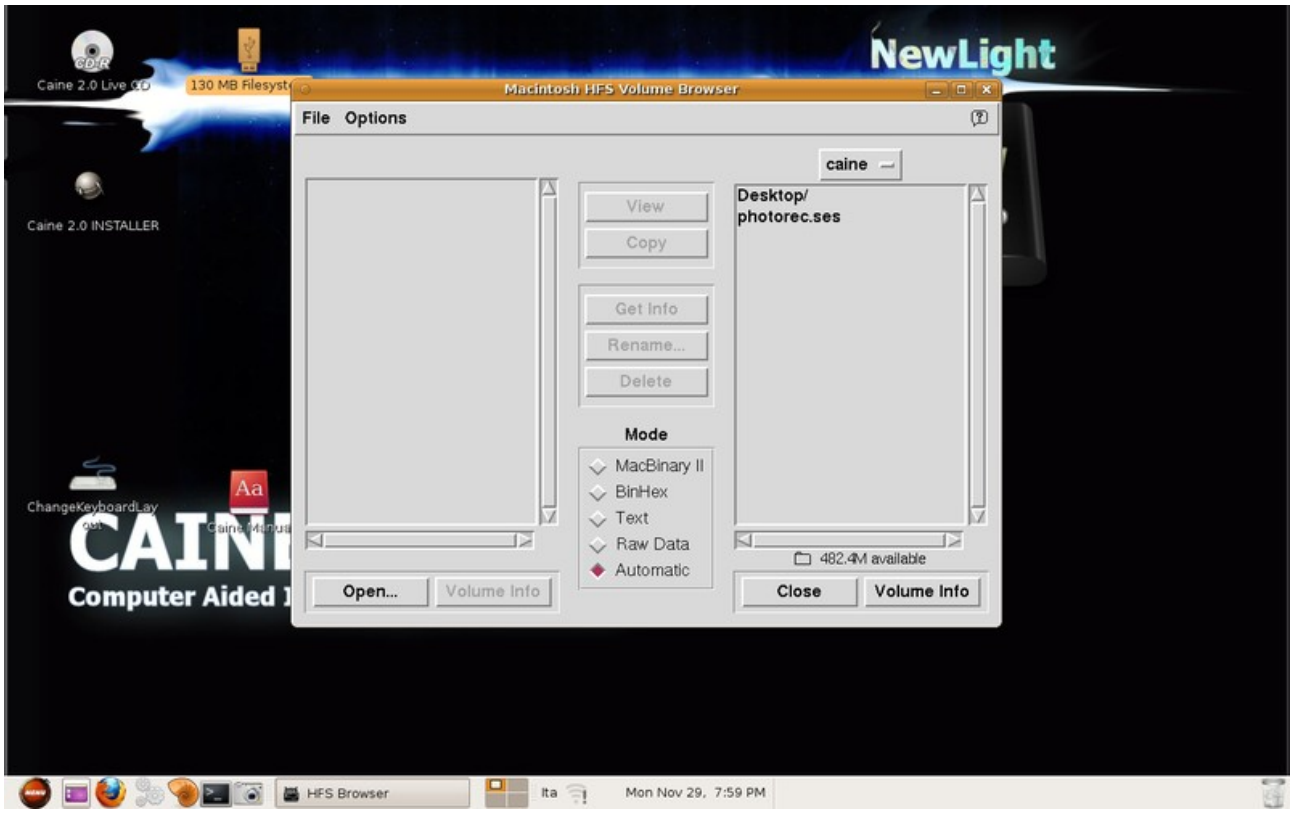
CAINE – PhoteRec – utilità di ripristino dei dati



CAINE – TestDisk: ripristino di partizioni danneggiate

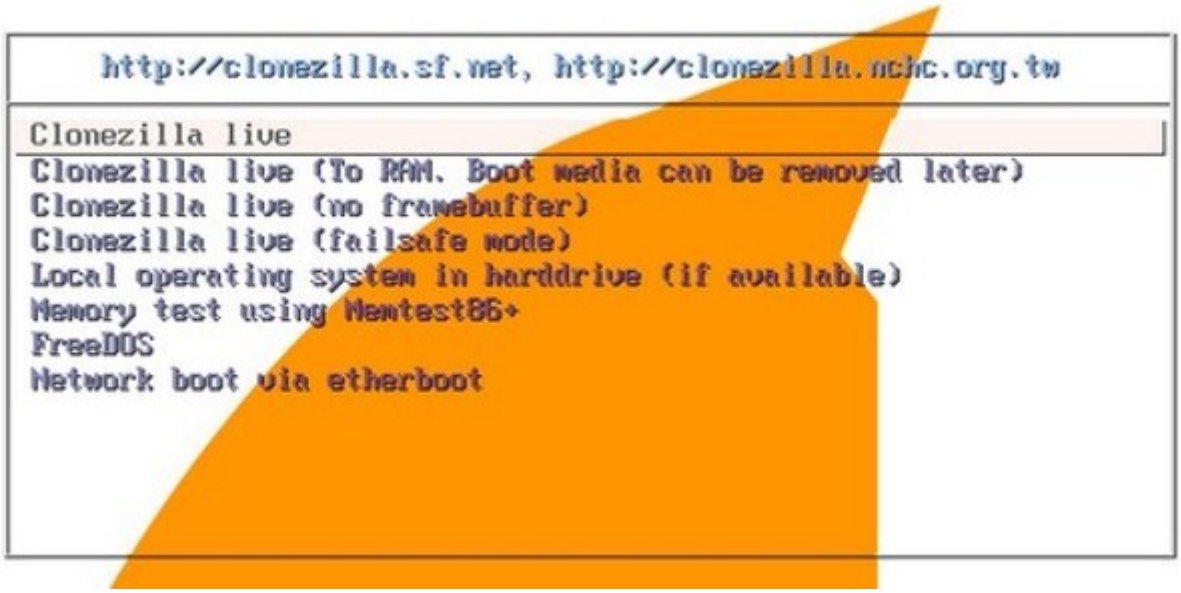


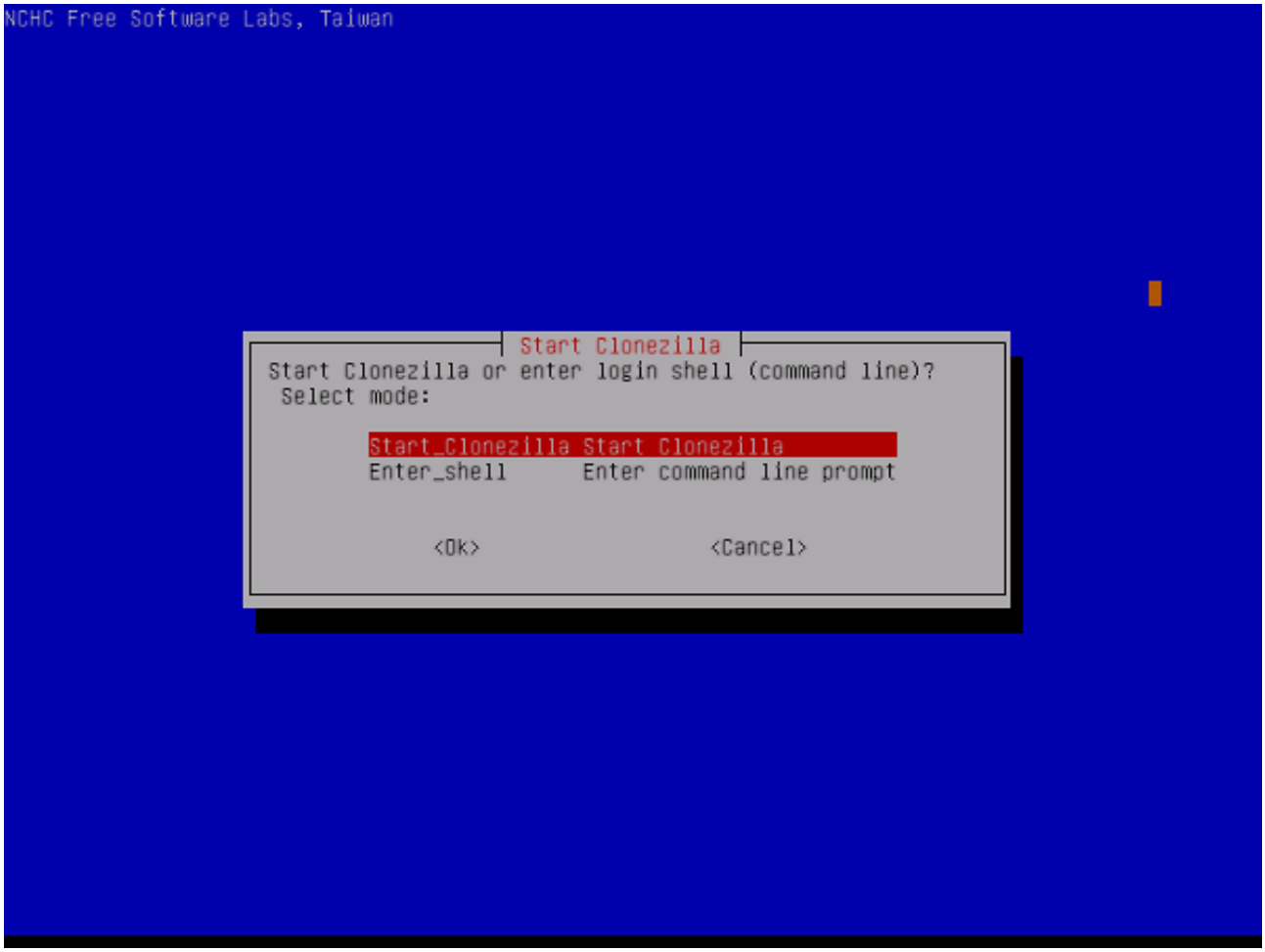
CAINE – esame di dischi Macintosh



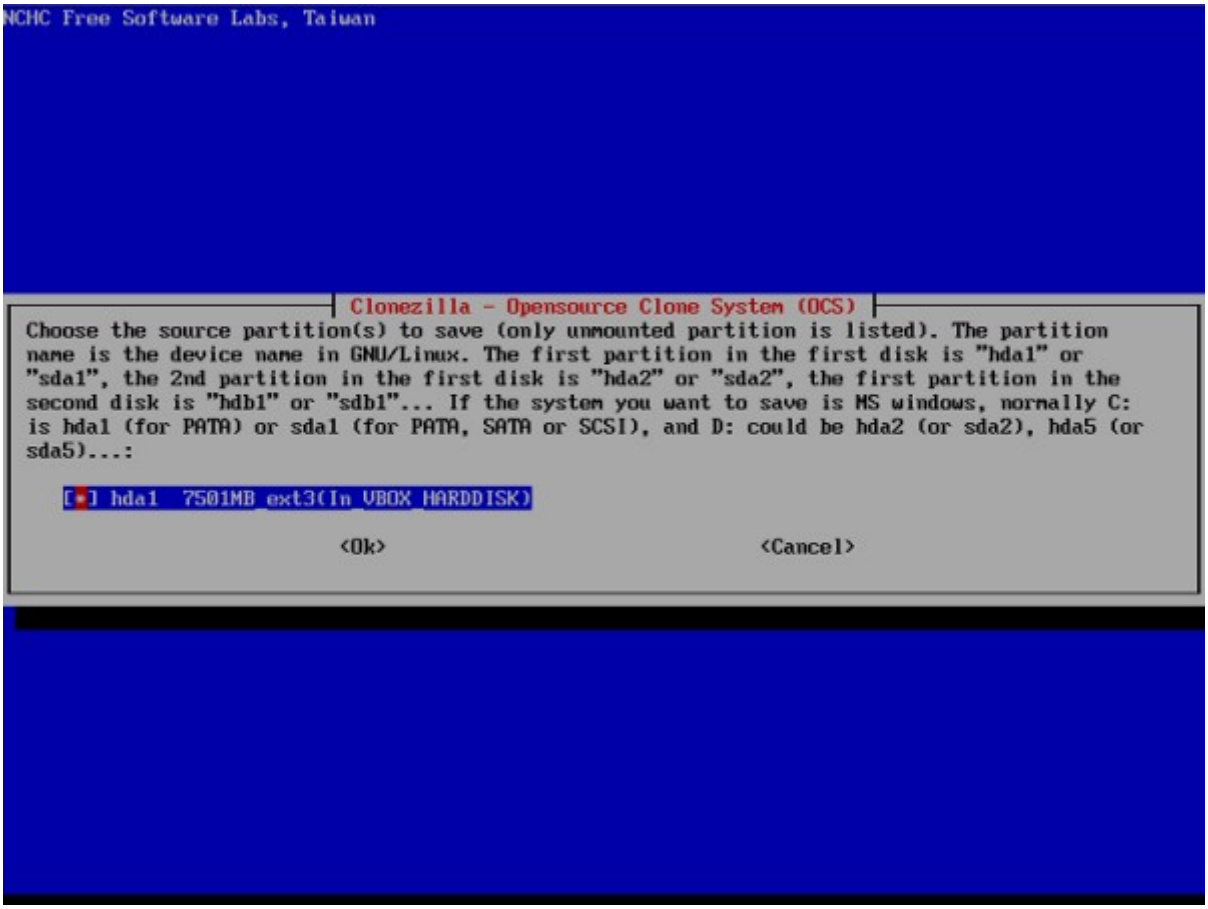
Clonezilla – Menu di avvio

Clonezilla è un programma gratuito da utilizzare per creare un'immagine del disco / partizione senza compromettere la loro integrità di origine.
Scelta della modalità operativa.

