RELAZIONE TECNICA

DOTT. XXXX XXXX

Nell'interesse di Paola Rossi

RELAZIONE TECNICA

del Consulente Tecnico di Parte nell'interesse di Paola Rossi

* * *

Il sottoscritto, **dott. XXXX XXXX**, in ordine all'incarico conferito da Paola Rossi

RILEVA ED ESPONE

il presente elaborato si pone il fine di evidenziare la presenza di tracce informatiche compatibili con la condotta di chi abusa delle proprie credenziali di accesso per consultare ed eventualmente copiare dati riservati aziendali, non pertinenti alle sue mansioni.

Inoltre, questo documento costituisce un insieme di considerazioni tecniche utili per apprezzare in primis l'attendibilità della documentazione prodotta dalla medesima AziendaX, nonché la rilevanza della documentazione attestante la conformità di AziendaX a ben precisi standard di sicurezza ed organizzativi, considerato che per l'azienda i dati rappresentano un patrimonio fondamentale, derivandone che la protezione di tale patrimonio diventa la condizione irrinunciabile per lo sviluppo e la buona riuscita delle proprie attività.

ASPETTI PRELIMINARI

L'AZIENDA AZIENDAX

I servizi e le consulenze erogate da AziendaX sono relative alla verifica di qualità del sottosuolo di siti inquinati ed alla progettazione di interventi di bonifica. Le attività sono svolte per clienti che necessitano di adeguare la qualità del sottosuolo ai limiti previsti dalla normativa.

I documenti prodotti da AziendaX per i propri clienti sono custoditi presso un file server aziendale, presso le sedi dei clienti che li hanno commissionati e presso gli uffici della Pubblica Amministrazione dove sono consegnati per le relative procedure: per quanto verrà esposto fin da ora è possibile affermare che non ci sono ragioni per cui tali documenti debbano essere presenti in altri luoghi o su altri computer.

La riservatezza dei documenti di AziendaX e le procedure di accesso da parte di terzi

Data la sensibilità dei dati ed argomenti trattati - che riguardano l'inquinamento del sottosuolo - e le delicate conseguenze connesse, l'accesso a tali documenti non è semplice e l'eventuale consultazione da parte di terzi è concessa dalla P.A. in conformità al DPR 184/2006 solo in casi motivati e solo a parti interessate. In ogni caso, l'accesso agli atti è soggetto a specifica procedura avviabile mediante idonea modulistica.

Dunque, qualora una parte interessata intenda accedere ad un documento, l'Ente che riceve la richiesta avvia una procedura di richiesta di accesso agli atti ed inoltra una comunicazione al cliente di AziendaX per salvaguardare il diritto di questi ultimi di conoscere chi ha fatto la richiesta di accesso e per rendere note le ragioni che motivano tale richiesta. Nell'ambito di tale procedura il cliente di AziendaX può opporsi alla diffusione di tutto o parte del documento richiesto argomentandone le ragioni.

Infine è garantito il diritto al cliente di AziendaX di conoscere le decisioni dell'Ente in merito alla decisione finale della P.A. di concessione dell'accesso agli atti.

Inoltre la necessità della riservatezza dei documenti (in particolare email e file trasmessi in allagato) era precisata anche nella firma automatica impostata nei client di posta elettronica che riporta il seguente formato e contenuti:

```
XXXXX - AziendaX
Via XXXX 10 - 00100 XXXX - Italy
Azienda certificata ISO 9001:2000 e ISO 14001:2004

P.IVA - VAT nr: IT02398401204
Tel: +39 051 7457013
Fax: +39 051 3762637
_____________________________

This email and any files transmitted with it are confidential.
It is for the intended recipient only. If you have received
the email in error please notify the author by replying to
this email. If you are not the intended recipient, you must
not disclose, distribute, copy, print, or rely on this email.
The administrative e-mail of Ecosurvey is: admin@ecosurvey.it
```

IL RUOLO DI MICHELA VERDI IN AZIENDAX

Prima di procedere alla descrizione dei dati informatici rinvenuti all'interno dell'hard disk analizzato, è opportuno precisare il ruolo della ex collaboratrice Michela Verdi (di seguito Verdi, ndr) all'interno di AziendaX all'epoca dei fatti ripercorrendo alcune email che sono transitate dal suo account di posta elettronica.

