Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Scienze di Internet

ANALISI FORENSE DI STRUMENTI WEB BROWSER PORTABLE

Tesi di Laurea in Informatica Forense

Relatore:

Chiar.mo Prof.

CESARE MAIOLI

Presentata da:

ANNARITA GROSSO

Sessione III

2011/2012

Indice

Introduzione

L'evoluzione della tecnologia ha permesso la diffusione di Internet sia negli uffici che nelle case di molte famiglie, ma se da un lato sono migliorate notevolmente sia la velocità di connessione che la potenza dei dispositivi, dall'altro risulta sempre più difficile garantire parametri di sicurezza per gli utenti, che sono sempre più spiati e vittime di hacker, virus e pirati informatici. Navigando in Rete, infatti, un utente lascia al suo passaggio un'infinità di informazioni che vengono memorizzate nei siti web visitati, nei motori di ricerca o nelle chat. Attraverso queste informazioni, è possibile essere a conoscenza di quale sistema operativo l'utente ha utilizzato, il browser, il colore e la definizione dello schermo, l'ultimo sito web visitato, e le ricerche effettuate sul web, con conseguente traccia di un preciso profilo dell'utente.

L'anonimato in rete rappresenta, quindi, la necessità di evitare un vero e proprio controllo della propria attività su Internet.

Di contro, però, metodi e strumenti per l'anonimato possono essere utilizzati da soggetti interessati a compiere reati informatici ed è dunque, necessaria l'implementazione di attività e procedure di monitoraggio, tipiche dell'informatica forense, al fine di indentificare chi opera nell'illegalità. L'obiettivo di questa tesi è quello di affrontare, in modo esaustivo e dettagliato, le tecniche attraverso le quali è possibile rinvenire su sistemi web Browser anonimi elementi, utili a fini investigativi e processuali, a ricostruire la navigazione in rete di un utente. A tale scopo, sono stati installati tre diversi web browser

portable (GoogleChrome, Firefox e Tor) su una pennina USB ed eseguiti una serie di test attraverso l'uso di tool open source.

Entrando nel dettaglio di questo lavoro, e precisamente nel primo capitolo, viene introdotto il concetto di computer forensics, partendo dalle origini di questa scienza forense fino alla sua evoluzione. In particolar modo, si farà riferimento allo sviluppo di questa disciplina in Italia, evidenziando alcuni famosi casi di cronaca italiana in ambito forense e definendo i reati ed i campi di applicazione in cui è opportuno utilizzare tali metodologie. Nel secondo capitolo, saranno descritte le discipline alla base dello svolgimento di un processo penale, evidenziando gli strumenti a disposizione delle parti per rinvenire elementi di carattere informatico, in particolar modo, verrà approfondito il ruolo del consulente tecnico ed il suo rapporto con le parti processuali.

Nel terzo capitolo l'argomento trattato sarà quello relativo alle principali norme che delineano il panorama giuridico italiano in ambito forense. Nello specifico, saranno esaminate le modifiche introdotte nel nostro ordinamento dalla legge 48 del 2008 di Ratifica della Convenzione sul cybercrime di Budapest (2001). Nel quarto capitolo, ci si concentrerà sugli aspetti informatici e giuridici della navigazione anonima in rete, focalizzando l'attenzione sulle norme relative alla tutela della privacy e sugli strumenti informatici più diffusi a garantire una navigazione in totale anonimato. Nel quinto capitolo, si procederà a descrivere gli obiettivi della realizzazione di tale progetto e le motivazioni della stesura di questa tesi, analizzando, sulle modalità di svolgi-

mento dello studio, le tecnologie utilizzate ed i test effettuati. In particolare, verranno mostrati i risultati dello studio, opportunamente analizzati e comparati. Dall'analisi dei dati di navigazione rinvenuti, tramite analisi forense, si metteranno a confronto i diversi tipi di web browser portable utilizzati ed enunciate delle considerazioni sui test che presentano punti di collegamento.

Capitolo 1

1 L'informatica forense

1.1 Scienze forensi

Il ricorso alla scienza per accertare i fatti nell'ambito del processo civile e penale è un fenomeno che risale a tempi passati: anche se il giudice è peritus peritorum (perito dei periti), ovvero colui che sa tutto in un processo, la realtà dei fatti è che egli è solo esperto di diritto, non ha altre competenze specialistiche e, molto spesso, si trova ad accertare o a valutare fatti la cui conoscenza presenta caratteristiche di natura scientifica per le quali solo un esperto specifico del settore è in grado di fornire informazioni e valutazioni attendibili. Accade, perciò, sempre più spesso che il giudice debba occuparsi di reati connessi a fenomeni complessi di natura scientifica, e che quindi richiedono, per essere accertati, l'impiego della scienza o del metodo scientifico. L'utilizzo di conoscenze scientifiche, inoltre, sembra fornire il mezzo più sicuro per accertare la verità dei fatti e ragioni come queste spiegano il rapido estendersi del ricorso alle prove scientifiche in tutti i tipi di processo. La scienza, in altri termini, sta occupando territori sempre più ampi che spaziano dalla chimica alla fisica, dalla medicina alla psicologia, nonché dalle scienze criminologiche a quelle più recenti relative alla computer forensics.

1.2 Evoluzioni tecnologiche

Lo sviluppo della "computer forensics" è strettamente correlato all'evoluzione delle tecnologie informatiche e telematiche nell'era moderna. Contestualmente al mutamento portato in ampi settori della società, dalle nuove tecnologie e, in particolare, dall'avvento dell'elaboratore elettronico e dalle reti, si è verificato un cambiamento nelle modalità di rilevazione, gestione, raccolta e analisi di quegli elementi che, in senso lato, possiamo definire "fonti di prova", capaci sì di individuare un fatto, ma inscindibilmente correlati ad un elaboratore elettronico o ad una rete informatica o telematica.

Il fiorire della tecnologia iniziò negli anni Novanta, periodo in cui avvenne la diffusione dei primi personal computer e dei primi sistemi informatici, fino ad arrivare più recentemente alla diffusione capillare dei cellulari internet, delle e-mail, chat, palmari, chiavi USB e reti WiFi. Questo espandersi di strumenti tecnologici e telematici ha portato ad un aumento elevato della quantità di dati trasmessi e memorizzati in formato elettronico e di conseguenza, anche l'attività forense ha subito un notevole sviluppo.

Tutti questi strumenti, infatti, mantengono tracce del loro utilizzo nella forma di file, log, record, documenti, frammenti ecc.., che spesso sono nascosti all'utente inconsapevole, che possono consentire ad un esperto informatico forense di ricostruire importanti informazioni sui relativi utilizzatori ed, all'occorrenza, possono diventare materiale di interesse giudiziario e fonte di prove applicabili in tribunale.

1.3 L'origine della Computer forensics

Il recente sviluppo della Computer forensics come scienza fonda le sue radici intorno al 1980 negli ambienti giuridici degli Stati Uniti quando l'FBI ed altre agenzie investigative americane iniziarono ad utilizzare software per l'estrazione e l'analisi dei dati presenti su un computer. La necessità, da parte delle forze dell'ordine, di far fronte alla continua crescita della criminalità informatica, infatti, aveva determinato la nascita di questa nuova disciplina, che permette di poter validamente utilizzare i dati digitali raccolti in sede processuale, fondendo così competenze informatiche e tecniche con quelle giuridiche.

Sempre nella prima metà degli anni Ottanta si colloca, all'interno dell'FBI, l'istituzione della prima organizzazione investigativa CART[1], ma una data significativa nell'evoluzione della Computer Forensics è sicuramente il 1994, quando il Dipartimento della Giustizia degli Stati Uniti decise di pubblicare un insieme di linee guida[2] [1], che definirono per la prima volta degli standard sulle modalità operative di questa disciplina.

Da allora, la pratica della computer forensics si è sviluppata sino a diventare una disciplina oggetto di studio anche negli altri Paesi.