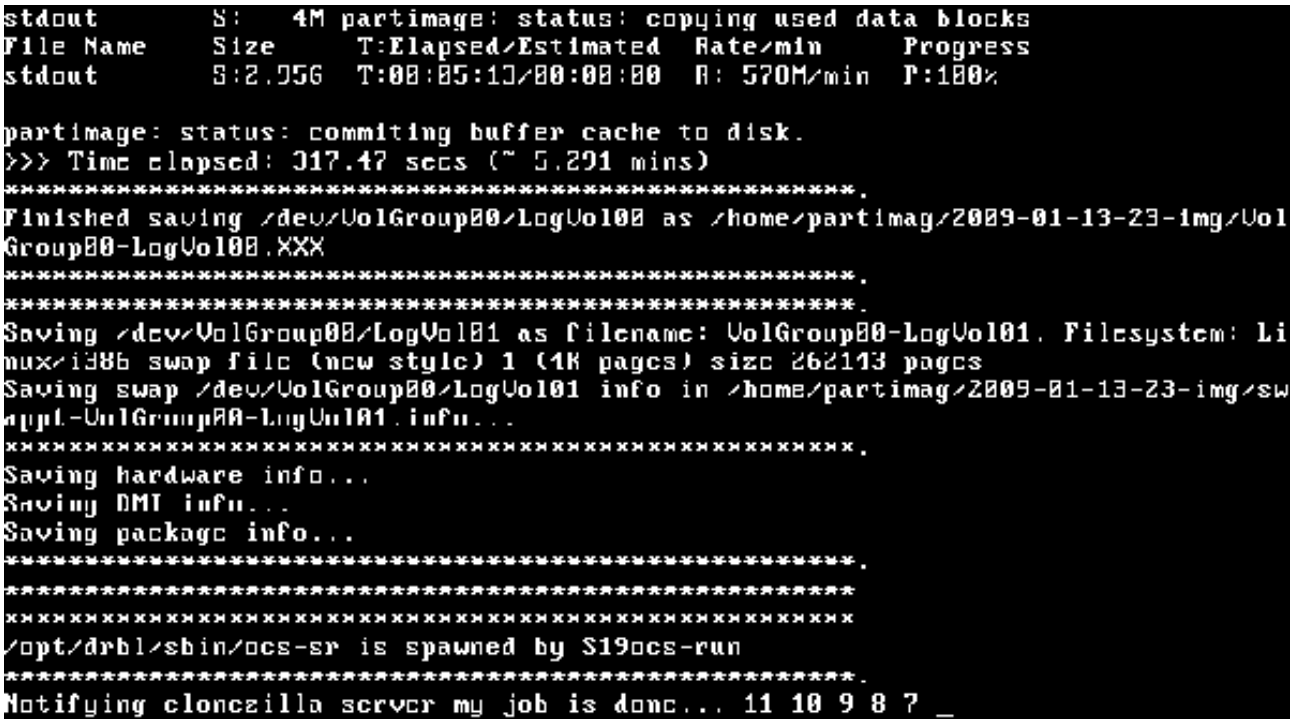




Clonezilla – Scelta della partizione da copiare



Clonezilla – Resoconto della copia della partizione



Osservazioni legali

Provocatoriamente si può affermare che l'analisi forense non è fatta solo di tecniche informatiche e che il computer non può finire in carcere: bisogna tener conto delle persone che stanno dietro al computer. Anche per l'analisi forense dovrebbero essere rispettate le norme di legge a tutela dei diritti delle persone indagate.
Le perquisizioni e i sequestri dovrebbero originarsi solo da notizie di reati preesistenti e non si dovrebbero usare le perquisizioni per acquisire notizie di reato del tutto nuovi dalle quali derivare prove a supporto di nuove ipotesi di reato.
Ad esempio non si potrebbe sequestrare un computer per il reato di *danneggiamento di sistemi informatici o telematici* c.p. 635-quater per poi documentare prove di *associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico* c.p. 270Bis.
Solo delle persone esperte dovrebbero effettuare le perquisizioni sui sistemi informatici come prescritto dall'art. 348 c.p.p *assicurazione delle fonti di prova.*
L'art 253 c.p.p. oggetto e formalità del sequestro al secondo comma dà una definizione di *corpo del reato*: *Sono corpo del reato le cose sulle quali o mediante le quali il reato è stato commesso nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo.*
Il Giudice normalmente dispone senza ritardo il sequestro con ordinanza escludendo le prove vietate dalla legge e quelle che palesemente sono superflue o irrilevanti.
La Polizia Giudiziaria dovrebbe quindi sequestrare solo i supporti di memorizzazione (dischi fissi, dischi esterni, dvd, cd, chiavette usb, schede di memoria (*memory / sim card*), ecc.) e non *monitor*, tastiere, *mouse*, schede *madri*, schede video, schede audio, stampanti, *scanner*, *modem*, schede di rete, *web cam*, ecc., perché *su* tutti questi ultimi dispositivi informatici non c'è traccia del reato e neppure c'è traccia di ciò che il reato ha *prodotto*.
Come alternativa al sequestro, la Polizia Giudiziaria può effettuare in loco la copia dei supporti di memorizzazione.
In ogni caso l'indagato dovrebbe ricevere un duplicato della *copia conforme* dei supporti di memorizzazione oppure avere la possibilità di verificare che sul computer siano apposti dei sigilli che ne impediscano l'utilizzo futuro non autorizzato.
Nelle attività di analisi forense occorre tener conto delle leggi in vigore, ad esempio:

- art.14 Costituzione: Inviolabilità del domicilio - *Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale*
- art.15 Costituzione: *La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge*
- art. 254 c.p.p.: Sequestro di corrispondenza - *Quando al sequestro procede un ufficiale di polizia giudiziaria, questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza aprirli o alterarli e*

senza prendere altrimenti conoscenza del loro contenuto

- art. 258 c.p.p.: Copie dei documenti sequestrati - *L'autorità giudiziaria può fare estrarre copia degli atti e dei documenti sequestrati, restituendo gli originali, e, quando il sequestro di questi è mantenuto, può autorizzare la cancelleria o la segreteria a rilasciare gratuitamente copia autentica a coloro che li detenevano legittimamente. In ogni caso la persona o l'ufficio presso cui fu eseguito il sequestro ha diritto di avere copia del verbale dell'avvenuto sequestro*

L'analista forense dovrebbe sempre ricordare che deve agevolare il Giudice nel comprendere le prove raccolte al fine della loro attribuzione alle persone indagate chiarendo quelle circostanze tecniche che, se non spiegate, potrebbero indurre il Giudice in errore.
Ad esempio se l'analista forense trovasse fra le bozze della posta elettronica dei messaggi penalmente rilevanti completi di mittente, destinatario, testo ed allegati e se si limitasse a certificare tale circostanza, potrebbe indurre il Giudice a ritenere *anche* il destinatario colpevole per i contenuti trovati nel messaggio.
Diversa sarebbe la valutazione del Giudice se l'analista forense avesse spiegato al Giudice che il messaggio non fu mai spedito all'ignaro destinatario e che l'indirizzo email del destinatario era di dominio pubblico.
Non è detto che un computer sia usato unicamente dalla persona che ne ha il possesso soprattutto quando lo stesso si trovi in un ufficio, sia o non sia il computer protetto da una password, password che normalmente è conosciuta da tutti i colleghi.
Anche se il computer era utilizzato da una sola persona, il computer potrebbe essere stato aggredito da programmi malevoli che lo utilizzavano come strumento *mascherato* con altra ignara identità per commettere reati in Internet; l'analista forense dovrebbe accertare che tali circostanze non sussistano.
Alle volte l'analista forense accerta che in una certa giornata e per un certo periodo di tempo il titolare del computer stava eseguendo programmi di elaborazione testi o di calcolo e che quindi non poteva trovarsi in altri luoghi.
A parte la considerazione che il titolare del computer potrebbe aver richiesto l'aiuto di un complice, è anche possibile siano stati creati dei programmi che automaticamente ad una certa ora vanno in esecuzione, modificano testi, fanno calcoli, aggiornano archivi e poi ad una certa ora smettono di funzionare.
Anche tali circostanze dovrebbero essere verificate ed escluse dall'analista forense.
Ogni prova acquisita dovrebbe essere sottoposta al *processo critico di eliminazione degli errori* come suggerito da Karl R. Popper nelle sue opere.
La prova ha *valore probatorio* se possiede i seguenti requisiti di:

- autenticità, perché proviene dai supporti di memorizzazione sequestrati
- integrità, perché corrisponde esattamente ai dati sui supporti sequestrati
- veracità, poiché non sono state inserite modifiche o variazioni ai dati
- completezza, poiché l'analisi non ha trascurato alcun elemento utile alle indagini
- legalità, nel rispetto delle leggi in vigore anche nel rispetto della persona inquisita

Profilo professionale ideale dell'analista forense

Un analista forense dovrebbe avere conoscenze di:

- diritto costituzionale
- diritto civile
- diritto penale
- diritto amministrativo
- procedura civile
- procedura penale
- principi di criminologia
- programmi e strumenti informatici per la gestione delle analisi forensi
- modalità di attacco e di intrusione ai sistemi informatici
- modalità di furto di identità
- truffe informatiche
- programmi e strumenti per la sicurezza informatica
- DPS (Documento Programmatico Sicurezza)
- metodi di accesso ai sistemi informatici
- modalità di trasmissione dati
- strutture dei dati sui supporti di memorizzazione
- sistemi di compressione, di crittografia e di steganografia
- applicazioni internet
- acquisizioni di prove informatiche
- validazione temporale dei dati
- strumenti e tecniche di effrazione degli strumenti informatici di
- sicurezza, prove informatiche (acquisizione, integrità, attendibilità)
- redazione di atti peritali
- procedure e usi di cancelleria

FAQ - Risposte alle domande più frequenti

Quale è il ruolo e quali sono le responsabilità del Ctu

Fatta la premessa che le attività della Ctu sono sempre formalmente condotte e gestite dal Giudice, il Ctu è semplicemente un suo ausiliario che possiede quelle competenze tecniche specifiche indispensabili per l'accertamento di fatti e circostanze utili per rispondere ai quesiti posti dal Giudice.
Il Giudice può infatti non accettare le conclusioni del Ctu e decidere in modo diverso, dandone però le motivazioni.
Dal momento del giuramento nell'udienza di conferimento dell'incarico, il Ctu è pubblico ufficiale e come tale acquisisce i diritti e i doveri di un pubblico ufficiale.
Il Ctu ha il compito principale di dare risposta ai quesiti posti dal Giudice in sede di conferimento dell'incarico, svolgendo tale compito con professionalità ed onestà al fine di fare conoscere al Giudice la verità, consentendo il contraddittorio fra le parti.
Il ruolo di pubblico ufficiale cessa nel momento del deposito dell'elaborato finale della Ctu in Cancelleria.