Francesco Azzurro inviava a Verdi un'email il 22.04.2009 con indicata la necessità di terminare i progetti a lei assegnati e di valutarne altri. Dopo altre proposte di collaborazione inviate ricevute da Verdi in data 27.04.2909 e 07.05.2009 per progetti da svolgere in AziendaX, in data 13 maggio 2009 Verdi comunicava a mezzo email che avrebbe interrotto il rapporto lavorativo con AziendaX a partire dal giorno 21 giugno 2009.

A fronte di tale comunicazione, all'interno di AziendaX sono state svolte diverse riunioni allo scopo di riorganizzare i compiti in seguito all'uscita della Verdi, oltre a definire il ruolo a lei spettante nel periodo fino alla data del 21 giugno 2009.

In particolare, in data 20 maggio 2009 è stata svolta una riunione alla quale è seguita una mail spedita da Marco Bianchi a Verdi in data 29 maggio 2009: in tale mail era evidenziato che Verdi si sarebbe occupata di portare a termine i progetti Pincopallino relativamente ai siti di Bari, Cagliari e Firenze mentre non si sarebbe più dovuta occupare dei siti Genova, Milano e Napoli. Tale circostanza è documentabile con la seguente email.

Figura 1 - Email con note riassuntive della riunione del 20 maggio 2009

Alcuni giorni dopo, in data 5 giugno 2009, lo stesso Bianchi inviava una mail a Verdi contenente un verbale di una riunione del 28 maggio 2009.

Figura 2 - Email con bozza del verbale della riunione del 28 maggio 2009 da completare

Il file del verbale è stato rinvenuto tra i file temporanei aperti con il client di posta elettronica, quale conferma che Verdi ha effettivamente aperto il file.

Figura 3 - File del verbale da completare aperto da Verdi

L'apertura del file è stata seguita molto probabilmente dalla compilazione di parte dei contenuti del documento che alla fine appariva come di seguito mostrato.

Figura 4

<u>Dalla lettura del documento emerge come tutti i progetti seguiti dalla Verdi fossero chiusi o, in alcuni casi, a breve consegna.</u>

INFORMAZIONI FORNITE DA PAOLA ROSSI ALLA POLIZIA POSTALE

In data 10 settembre 2009, Paola Rossi presentava una denuncia-querela consegnando l'hard disk del personal computer (lo stesso oggetto di analisi della presente relazione) assegnato a Verdi, segnalando:

- "comportamenti inusuali" di Verdi che "portava con sè e collegava continuamente al personal computer, dalla stessa utilizzato per lo svolgimento della attività lavorativa, un apparecchio per la registrazione e la riproduzione di files musicali nonché utile al trasferimento di dati di qualsivoglia genere che, al suo interno, conteneva una memoria di tipo fisico di elevata capacità e denominato apple i-pod.";

- che Verdi “operava tramite un personal computer da lei esclusivamente utilizzato e collegato ad un sistema di storage di dati rappresentato da un hard disk connesso alla rete locale e contenete documentazione riservata, brevetti e dati relativi ad aziende per le quali erano e sono in corso delicate attività di consulenza ambientale”;
- che il tecnico informatico “ha posto attenzione nella cartella denominata “documenti recenti” e di aver reperito all’interno di detta cartella diversi documenti ai quali la stessa Verdi Michela non doveva, nel periodo sopra indicato, in maniera assoluta accedere poiché non rientravano all’interno delle sue competenze come stabilito per mezzo di atto aziendale interno (verbale di riunione).

[…..]

[…..]

[…..]

ANALISI FORENSE

ACQUISIZIONE

In data 11 marzo 2012 veniva eseguita la copia forense dell’hard disk marca Maxtor modello DiamondMax 10 da 200 GB S/N R56EGHG presso il Compartimento della Polizia Postale di XXXXX alla presenza della Rossi e di un Agente della Polizia Postale. L’attività di copia forense veniva svolta utilizzando copiatore hardware marca Logicube modello Quest, calcolando l’impronta hash MD5 che veniva riportata a verbale dall’Assistente Neri della Polizia Postale. Al termine dell’attività di copia, l’hard disk veniva riconsegnato alla parte (Paola Rossi) nella persona dello scrivente (sia l’hard disk originale che la copia effettuata), come in un diretto passaggio di consegne dalla Polizia Postale al sottoscritto.

Si precisa che l’hard disk è lo stesso dispositivo che era stato rimosso dal PC assegnato a Verdi e consegnato alla Polizia Postale in data 10 settembre 2009 da Rossi.