[1] Computer Analysis and Response Team.
[2] "Handbook of forensic"

1.4 L'informatica forense in Italia

La disciplina che portò i precetti della Computer forensics in Italia fu l'Informatica Forense. La sua nascita si colloca dopo circa un decennio della nascita della Computer forensics, quando anche le forze dell'ordine italiane cominciano a istituire reparti operativi specializzati in computer crimes e procedure informatiche.

Significativi passi iniziali furono rappresentati dalla creazione, nel 1996, del Nucleo Operativo di Polizia delle Telecomunicazioni (N.O.P.T.), con lo specifico compito di svolgere attività di contrasto ai crimini del settore delle telecomunicazioni, seguito nel 1998 dall'istituzione del Servizio Polizia Postale e delle Comunicazioni, al cui interno confluirono le risorse dei dipartimenti precedentemente esistenti. Il termine "Informatica Forense" venne coniato all'inizio dell'anno 2000[3], intendendo:

"La disciplina che concerne le attività di individuazione, conservazione, protezione, estrazione, documentazione ed ogni altra forma di trattamento ed interpretazione del dato informatico al fine di essere valutato come prova in un processo, e studia a fini probatori i processi, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici (hard disk, nastri...) nonchè l'analisi forense di ogni sistema informatico e telematico (computer, palma-

[3]L'espressione "informatica forense" fu presentata per la prima volta nel 2003 dall'Avv. A. Gammarota durante la presentazione tenuta al I Master CSIG di Bari; le prime lezioni universitarie aventi ad oggetto tale materia si tennero alla Facoltà di Giurisprudenza dell'Università di Bologna a partire dal 2004/2005.

re, rete...), l'esibizione della prova elettronica, l'esibizione del dato digitale, il recupero di dati e la loro esibizione."

Gli scopi di questa disciplina, dunque, sono quelli di *"conservare, identificare, acquisire, documentare o interpretare i dati presenti in un computer [2]."*

Molto importante, ai fini della corretta qualificazione della disciplina, è anche l'individuazione del momento in cui essa entra in gioco. Gli studiosi, infatti, sono ormai concordi nell'affermare che, a differenza della sicurezza informatica, essa è un'attività da compiere dopo che un sistema informatico è stato violato con lo scopo di esaminare i reperti informatici in modo esaustivo, completo, accurato, incontaminato e documentato.

Seppure, queste due aree di attività siano strettamente collegate, si può pensare alla sicurezza informatica da un lato come elemento di ostacolo e dall'altro come fonte di strumenti e opportunità per l'informatica forense. Infatti, la sicurezza informatica ha come proposito finale l'avvicinarsi alla realizzazione di sistemi il più possibile sicuri, ma qualora tale grado di sicurezza venisse elevato (ad esempio da parte del responsabile di un illecito), allora per definizione dal sistema sarebbe più complicato estrarre il desiderato contenuto informativo. L'acquisizione dei reperti informatici richiederà, in tal caso, la "violazione" del sistema oggetto dell'analisi ed in questo campo la stessa sicurezza informatica sarà d'aiuto, in quanto fonte di studi sulle tecniche di hacking (utili per realizzare l'accesso alle informazioni protette) e sulla loro applicazione pratica. Inoltre, le "best practice" di sicurezza definiscono molti

requisiti sui sistemi che, se opportunamente applicati, potranno in un secondo momento rendere disponibili un gran numero di informazioni aggiuntive, utilizzabili per l'analisi forense.

L'ingresso della prova informatica in sede processuale ha sempre rappresentato motivo di accesi dibattiti a livello dottrinale e processuale, anche in seguito alla intangibile e volatile natura dei dati digitali.

La tecnologia fa diventare il processo d'investigazione e raccolta dei dati, a fini probatori, estremamente vulnerabile e soggetto al rischio di malfunzionamenti tecnici, danneggiamenti o contraffazioni, corroborato dalla scarsa preparazione di tanti operatori.

Non esiste, inoltre, uno standard o una metodologia per il trattamento delle prove digitali forensi, ma solo un insieme di procedure e strumenti più o meno consolidati attraverso l'esperienza di tutte le forze di polizia, degli esperti del mondo accademico, dei consulenti e del "mondo della Rete". E proprio l'assenza di validità scientifica ufficiale, rende alcune volte discutibile in fase processuale l'utilizzo di strumenti e metodologie di acquisizione probatoria, ritenute affidabili soltanto sulla base dell'esperienza [3]. A tal proposito, la prima sentenza in Italia in tema di Informatica Forense è stata emessa dal Tribunale di Bologna in data 21 luglio 2005 nel procedimento comunemente noto con il nome di "caso Vierika" [5, 4], in cui l'accusa si basò interamente sulla discussione delle tecniche investigative e forensi utilizzate dalla Polizia Giudiziaria.

1.4.1 Il caso Vierika

In Italia ha fatto molto scalpore la sentenza del Tribunale di Bologna che ha pronunciato una condanna per reato esatto[4] nel caso "Vierika". Da quanto ricostruito in sede dibattimentale è emerso che il programma Vierika era un *worm*[5], programmato in linguaggio Visual Basic Script, costituito da un primo script che veniva allegato come file immagine ad un'e-mail: una volta lanciato tale file, il registro di configurazione di Windows veniva modificato all'insaputa dell'utente, abbassando le protezioni del browser Internet Explorer e impostando come home page dello stesso browser una pagina web che conteneva un secondo script in Visual Basic. L'utente, quindi, collegandosi ad internet e venendo indirizzato a tale home page attivava, a propria insaputa, il secondo script che aveva lo scopo di creare nel disco rigido del computer un file che inviava agli indirizzi trovati all'interno della rubrica di Outlook una e-mail con allegato il primo script, provocando quindi una reiterata duplicazione di Vierika.

L'argomento è di particolare rilievo, in quanto il contraddittorio tra le parti (P.M. e difesa) si è svolto quasi esclusivamente sul tema della metodologia utilizzata dalla polizia giudiziaria nell'acquisire i mezzi di prova e sulla corrispondenza della metodologia applicata dalla polizia giudiziaria, nella formazione ed acquisizione delle prove. In particolare, la difesa dell'imputato ha posto in discussione la correttezza sia del metodo utilizzato dalla polizia

[4]. 615-ter c.p.p. "Reato di accesso abusivo ad un sistema informatico o telematico"
[5]Una particolare categoria di malware in grado di autoreplicarsi.

giudiziaria per estrarre i programmi dal computer dell'indagato, sia il metodo applicato dalla stessa e dalle società *Infostrada s.p.a.* e *Tiscali s.p.a.* per individuare l'amministratore degli spazi web (uno dei quali contenente il secondo script del programma Vierika).

Di contro, Il Tribunale ha affermato che non era suo compito determinare un protocollo relativo alle procedure informatiche forensi, ma semmai verificare se il metodo utilizzato dalla polizia giudiziaria se nel caso in esame avesse concretamente alterato alcuni dei dati ricercati. Il Giudice, in particolare, in assenza della allegazione di fatti dai quali si potesse astrattamente desumere una qualsiasi forma di alterazione dei dati, ha sostenuto che non fosse suo compito determinare un protocollo relativo alle procedure informatiche forensi. La difesa si limitò solamente a definire tali metodi come non conformi rispetto a quelli previsti dalla migliore pratica scientifica, senza però produrre documentazioni relative alle eventuali alterazioni avvenute. Viene di seguito riportato un passaggio esaustivo della sentenza d'appello:

"[...] (procedimento) viziato da ricostruzione tecnico informatica priva di fondamento peritale, ed il correlativo ingiustificato diniego dell'espletamento di perizie, chieste dalla difesa, sulle modalità di generazione e conservazione dei log (registri di collegamento), acquisiti presso il gestore [...], nonché sull'originale del codice sorgente del software per cui causa."