Come si diventa Ctu

Si diventa Ctu seguendo una procedura molto simile in tutti i tribunali italiani.
La procedura in vigore presso il Tribunale di Milano (Ufficio Volontaria Giurisdizione e Consulenti Tecnici, presso il palazzo di Giustizia) prevede che possano essere iscritti nell'albo dei consulenti tecnici del Giudice chi sia in possesso della cittadinanza italiana o di uno stato UE mediante domanda al Presidente del Tribunale nella cui circoscrizione l'aspirante risiede, contenente la dichiarazione di iscrizione all'albo professionale, l'indicazione della categoria e della o delle specialità.
La domanda deve essere compilata in carta libera ed essere corredata da marca da 14,62 euro, curriculum vitae firmato, fotocopia di documento di identità, documenti vari per dimostrare la capacità tecnica e l'esperienza professionale acquisita (titoli scolastici, attestazioni di terzi, perizie effettuate, pubblicazioni e così via) e versamento della somma di 168,00 euro sul c/c 8003 (intestato all'Agenzia delle Entrate, Centro Operativo di Pescara, tasse e concessioni governative).
Il certificato generale del casellario giudiziario sarà acquisito d'ufficio.
Per coloro che fanno parte di categorie che non sono organizzate in ordini o collegi professionali e quindi non sono provviste di albi professionali (come è il caso dell'ICT), è necessario allegare un certificato di iscrizione nell'Albo dei Periti e degli Esperti, tenuto dalla Camera di Commercio (per Milano è la categoria XXV Funzioni Varie sub Sistemi informativi per la gestione aziendale, via Meravigli 9/B) in carta bollata da 14,62 euro (o, in alternativa, la dichiarazione sostitutiva di certificazione ai sensi dell'articolo 46 DPR 445/2000).
All'indirizzo http://www.mi.camcom.it sono indicati i requisiti di carattere personale, morale e professionale, oltre alla documentazione da produrre.

L’iscrizione all’albo della Camera di Commercio è subordinata al parere favorevole di un’apposita commissione di valutazione. Una volta effettuata, è possibile presentare la domanda di iscrizione nell’albo dei consulenti tecnici di ufficio del Tribunale.
Anche in questo caso, però, l’iscrizione è subordinata al parere favorevole di un’altra commissione di valutazione interna al Tribunale, che si riunisce circa due volte all’anno.

Qual'è la formula di giuramento

Le formule di giuramento del Ctu in occasione del conferimento dell'incarico possono marginalmente variare da Tribunale a Tribunale e da Giudice a Giudice; in generale tutte si rifanno alla seguente formula: *Giuro di adempiere bene e fedelmente alle operazioni a me commesse al solo scopo di far conoscere al Giudice la verità*.

Quali sono i comportamenti e le procedure più importanti da rispettare

- consentire il contraddittorio fra le parti e verbalizzare quanto le parti richiedono sia verbalizzato
- redigere i verbali per gli aspetti rilevanti emersi nelle singole riunioni di Ctu raccogliendo i dati identificativi e le firme dei partecipanti (il Ctu, i Ctp, eventuali Legali, eventuali Parti in causa)
- inviare con tempestività ogni verbale ai partecipanti, ai Ctp e ai Legali anche se non presenti alla riunione di Ctu, verbale nel quale è fissata la data, l'ora e il luogo (città, via e numero civico) della prossima riunione
- rispettare i limiti posti dal Giudice nei quesiti ricevuti
- tenere in considerazione la non attendibilità dei dati sui supporti digitali (un archivio datato due anni fa potrei averlo creato oggi) e cercare altri elementi probatori
- se le riunioni di Ctu fossero destinate a protrarsi per diversi giorni, assicurarsi che i sistemi, i programmi e i dati oggetto delle verifiche non possano essere manomessi o contraffatti fra una riunione e la successiva (apposizione di sigilli ai locali / computer, copia dei dati su cd e successivo confronto di corrispondenza all'inizio della riunione successiva, ecc.)
- non esprimere pareri che possano intendersi anticipazione di giudizio
- nel caso il Ctu, in corso di riunione, ricevesse documenti cartacei o digitali da un Ctp, deve fornirne copia al Ctp di parte avversa; per ogni documento, cartaceo o digitale, è necessario sempre citarne la fonte
- evitare di discorrere, anche se di argomenti futili, alla presenza di un solo Ctp o legale di parte
- il Ctu, essendo anche pubblico ufficiale, ha il dovere di rilevare circostanze di illecito anche estranee ai quesiti posti, informando tempestivamente il Giudice di quanto rilevato (es. DPS mancante)

Cosa significa garantire il contraddittorio fra le parti in lite

- le parti, con particolare riferimento ai Ctp, devono poter essere presenti a tutte le riunioni di Ctu
- nel caso un Ctp non potesse essere presente, il Ctu deve tenerne conto rimandando ad altra riunione gli accertamenti più importanti, raccogliendo nel frattempo ampia documentazione degli accertamenti effettuati alla presenza del Ctp di parte avversa
- consentire ai Ctp il dibattito e il contraddittorio sulle modalità e sulla validità dei risultati raccolti
- verbalizzare le opinioni dei Ctp alle quali il Ctu può aggiungere le proprie; il Ctu ha comunque il diritto / dovere di richiamare i Ctp al contenuto dei quesiti del Giudice se un Ctp reclamasse una verifica del tutto estranea ai fini della Ctu
- nel caso il contraddittorio degenerasse a tal punto di rendere impossibile la continuazione della Ctu, il Ctu potrebbe indire una riunione con la presenza dei Legali delle parti nel tentativo di riportare il contraddittorio nei binari di un educato confronto di opinioni; se anche questo tentativo fosse inutile, il Ctu dovrà rivolgersi al Giudice per le opportune decisioni in merito.

Quali sono i compiti, le responsabilità e i diritti dei Ctp

I Ctp, pur rappresentando ognuno una parte in lite, collaborano con il Ctu per far conoscere al Giudice la verità.
I Ctp, a differenza del Ctu, non prestano giuramento e possono tacere al Ctu circostanze e conoscenze di fatti tecnici che potrebbero essere a sfavore della parte rappresentata; pur con questa premessa il Ctp non può dichiarare il falso a fronte di una precisa domanda tecnica a lui rivolta dal Ctu; sarebbe imbarazzante per il Ctp dare spiegazioni quando verifiche tecniche successive dimostrassero la falsità di sue precedenti dichiarazioni; il Ctp può non rispondere ma non può dire il falso.

Accorgimenti particolari nelle verifiche tecniche sui sistemi ICT

La massima giurisprudenziale tratta dalla sentenza della Corte di Cassazione, Sezione lavoro n. 2912 del 18 febbraio 2004 (Pres. Mattone, Rel. Spanò), recita che: *"la copia di una pagina web su supporto cartaceo ha valore probatorio solo se raccolta con le dovute garanzie per la rispondenza all'originale e la riferibilità ad un momento ben individuato"*.
Le informazioni tratte da una rete telematica sono per loro natura volatili e suscettibili di continua trasformazione.
Gli archivi memorizzati su supporti magnetici sono, per loro natura, facilmente manipolabili; le versioni precedenti degli archivi scompaiono in modo totale e, a differenza di ciò che accade nel mondo del reale, non restano tracce della loro precedente realtà, salvo ricorrere a particolari e sofisticate tecniche di estrazione dei dati.
Nel mondo del digitale non sono disponibili tecniche equivalenti alla ricerca del

DNA che esistono nel mondo del reale.
Ad esempio, oggi io posso creare un archivio elettronico con contenuti da me oggi voluti ma posso farli apparire come se fossero stati creati nel passato, assegnando all'archivio la data e l'ora di creazione per me più opportune; posso registrare oggi l'archivio su di un vecchio supporto di cdrom ancora vergine e non riscrivibile, camuffando per vecchio ciò che ho appena realizzato.
La stampa successiva della pagina web ottenuta dal cdrom, sapientemente invecchiato, costituirebbe un clamoroso falso anche se ad un primo esame parrebbe avere le dovute garanzie per la rispondenza all'originale e la riferibilità ad un momento ben individuato.
La rispondenza della pagina web su supporto cartaceo all'originale e la riferibilità' ad un momento ben individuato non può tecnicamente limitarsi alla rispondenza fra i contenuti grafici della pagina web che appaiono in stampa ed il corrispondente archivio digitale per le considerazioni appena fatte.
Occorre invece trovare rispondenze esterne ed indipendenti.
Ad esempio esiste un sito esterno ed indipendente che contiene la memoria storica delle pagine web sia nel loro aspetto grafico, sia in quello di linguaggio interno (es. html).
Questo sito (www.archive.org) non contiene tutto il pubblicato in tutti i siti e per ogni giorno; contiene però molto ed e' facile trovare quello che può interessare per verificare se una certa pagina web stampata e riferita al 2001 sia veramente coincidente con l'analoga pagina memorizzata nell'archivio storico in relazione al medesimo periodo.
Altre volte può accadere che le parti in lite abbiano prodotto, nei fascicoli di causa, i cdrom contenenti i programmi simbolici di funzionamento del sito, pero' privi dei dati necessari alla parte dinamica ed interattiva del sito stesso.
Ipotizziamo che il Consulente Tecnico di Ufficio abbia accertato la loro reciproca perfetta identità; in questo caso il Ctu potrebbe richiedere la ricostruzione di un archivio dei dati che sia compatibile con i simbolici contenuti nei cdrom delle parti in lite; l'esame tecnico del sito ricostruito sarebbe in grado di accertare il funzionamento o meno dei programmi anche nelle loro funzionalità dinamiche ed interattive.
Altre volte ancora e' necessario trovare i riscontri presso terzi: fornitori di connessione ad Internet, consulenti, programmatori, web designer, ecc., naturalmente dopo aver ottenuto l'autorizzazione del Giudice.
In conclusione non ritengo ci sia qualche possibilità tecnica di rendere probatoria una pagina web (o altri documenti) su supporto cartaceo in base al loro contenuto o semplicemente facendo riferimento ad un archivio digitale di supporto se tutti provenienti dalla stessa fonte.

Esempio di riferibilità temporale di documenti informatici

In una mia Ctu relativa ad una controversia per la duplicazione abusiva di un sito web di raccolta e di elaborazione di dati clinici, una parte accusava la parte avversa di avere sottratto i programmi simbolici e gli archivi necessari al funzionamento del sito web e di averlo pubblicato a suo nome in Internet apportando solo marginali modifiche.

La parte attrice mi consegnò dei documenti risalenti a molti mesi prima e provenienti da tre diverse persone identificabili e identificate dove si poteva constatare la totale uguaglianza fra il sito originale e quello gestito dalla parte convenuta.
All'epoca della Ctu il sito gestito dalla parte avversa si presentava con modalità diverse nelle parti prima identiche.
Io, come Ctu e per i motivi prima elencati, non potevo ritenere affidabili i documenti provenienti dalle tre persone.
La parte convenuta insisteva nel produrre copia di denunce alla Polizia Postale per presunte intrusioni telematiche nel loro sito web da parte di persone ignote fornendo date e orari di tali presunte intrusioni.
Io, come Ctu, feci presente che le presunte intrusioni non avevano alcun interesse ai fini degli obiettivi della Ctu e che soprattutto non poteva essere considerata intrusione la semplice navigazione nella home page del sito web con visione del codice sorgente sottostante la home page, perché sono operazioni a tutti consentite senza obbligo di digitare alcuna password.
Poiché la parte convenuta insisteva nel produrre le copie delle denunce, accettai i documenti.
Con meraviglia accertai che le date e le ore delle tre presunte intrusioni coincidevano perfettamente con i documenti prodotti dalla parte attrice.
I tre documenti che documentavano la totale uguaglianza fra il sito originale e quello gestito dalla parte convenuta divennero così affidabili perché la parte convenuta aveva prodotto *prove a suo sfavore* dando riferibilità temporale ai documenti della parte attrice.