ANALISI

L’analisi forense si poneva l’obiettivo di individuare tracce di attività compatibili con la condotta di chi, abusando delle proprie credenzialidi accesso, è interessato a conoscere e/o copiare il contenuto di documentazione riservata.

Per evidenziare tali attività è stata operata una ricerca di una serie di elementi attraverso:

- la generazione di una timeline;
- l’analisi degli ultimi file acceduti in lettura;
- l’analisi statistica del numero file acceduti in lettura nel tempo;
- l’analisi relativo all’uso di dispositivi di memorizzazione esterni (ad esempio, chiavette usb).

Di seguito vengono dettagliate le varie attività svolte.

Timeline

Innanzitutto vale la pena introdurree la definizione di *timestamp*: per timestamp si intende il dato temporale costituito da data, ora e fuso orario.

La timeline rappresenta l'elenco delle attività svolte sul sistema in relazione al timestamp di ultimo accesso, ultima modifica e creazione di tutti i file (in chiaro e cancellati) presenti sull'hard disk oggetto di analisi.

A titolo esemplificativo, l'analisi della timeline consente di determinare i momenti in cui il sistema risultava acceso (è infatti evidente che è necessario che il sistema sia attivo affinchè si verifichino degli accessi, delle modifiche o delle creazione di file), verificare interazioni da parte di un utente umano oppure accessi da software in maniera automatica, identificare possibili attività di copia massiva di file, oltre varie altre attività. Nel caso dell'analisi della presente relazione tecnica, l'obiettivo è quello di identificare i file acceduti che non erano di pertinenza lavorativa dell'utente ed eventuali attività di copia massiva di tali dati.

Analisi degli ultimi file acceduti

Concentrandosi sugli ultimi file acceduti (settimana da 8 a 12 giugno 2009), è stato ristretto il campo di osservazione ai file di tipo documentale (documenti di word, fogli elettronici di excel, file pdf, eccetera).

La rete locale di AziendaX è costituita da un file server che conteneva cartelle con diverso grado di accesso:

- nella cartella *Lavori* erano contenuti i file dei progetti
- nella cartella *Scambio* erano contenuti i file da scambiare con i colleghi o con gli stagisti che non avevano accesso alla cartella dei lavori.

Un file server è un sistema informatico che consente di condividere file tra i vari utenti della rete in modo tale da ottimizzare la gestione informatica della rete stessa.

Ad esempio, le copie di backup possono essere lanciate automaticamente su un unico sistema invece che su tutti i pc: cambiando pc, l'utente può immediatamente accedere ai propri documenti, ovvero utenti che lavorano allo stesso progetto

lavorano su un'unica copia dei dati invece che far girare copie (che possono poi risultare "non allineate") dello stesso file.

Gli addetti di AziendaX venivano istruiti sulle modalità di archiviazione dei dati sul file server, utilizzando opportuni codici per classificare i dati: ad esempio, il file salvato in

`\\LACIE-2BIG\LAVORI·[.....]\AAAAA.pdf`

è un file relativo al cliente […..].

Va evidenziato come attraverso questo meccanismo ben definito di classificazione dei file, l'addetto che segue uno specifico progetto, conoscendo il codice, riesca a raggiungere in maniera rapida la cartella in cui è presente il documento di proprio interesse, il cui nome costituisce un ulteriore meccanismo di identificazione.

Quindi in tale maniera non è necessario aprire un documento per evincerne il contenuto, in quanto la denominazione stessa ne permette la conoscenza.

Tuttavia, poiché tale denominazione consente solo di risalire agli argomenti trattati nel file, risulta necessario da parte dell'utente interessato a conoscere i contenuti aprire il file di proprio interesse.

Analisi statistica dei file acceduti

L'accesso ai file di stretta pertinenza lavorativa è stata anche prerogativa dell'attività lavorativa della Verdi nel suo periodo di lavoro precedente il mese di giugno 2009: infatti, nella settimana compresa tra i giorni 8 giugno e 12 giugno del 2009 (ultima settimana lavorativa della Verdi in AziendaX), risulta un numero di accessi a documenti di lavoro che appare quanto meno anomalo, soprattutto ove venga considerato che diversi documenti si riferiscono a progetti chiusi o la cui competenza non era in capo alla Verdi.