Nel processo si sono affrontati aspetti tecnologici di notevole portata e situazioni tecniche indissolubilmente connesse alla costante ed incessante evoluzio-

ne tecnologica, in cui il dibattimento si è concentrato proprio sulle modalità di acquisizione dei dati da parte della Polizia Giudiziaria.

1.4.2 Il caso dell'omicidio di Garlasco

La cronaca giudiziaria più recente riferisce di un altro dei maggiori esempi di cronaca italiana in cui i dati digitali hanno assunto un ruolo probatorio notevole, in un caso di omicidio avvenuto a Garlasco [6].

L'omicidio è avvenuto il 13 agosto 2007, quando è stata ritrovata morta Chiara Poggi, una ragazza 26enne residente a Garlasco (PV). Secondo una prima ricostruzione, la sera di domenica 12 agosto 2007, Chiara Poggi (poi uccisa) ed il fidanzato Alberto Stasi hanno cenato assieme e successivamente ognuno fece ritorno alla propria casa per trascorrervi la notte. La mattina seguente, Stasi tentò più volte di contattare la Poggi al telefono cellulare ma inutilmente. Intorno alle ore 14:00 del 13 agosto, Stasi si recò nuovamente presso l'abitazione della Poggi e lì trovò la porta aperta. Entrato in casa, trovò il corpo esanime della ragazza riverso per terra in un lago di sangue. Lasciata la casa, lo Stasi si recò presso la vicina caserma dei Carabinieri per dare l'allarme [7].

Sin dalle prime fasi, il principale indagato è stato Alberto Stasi, il quale, in sua difesa, aveva dichiarato di aver trascorso la mattinata del 13 agosto lavorando alla tesi sul proprio portatile, presso la propria abitazione, provando ripetutamente a contattare la fidanzata sia con il cellulare che con il

telefono di casa. L'analisi del telefono cellulare della vittima e dei tabulati dello stesso ha confermato la serie di chiamate non risposte, così pure l'analisi dei tabulati dell'utenza fissa. Inoltre, sul portatile è stato rinvenuto del materiale di carattere pedopornografico, per il quale sono state formulate a Stati delle nuove accuse di detenzione dello stesso[6]. L'analisi del portatile di Stasi, invece, a causa dell'impropria gestione del reperto ad opera delle forze di polizia a cui era stato affidato, ha reso inutilizzabile, come fonte di prova, il contenuto del computer portatile.

É da sottolineare, dunque, come sia importante una corretta acquisizione ed analisi dei reperti relativi a crimini informatici. Gli accertamenti tecnici compiuti sul portatile di Stasi, se correttamente eseguiti, sarebbero stati di enorme importanza nella formulazione del giudizio.

Riscontrando invece un'alterazione diffusa di dati (in particolare dei metadati di ultima lettura) è stato impossibile dimostrare l'alibi dell'indagato.

1.5 Reati informatici

Contestualmente all'evoluzione delle tecnologie informatiche si è avuta la nascita, l'evoluzione e la proliferazione di molte e nuove forme di reato e di aggressione criminosa, talvolta, commesse per mezzo di sistemi informatici e telematici.

[6]Tale fattispecie penale generò un nuovo processo ai danni dello Stasi

Quando entra in gioco la prova informatica, i reati non sono necessariamente informatici ma possono essere classificati nel seguente modo:

- **Reati tradizionali o comuni in cui il computer assume la qualità di strumento del reato.** É il caso di frodi o falsificazioni o, più in generale, di qualsiasi utilizzo di informazioni con modalità pregiudizievoli e malevole.
- **Reati relativi a contenuti, in cui si utilizzano le TIC (Tecnologie dell'Informazione e della Comunicazione) per facilitare la distribuzione di materiali illegali o illeciti.** Possiamo pensare, ad esempio, alla violazioni dei diritti d'autore ed alla pornografia minorile.
- **Reati di cui si rinvengono tracce o indizi nei sistemi informatici.** Un caso tipico è il falso in bilancio o omicidi.

1.6 Le cinque fasi dell'informatica forense

Il fine ultimo di ogni investigazione digitale consiste nel recupero di tutti i dati che possano costituire una prova utilizzabile durante il processo. In particolare, la formazione della "prova informatica" si delinea seguendo cinque fasi fondamentali:

1. Individuazione
2. Acquisizione e Conservazione

3. Analisi

4. Valutazione

5. Presentazione

Di seguito verranno analizzate in dettaglio.

1.6.1 Individuazione

La fase d'individuazione consiste nella ricerca di qualunque dispositivo che sia in grado, almeno teoricamente, di memorizzare informazioni digitali attendibili ed inerenti al caso. É un'attività che non si limita soltanto al repertamento ed all'analisi dei personal computer, ma si estende ad una grande varietà di sistemi elettronici digitali ed è per questo che la valutazione di quale tra i sistemi digitali, presenti nell'area di competenza, debba essere repertato non risulta immediata. Non solo i personal computer possano essere oggetto della computer forensics, ma qualsiasi dispositivo elettronico capace di immagazzinare dati, quali ad esempio:

- un lettore multimediale (mp3/mp4), che può essere utilizzato come memoria di massa generica;
- un drive USB, che può contenere piccole memorie flash disk;
- alcune stampanti potrebbero avere un'interfaccia di rete utilizzabile come repository di file. Molte moderne stampanti, infatti, possono

contenere al loro interno, un hard disk sul quale vengono memorizzati dati prima di essere effettivamente stampanti oppure dopo essere stati scannerizzati [8].

1.6.2 Acquisizione e Conservazione

La fase di acquisizione consiste nell'ottenere "materialmente" i dati da analizzare. Le modalità con le quali può svolgersi sono il sequestro o la duplicazione. Il sequestro è considerato il modo più veloce e semplice di eseguire un'operazione di acquisizione dei dati informatici, dal momento che uniche attenzioni richieste sono la cura del supporto fisico e un corretto mantenimento della catena di custodia. Inoltre, tale procedimento offre la possibilità di rilevare eventuali evidenze fisiche sul supporto sequestrato (impronte, polveri...), che altrimenti potrebbero venire erroneamente alterate. La procedura alternativa è, invece, la duplicazione del supporto tramite copie *bit-a-bit* dei dati, un'operazione senza dubbio meno veloce ma necessaria nel caso in cui i dati da analizzare risiedano su sistemi inamovibili (perchè di grandi dimensioni o che non possano essere spenti o che non possano privarsi dell'alimentazione elettrica). Rappresenta, forse, la fase più delicata perché, se svolta da personale non dovutamente formato, può portare alla distruzione di dati potenzialmente rilevanti o all'invalidazione del supporto e dei dati in esso contenuti. Per chiarire queste problematiche possiamo fare riferimento alle seguenti circostanze:

- trovandosi a dover acquisire i dati immagazzinati su un computer acceso, la sola azione di spegnerlo seguendo la procedura standard potrebbe portare all'avvio di programmi o procedure che, in chiusura di sessione, potrebbe causare la cancellazione di dati importanti (come le cronologie dei files aperti dai diversi player, di internet, lo svuotamento dei file di swap e di spool).

- trovandosi a dover acquisire i dati immagazzinati in un sistema spento è essenziale che non si proceda con l'accessione standard dello stesso. L'avvio del sistema operativo, oltre a poter causare la cancellazione di file.

"...La speciale natura delle prove digitali richiede considerazioni aggiuntive ed alcuni cambiamenti rispetto le prove reali" [9], ed è quindi evidente che tale tipologia di acquisizione dei dati vada ponderata caso per caso da personale specializzato. Infine, non meno importante risulta la gestione degli elementi di prova acquisiti, il loro trasporto e archiviazione per evitare che le stesse vengano alterate o comunque che possa essere messa in discussione la loro integrità, a partire dal sequestro fino al termine del processo.