Esempio di accertamenti tecnici impossibili

Sappiamo che una Ctu può iniziare a distanza di alcuni anni dal sorgere della controversia.
In cinque anni la tecnologia Ict ha registrato e ancora registra, progressi notevoli nelle prestazioni delle applicazioni e dei servizi.
In particolare le prestazioni della rete Internet usufruisce dei vantaggi dei server sempre più veloci e di bande di trasmissione dei dati sempre più *larghe*.
Ricordo di essere stato convocato per accettare una Ctu nella quale la parte attrice lamentava che un sito dinamico installato in Internet cinque prima denunciava, sempre cinque anni prima, tempi inaccettabili di risposta nell'aggiornamento delle pagine richieste dagli utenti.
Un perito prima di accettare l'incarico di Ctu riceve dal Giudice il fascicolo perché possa decidere se accettare l'incarico oppure motivare l'eventuale rifiuto.
Il Giudice aveva un certa preparazione in informatica e quindi fu d'accordo nel ritenere condivisibile la mia opinione della non fattibilità della perizia, soprattutto perché le prestazioni della rete Internet negli ultimi cinque anni erano notevolmente migliorate e non era praticamente possibile configurare una rete privata che funzionasse su una rete Internet mondiale di cinque anni prima certamente non riproducibile .
Il Giudice chiese di verbalizzare il mio parere e la Ctu fu cancellata con rammarico del legale della parte attrice che avrebbe voluto differire ulteriormente la

conclusione della causa.

Quando richiedere un fondo spese e per quale ammontare

L'eventuale fondo spese normalmente è stabilito dal Giudice nell'udienza di nomina a Ctu su iniziativa diretta del Giudice o su richiesta del Ctu.
Il suo ammontare è proporzionato alla durata prevista della Ctu, alle località di convocazione delle riunioni, alle prevedibili spese accessorie di Ctu, ecc.
Nel Tribunale di Milano, per Ctu da svolgersi nell'area milanese con durata di 90 giorni, è normalmente concesso un fondo spese di euro 500, mentre per Ctu della stessa durata ma con riunioni da svolgersi in altre regioni il fondo spese può raddoppiare o triplicare.
Il fondo spese è normalmente posto a carico solidale delle parti e il Ctu emetterà una fattura proforma del 50% verso ognuna delle parti in lite.

Come scrivere i verbali delle riunioni di Ctu

Non esistono norme codificate sulla forma che devono avere i verbali delle riunioni di Ctu.
I verbali hanno il principale obiettivo di informare i Ctp, i legali delle parti e poi il Giudice, quando leggerà l'elaborato della Ctu, sulle circostanze, sulle verifiche e sui risultati più significativi riscontrati durante tali riunioni, ancora con particolare riguardo all'obiettivo della trasparenza e del favorire il contraddittorio.
Il verbale costituisce anche il documento di prova del corretto operare del Ctu e dei Ctp nell'ambito dell'incarico ricevuto.
Il verbale dovrebbe contenere:

- dati identificativi della Ctu (parti in causa, numero di registrazione in cancelleria dei fascicoli di causa) data e luogo della riunione, partecipanti, ora di inizio delle operazioni peritali
- descrizione delle circostanze, delle prove / verifiche effettuate, dei risultati raggiunti nel corso della riunione
- dichiarazioni dei Ctp ed eventuali commenti del Ctu
- eventuali dichiarazioni delle parti
- riferimenti ai documenti tecnici acquisiti dal Ctu che saranno allegati all'elaborato finale della Ctu
- data ed ubicazione della riunione successiva
- piano di lavoro della riunione successiva
- firme dei partecipanti e loro riferimenti logistici (indirizzo, telefono fisso, fax.
- cellulare, indirizzo email)

Come scrivere la relazione finale della Ctu

Non esistono norme codificate sulla forma che deve avere l'elaborato finale della Ctu.
Di certo essa deve essere comprensibile, scritta in italiano corretto, priva di termini informatici non spiegati con parole comuni, tenendo sempre in mente che il Giudice è esperto in legge e non in informatica e se anche lo fosse non è detto che

lo sia un altro Giudice che dovesse ereditare i fascicoli di causa e l'elaborato della Ctu.
Le argomentazioni, le prove effettuate e i risultati raggiunti devono sempre fare diretto riferimento ai quesiti posti dal Giudice; considerazioni del Ctu su circostanze o fatti collaterali potrebbero essere utilizzate dalla parte che si sentisse danneggiata dalle conclusioni finali della Ctu per chiedere al Giudice di censurare (o render nulla) l'opera del Ctu per non essersi limitato a rispondere ai quesiti posti dal Giudice.
L'elaborato finale della Ctu dovrebbe essere articolato nei seguenti punti:

- riferimenti (Tribunale, Sezione, Numero di causa, Giudice, Ctu, Parti in causa e rispettivi Legali / Ctp)
- indice con riferimento alla pagina di inizio di ogni capitolo della relazione (**Oggetto, Quesiti, Risposta Sintetica, Svolgimento delle operazioni, Evasione dei Quesiti, Risposta dettagliata ai Quesiti, Commenti alle eventuali Relazioni dei Ctp, Allegati, Data e firma del Ctu**)
- **Oggetto** della Ctu, riferimento alla data di conferimento dell'incarico e dati anagrafici e professionali del Ctu (es. n° di iscrizione all'albo dei periti presso il Tribunale)
- **Quesiti** della Ctu: riportare fedelmente ed integralmente i quesiti posti dal Giudice
- **Risposta sintetica** ai quesiti: per agevolare il Giudice è opportuno riportare, immediatamente dopo i quesiti, le conclusioni e le risposte sintetiche ai Quesiti posti
- **Svolgimento delle operazioni** riferibili alla Ctu: ripercorrere cronologicamente i verbali delle riunioni ed illustrare in sintesi le circostanze più significative e i risultati principali conseguiti mettendo in luce soprattutto gli aspetti metodologici e procedurali seguiti
- **Evasione dei quesiti**: è la parte più corposa dell'elaborato nella quale il Ctu illustra nel massimo dettaglio le prove effettuate, i documenti raccolti ed allegati, i risultati raggiunti e per quelli non conseguiti indicarne i motivi
- **Risposta dettagliata ai quesiti**: è lo sviluppo dettagliato ed argomentato della Risposta sintetica indicata al punto precedente
- **Commenti alle eventuali relazioni dei Ctp**: commenti tecnici del Ctu alle relazioni dei Ctp che devono essere allegate all'elaborato
- **Allegati**: indice dei documenti allegati (cartacei e digitali cdrom)
- **Data e firma** del Ctu (non devono mai mancare pena la nullità dell'elaborato)

Esempio di relazione finale di CTU

TRIBUNALE CIVILE DI MILANO
PRIMA SEZIONE
****
CONSULENZA TECNICA DI UFFICIO

Causa	RG 99999/06
Giudice	Dott. Xxxxx Yyyyy
CTU	Dott. Roberto Bello
Attore	ABC s.r.l.
	assistito da Avv. Cccc Ddddd
	e dal CTP Dott. Eeeee Fffffff
Convenuto	XYZ s.r.l.
	assistito da Avv. Ggggg Hhhhhh
	e dal CTP Sig. Mmmmm Nnnnnn

Indice

La presente relazione si compone dei seguenti capitoli:

per un totale di 12 pagine.

Cap. 1. OGGETTO DELLA CTU

La presente consulenza ha per oggetto l'evasione del quesito del Giudice in merito alla causa in corso fra le parti sopra elencate che nel seguito della relazione saranno riferite usando le seguenti abbreviazioni:
ABC per ABC s.r.l.
XYZ per XYZ s.r.l
Il Giudice Dott. Xxxxx Yyyyy della I° Sezione del Tribunale di Milano, ha incaricato il __/__/2006 il sottoscritto, Dott. Roberto Bello, nato a Milano il __/__/____, domiciliato a Milano in via Aaaaaaa 4, con studio in Milano, via Bbbbbb 6 , iscritto all'albo dei periti estimatori presso la Camera di Commercio di Milano ed in quello dei Consulenti Tecnici d'Ufficio del Tribunale di Milano al n. 7890, di effettuare una CTU rispondendo al quesito di seguito specificato.

Cap. 2. QUESITO

“Dica il CTU, sentiti i Consulenti di parte, analizzi i programmi delle parti, e per quanto riguarda XYZ, analizzi i backup delle fasi di sviluppo, nella loro operatività e funzionalità se necessario acquisisca, mantenendo la riservatezza sugli stessi, i codici sorgenti, all'esito di tali esami, dica quindi se il programma sviluppato da XYZ sia in tutto o in parte riproduzione e/o evoluzione della piattaforma ABC.”

Cap. 3. RISPOSTA SINTETICA AL QUESITO

Il CTU premette che, essendo i mesi trascorsi dal sorgere della lite ad oggi teoricamente sufficienti ad un'eventuale traduzione dell'applicativo di ABC, ha rivolto la sua attenzione più a ricercare le tracce residue di un'ipotetica antica origine che ad esaminare nel dettaglio gli attuali sorgenti di XYZ, sorgenti che potevano teoricamente presentare aspetti mutati nascondendo del tutto la loro antica origine, ben sapendo che gli archivi informatici non possiedono un DNA.
Il programma sviluppato da XYZ è una riproduzione della piattaforma di ABC, riproduzione ottenuta “traducendo” i programmi dal linguaggio vbscript al linguaggio javascript, linguaggi fra di loro molto simili (come lo sono il dialetto fiorentino e la lingua italiana), mantenendo sostanzialmente inalterate le altre componenti tecnologiche (ambiente di erogazione del servizio, struttura degli archivi in formato Microsoft, con totale identità di due archivi di lavoro, totale identità della pagina iniziale di accesso, iniziale totale identità della documentazione destinata all'utente).
Particolarmente significativa è la circostanza della rimozione da parte di XYZ della dichiarazione di copyright di ABC dalla barra rettangolare posta al fondo della home page dell'applicazione di XYZ.
Il vantaggio maggiore conseguito da XYZ è derivato dall'acquisizione della conoscenza specialistica ..... originale di ABC, non riscontrabile in altri applicativi concorrenti, conoscenza che XYZ non ha dimostrato di possedere in modo originale.
Il brevissimo tempo di realizzazione dell'applicazione è una prova indiretta del vantaggio conseguito da XYZ nella riproduzione dell'applicativo di ABC.
Il CTU ha visionato le evoluzioni che XYZ ha presentato al solo CTU come innovative, evoluzioni non mostrate al CTP di parte avversa perché da XYZ dichiarate riservate così da non poter essere presentate nell'elaborato; il CTU ritiene che tali evoluzioni siano di marginale importanza.
Il CTU e i CTP hanno raccolto molta documentazione, anche in formato digitale (vedere cdrom allegato), che potrà essere utile nel giudizio di merito quando anche le parti delle applicazioni ABC e XYZ, ora riscontrate identiche dal CTU, non saranno più tali per eventuali ulteriori traduzioni da parte di XYZ.

Cap. 4. RIUNIONI DI CTU (verbali allegati)

in data __/__/2006	alle ore 10:30 presso la I Sezione del Tribunale di Milano per il giuramento del CTU

in data __/__/2006	Alle ore 10:00 nella studio del CTU per inizio delle operazioni peritali (allegato A1)
in data __/__/2006	alle ore 9:45, nella sede di XYZ per l'esame dell'applicazione e l'acquisizione di documenti ed immagini digitali (allegato A2)

….....
….....
….....

Cap. 5. EVASIONE DEL QUESITO

5.0. Premessa

….....
….....
….....
….....
….....
….....

5.1. Struttura e composizione delle applicazioni di ABC e di XYZ

Entrambe le applicazioni, come tutte le applicazioni informatiche, hanno per componenti:

- un contenuto applicativo
- un sistema operativo e un software intermedio di substrato
- un insieme di archivi di dati strutturati secondo un formato formale
- un insieme di programmi applicativi scritti in un determinato linguaggio
- un ambiente di fruizione dell'applicazione da parte dell'utilizzatore.

Per un'applicazione di …....., come per qualsiasi altra applicazione informatica, lo sviluppatore ha ampia scelta di quali componenti, sistemi, architetture e linguaggi utilizzare.

5.2. Contenuto applicativo

….....
….....
….....

Il CTU ritiene che la sola fase di analisi dell'applicazione, fino a giungere alla redazione di un documento completo del progetto, tale che la successiva preparazione dei programmi di elaborazione possa procedere senza intoppi e ripensamenti, richieda un impegno di almeno un anno da parte di una persona che si avvalga della consulenza applicativa di uno o più …..... esperti in sperimentazione ….....

Il CTP di XYZ nel verbale della riunione del __/__/2006 dichiara che:

“ ... i tempi di sviluppo sono stati: analisi dell'applicazione: 1 mese e

programmazione: 3 mesi”
…….
…….
…….
Sono invece del tutto ragionevoli i tempi di sviluppo evidenziati da ABC (verbale riunione del __/__/2006): “1) ricerca iniziale / progettazione (ideazione, affinamento, prototipi, programmazione iniziale) per 24 mesi / uomo
2) programmazione e prove dell'applicativo, oggetto di causa (per) 3 mesi”
…….
…….
…….