Analisi dei file acceduti rinvenuti dalla Polizia Postale

Una prima analisi prende in esame i file che sono stati evidenziati dall'analisi effettuata da parte della Polizia Postale. In data 29 settembre 2009, la Rossi indicava come riservati soltanto 14 file. La seguente analisi, prendendo in esame la stessa

tabella di file acceduti prodotta dalla Polizia Postale e ristretta all'ultima settimana, cerca invece di evidenziare come i file strategici e riservati sono in numero superiore.

[……]

[……]

[……]

Si precisa inoltre che Verdi aveva pianificato di lasciare il lavoro in AziendaX fin dai primi giorni di Aprile 2009, pertanto è anche possibile che ci fossero state attività di copia di file in momenti precedenti. Infatti, lo stesso esame della Polizia Postale ha evidenziato l'accesso a file non di pertinenza di Verdi acceduti sin dal mese di aprile 2009, alcuni dei quali sarebbero dovuti essere salvati salvati (con il solito meccanismo dettagliato di sottocartelle) sul file server aziendale e che invece risultano presenti sull'hard disk del pc utilizzato da Verdi. Tra questi si evidenziano

- due file acceduti il 25.05.2009 alle ore 12:56 relativi a dati di una gara Pippo del 2007 contenuti i documenti tecnici ed amministrativa:
- […]
- […]
- […]

Analisi dei file acceduti rinvenuti dallo scrivente

La seguente tabella è stata generata utilizzando le tracce informatiche presenti nella cartella "Recent" dell'utente utilizzato dalla Verdi: in questa cartella viene creato un file di tipo LNK (che sta per *link*, cioè un collegamento ad un file) che registra i file acceduti più di recente.

La tabella è organizzata in 4 colonne: la seconda colonna rappresenta il nome (o nella maggior parte dei casi l'intero percorso) del file; la terza colonna rappresenta la data e l'ora di ultimo accesso del file. Nella prima colonna, la presenza di una "X" indica che il file era relativo a diversi documenti ai quali la stessa Verdi non doveva in quel periodo accedere poichè non rientravano all'interno delle sue competenze, come stabilito per mezzo di atto aziendale interno (verbale di riunione): in questo caso, nella quarta colonna viene data una descrizione del file (o della cartella) ed eventualmente l'importanza dello stesso.

[….]

[….]

[….]

Alla luce di quanto esposto, considerando anche che in virtù delle denominazione "parlante dei documenti" che permetteva di apprezzare il contenuto dei documenti senza aprirli, giova rilevare come risulta alquanto anomala la consultazione di così numerosi file al di fuori delle mansioni della Verdi specificamente assegnate proprio in prossimità della data di fine collaborazione.

La denominazione "parlante" forniva già di per sé una indicazione di massima del contenuto: tuttavia, probabilmente l'utente ha aperto i file per esser sicuri di cosa si trattasse (o per entrare a conoscenza di alcuni dettagli).

Tale anomalia può essere ritenuta elemento compatibile con la condotta di colui che è interessato a conoscere in dettaglio il contenuto di un documento per poi eventualmente provvedere alla copia su un dispositivo esterno o "chiavetta USB".

Va infine evidenziato che altro elemento che conferma questa compatibilità di condotta riposa nella cirVerdinza dell'accesso ad alcune cartelle il cui contenuto afferiva a progetti che palesemente non rientravano nelle mansioni della Verdi.

Analisi relativo all'uso di dispositivi di memorizzazione esterni

Ulteriore analisi compiuta riguarda l'utilizzo di dispositivi di memorizzazione di massa connessi via usb. L'analisi, compiuta utilizzando il software Access Data Registry Viewer, si riassume con i seguenti timestamp di prima connessione, ovvero nei momento in cui il sistema operativo installa i driver necessari al corretto funzionamento della periferica di memorizzazione, dovendo tuttavia far presente che non è possibile evidenziare successive connessioni di uno stesso dispositivo. Di seguito sono indicati i dispositivi di memorizzazione connessi al sistema informatico oggetto di accertamento nell'anno 2009.

31/03/2009 08:37:45 UTC

06/04/2009 08:27:43 UTC

Se nel passato questo dato può apparire fisiologico, stringendo il campo di attenzione agli ultimi giorni di lavoro risulta particolarmente rilevante il dato relativo all'ultima chiavetta collegata il giorno 3 giugno 2009: successivamente a tale data si sono infatti verificati gli accessi a file memorizzati sul file server aziendale, come già esposto in precedenza.