1.6.3 Analisi

Una volta acquisiti i dati, è necessario procedere alla loro analisi mediante procedure eseguite esclusivamente su copie forensi del reperto. Ai fini probatori, infatti, l'operazione di analisi deve essere riproducibile ed ogni singola

operazione eseguita deve produrre sempre lo stesso risultato. Tra le numerose informazioni che si possono rilevare da un dispositivo di memoria troviamo:

- dati volatili;
- file di swap;
- file logici;
- file di registro delle configurazioni;
- e-mail;
- log delle applicazioni e di sicurezza;
- file temporanei;
- log di sistema;
- spazio libero;
- cache del browser;
- history file;
- file cancellati;

La funzione principale di questa attività è quella di poter rintracciare tutte le possibili prove informatiche utili in sede processuale, anche se i dispositivi di memoria offrono una considerevole quantità di informazioni, spesso non semplici da visualizzare.

1.6.4 Valutazione

La fase di valutazione consiste nell'attribuire un significato ai dati emersi in fase di analisi e nell'accertare la legittimità delle operazioni svolte per acquisirli [2].

Viene fornito un giudizio sulle modalità di svolgimento delle operazioni eseguite, focalizzando l'attenzione sugli aspetti di attendibilità, integrità ed autenticità del reperto in esame, in modo tale da essere ritenuto valido in sede processuale.

1.6.5 Presentazione

Ultima, ma non meno importante, è la fase di presentazione dei risultati. Un'idea sulla crucialità di tale fase può essere ben riassunta da un'affermazione del Maggiore dei Carabinieri, e noto esperto di computer forensics, Marco Mattiucci [9]:

"Contrariamente a quanto si possa pensare il risultato di una indagine tecnica poggia al 50% sulla pura attività tecnica ed al rimanente 50% sulla professionalità, preparazione e capacità espositiva di chi porta tali risultati nell'ambito dibattimentale."

Tale presentazione avviene tramite una relazione tecnica che verrà poi presa in esame durante il dibattimento, contenente la sintesi dei principi scientifici accademicamente riconosciuti su cui l'analisi ed il repertamento si basano,

la catena di custodia dei reperti (generalmente formata dai verbali che ne testimoniano prelievi, trasferimenti e luoghi di permanenza)e la loro accurata descrizione, le specifiche richieste dell'Autorità Giudiziaria con annesse le necessarie e precise autorizzazioni della Procura competente, la descrizione delle operazioni tecniche svolte in laboratorio e l'esito finale. Inoltre, una presentazione deve rispondere a precisi criteri di esposizione, in modo da risultare:

- *Sintetica:* non vi è necessità di riportare eccessivi particolari tecnici dell'analisi, ma solo di menzionare ciò che interessa dal punto di vista giuridico.

- *Semplificata:* colui che legge e valuta l'esito è di principio un fruitore inesperto nel settore informatico e quindi, nell'ipotesi che sia possibile, bisogna eliminare terminologie non consuete e spiegare a livello elementare quanto rilevato.

- *Asettica:* non deve contenere giudizi personali dell'operatore né tanto meno valutazioni legali sulle informazioni rilevate a meno che tali considerazioni non siano state espressamente richieste.

La relazione tecnica è quindi, assieme ad altri elementi provenienti dalle indagini classiche, la base per il dibattimento in sede processuale.

Capitolo 2

2 L'informatica forense nel Processo Penale

Come già affermato precedentemente, l'informatica forense è *"la scienza che studia le tecniche, metodologie, procedure e strumenti per l'individuazione, estrazione, conservazione, protezione, analisi, documentazione, interpretazione ed ogni altra forma di trattamento dei dati in formato digitale, rilevanti ai fini probatori in un processo"* [2]. Ed è per questo che, conoscere la corretta gestione del dato digitale, derivante sia dalle *best pratices* dell' informatica forense, sia dalle norme di procedura penale, relative all'attività di consulenza e perizia, è di fondamentale importanza per l'utilizzazione delle prove informatiche in sede processuale. In questo capitolo, quindi, ci occuperemo di descrivere il panorama giuridico italiano relativo all'informatica forense, evidenziando le principali normative legate alla formazione e all'utilizzo delle prove in ambito informatico. Verranno, poi, analizzate le norme più rilevanti, che disciplinano lo svolgimento del processo penale, la formazione della prova e l'esecuzione degli accertamenti tecnici, approfondendo molti degli aspetti riguardanti le attività dei consulenti tecnici.

2.1 Il processo penale

L'articolo 111 della Costituzione contiene le disposizioni fondamentali del processo penale, ed è quindi il punto di partenza per poterne comprendere le caratteristiche. In particolare detto articolo prevede che:

La giurisdizione si attua mediante il giusto processo regolato dalla legge. Ogni processo si svolge nel contraddittorio tra le parti, in condizioni di parità, davanti al giudice terzo e imparziale. La legge assicura che la persona accusata del reato disponga del tempo e delle condizioni necessari per preparare la sua difesa; di ottenere l'acquisizione di ogni altro mezzo di prova a suo favore. Il processo è regolato dal principio del contraddittorio nella formazione della prova. La legge regola i casi in cui la formazione della prova non ha luogo in contraddittorio per consenso dell'imputato o per accertata impossibilità di natura oggettiva.

Ciò che emerge, in particolare, sono i seguenti tre principi fondamentali:

- Il principio del contradditorio nella formazione della prova, secondo il quale la stessa deve formarsi dialetticamente con l'altra parte nei cui confronti può essere fatta valere. Da questo principio discende che la prova nel processo penale è sostanzialmente orale e si forma in giudizio nella fase denominata "dibattimento".

- La legge regola delle situazioni in cui la formazione della prova non ha luogo in dibattimento per consenso dell'imputato o per accertata

irripetibilità sopravvenuta. È questo il caso degli accertamenti tecnici non ripetibili (si veda il paragrafo 2.5).

- Nel processo penale la legge assicura che la persona accusata di un reato sia, nel più breve tempo possibile, informata riservatamente della natura e dei motivi dell'accusa elevata a suo carico e che disponga del tempo e delle condizioni necessari per preparare la sua difesa. La persona accusata dei fatti deve avere, dunque, la facoltà davanti al giudice di interrogare o di far interrogare le persone che rendono dichiarazioni a suo carico, di ottenere la convocazione e l'interrogatorio di persone a sua difesa nelle stesse condizioni dell'accusa l'acquisizione di ogni altro mezzo di prova a suo favore.

2.2 La prova digitale

La prova è *"un mezzo dimostrativo della veridicità di un fatto"* e la sua funzione principale è quella di permettere al Giudice la corretta ricostruzione e dimostrazione dei fatti affermati dalle parti nel corso del processo.

Durante il processo, infatti, sia in sede civile che penale, il giudice deve ricostruire, sulla base delle prove raccolte , la verità dei fatti ai fini della propria decisione.

Sono considerati oggetti di prova[7] i fatti che si riferiscono all'imputazione, alla punibilità e alla determinazione della pena o della misura di sicurezza,

[7]Art.187 c.p.p.

mentre per quel che riguarda l'ammissione della prova scientifica, il legislatore non fornisce al Giudice un criterio espresso.

I riferimenti che troviamo nel codice sono quelli comuni a tutti i mezzi di prova nel momento in cui le parti ne chiedono l'ammissione: pertinenza, rilevanza, non sovrabbondanza e legalità[8].

Tuttavia, quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona[9].

2.3 La perizia

La perizia è uno dei mezzi di ricerca della prova utilizzato quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze scientifiche o tecniche[10]. Può essere anche disposta d'ufficio dal giudice con ordinanza motivata, contenete la nomina del perito, la sommaria enunciazione dell'oggetto delle indagini, l'indicazione del giorno, dell'ora e del luogo fissati per la comparizione del perito[11]. A seguito della nomina del perito da parte del giudice, il Pubblico Ministero e le parti hanno la facoltà di nominare i propri consulenti tecnici in numero non superiore, per ciascuna parte, a quello dei periti. Tuttavia, anche quando non è disposta la perizia,

[8] Art.190 c.p.p
[9] Art.189 c.p.p.
[10] Art.220 c.p.p.
[11] Art.225 c.p.p.

ciascuna parte può nominare, in numero non superiore a due, i propri consulenti tecnici con lo scopo di ricercare elementi a favore delle supposizioni della parte.