5.3. Sistema operativo e un software intermedio di substrato

…….
…….
…….

5.4. Insieme di archivi di dati strutturati secondo un formato formale

Entrambe le applicazioni di XYZ e di ABC utilizzano lo stesso formato di rappresentazione dei dati all'interno degli archivi sui dischi del server (formato SQL di Microsoft). Sono disponibili molte altre alternative: MySQL, PostgreSQL, Oracle, FirebirdSQL, Sybase, SAP, Informix, ecc.).
Il CTU evidenzia il rilievo della circostanza dell'identità riscontrata in questo punto ed il suo contributo alla risposta al quesito posto.
Inoltre, e di rilievo ancora maggiore, è stata la scoperta, mostrata e commentata con i CTP, che due archivi dell'applicazione di XYZ erano configurati in modo totalmente identici ai corrispondenti due archivi dell'applicazione di ABC, avendo identità nei nomi dei campi, nella loro successione e nelle loro dimensioni (allegato B1).
Il CTU ritiene totalmente improbabile che XYZ abbia indovinato come configurare e comporre i due archivi facendoli esattamente uguali a quelli dell'applicazione di ABC, risultato possibile solo se l'applicazione fosse stata esplorata prima al suo interno.
Il CTU evidenzia il rilievo della circostanza dell'identità riscontrata ed il suo contributo alla risposta al quesito posto.

5.5. Insieme di programmi applicativi scritti in un determinato linguaggio

Entrambe le applicazioni di XYZ e di ABC utilizzano due linguaggi molto simili fra di loro: il linguaggio VBscript nel caso dell'applicazione di ABC e JavaScript nel caso di XYZ. Esempi di somiglianza e quasi uguaglianza dei due linguaggi sono descritti all'allegato B2.
Inoltre esistono dei programmi che automaticamente traducono il linguaggio Vbscript in linguaggio JavaScript, come ad esempio il programma ScriptConverter

(allegato B3) che è in grado di tradurre automaticamente il 90% delle istruzioni da VBScript a JavaScript lasciando solo il restante 10% all'esperienza del programmatore.
Il CTU non ha elementi per dichiarare che ciò sia avvenuto, ma può sicuramente affermare che i due linguaggi sono formalmente quasi identici e che le piccole differenze formali possono essere quasi tutte automaticamente colmate.
Il CTU rileva che, pur essendo disponibili moltissimi linguaggi di programmazione (ASP, Cgi, PHP, Perl, XML, ecc), XYZ ha scelto quello più somigliante e quasi identico a quello utilizzato nell'applicazione di ABC.
Il CTU evidenzia il rilievo della circostanza per il suo contributo alla risposta al quesito posto.

5.6. Ambiente di fruizione dell'applicazione da parte dell'utilizzatore.

….....
….....
….....

Cap. 6. Dati sensibili e DPS

Il CTU in data __/__/2006 chiede a XYZ l'esibizione del DPS (Documento Programmatico sulla Sicurezza) con lo scopo, non dichiarato dal CTU, di esaminarlo per verificare l'esistenza di documenti cartacei o digitali utili alla CTU.
….....
….....
….....

Cap. 7. Commenti alla relazione del CTP di ABCl e a quanto fatto verbalizzare da XYZ

….....
….....
….....

Cap. 8. Dichiarazione finale del CTU

….....
….....
….....

Cap. 9. Allegati

verbale della riunioni di CTU	da A1 ad A6
documenti del CTU di confronto siti web	da B1 a B9
documenti riferibili alla documentazione utente	B10
DPS - Documento Programmatico sulla Sicurezza di XYZ	B11

proprietà tecniche del sistema server	B0
dati di prestazione del sistema server	B1
conclusioni del CTP ABC	C1
documenti vari di fonte ABC	D1
documenti vari di fonte XYZ	D2
cdrom dei documenti ed archivi digitali	cdrom A

La presente relazione è stata redatta con la consapevolezza di aver agito in scienza ed in coscienza.

In fede
Dott. Roberto Bello - 02 99999999 - 338 9999999

Milano, gg mese 2006

Come il Ctp può scrivere la sua eventuale relazione

Il Ctp può scrivere la sua relazione sulla falsariga di quanto raccomandato per l'elaborato finale del Ctu.
Naturalmente il Ctp, sempre dichiarando il vero, può mettere in evidenza i fatti a favore della parte rappresentata e in contraddittorio con quelle del Ctp di parte avversa e delle posizioni che il Ctp prevede siano del Ctu.
Il Giudice valuterà le sue considerazioni ponendole a confronto con quelle del Ctu e del Ctp di parte avversa.

Come il Ctu può preparare la proposta di parcella

Su questo argomento purtroppo i Ctu devono esprimere molte lamentele.
Le modalità di retribuzione dell'opera del Ctu sono contenute nelle leggi:DPR 27.7.88 n° 352, legge 319/80, DPR 5 dicembre 1997, DPR n° 30 maggio 2002.
Per Ctu in ambito ICT si deve quasi sempre adire al calcolo della proposta di parcella ricorrendo alle *vacazioni*: termine strano che rappresenta un'attività del Ctu della durata di 2 ore.
Le disposizioni in vigore prevedono:

- la prima vacazione di Ctu è retribuita a euro 14,68
- le vacazioni successive a euro 8,15
- le vacazioni massime concedibili per giornata sono 4 pari a 8 ore di attività.

Quindi un Ctu, fatta eccezione della prima giornata, è retribuito ad euro 32,60 a giornata: ogni commento sarebbe inutile.
Quindi teoricamente una Ctu con 90 giorni di durata, più una giornata per la nomina a Ctu, più una giornata per il deposito dell'elaborato finale in Cancelleria, potrebbe essere retribuita per un importo massimo di euro 3.005,73 (euro 39,13 per l'udienza di nomina, euro 2.934,00 per attività di Ctu ed euro 32,60 per il deposito dell'elaborato in Cancelleria.
I Ctu per sopperire al valore irrisorio della vacazione sono costretti:

- a richiedere al Giudice durate di incarico eccedenti il necessario, con evidenti conseguenze sulla durata del processo

- a dichiarare di aver effettuato attività di Ctu anche quando in realtà si sono occupati di altro.

Esempio di proposta di parcella

Ing. Pinco Pallino
Via Milano 4
20100 - Milano (MI)
tel 02xxxxxxxx

Tribunale DI MILANO'
n° SEZIONE CIVILE
Giudice: Dott. X Y
R.G. nnnnn/aa
Parte AAAA s.r.l. / Parte BBBB s.r.l.

RICHIESTA DI LIQUIDAZIONE (SPESE E COMPETENZE)
Ad avvenuta esecuzione del mandato conferito, il sottoscritto Ing. Pinco Pallino, quale Ctu nella Ctu indicata in epigrafe, sottopone la seguente sua nota di spese, competenze ed onorario.

SPESE:

per spese viaggio alle sedi di Parte AAAA e di Parte BBBB	euro	20,00
per spese di cancelleria, fotocopie, rilegatura e collazione atti della Ctu, cdrom	euro	80,00
per la scritturazione delle varie bozze e della versione definitiva	euro	220,00
per telefonate urbane, interurbane, con cellulare, servizio fax ed internet	euro	60,00
Totale Spese	euro	380,00

COMPETENZE

Per la parte descrittiva sulla base di quanto stabilito dal DPR 27.7.88 n° 352, legge 319/80 e DPR 5 dicembre 1997 e decreto n° 30 maggio 2002, si ha:		
vacazioni per il giuramento del 05/10/2006 (n° 1 a euro 14,68 e n° 3 a euro 8,15)	euro	39,13
vacazioni per operazioni peritali nei giorni 11/10/06, 16/10/06, 17/10/06, 20/10/06, 31/10/06, 09/11/06 e nei giorni successivi in studio (n° 175 x € 8,15)	euro	1.426,25
vacazioni per il deposito della Ctu (n° 4 a euro 8,15)	euro	32,60
Totale competenze	euro	1.497,98
Per un totale di spese (euro 380,00) + competenze (euro 1497,98)	euro	1.877,98

IVA 20% R.Acc. 20%

Il Ctu ha ricevuto dalle parti un acconto di euro 200,00
per un importo totale di euro 400,00.

Milano, 24 novembre 2006 Firma del Ctu

Cos'è l'Accertamento Tecnico Preventivo (ATP)

L'Accertamento Tecnico Preventivo (ATP) è uno strumento processuale previsto dall'art. 696 bis c.p.c dal doppio aspetto: il primo è quello che permette di utilizzare l'ATP quale strumento di conciliazione della controversia tra le parti; il secondo è quello che riconosce alle parti il diritto di precostituire una prova prima e al di fuori del processo.
Nell'ATP al Ctu è delegato l'incarico di cercare la conciliazione fra le parti; se ciò avvenisse il Ctu sarebbe retribuito dalle parti senza i vincoli dei valori delle vacazioni sopra menzionate ma anche senza la tutela derivante dal titolo esecutivo della ATP basata sulle vacazioni.
Il Giudice, al fine di facilitare la conciliazione della lite, può fissare altri termini anteriori al deposito dell'elaborato della ATP, per l'inoltro dell'elaborato della ATP da parte del consulente alle parti in lite ed un ulteriore termine alle parti in lite per le loro osservazioni dirette al consulente della ATP.

Cos'è la Consulenza Tecnica Preventiva (CTP)

La Consulenza Tecnica Preventiva ai fini della composizione della lite è uno strumento processuale previsto dall'art. 696-bis del Codice di Procedura Civile.
Volendo sinteticamente differenziare la Consulenza Tecnica Preventiva (CTP) rispetto all'Accertamento Tecnico Preventivo (ATP), si può affermare che, mentre l'ATP ha l'obiettivo principale di costituire delle prove *prima del processo*, la CTP tende ad una soluzione in *luogo del processo*.
I pareri tecnici del consulente della CTP, nominato dal Giudice, sono formulati e argomentati perché siano persuasivi ai fini della composizione della lite.
Il consulente della CTP è tenuto a proporre alle parti in causa una soluzione conciliativa anche estranea alle proprie competenze tecniche e alle verifiche effettuate sugli elementi a disposizione.
La soluzione conciliativa può essere proposta non solo prima del deposito della perizia, ma addirittura nel corso della stessa relazione.
Il Giudice, al fine di facilitare la conciliazione della lite, può fissare altri termini anteriori al deposito dell'elaborato della CTP, per l'inoltro dell'elaborato della CTP da parte del consulente alle parti in lite ed un ulteriore termine alle parti in lite per le loro osservazioni dirette al consulente della CTP.
Il processo verbale di conciliazione è esente dall'imposta di registro e, con decreto del Giudice, può essere dotato dell'efficacia di titolo esecutivo.
Nel caso la CTP non portasse ad alcuna conciliazione, le parti in causa nel successivo giudizio ordinario potrebbero chiedere di acquisire agli atti la relazione depositata dal consulente della precedente CTP (penultimo comma dell'art. 696-bis), senza che tale relazione abbia una valenza istruttoria o possa essere considerata un'integrazione alla relazione della nuova CTU.
Nel caso di fallimento del tentativo di conciliazione per mancata adesione di una delle parti ai pareri del consulente della CTP e se la successiva sentenza di merito riconoscesse valida una soluzione della lite in linea con l'orientamento del consulente della CTP, la parte soccombente potrebbe essere condannata dal Giudice a risarcire la parte avversa per *lite temeraria* non avendo la parte

soccombente accettato la conciliazione proposta nella precedente CTP.