Di seguito sono riportati i dati relativi all'ultima chiavetta usb, connessa il 03/06/2009 alle ore 15:55:09 UTC: tali dati sono stati forniti in output dal software di analisi forense Access Data Registry Viewer:

```
ControlSet001\Enum\USBSTOR\Disk&Ven_USB_2.0&Prod_Flash_Disk&Rev_1100\AA04012700009007&0
Ora di ultima scrittura: 03/06/2009 15:55:09 UTC
Nome            Tipo            Dati
DeviceDesc      REG_SZ          Unità disco
Capabilities    REG_DWORD       0x00000010 (16)
       time_t (memorizzato)   Thu Jan 01 00:00:16 1970
       time_t (come locale)   Thu Jan 01 01:00:16 1970
       Data/ora DOS   - 00:00:32
UINumber        REG_DWORD       0x00000000 (0)
       time_t (memorizzato)   Thu Jan 01 00:00:00 1970
       time_t (come locale)   Thu Jan 01 01:00:00 1970
       Data/ora DOS   - 00:00:00
HardwareID      REG_MULTI_SZ    USBSTOR\DiskUSB_2.0_Flash_Disk_____1100
                USBSTOR\DiskUSB_2.0_Flash_Disk_____
                USBSTOR\DiskUSB_2.0_
                USBSTOR\USB_2.0_Flash_Disk_____1
                USB_2.0_Flash_Disk_____1
                USBSTOR\GenDisk
                GenDisk

CompatibleIDs   REG_MULTI_SZ    USBSTOR\Disk
                USBSTOR\RAW

ClassGUID       REG_SZ  {4D36E967-E325-11CE-BFC1-08002BE10318}
Service         REG_SZ  disk
ConfigFlags     REG_DWORD       0x00000000 (0)
       time_t (memorizzato)   Thu Jan 01 00:00:00 1970
       time_t (come locale)   Thu Jan 01 01:00:00 1970
       Data/ora DOS   - 00:00:00
ParentIdPrefix          REG_SZ  7&2e794afd&0
Driver  REG_SZ  {4D36E967-E325-11CE-BFC1-08002BE10318}\0015
Mfg     REG_SZ  (unità disco standard)
FriendlyName    REG_SZ  USB 2.0 Flash Disk USB Device
```


Inoltre si noti come sono emerse prime connessioni di chiavette usb anche in data 31 marzo e 6 aprile, comunque pochi giorni prima dello scambio di mail con il quale si comunicava il termine della collaborazione.

La connessione di una chiavetta usb di per sè non ha particolare significato; tuttavia, correlata ad altri eventi quale l'accesso massivo a file, può rappresentare un evento tipico di chi copia massivamente quei file acceduti in rapida successione.

Nel caso dell'hard disk sottoposto ad analisi, non è stato possibile appurare se c'è stata una copia massiva in ragione del fatto che i file non erano residenti sull'hard disk stesso, ma su un file server: in questa cirVerdinza, l'alterazione dei dati temporali si sarebbe verificata sul file server, ma poiché ormai è passato molto tempo eventuali tracce di questo tipo sono certamente andate distrutte. **Resta comunque la traccia di numerosi accessi (inteso come apertura di file) a file sul file server non di competenza e quindi la compatibilità degli eventi (connessione chiavetta usb, accesso a diversi file di tipo documentale anche esterni all'attività lavorativa) con la condotta di chi cerca documentazione di rilevante valore in termini di proprietà intellettuale per poi effettuarne eventualmente una copia.**

VALUTAZIONE DEGLI ULTIMI FILE ACCEDUTI

I file messi in evidenza (con il simbolo "X" nella prima colonna) nella tabella esposta in precedenza sono relativi a progetti non di competenza di Verdi, dove la competenza era stabilita nei verbali di riunione del 20.05.2009 e del 28.05.2009 tra Verdi e Bianchi.

I documenti associati ai file elencati nella tabella contengono dati sensibili di proprietà di AziendaX e includono dati sullo stato di contaminazione del sottosuolo di siti di pertinenza di clienti di AziendaX. Molti file non sono relativi ai progetti che negli ultimi giorni di attività erano assegnati a Verdi, la quale aveva l'incarico di completare i soli rapporti dei progetti

[…]

Per comprendere l'importanza dei file evidenziati va considerato che al loro interno sono presenti:

- informazioni riservate sui clienti di AziendaX,
- informazioni strategiche per l'azienda AziendaX che costituiscono know-how acquisito in anni di lavoro,
- informazioni strategiche per l'azienda AziendaX quali offerte economiche che consentirebbero ai concorrenti di offrire prezzi concorrenziali,
- modulistica che consentirebbe ad un concorrente di operare immediatamente in concorrenza all'azienda AziendaX.