2.4 L'acquisizione delle fonti di prova

L'acquisizione delle fonti di prova avviene attraverso i cosiddetti "mezzi di ricerca della prova", ossia quegli strumenti volti alla acquisizione di fonti di prova cioè di cose materiali, tracce, dichiarazioni o persone da cui si possa ricavare la prova. Tali mezzi di ricerca della prova sono disciplinati dal Codice di Procedura Penale e riguardano:

1. ispezioni;
2. perquisizioni;
3. sequestri probatori;
4. intercettazioni.

2.4.1 Ispezione

L'ispezione[12] è un'attività mirata all'osservazione di persone, luoghi, cose e volta all'accertamento di tracce o altri effetti materiali del reato. La sua funzione è quella di consentire all'autorità giudiziaria di percepire direttamente elementi utili alla ricostruzione del fatto.

[12]Art.244 e segg. c.c.p.

Durante il dibattimento, il potere di disporre le ispezioni compete sempre al Giudice, invece, durante la fase delle indagini preliminari, possono essere compiute oltre che dal Pubblico Ministero[13] anche dalla Polizia Giudiziaria. Tuttavia, si ritiene che possa essere esclusa la possibilità per il Pubblico Ministero di delegare alla Polizia Giudiziaria l'ispezione, dal momento che è un'attività che limita alcune libertà costituzionali (libertà personale, domiciliare...), per cui è richiesta soltanto a seguito di atto motivato dall'autorità giudiziaria. Tale operazione è caratterizzata dall'irripetibilità e, pertanto, ove siano stati utilizzati i metodi di acquisizione idonei a garantire l'integrità e la genuinità dei dati, essi potranno essere pienamente utilizzati in dibattimento.

2.4.2 Perquisizione

La perquisizione[14] è un'attività diretta ad individuare e acquisire e il corpo del reato o le cose che ad esso si riferiscono, qualora si ritengano, con "fondati motivi", nascoste sulla persona o in un determinato luogo. Può prodursi in sede d'indagini preliminari a seguito del Pubblico Ministero, il quale, attraverso decreto motivato la dispone prevedendo altresì se eseguirla personalmente o delegarla a ufficiali della Polizia Giudiziaria. Può accadere, però, che sempre in sede d'indagini preliminari, la Polizia Giudiziaria possa dar luogo di propria iniziativa a perquisizione locale o personale nei casi

[13] Art. 364 c.p.p.
[14] Art.247 e 253 c.c.p.

di flagranza del reato o evasione. È tuttavia necessario sottolineare che la perquisizione, come l'ispezione, è un'attività che limita alcune libertà costituzionali (libertà personale, domiciliare...), e per questo è richiesta soltanto a seguito di atto motivato dall'autorità giudiziaria. Inoltre, la perquisizione necessita che ogni operazione avente ad oggetto lo strumento informatico, sia conforme ad una metodologia operativa conforme ai protocolli internazionali (*best practices*) che garantisca l'integrità e la genuinità dei dati, affinché non siano possibili contestazioni in sede dibattimentale.

2.4.3 Sequestro probatorio

Il sequestro probatorio è un mezzo di ricerca della prova attraverso il quale l'autorità giudiziaria acquisisce il corpo del reato o le cose pertinenti e necessarie per l'accertamento dei fatti[15].

Esso è strettamente collegato alla perquisizione, essendone spesso una diretta conseguenza e rappresenta il tipo di sequestro più usato dalla Polizia Giudiziaria, poichè è la procedura più semplice ed immediatamente accessibile. Infatti, laddove non sia possibile l'intervento tempestivo dell'Autorità giudiziaria, è consentito agli ufficiali di Polizia giudiziaria sequestrare i medesimi beni prima che essi si disperdano.

Fondamentale importanza svolge la motivazione del decreto di sequestro, perchè consente di valutare la sussistenza dei requisiti di legge e, dunque, la

[15] Art.253 c.p.p.

legittimità del provvedimento.

Contro il decreto di sequestro tanto l'imputato quanto la persona cui le cose sono state sequestrate, nonché colei che avrebbe diritto alla restituzione di esse, possono proporre richiesta di riesame[16] . I beni sequestrati sono custoditi in cancelleria del Giudice ovvero in segreteria del Pubblico Ministero; laddove ciò non fosse possibile od opportuno, l'autorità Giudiziaria provvede ad indicare altro luogo adatto, nominando per tale scopo un custode ed avvertendolo dei suoi doveri e delle responsabilità penali cui va incontro in caso di violazione [10].

2.4.4 Intercettazione

L'intercettazione[17] è un'attività diretta a captare comunicazioni e conversazioni, nonché flussi di comunicazioni informatiche o telematiche mediante strumenti della tecnica. L'intercettazione tende a limitare gravemente alcune importanti libertà costituzionali, fra cui la libertà di comunicazione del pensiero e la libertà domiciliare, per cui sono dettate particolari norme procedurali volte a garantire la legittimità formale e sostanziale dell'attività.

Di regola, l'intercettazione è autorizzata dal giudice per le indagini preliminari con decreto motivato su richiesta del Pubblico Ministero. Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio ai fini della prosecuzione delle indagini, è lo stesso

[16] Art. 324 c.p.p.
[17] Art.266 e segg. c.p.p.

pubblico ministero a disporre l'intercettazione con decreto motivato. Le forze di polizia, che eseguono su incarico del pubblico ministero le attività di intercettazione, hanno a disposizione diverse tecniche. La più utilizzata in termini numerici è l'intercettazione telefonica richiesta agli operatori telefonici, che sono obbligati ad adempiere alle richieste dell'Autorità Giudiziaria tramite le proprie strutture tecnologiche ed organizzative. Seguono, poi, le intercettazioni ambientali, realizzate principalmente con l'impiego di microspie e telecamere nascoste e le intercettazioni informatiche che utilizzano particolari strumentazioni software ed hardware [11].

2.5 Ripetibilità ed irripetibilità degli accertamenti tecnici

L'accertamento tecnico è un'attività d'indagine del Pubblico Ministero che assume grande rilevanza nell'Informatica forense. È ormai noto che, per sua natura, il dato digitale, sottoposto ad acquisizione ed analisi, debba essere trattato con specifiche conoscenze e strumentazioni tecniche.

Nel corso del procedimento penale, dunque, è frequente che il Pubblico Ministero debba avvalersi dell'ausilio di consulenti tecnici esperti del settore, laddove abbia bisogno di acquisire conoscenze che presuppongono specifiche competenze di natura tecnico-scientifica. Queste competenze saranno esercitate dal consulente tecnico incaricato, tramite accertamenti, rilievi segnaletici, fotografici o descrittivi.

Un tipico caso di accertamento è l'esame di supporti informatici, posti sotto sequestro probatorio durante le indagini preliminari.

2.5.1 Accertamento tecnico ripetibile

È opportuno premettere che la dizione *"Accertamenti Tecnici Ripetibili"* non è contemplata nel c.p.p. Si può però affermare che rientrano in questa categoria tutti gli accertamenti svolti dai consulenti Tecnici del Pubblico Ministero, con i limiti previsti dall'Art. 360 c.p.p. (*"Accertamenti Tecnici non Ripetibili"*) [12].

È ovvio, pertanto, che tutto quanto non rientra nelle disposizioni del predetto articolo 360 è chiaramente ripetibile, dove per "ripetibile" si intende che l'analisi forense in questione non sia invasiva e che quindi non comprometta lo stato dell'informazione contenuta.