Quando conviene ricorrere ad una perizia tecnica preventiva *non giudiziale*

Molti Ctu hanno dovuto esaminare, a distanza di anni progetti ICT che non dovevano neppure iniziare.
Tutte le informazioni per sconsigliarne lo sviluppo, erano disponibili prima ancora che il progetto partisse.
Dopo anni di danni reclamati e non ammessi, di scambio di raccomandate, di ingiunzioni ad adempiere, di memorie di avvocati, di udienze, di testimonianze contestate, finalmente il Ctu nominato dal Giudice evidenzia che il progetto era viziato fin dall'origine, perché destinato a sicuro insuccesso e, nell'interesse di entrambe le parti, non doveva iniziare.
Come ci si dovrebbe comportare?
Prendere coscienza che i prodotti e le applicazioni ICT sono come le medicine che dovrebbero essere assunte solo dietro prescrizione medica.
Un'applicazione ICT idonea e perfetta per un cliente, potrebbe essere inadeguata, costosa e pericolosa per un altro.
Come per l'assunzione di medicine inadeguate, si scoprono i danni quando è trascorso troppo tempo e si è passati, senza giudizio, da medicina a medicina (e da applicazione ICT ad applicazione ICT), aggiungendo ulteriori problemi a quelli già presenti.
Con utili e salutari reciproche diffidenze ben stampate nella mente, cliente e fornitore dovrebbero accordarsi nel definire gli obiettivi del progetto e nel dettagliare le risorse ICT che si intendono destinare al progetto comune.
Dovrebbero nominare un perito, esperto in materia, che al di sopra delle parti, possa esaminare la struttura organizzativa e le potenzialità del cliente e dall'altra parte le caratteristiche e le potenzialità delle risorse ICT proposte dal fornitore.
Il perito nominato dalle parti non deve avere alcuna possibilità di proporsi o di proporre altri fornitori in grado di fornire quelle soluzioni ICT che, a suo avviso, potrebbero meglio realizzare gli obiettivi del cliente.
Escludendo a priori al perito ogni possibilità di lucrare sulle carenze della soluzione proposta dal fornitore, sarebbe un'ulteriore garanzia dell'imparzialità del perito, imparzialità che dovrebbe essere data per scontata se il perito fosse iscritto all'albo dei periti estimatori del Tribunale.
E' una proposta semplice e facilmente percorribile; richiede solo la volontà delle parti di prevenire prima invece di litigare poi.
Basta che cliente e fornitore, con scrittura privata, si accordino sulla scelta del perito imponendogli i doveri appena richiamati, comportandosi poi con lo stesso perito in modo conforme alle regole pattuite.
La soluzione non è nuova in assoluto, ma è nuova nel settore dell'ICT.
In realtà quanto suggerito è alle volte formalmente prescritto nelle forniture alla Pubblica Amministrazione e nei progetti ICT con finanziamento agevolato.

Quando ricorrere ad una perizia asseverata / giurata

Spesso accade che un progetto informatico sia in parte finanziato da organismi

regionali, statali o comunitari che richiedono, prima dell'erogazione del saldo del finanziamento, una perizia tecnica a giustificazione dello stato di avanzamento delle attività pianificate e dei costi sostenuti.
Normalmente per ottenere un finanziamento è necessario presentare un progetto indicandone le finalità, le caratteristiche tecniche, i benefici attesi, le risorse necessarie al suo sviluppo, i costi da sostenere, i tempi previsti di attuazione e quant'altro sia significativo in merito.
Normalmente la perizia può essere svolta solo da un perito che sia iscritto nell'apposito albo dei periti del Tribunale.
Il perito, in questo caso, si accorda con responsabile del progetto e beneficiario del finanziamento sui modi, sui tempi e sui compensi professionali senza i vincoli delle tariffe applicabili in caso di Ctu.
Si ricorre ad una perizia asseverata / giurata anche nel caso si voglia documentare una situazione tecnica o operativa di sistemi informatici (computer, reti, programmi, siti web, ecc.) riferendola alla *data certa* della perizia.
La perizia asseverata / giurata non ha però lo stesso valore di una perizia di Ctu, perché la perizia asseverata / giurata è comunque una perizia di parte anche se sottoscritta da un perito professionista iscritto all'albo dei periti del Tribunale: manca il controllo del Giudice e manca il contraddittorio della parte avversa che non esiste.
Una perizia asseverata / giurata può essere prodotta in sede di successivo contenzioso ma essa potrebbe essere smentita dal nuovo Ctu incaricato dal Giudice.
Il perito redige la perizia facendo riferimento ai contenuti del progetto per il quale si è richiesto il finanziamento o per gli obiettivi del cliente committente nel caso si voglia documentare una situazione tecnica o operativa di sistemi informatici riferendola alla *data certa* della perizia.
La asseverazione di una perizia è un atto pubblico di competenza del Cancelliere, atto nel quale il perito dichiara sotto la propria responsabilità civile e penale la veridicità del contenuto.
Il documento della perizia deve contenere:

- i riferimenti anagrafici del perito (nome, cognome, indirizzo, telefono)
- il riferimento ad un documento di identità valido (tipo di documento, numero e data di emissione)
- il codice di iscrizione all'albo dei periti del Tribunale
- i riferimenti all'oggetto della perizia e ai dati identificativi del committente
- la descrizione delle attività peritali svolte
- le verifiche tecniche effettuate e le conclusioni raggiunte
- è conveniente che le pagine siano numerate nella forma pag. __ di __
- Il luogo, la data e la firma leggibile del perito
- il verbale del giuramento su modulo specifico disponibile nel Tribunale interessato; il verbale deve essere datato e firmato
- seguono, come allegati, i documenti a giustificazione delle conclusioni raggiunte (tabelle di calcolo, fotografie, disegni, schemi di flusso, immagini, riferimenti esterni, ecc.)

Tutte le pagine costituenti la perizia e gli allegati devono essere firmati dal perito ed

eventualmente timbrati nel caso il perito sia in possesso di un suo timbro personale.
Sulle pagine componenti la perizia devono essere apposte delle marche da bollo da euro 14,62 partendo dal primo foglio e successivamente ogni centesima riga del testo della perizia.
Anche sul verbale di giuramento deve essere applicata una marca da bollo da euro 14,62.
Per ciascun allegato si applica una marca da euro 0,52.
Le pagine costituenti la perizia e gli allegati devono presentarsi in forma di fascicolo con fogli non rimovibili (graffati con cucitrice o termo saldati).
Il perito deve presentarsi personalmente davanti al Cancelliere e deve esibire il documento di identità citato nel testo della perizia e nel verbale di giuramento consegnando il fascicolo della perizia e degli allegati al Cancelliere
il Cancelliere, previa ammonizione sulla responsabilità penale (art.483 c.p.) derivante da dichiarazioni mendaci, può richiedere al perito di ripetere a voce la formula di giuramento normalmente presente nel verbale di giuramento: *Giuro di avere bene e fedelmente adempiuto all'incarico affidatomi al solo scopo di far conoscere la verità*.
Il Cancelliere *protocolla* la perizia e si accerta che sia apposto il timbro della cancelleria sulle congiunzioni dei fogli componenti la perizia e su tutte le marche da bollo.
La perizia è poi riconsegnata al perito.
Le avvertenze sopra descritte potrebbero variare da Tribunale a Tribunale soprattutto per le modalità dell'apposizione di timbri / firme e di conteggio delle linee di testo / numero di pagine.

Esempio di perizia asseverata / giurata

Il sottoscritto Dott. Roberto Bello nato a Milano il XX/XX/XXXX C.F. xxxxxxxxxxxxxxx domiciliato in via yyyyyyyyy xx – 20124 Milano, tel. Xxxxxxxxxx, iscritto all'Albo dei Periti (settore Informatica) del Tribunale di Milano al N° 9999 e all'Albo dei Periti Estimatori della Camera di Commercio di Milano, incaricato da ABC srl (di seguito citata come ABC) con sede in Milano (Mi), via xxxxxxxxxxx Partita IVA 00000000000, esterno alla Ditta stessa,

ATTESTA

con perizia asseverata a giuramento quanto segue:

La società ABC, sta presentando domanda ai fini delle agevolazioni previste nella legge 488 del 19/12/1992.
Il sottoscritto perito estimatore, considerando l'articolo 8 del decreto del Ministero delle Attività Produttive di concerto con il Ministero dell'Economia e delle Finanze del 1° febbraio 2006, comma 11, lettera b.5 che recita: *"piattaforme e tecnologie digitali per la gestione dei sistemi di interfaccia e transazione con clienti e fornitori e correlati servizi per la realizzazione o la personalizzazione di applicazioni informatiche a supporto dell'utilizzo delle predette piattaforme e tecnologie"*, ha esaminato la proposta di investimento preparata da ABC con particolare attenzione ai punti che seguono.

1. Applicazione

SistemaXY è un'applicazione software che permette la gestione del processo di Pianificazione e Controllo degli Obiettivi secondo le modalità e le logiche organizzative in uso nella Pubblica Amministrazione.
Il cuore dell'applicazione è costituito da una componente Server (centrale), funzionante presso ABC, e da una componente Client (presso gli utilizzatori) scaricabile, entrambe necessarie congiuntamente per l'erogazione del servizio.
….....
….....
….....
Per quanto previsto nel progetto il sottoscritto perito rileva la caratteristica fortemente innovativa dell'applicazione poiché essa consente all'organizzazione o pubblica amministrazione una fruizione condivisa e cooperativa delle informazioni rendendo la stessa applicazione rispondente ai requisiti richiesti al punto b.5 del decreto ministeriale del 1° febbraio 2006 prima citato.
L'applicazione progettata è tecnicamente descrivibile come sistema funzionante in Internet, usando un semplice browser, per la pianificazione, consuntivazione e controllo di progetti che vedono coinvolte risorse finanziarie e di attività amministrativa. Le tecnologie che si intendono applicare sono quanto di più aggiornato attualmente disponibile sia per ciò che attiene l'utilizzo degli ambienti di sviluppo sia per le macchine e i dispositivi hardware e di rete che si intendono installare.
L'applicazione presenta inoltre ottime caratteristiche di *scalabilità*

(dimensionamento variabile) consentendo di essere utilizzata anche da organizzazioni ed enti pubblici di modeste dimensioni.
Le tecnologie che si intendono applicare, pur essendo innovative, danno ampie garanzie di affidabilità e di sicuro buon funzionamento quando sarà operativa l'applicazione progettata.

Il sottoscritto perito ha esaminato le pagine (da 14 a 19) del Business Plan descrittivo del progetto, che contengono le caratteristiche tecnico-funzionali dell'applicazione e ne apprezza i contenuti non avendo nulla da rilevare di negativo.

2. Hardware, software di sistema e servizi di rete

- Server HP PL DL585R : 4Processori AMD 2.4 DUAL CORE 8GB Ram
- Hard Disk 145.6GB SCSI Ultra 320, 15KRPM UNIVER. HOTPLUG
- HP MSA1000 Kit SAN
- Hard Disk 300GB U320 10KRPM UNIVER. HOTPLUG
- …..
- …..
- …..
- …..

Il sottoscritto perito segnala che l'hardware, il software di sistema e i servizi di rete sono tutti adeguati e necessari per la realizzazione e la gestione dell'applicazione oggetto del progetto.
L'hardware, il software di sistema e i servizi di rete sopra elencati sono quanto di più attuale ora disponibile sul mercato e a priori consentono di garantire un funzionamento non degradabile dell'applicazione per almeno i prossimi cinque anni.

In conclusione, il sottoscritto perito, sulla base dell'analisi delle caratteristiche tecniche degli investimenti sopra descritti,

ATTESTA

la rispondenza ai requisiti richiesti al punto b.5 del decreto ministeriale del 1° febbraio 2006 prima citato dei seguenti investimenti previsti:

DESCRIZIONE DEGLI INVESTIMENTI INNOVATIVI	Valore (KEU)
Macchinari	**0**
APPLICATION SERVER ASP TREND composto da	0
Library manager (moduli per la gestione del modello organizzativo, per la gestione del modello dei dati, per la gestione della struttura delle azioni)	0,0
Sistema XY Web Trend (moduli per la definizione iniziale dei	0,0

DESCRIZIONE DEGLI INVESTIMENTI INNOVATIVI	Valore (KEU)
progetti, approvazione e blocco progetti, modifica progetti bloccati, consuntivazione)	
PLUG-IN TREND DONWLOADABLE composto da	0
Modulo per il monitoraggio	0
Modulo per la reportistica personalizzata	0
Modulo di stampa	0
Impianti	**00,0**
N.2 SERVER UNIX (LOAD BALANCED, MIRRORED) composti da	00,0
n.2 Server HP PL DL585R : 4Processori AMD 2.4 DUAL CORE 8GB Ram	00,0
n.4 Hard Disk 145.6GB SCSI Ultra 320, 15KRPM UNIVER. HOTPLUG	0,0
……	
……	
Software	**0**
SOFTWARE DI GESTIONE ED OTTIMIZZAZIONE DI RETE E DI SERVIZIO composto da	0
Red Hat Enterprise Linux AS	0
Software Cluster Linux	0
……	0
Oracle - Internet Application Server Standard Edition - 1 Processor License - Full - Durata Perpetua - Release 9i,10g	0
Totale Investimenti innovativi	**XXXXXX**

Il valore complessivo di questi investimenti innovativi è quindi pari a XXXXXX Euro, rispetto ai YYYYYY Euro di investimenti complessivi previsti dal programma.