Si tiene a precisare che numerosi file esposti possono essere riutilizzati ricopiandone le impostazioni tecniche e le informazioni contenute.

ASPETTI ORGANIZZATIVI AZIENDALI

L'ORGANIZZAZIONE AZIENDALE DI AZIENDAX

Di seguito sono illustrate considerazioni tecniche per apprezzare la rilevanza della documentazione attestante la conformità di AziendaX a ben precisi standard di sicurezza e organizzativi, tenendo presente che per per l'azienda i dati rappresentano un patrimonio fondamentale, derivandone pertanto che la protezione di tale patrimonio diventa la condizione irrinunciabile per lo sviluppo e la buona riuscita delle proprie attività.

[…]

[…]

[…]

CONCLUSIONI

Alla luce di quanto esposto va evidenziato quanto segue:

- in occasione delle informazioni fornite […] ma che al contrario sono risultati essere ragionevolmente più numerosi;
- presso la AziendaX erano in essere rigorosi standard organizzativi e di documentazione delle attività svolte, i quali permettevano di considerare attendibile la documentazione prodotta e di poter individuare con precisione *"chi faceva che cosa"* all'epoca dei fatti;
- dall'analisi forense è emerso che il numero di file acceduti nell'ultima settimana di lavoro da parte di Verdi è stato statisticamente superiore al numero di file acceduti nel periodo precedente da parte della stessa. Tali file sono classificati in maniera molto scrupolosa all'interno di AziendaX;
- l'identificazione approfondita dei documenti ha consentito di classificare come "documenti estranei alle mansioni affidate alla Verdi" diversi fra quelli consultati nella sua ultima settimana di lavoro;
- in virtù dei criteri organizzativi adottati e di classificazione dei documenti presenti sul server di AziendaX era possibile evincere il contenuto di un documento dalla denominazione dello stesso;
- quindi considerando che la denominazione "parlante dei documenti" che permetteva di apprezzare il contenuto dei documenti senza aprirli, va rilevato come risulta alquanto anomala la consultazione di così numerosi file, al di fuori delle mansioni assegnate alla Verdi, proprio in prossimità della data di fine collaborazione con AziendaX;
- ulteriore elemento che conferma questa compatibilità di condotta è la cirVerdinza dell'accesso ad alcune cartelle il cui contenuto afferiva anche a progetti chiusi da diversi anni;
- nello stesso periodo, risulta la connessione di un dispositivo di memorizzazione usb.

Pertanto, alla luce di quanto esposto è possibile affermare con ragionevole certezza che dall'esame del disco rigido del PC utilizzato da Michela Verdi emerge la presenza di numerosi riscontri compatibili con la condotta di chi abusa delle proprie credenziali di accesso per consultare ed eventualmente copiare dati riservati aziendali, non pertinenti alle proprie mansioni.

A disposizione per qualsiasi chiarimento.

XXXXXXXXX, lì XXX maggio 2012

Dott. XXXXXX XXXXXX

GLOSSARIO

Client: in un'infrastruttura di rete informatica, un client è un sistema informatico che effettua richieste ad un server che offre un servizio.

File recenti: file di tipo link che vengono salvati in una cartella del sistema operativo per tenere traccia degli ultimi file acceduti dall'utente; gli ultimi 15 file recenti vengono mostrati nel menù dati recenti del menù Avvio di Windows.

LNK (file di tipo): file che rappresenta un collegamento per aprire un altro file; esempi di link sono le icone presenti sul desktop di un computer che hanno un simbolo di una freccetta nell'angolo in basso a sinistra.

Server: in un'infrastruttura di rete informatica, un server è un sistema informatico che risponde a richieste poste da un client (ad esempio, richiesta del contenuto di un sito web o della propria posta elettronica, richiesta di file condivisi, eccetera).

Timestamp: dato temporale costituito dalla triade data, ora e fuso orario; ad esempio, "01/01/1950 12:00:00 UTC" rappresenta il mezzogiorno del primo gennaio 1950, dove l'ora è espressa in formato universale (UTC).

BIBLIOGRAFIA

1. […]
2. […]
3. […]

Note autobiografiche

[…]

[…]

[…]