2.5.2 Accertamento tecnico non ripetibile

Si definiscono accertamenti tecnici non ripetibili[18] quegli accertamenti che riguardano persone, cose o luoghi il cui stato è soggetto a modificazione. Il concetto di irripetibilità esprime la necessità che è fondamentale compiere quell'accertamento il prima possibile, in quanto, con molta probabilità, tale atto potrebbe non essere più disponibile nell'immediato futuro. La norma, pertanto, può essere applicabile anche nelle ipotesi di acquisizione ed analisi

[18] Art.360 c.p.p.

di dati contenuti su supporti informatici, in assenza di strumentazione tecnica idonea e sufficiente a garantire la ripetibilità dell'operazione.

Gli accertamenti tecnici non ripetibili costituiscono lo strumento mediante il quale la formazione della prova avviene nella fase delle indagini preliminari, antecedentemente al dibattimento. Ai sensi dell'art. 360 c.p.p. quando gli accertamenti previsti riguardano persone, cose o luoghi il cui stato è soggetto a modificazione, il pubblico ministero avvisa, senza ritardo, la persona sottoposta alle indagini, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici. I difensori, nonché i consulenti tecnici eventualmente nominati, hanno diritto di assistere al conferimento dell'incarico, di partecipare agli accertamenti e di formulare osservazioni e riserve.

2.6 Consulenti tecnici

Una volta esaurite le fasi di ricerca delle fonti di prova, i supporti sequestrati devono essere sottoposti ad approfondite analisi, al fine di recuperare e informazioni in esse contenute.

Questo tipo di attività è solitamente demandata ad un consulente tecnico, cioè un soggetto chiamato non a decidere in luogo del giudice o insieme con esso, ma semplicemente a consigliare il giudice con relazioni o pareri non vincolanti. Si tratta, pertanto, di una figura che ha particolari e specifiche competenze tecniche.

2.6.1 Consulenti tecnici d'ufficio

Il Pubblico Ministero, quando procede ad accertamenti per cui sono necessarie specifiche competenze, può nominare ed avvalersi di consulenti[19]. Solitamente, il consulente deve essere scelto tra i soggetti iscritti nell'apposito albo di categoria istituito presso ogni tribunale e, solo in via meramente sussidiaria, può essere scelto tra persone particolarmente competenti nella materia. Il CTU, quando è nominato dal Giudice che lo ha scelto tra gli esperti iscritti all'Albo, è obbligato a svolgere l'incarico ricevuto, salvo ricorrano particolari motivazioni espressamente previste dal c.p.c. per le quali lo stesso ha la possibilità di rinunciare all'incarico (ad es.: legame di parentela con le parti in causa, aver già prestato l'opera di CTU in un precedenti gradi di giudizio nella stessa causa, ecc). L'attività del consulente tecnico d'ufficio è principalmente quella di rispondere in maniera puntuale e precisa ai quesiti che il Giudice formula nell'udienza di conferimento dell'incarico e di esporne i risultati in un'apposita relazione che prende il nome di Consulenza Tecnica d'Ufficio [14]. Qualunque sia il caso nel quale è richiesto l'intervento del CTU, questi deve essere sintetico e preciso rispetto alle domande che gli vengono poste, così da potere chiarire al giudice esattamente quegli elementi che egli intende valutare per giungere ad una decisione. In particolare, è importante che il CTU faccia sempre riferimento a dati certi e, possibilmente, che accompagni tutto ciò che afferma con opportuna documentazione focalizzandosi, nella parte finale, sulle proprie conclusioni tecniche. Queste devono

[19] Art. 359 del c.p.p.

essere il risultato di un procedimento logico ben preciso, ma non devono contenere in alcun modo giudizi che possano influenzare le decisioni del giudice. Tra i doveri principali del Consulente Tecnico d'Ufficio, infatti, vi è quello di garantire la propria imparzialità nei confronti delle parti e di consentire sempre il contradditorio ovvero la possibilità delle parti di esprimere i loro punti di vista.

Il CTU, dunque, svolge un ruolo importantissimo e decisivo, soprattutto quando l'esito della causa è legato alla corretta valutazione e rappresentazione dei vari aspetti tecnici. Nell'espletamento del suo incarico può incorrere in responsabilità penale:

- **per falsa perizia o interpretazione**[20], secondo la quale, il consulente dà pareri o interpretazioni mendaci ed afferma fatti non conformi al vero. La condanna importa, oltre l'interdizione dai pubblici uffici, l'interdizione dalla professione.

- **per frode processuale**[21], secondo la quale il consulente nella esecuzione di una perizia immuta artificiosamente lo stato dei luoghi, delle cose o delle persone. La condanna, qualora il fatto non sia preveduto come reato da una particolare disposizione di legge, con la reclusione da sei mesi a tre anni.

[20] Art. 373 c.p
[21] Art. 374 c.p.

- **per false dichiarazioni o attestazioni in atti destinati all'autorità giudiziaria**[22], salvo che il fatto costituisca più grave reato, è punito con la reclusione da uno a cinque anni.

- **per intralcio alla giustizia**[23], per cui chiunque offre o promette denaro o altra utilità alla persona chiamata a svolgere attività di perito, consulente tecnico o interprete per indurla a commettere i reati previsti dagli articoli *371bis, 371ter, 372 e373,* soggiace, qualora l'offerta o la promessa non sia accettata, alle pene stabilite dagli stessi articoli, ridotte dalla metà ai due terzi e l'interdizione dai pubblici uffici.

2.6.2 Consulenti tecnici di parte

La consulenza giudiziaria può anche prevedere l'intervento di altri professionisti che svolgono la propria opera non tanto per il giudice quanto per le parti in causa: il loro ruolo è detto *consulente di parte* (CTP). Il consulente tecnico di parte non è altro che un libero professionista con specifiche competenze tecniche, il quale ha il compito di affiancare il consulente tecnico nominato dal giudice nell'esecuzione del suo incarico e di svolgere le proprie osservazioni a supporto o critica del risultato al quale il perito del giudice sarà giunto.

Il consulente di parte assume un ruolo fondamentale per la risoluzione di questioni che, sempre più spesso, dipendono da valutazioni di carattere tecnico

[22] Art.374 bis c.p
[23] Art.377 c.p

molto precise. Il consulente tecnico di parte, inoltre, è sempre pagato dalla parte che lo nomina ed ha diritto di essere compensato in relazione alla propria parcella professionale (se presente), ma anche in base ad una eventuale convenzione stipulata con il cliente. Il professionista incaricato dalla parte non deve necessariamente essere iscritto ad un albo professionale, poiché il rapporto tra la parte che lo nomina ed il consulente è, più che altro, di natura fiduciaria. Ciò non toglie che, di fronte alla nomina come consulente di parte di un professionista iscritto ad uno specifico albo, la credibilità delle osservazioni che questo potrà svolgere sarà maggiore agli occhi del giudice.

Al contrario del consulente tecnico, nominato dal giudice, il perito di parte può rifiutare di prestare la sua opera e non è tenuto a motivare il rifiuto di un incarico perché tutto ciò rientra nelle sue piene facoltà. È altresì esonerato da qualsiasi obbligo di cooperazione o quant'altro nei confronti dell'autorità giudiziaria (obblighi ai quali invece è sottoposto il CTU), al di fuori del divieto di ostacolare illegittimamente l'attività del consulente del giudice. Non va comunque dimenticato che la sua opera deve sempre rispettare i principi stabiliti dal proprio codice deontologico (se presente) e dai tradizionali parametri di correttezza professionale, legalità e moralità.

Capitolo 3

3 Il panorama normativo italiano

3.1 La convenzione sul cybercrime e la sua ratifica

La Convenzione di Budapest sulla criminalità informatica è stata resa dal Consiglio d'Europa in data 23 marzo 2001 ed è stata ratificata ed attuata in Italia soltanto in tempi recenti, con la legge del 18 marzo 2008 n.48.