Milano, 13 Settembre 20xx

Dott. Roberto Bello

Firma ……

Allegati: AAAA, BBBB, CCCC

Appendice: La sicurezza informatica nelle Imprese e nella Pubblica Amministrazione

Regolamento interno per dipendenti e collaboratori

Premessa

La sicurezza del sistema informativo richiede che siano fissate delle regole per l'uso del computer.
Dare sicurezza al sistema informativo significa proteggere le informazioni dai possibili danni al fine di assicurare la continuità operativa dell'organizzazione, minimizzando i rischi di gestione e massimizzando il ritorno degli investimenti e delle opportunità d'impresa.
La sicurezza del sistema informativo si migliora mettendo in essere gli opportuni controlli, procedure, regolamenti, adeguamenti delle strutture organizzative ed attivando gli opportuni strumenti di hardware e di software.
La sicurezza del sistema informativo si riferisce a tre diversi aspetti:

- riservatezza, intesa come prevenzione contro l'accesso non autorizzato ai dati e ai programmi
- integrità, intesa come protezione contro le alterazioni dei dati e dei programmi per eventi naturali o per comportamenti dolosi / colposi delle persone
- disponibilità, intesa come fruibilità dei dati e dei programmi da parte degli utenti autorizzati con conseguente esclusione degli utilizzatori non autorizzati e degli estranei

Per la sicurezza del sistema informativo è necessario porre in essere:

- procedure, regolamenti, mansionari
- corsi di formazione e di aggiornamento tecnologico
- modifiche alla struttura dell'organizzazione e ai compiti individuali delle persone
- sistemi hardware di controllo, di salvataggio e di ripristino della continuità elaborativa
- sistemi software di controllo, di autorizzazione all'accesso, di salvataggio e di ripristino della continuità elaborativa
- periodiche ispezioni al sistema informativo atte ad individuare aree di possibili danni potenziali ponendovi poi i preventivi necessari rimedi

E' importante notare che tutte le azioni che l'organizzazione ha intenzione di porre in essere per il miglioramento della sicurezza del sistema informativo devono rispettare le norme in vigore in relazione alla privacy dei dipendenti e agli altri loro diritti previsti dallo statuto dei lavoratori oltre al rispetto delle norme cogenti in merito al DPS (Documento Programmatico sulla Sicurezza).
I controlli preventivi e quelli continui sull'uso degli strumenti informatici devono garantire sia il diritto del datore di lavoro di proteggere la propria organizzazione (essendo i computer aziendali strumenti di lavoro per i quali l' utilizzazione a titolo personale è preclusa o perlomeno molto limitata), sia il diritto del lavoratore a non

vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sancito dallo Statuto dei Lavoratori (L. 300/70) e dal D.lgs 196/03 sulla tutela e protezione di dati personali.
Il rispetto dei diritti dei lavoratori ha conseguenze rilevanti nella scelta degli strumenti e nelle modalità per la garanzia della sicurezza del sistema informativo con la complicazione che il tema della sicurezza informatica, sebbene di stretta attualità, non è ancora stato oggetto di una regolamentazione giuridica che lo disciplini compiutamente in maniera organica.
In attesa che si definiscano i confini normativi per un corretto rapporto tra tecnologia, impresa e lavoro, al momento tocca al buon senso interpretare ed individuare il punto di equilibrio tra il diritto del lavoratore al rispetto della propria sfera privata e quello del datore di lavoro di controllare l'attività del dipendente, per evitare danni o illeciti, siano essi di natura colposa o dolosa.
Infatti non tutto ciò che è tecnicamente possibile è anche giuridicamente legittimo.
La diffusione delle nuove tecnologie informatiche, con particolare riferimento all'accesso ad Internet dai Personal Computer, può esporre l'Azienda / Organizzazione ai rischi sia di contenzioso civile sia di rilevanza penale; per tale considerazione l'Azienda / Organizzazione si può tutelare emanando un opportuno regolamento interno da far sottoscrivere ai dipendenti e ai collaboratori.
Dal web: *23.5.2008-Lo statale che naviga troppo sul web e scarica su archivi personali materiale non legato al suo lavoro rischia la sospensione dal posto di lavoro. Un comportamento di questo tipo, infatti, dice la Cassazione, può configurare il reato di peculato punito al pari delle telefonate private fatte dall'ufficio. Applicando questo principio, la Sesta sezione penale ha accolto il ricorso della Procura di Bari contro la revoca della sospensione dall'esercizio di pubblico servizio accordata a un dipendente del comune di Trani, Maurizio D.A., pizzicato a servirsi «del computer d'ufficio, cui era collegato un masterizzatore dvd, per uso personale usufruendo della rete informatica del comune».*
L'impiegato comunale, ricostruisce la sentenza 20326, «navigava in internet su siti non istituzionali, scaricando su archivi personali dati e immagini non inerenti alla pubblica funzione, prevalentemente materiale di carattere pornografico, con danno economico dell'ente».
Indagato per peculato, l'impiegato comunale era stato prima sospeso dal Tribunale di Trani, aprile 2007, e riammesso dal Tribunale di Bari, un mese dopo, sulla base del fatto che il reato di peculato «tutela il patrimonio della P.A. e che lo stesso non poteva essere depauperato a seguito dei collegamenti in questione di un computer comunque e sempre collegato alla rete elettrica e telefonica indipendentemente dall'uso della navigazione».

Regolamento interno per la sicurezza del sistema informativo

Nel seguito si fa riferimento ad una ipotetica Azienda / Organizzazione di seguito nominata "ABC"
Premesso che l'utilizzo delle risorse informatiche di ABC deve sempre ispirarsi a comportamenti di diligenza, di correttezza e di sicurezza, comportamenti che normalmente si usano nell'ambito di un rapporto di lavoro, ABC dichiara che il

presente regolamento interno è diretto ad evitare che comportamenti consapevoli o inconsapevoli possano innescare problemi o minacce alla sicurezza, alla gestione e alla memorizzazione dei dati, coinvolgendola in cause civili o in denunce penali.
Il mancato rispetto o la violazione delle regole contenute nel presente regolamento costituisce inosservanza delle disposizioni al personale e può essere quindi oggetto di provvedimenti disciplinari ai sensi della vigente normativa contrattuale,nonché nei casi più gravi di azioni civili e/o penali, ove consentite, nei confronti del trasgressore.
Il presente Regolamento è consegnato a tutti i dipendenti e collaboratori.

Responsabile del Sistema Informativo

Il Responsabile del Sistema Informativo, esclusivamente per l'espletamento delle funzioni a lui riservate per il salvataggio e il ripristino dei dati, ha la facoltàdi accedere agli archivi trattati da ciascun utilizzatore di computer, ivi compresi gli archivi di posta elettronica interna ed esterna.
Il Responsabile del Sistema Informativo non ha la facoltà di accedere alle informazioni contenute nei messaggi di posta elettronica degli utenti pur potendo revocare la password dell'utente previa comunicazione al diretto interessato.
Il Responsabile del Sistema Informativo può, in qualunque momento, procedere alla rimozione di ogni archivio o applicazione che ritenga siano pericolosi per la sicurezza sia sui personal computer degli utenti sia sulle unità di rete, informandone gli utenti interessati.

Utilizzo del personal computer

Il dipendente è responsabile del personal computer assegnatogli in utilizzo; deve custodirlo e usarlo con diligenza e professionalità.
Il personal computer affidato al dipendente è uno strumento di lavoro.
Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
Il personal computer deve essere spento ogni sera prima di lasciare gli uffici ed ogni qual volta ci sia la necessità di allontanarsi dal posto di lavoro per un tempo superiore a un'ora.
Lasciare inutilmente acceso un computer non in utilizzo, oltre a costituire un potenziale rischio di incendio, rappresenta anche un'inutile spreco di energia elettrica con conseguente aggravio di costi ed inutile danno all'ambiente.
I personal computer devono essere sempre disponibili per eventuali interventi di manutenzione e l'utente non può impedire che l'addetto alla manutenzione intervenga allo scopo.

Parole di accesso (password)

L'accesso al personal computer è protetto da password per impedire gli accessi non autorizzati, password che devono essere custodite dal dipendente con la massima diligenza; devono essere mantenute personali e segrete.
Qualora un dipendente venisse a conoscenza delle password di altro dipendente, è tenuto a darne immediata notizia alla Direzione o alla persona dalla stessa

incaricata (Responsabile del Sistema Informativo).
Le password devono essere utilizzate per l'accesso alla rete, per l'accesso a qualsiasi applicazione che lo preveda, per il salvaschermo (*screen saver*) e per il collegamento senza restrizioni ad Internet.
Le password personali devono avere una lunghezza di almeno 8 caratteri e devono essere rinnovate almeno ogni 6 mesi.
Le password devono essere formate da sequenze di caratteri e di numeri senza alcun senso compiuto; sono da evitare date di compleanno, di onomastico, nomi di mogli, figli, fidanzate, animali domestici, squadra del cuore, ufficio di appartenenza, mese e anno corrente e di quant'altro possa essere facilmente associabile alla persona del dipendente o all'ambiente di lavoro.
In caso di assenze prolungate dall'ufficio è obbligatorio bloccare il personal computer attivando il salvaschermo (*screen saver*) con l'opzione di richiesta di password per il ritorno all'operatività normale.
Lasciare un computer incustodito e non protetto da accessi indesiderati può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provare in seguito l'indebito uso.
Per i pc portatili (notebook e netbook), data la relativa facilità del loro smarrimento (o furto), è obbligatorio utilizzare la password di accensione per prevenire che estranei possano facilmente accedere ai dati contenuti nel disco fisso, dati che possono avere un valore di gran lunga superiore a quello del personal computer e dei programmi installati sullo stesso.
I pc portatili utilizzati all'esterno, quando non vengono utilizzati, devono essere custoditi in un luogo sicuro e protetto.

Anti virus e programmi anti intrusione

I personal computer sono protetti da appositi programmi anti virus e anti intrusione. E’ proibito disinstallare o disattivare anche solo temporaneamente i programma anti virus e anti intrusione.
Violazioni a questa regola possono causare seri danni al personal computer e a quelli ad esso collegati.
Ogni dipendente deve essere particolarmente attento agli archivi, ai messaggi di posta elettronica, e agli altri documenti informatici ricevuti dall’esterno, avvertendo immediatamente il Responsabile del Sistema Informativo nel caso in cui siano stati rilevati dei virus e nel caso il personal computer sia diventato particolarmente lento o dimostri dei comportamenti anomali (mouse mal funzionante, spegnimento inatteso, aperture di *finestre* non richieste, programmi che smettono di funzionare, ecc.).
Se l'anti virus non fosse in grado di ripulire il documento infetto si deve:

- sospendere ogni elaborazione in corso senza spegnere il computer
- isolare il computer dagli altri eventualmente collegati per evitare la diffusione dell'infezione attraverso la rete locale interna

Internet

Possono collegarsi ad Internet solo i dipendenti a ciò autorizzati.

ABC ha la facoltà:

- di controllare, con strumenti software, che possano collegarsi ad Internet solo i dipendenti autorizzati
- di controllare, con strumenti software, che i dipendenti autorizzati accedano ai soli siti inclusi nella lista dei siti autorizzati da ABC
- in mancanza di strumenti software L'Azienda ABC potrà informare i dipendenti quali siano le persone autorizzate e quali siano i siti autorizzati alla navigazione.