La Convenzione, firmata nel 2001, è entrata in vigore il 1° luglio 2004 con l'obiettivo di realizzare una politica europea comune in grado di coordinare e rendere più efficace la lotta ai crimini informatici. In particolare, la Convenzione tende ad uniformare i reati legati alla criminalità informatica, a dotare i Paesi firmatari degli strumenti adeguati allo svolgimento delle indagini dei crimini correlati all'area informatica e a costruire, infine, un efficace regime di cooperazione internazionale.

La Convenzione di Budapest è di fatto il primo accordo internazionale a inquadrare i crimini legati a internet e alle reti informatiche e ad estendere la portata dei reati informatici a "*...tutti i reati in qualunque modo commessi mediante un sistema informatico, anche nel caso in cui la prova del reato sia sotto forma elettronica*". Per allinearsi alla Convenzione, gli Stati membri hanno apportato importanti novità ai reati previsti dal Codice penale. Nel caso dell'Italia, il codice penale già prevedeva quasi tutte le fattispecie,

pertanto le modifiche sono state imposte inserendo degli incisi nelle norme esistenti.

3.1.1 Modifiche al codice penale

La Legge di ratifica 48/2008 ha portato alle seguenti modifiche degli articoli del codice penale:

art. 491 bis (Documenti informatici)

> *Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine, per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.*
>
> **[SOPPRESSO: a tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.]**

Art. 615-quinquies (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)

L'articolo 615-quinquies del codice penale è sostituito dal seguente:

1. *Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.*

3.1.2 Modifiche al Codice della privacy

La Legge di ratifica 48/2008 ha introdotto i seguenti commi all'articolo 10 del Codice della Privacy:

art. 10. (Conservazione dei dati di traffico)

4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonchè gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto

legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale.

4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia.

3.1.3 Modifiche al Codice di Procedura Penale

La Legge di ratifica 48/2008 ha portato alle seguenti modifiche degli articoli del codice di procedura penale:

art. 244 (Casi e forme delle ispezioni)

1. L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.

2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, ***anche in relazione a sistemi informatici o telematici, adottando misure***

tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

Art. 247 (Casi e forme delle perquisizioni)

1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.

1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

2. La perquisizione è disposta con decreto motivato.

3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.

Art. 248(Richiesta di consegna)

1. Se attraverso la perquisizione si ricerca una cosa determinata, l'autorità giudiziaria può invitare a consegnarla. Se la cosa è presentata, non si procede alla perquisizione, salvo che si ritenga utile procedervi per la completezza delle indagini.

2. Per rintracciare le cose da sottoporre a sequestro o per accertare altre circostanze utili ai fini delle indagini, l'autorità giudiziaria o gli ufficiali di polizia giudiziaria da questa delegati possono esaminare ***presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici.*** *In caso di rifiuto, l'autorità giudiziaria procede a perquisizione.*

Art. 254(Sequestro di corrispondenza)

SOSTITUITO: 1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato.

2. 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.*

3. Le carte e gli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati.

Art. 254-bis(Sequestro di dati informatici)

1.L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.

Art. 256(Dovere di esibizione e segreti)

1.Le persone indicate negli artt. 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, ***nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto,*** *e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreti di Stato ovvero di segreto inerente al loro ufficio o professione.*

2. Quando la dichiarazione concerne un segreto di ufficio o professionale (200), l'autorità giudiziaria, se ha motivo di dubitare della fondatezza di essa e ritiene di non potere procedere senza acquisire gli atti, i documenti o le cose indicati nel comma 1, provvede agli accertamenti necessari. Se la dichiarazione risulta infondata, l'autorità giudiziaria dispone il sequestro.

3.Quando la dichiarazione concerne un segreto di Stato, l'autorità giudiziaria ne informa il presidente del Consiglio dei Ministri, chiedendo che ne sia data conferma. Qualora il segreto sia confermato e la prova sia essenziale per la definizione del processo, il giudice dichiara non doversi procedere per l'esistenza di un segreto di Stato.

4. Qualora, entro sessanta giorni dalla notificazione della richiesta, il Presidente del Consiglio dei Ministri non dia conferma

del segreto, l'autorità giudiziaria dispone il sequestro.

Art. 259. (Custodia delle cose sequestrate)

1. Le cose sequestrate sono affidate in custodia alla cancelleria o alla segreteria. Quando ciò non è possibile o non è opportuno, l'autorità giudiziaria dispone che la custodia avvenga in luogo diverso, determinandone il modo e nominando un altro custode, idoneo a norma dell'art.120.

2. All'atto della consegna, il custode è avvertito dell'obbligo di conservare e di presentare le cose a ogni richiesta dell'autorità giudiziaria nonché delle pene previste dalla legge penale per chi trasgredisce ai doveri della custodia. Al custode può essere imposta una cauzione. ***Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria.*** *Dell'avvenuta consegna, dell'avvertimento dato e della cauzione imposta è fatta menzione nel verbale. La cauzione è ricevuta, con separato verbale , nella cancelleria o nella segreteria.*

Art. 260 (Apposizione dei sigilli alle cose sequestrate. Cose deperibili).

1. Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che la assiste (126) ovvero, in relazione alla natura delle cose, con altro mezzo, ***anche di carattere elettronico o informatico****, idoneo a indicare il vincolo imposto a fini di giustizia.*

2. L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti, disponendo, quanto alle cose, in conformità dell'art.259. ***Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria.***

3. Se si tratta di cose che possono alterarsi, l'autorità giudiziaria ne ordina, secondo i casi, l'alienazione o la distruzione.

Art. 352. (Perquisizioni)

1. Nella flagranza del reato o nel caso di evasione, gli ufficiali di polizia giudiziaria procedono a perquisizione personale o locale,

quando hanno fondato motivo di ritenere che sulla persona si trovino occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero che tali cose o tracce si trovino in un determinato luogo o che ivi si trovi la persona sottoposta alle indagini o l'evaso.

1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.

2. Quando si deve procedere alla esecuzione di un'ordinanza che dispone la custodia cautelare o di un ordine che dispone la carcerazione nei confronti di persona imputata o condannata per uno dei delitti previsti dall'art.380 ovvero al fermo di una persona indiziata di delitto, gli ufficiali di polizia giudiziaria possono altresì procedere a perquisizione personale o locale se ricorrono i presupposti indicati nel comma 1 e sussistono particolari moti-

vi di urgenza che non consentono la emissione di un tempestivo decreto di perquisizione.

3. La perquisizione domiciliare può essere eseguita anche fuori dei limiti temporali dell'art.251 quando il ritardo potrebbe pregiudicarne l'esito.

4. La polizia giudiziaria trasmette senza ritardo, e comunque non oltre le quarantotto ore, al pubblico ministero del luogo dove la perquisizione è stata eseguita il verbale delle operazioni compiute. Il pubblico ministero, se ne ricorrono i presupposti, nelle quarantotto ore successive, convalida la perquisizione.

Art. 353. (Acquisizione di plichi o di corrispondenza)

1. Quando vi è necessità di acquisire plichi sigillati o altrimenti chiusi, l'ufficiale di polizia giudiziaria li trasmette intatti al pubblico ministero per l'eventuale sequestro.

*2. Se ha fondato motivo di ritenere che i plichi contengano notizie utili alla ricerca e all'assicurazione di fonti di prova che potrebbero andare disperse a causa del ritardo, l'ufficiale di polizia giudiziaria informa col mezzo più rapido il pubblico ministero il quale può autorizzarne l'apertura immediata e l'**accertamento del contenuto**.*

*3. Se si tratta di lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, **anche se in forma elettronica***

***o se inoltrati per via telematica**, per i quali è consentito il sequestro a norma dell'art.254, gli ufficiali di polizia giudiziaria, in caso di urgenza, ordinano a chi è preposto al servizio postale, **telegrafico, telematico o di telecomunicazione** di sospendere l'inoltro. Se entro quarantotto ore dall'ordine della polizia giudiziaria il pubblico ministero non dispone il sequestro, gli oggetti di corrispondenza sono inoltrati.*

Art. 354. (Accertamenti urgenti e sequestro)

1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.