Valgono comunque i seguenti principi:

- è proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.
- è vietato scaricare software gratuito (*freeware* o *shareware*) o commerciale prelevato da siti Internet o con strumenti *peer to peer* (condivisione di archivi)
- è tassativamente vietata l'effettuazione di ogni genere di transazione Giudice finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili che non siano autorizzati dalla Direzione o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto
- è da evitare ogni forma di registrazione a siti i contenuti dei quali non siano legati all'attività lavorativa
- sono attività vietate la partecipazione a forum non professionali, l'utilizzo di *chat line* (esclusi gli strumenti autorizzati), l'uso di bacheche elettroniche e l'effettuazione di registrazioni in libri dei visitatori (*guest books*) anche utilizzando pseudonimi (*nicknames*), se non attinenti l'attività lavorativa svolta
- non è consentito usare il computer e l'accesso ad Internet per connettersi a siti di *social network* (*Facebook* e simili) fatte salve le eventuali specifiche autorizzazioni della Direzione
- non è consentita la navigazione in siti ove sia possibile conoscere le opinioni politiche, religiose o sindacali delle persone
- non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura pornografica e/o oltraggiosa e/o discriminatoria per sesso / etnia / religione / opinione e/o appartenenza sindacale e/o politica
- non è consentito accedere a siti di giochi d'azzardo e a quelli di condivisione di archivi musicali e di video (*peer to peer*)

ABC, in alcun modo, non farà esami sui siti effettivamente visitati dai dipendenti siano i siti autorizzati o meno .

Si ricorda che la navigazione in Internet non è assolutamente anonima.

La semplice visualizzazione di una pagina web comporta l'inserimento automatico in una certa serie di LOG mantenuti dalle varie macchine tra cui l'eventuale LOG del *proxy server* di ABC dal quale è effettuata la connessione, dal LOG del *provider* Internet che fornisce la connessione ad Internet ed infine dal LOG del sito internet consultato.

La navigazione è quindi tracciata da parecchie macchine potendo così risalire al computer e all'utente in navigazione nella tal pagina, il tal giorno e la tal ora.

Sono tutti LOG automatici raccolti solo per eventuali problemi di ordine giudiziario: in caso di attività illegali svolte su Internet, la Polizia Postale, dietro autorizzazione

del Giudice, può richiedere l'accesso ai LOG dei vari provider e verificare da quale connessione internet risulti essere stato generato il traffico.
ABC, si riserva di attivare in qualsiasi momento e senza ulteriori comunicazioni agli utenti, un servizio di memorizzazione dei LOG del *proxy server* al solo fine di avere la possibilità di risalire al dipendente che ha effettuato eventuali attività illecite su Internet, in caso di indagini svolte dalla magistratura a carico di ABC.
Non ci sono altre finalità nella raccolta di questi LOG da parte di ABC e non sono previsti strumenti per la visualizzazione e l'analisi di detti LOG.
I LOG sono archiviati con periodicità mensile e sono conservati per un periodo di 2 anni su CD-R, trascorso tale periodo i CD-R saranno distrutti.
I metodi alternativi per accedere ad Internet dalla sede di ABC, ad esempio mediante modem, *wireless* e cellulari connessi al computer aziendale,sono tassativamente vietati per seri problemi di sicurezza.

Hardware, software e memorizzazione dei dati

Non è consentito all'utente:

- apportare modifiche all'hardware (aggiungere e/o togliere dispositivi, schede, periferiche, ecc.)
- apportare modifiche al software di sistema ed applicativo (aggiungere, modificare, togliere) sistemi operativi e/o programmi applicativi anche se di tipo *open source*
- memorizzare archivi non inerenti l'attività lavorativa
- memorizzare brani musicali o filmati che siano una violazione alla normativa sul diritto di autore
- memorizzare documenti informatici di natura pornografica e/o oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica
- salvare i documenti in forma crittografata , salvo esplicite deroghe
- salvare archivi nei formati AVI, MPEG, DIVX, XVID, MP3 ecc. che contengano copie di film o brani musicali, escludendo i casi autorizzati esplicitamente e cioè quando questo materiale risulti auto prodotto (esempio corso interattivo) e del quale si possa dimostrare l'effettiva titolarità dei diritti.

Valore dei dati e furto di identità

Molto spesso gli utenti non danno importanza alle informazioni memorizzate nel computer portatile o nel palmare.
Raramente si pensa alle conseguenze derivanti dal furto del portatile e della conseguente perdita dell'identità.
Molto spesso sul portatile esiste un archivio (password.txt, password.doc, password.xls e simili), non protetto e che contiene tutte le password necessarie per l'accesso ad Internet e alle diverse applicazioni, ma anche alle carte di credito, ai collegamenti alle banche *on-line*, al collegamento all'impianto di allarme, alle caselle della posta elettronica, alle sim dei cellulari, ecc.
Nel caso di furto, il malintenzionato si trova in mano un oggetto con cui può connettersi ad Internet con un'identità rubata, svolgere attività illegali su Internet,

inviare mail oltraggiose il tutto sfruttando l'identità dell'utente al quale è stato rubato il portatile.
Il problema quindi va oltre il semplice danno economico e la sottrazione di qualche archivio; è la perdita dell'identità che deve destare le maggiori preoccupazioni.
L'utente deve quindi essere coscienzioso e salvare sempre, in modo ordinato e ben organizzato, le password di tutti i servizi ai quali ha accesso per potere sempre in qualsiasi momento ricollegarsi e cambiare tutte le password, se avesse qualche dubbio che la riservatezza sia venuta meno.
Ovviamente queste informazioni non devono essere conservate sul portatile; molto meglio ricorrere al sempre valido supporto della carta e della matita, conservando poi il foglio cartaceo scritto dove si vuole, ma non nella borsa del portatile.

Software installato

Il software per elaboratori e' considerato opera di ingegno e come tale è tutelato dalle leggi sul diritto di autore.
L'utilizzo del software è regolamentato da licenze d'uso che devono essere assolutamente rispettate da tutti. (DLG. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).
Non è consentito l'utilizzo di programmi diversi da quelli distribuiti ufficialmente da ABC, perché in caso contrario potrebbero verificarsi l'eventualità di portare nel computer virus informatici con effetti negativi anche sulla stabilità delle applicazioni del computer, applicazioni per le quali ABC possiede le regolari licenze di utilizzo.
E' vietato installare il software contenuto nei vari CD ROM distribuiti con le riviste, con i libri e con i quotidiani, anche se si tratta di software allegato a riviste del settore di ABC.
Non è ammesso l'uso di strumenti atti a catturare o rivelare le password *(password crack, keylogger*, ecc.) per accedere in modo non autorizzato a dati, sistemi, programmi (ad esempio al fine di poter poi rendere il programma copiabile ed installabile su un altro computer violando, in tal modo, i diritti a tutela del copyright).
Inoltre un programma al quale sia stata rimossa la protezione (*crackato*), oltre a costituire una violazione alle norme che regolano il diritto d'autore, costituisce anche un'autentica minaccia alla sicurezza e all'affidabilità dei computer.
Lo sblocco del programma (*cracking*) viene infatti effettuato modificando i codici originali del programma per aggirarne le protezioni sostituendo pezzi del programma originale con parti modificate; queste sostituzioni, oltre ad aggirare le originali protezioni, possono anche introdurre del codice dannoso in grado di compromettere il funzionamento del computer interessato e dei sistemi ad esso collegato.
Non sono ammesse condivisioni di risorse locali (dati e programmi) tra i singoli personal computer.
Costituisce buona regola la pulizia periodica degli archivi, con cancellazione dei file obsoleti o inutili.
Particolare attenzione deve essere prestata alla duplicazione dei dati; è infatti assolutamente da evitare un'archiviazione ridondante, fatta eccezione degli archivi di salvataggio (*backup*).
Se su un computer in uso agli utenti venisse trovato, a cura del Responsabile del

Sistema Informativo o di altri responsabili della sicurezza, un programma per la connessione a reti *peer to peer* (*napster, winmx, deluge, emule, bittorrent, azureus*, ecc.) o un programma di messaggistica istantanea (*messanger, icq*, ecc.) il fatto costituirebbe una grave violazione delle regole aziendali.

Stampe e supporti magnetici/ottici

Le stampe dimenticate o i dati memorizzati su supporti rimovibili possono spesso costituire un'involontaria fuga di notizie.
Si deve usare la massima attenzione nell'utilizzo delle stampe e dei diversi dispositivi di memorizzazione con particolare riferimento alle opportune modalità di distruzione dei documenti e dei supporti di memorizzazione che non servono più.
L'utente deve effettuare la stampa dei dati solo se strettamente necessaria, ritirandola prontamente dai vassoi delle stampanti comuni.
E' vietato portare fuori dall'azienda tabulati, stampe, supporti di memorizzazione sia magnetici sia ottici salvo esplicita autorizzazione della Direzione.
Qualsiasi CD, DVD o floppy disk prodotto all'interno di ABC deve obbligatoriamente essere realizzato mediante i supporti ufficiali di ABC.
Tutti i supporti magnetici e/o ottici (dischetti, cassette, CD-R, CD- RW, DVD-R, DVD-RD) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato o cadere in mano a terzi non autorizzati (art. 7 del DPR 318/99).
Sono considerati equivalenti ai dati sensibili, i dati importanti / vitali di ABC come ad esempio i dati relativi a clienti, fornitori, ricette, costi, margini lordi, ricavi, redditi, schede di produzione, progetti in sviluppo, budget e piani, ecc.
La semplice cancellazione dei supporti non garantisce l'effettiva eliminazione dei dati in essi memorizzati; una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro apparente cancellazione; per tale motivo i supporti di memorizzazione contenenti dati sensibili (o importanti / vitali) e considerati ormai obsoleti devono essere consegnati al Responsabile del Sistema Informativo che provvederà alla loro adeguata distruzione.
I supporti magnetici o tabulati, contenenti dati sensibili (o importanti / vitali) devono essere custoditi in archivi chiusi a chiave come prescritto dalla Legge sulla tutela dei dati personali.
Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, nastri magnetici, penne USB di provenienza esterna e/o ignota.
In caso se ne preveda l'utilizzo, ogni dispositivo magnetico di provenienza esterna all'azienda e/o ignota dovrà essere verificato mediante il programma anti virus prima del suo utilizzo e, nel caso sia rilevato un virus, il dispositivo magnetico dovrà essere consegnato al Responsabile del Sistema Informativo.

Posta elettronica

La casella di posta, assegnata dall'Azienda ABC all'utente, è uno strumento di lavoro e come tale non deve essere usato a fini diversi rispetto alla normale attività lavorativa evitando messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili

e soprattutto gli allegati ingombranti che siano già stati spostati nelle cartelle destinatarie di interesse.
E’ vietato utilizzare l’indirizzo della posta elettronica aziendale, nel formato previsto nome.cognome@abc.it, per l’invio di messaggi personali o per la partecipazione a dibattiti, *forum* o *mailinglist*, salvo diversa ed esplicita autorizzazione da parte della Direzione. E' importante comprendere che un messaggio di email inviato con un indirizzo di posta aziendale è in qualche modo assimilabile ad una lettera su carta intestata di ABC.
La partecipazione ad un *forum* su Internet con un indirizzo aziendale potrebbe trarre in inganno gli altri utenti che, vedendo il nome del dominio,potrebbero supporre che questo sia un parere / comunicazione ufficiale di ABC e non un semplice messaggio personale di un suo dipendente.
Questo potrebbe avere anche conseguenze in termini di immagine per ABC.
E' vietato dare seguito alle catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicare immediatamente la circostanza al Responsabile del Sistema Informativo.
Non si devono, in alcun caso, accedere agli allegati di tali messaggi.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per ABC, oppure contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura riservata o da analoga dicitura, deve essere visionata od autorizzata dalla Direzione.
E’ vietato utilizzare i dati identificativi di un altro dipendente (*login / password*) per accedere alla sua posta elettronica anche in sua assenza.
Per avere la conferma dell’avvenuta lettura del messaggio da parte del destinatario è possibile ottenere per via informatica, nelle comunicazioni esterne all’azienda, la ricevuta di ritorno oppure si può chiedere al destinatario di confermare l'avvenuta lettura.
La tendenza in atto è di ricorrere alla Posta Elettronica Certificata (*PEC*) che, rispetto alla normale email, offre maggiori garanzie di certezza della fonte e del corretto inoltro al destinatario.

Violazioni al regolamento interno per la sicurezza del sistema informativo

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari dando anche seguito alle eventuali azioni consentite in ambito civile e penale.

Luogo e data .....

DIPENDENTE / COLLABORATORE ABC la Direzione

..... ….....

RAPPRESENTANTE SINDACALE (eventuale) …..

Indice generale