2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente ovve-

ro non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. ***In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità****. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.*

3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale.

3.2 Normative sul trattamento dei dati personali

3.2.1 Testo unico sulla Privacy

Il Codice in materia di protezione dei dati personali è stato adottato in Italia in conformità alla Legge delega 127/2001 e promulgato dal Presidente della Repubblica con il Decreto legislativo 196/2003. Attualmente noto come Testo

Unico sulla privacy, il Codice introduce alcune novità e, in particolare, una serie di adempimenti a carico delle aziende. Nello specifico, questa normativa dispone l'adozione delle precise misure organizzative e di sicurezza che devono applicarsi al trattamento dei dati. Infatti, chiunque ha diritto non solo alla protezione dei dati personali che lo riguardano ma, anche, di esercitare un controllo sulle informazioni che lo riguardano. Di contro, chiunque tratti dati personali deve assicurare un elevato livello di tutela del diritto alla protezione dei dati personali dell'interessato.

3.2.2 Delibere del Garante della Privacy

Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente volta ad assicurare la tutela dei diritti e delle libertà fondamentali e il rispetto della dignità nel trattamento dei dati personali. I suoi compiti sono molteplici, ma principalmente si occupa di controllare se il trattamento dei dati personali da parte di privati e pubbliche amministrazioni è lecito e corretto. Le delibere emesse dal Garante sono molte, ma tra quelle di interesse per i soggetti connessi all'informatica forense ricordiamo:

- **del. Garante 46/08**, Trattamento dei dati ad opera dei consulenti tecnici e periti del giudice e del Pubblico Ministero. In particolare, per quanto riguarda il Consulente tecnico nominato dalle parti, questi dovrà:

-rispettare i principi di liceità e di esattezza dei dati, nonché le misure di sicurezza volte alla protezione dei dati stessi;

-potrà trattare lecitamente i dati personali nei limiti delle necessità per lo svolgimento dell'incarico ricevuto, utilizzando dati sensibili o giudiziari se indispensabili;

-potrà acquisire solo i dati personali pertinenti e non eccedenti le finalità dell'incarico;

-fermo restando il dovere di segreto professionale, potrà comunicare a terzi i dati solamente se necessario per la tutela dell'assistito;

-a differenza di quanto previsto per il C.T.U. sarà tenuto ad informare i soggetti interessati del trattamento dei dati e dovrà ottenerne il consenso.

- **Del. Garante 178/08**. Recepimento normativo su traffico telefonico e telematico.
- **Del. Garante 60/08**. Trattamento dei dati nell'ambito dello svolgimento di investigazioni difensive.
- **Del. Garante 35/08**. Trattamento dei dati ad opera dei liberi professionisti.
- **Del. Garante 37/08**. Trattamento dei dati ad opera degli investigatori privati.

Capitolo 4

4 Strumenti e tecniche per la navigazione anonima in rete

In passato, quando gli archivi erano per lo più cartacei, chi voleva reperire informazioni relative a terzi doveva affrontare le difficoltà connesse alla dislocazione fisica degli archivi, al loro accesso ed al reperimento ed estrazione delle informazioni. Oggi, invece, si ha la possibilità di effettuare una ricerca su Internet per reperire molteplici informazioni idonee a rivelare passato e presente delle persone, le loro abitudini, professione, status, hobbies ed interessi.

Quando navighiamo in Internet lasciamo, dunque, inevitabilmente delle tracce, non solo nel nostro PC, ma anche nei siti web che andiamo a visitare. Se navighiamo nella Rete attraverso il nostro browser web[24] (Chrome, Internet Explorer, Firefox, Safari, Opera, ecc..) vengono memorizzate sul nostro computer alcune informazioni, quali:

- siti visitati;
- file scaricati;

[24]Un browser web è un software che permette di navigare su Internet e di visualizzare i contenuti delle pagine web.

- eventuali credenziali di accesso (es. utente e password utilizzati per accedere a Facebook);
- eventuali dati personali (es. abbiamo acquistato online un articolo ed abbiamo fornito attraverso un apposito modulo del sito i nostri recapiti, indirizzo di casa, ecc.);
- momento esatto in cui è stato effettuato l'accesso;
- frequenza di accesso.

Tutte queste informazioni potrebbero essere raccolte a nostra insaputa da qualche *spammer*[25], da altri siti web che vogliono conoscere le nostre tendenze di navigazione o ancora da truffatori (attraverso virus, trojan, malware ed altri codici malevoli), che potrebbero utilizzare tali dati per violare illegalmente la nostra privacy. É il caso, ad esempio, di un utente che visitando un sito web o accettando il contratto di licenza di un software, potrebbe attivare inconsapevolmente uno *spyware*[26]. Questo "programma spia", una volta installato su un computer, infatti, potrebbe inviare ad un computer remoto le informazioni relative ai siti visitati, in modo da tracciare i gusti e le preferenze dell'utente e poter inviare così pubblicità mirata sulle preferenze ricavate sotto forma di pop-up o banner pubblicitari.

[25]Lo spamming è l'invio di messaggi indesiderati (generalmente commerciali)

[26]Programmi informatici finalizzati a spiare le nostre attività on line e a compiere determinate operazioni a nostra insaputa e senza il nostro consenso.

Per questi motivi la navigazione anonima sul Web rappresenta ormai un'esigenza sempre più diffusa da parte degli utenti della Rete.

4.1 Privacy ed Internet

Il termine privacy è un concetto di origine anglosassone, inizialmente riferito alla sfera della vita privata. Tale concetto fu citato per la prima volta nell'articolo di Warren & Brandeis, intitolato "*The right to privacy*[27]". Questo diritto ad essere lasciato solo era inizialmente legato alla proprietà privata ed ai mezzi di tutela di tale diritto. Con il forte sviluppo tecnologico, però, la privacy ha assunto nuova dimensione, inglobando i concetti di segretezza e informazione dei dati telematici. La diffusione della Rete, infatti, non solo ha cambiato radicalmente i comportamenti ed il modo di relazionarsi degli individui, ma anche la percezione della propria identità personale, soprattutto in ragione delle nuove forme con le quali gli utenti esprimono la loro creatività, si connettono o condividono parte della loro intimità. A livello concettuale, quindi, si crea la contrapposizione tra identità reale o fisica ed identità virtuale, quale possibile identificazione di un soggetto coinvolto nelle attività in rete.

La memorizzazione di massicce quantità di dati personali in banche dati, sempre più numerose, che possono essere non solo facilmente consultate, ma anche messe in relazione fra loro, ha fatto sì che ogni individuo veda oggi

[27] L.D.Brandeis-S.Warren, The Right of Privacy, in 4 Harvard Law Review, 1890.

affiancarsi al corpo fisico un nuovo «corpo elettronico», formato dall'insieme di tutti i dati personali che lo riguardano. I vari archivi della Rete raccolgono informazioni che vanno dai dati ufficiali, a quelli relativi alle transazioni effettuate, alla navigazione su Internet o alle email. Per la sua stessa struttura, infatti, nella Rete i dati sono replicati su vari siti e nelle *cache* e, quindi, facilmente rintracciabili e raramente cancellati [14]. La sensazione che ogni individuo possieda un «corpo elettronico» è palesemente avvertita quando si utilizzano i motori di ricerca. Digitando un nome, si è raggiunti da un insieme affollato di informazioni correlate a quel nome, le quali non hanno necessariamente tutte rilevanza, qualità o affidabilità. Se ciò ha comportato, da un lato, indiscutibili vantaggi in termini di semplicità e rapidità nel reperimento e nello scambio di informazioni fra utenti della Rete, dall'altro ha determinato un enorme incremento di dati personali trasmessi, scambiati e memorizzati con i conseguenti pericoli connessi al loro illecito utilizzo da parte di terzi non autorizzati. Determinate informazioni personali, magari socialmente pregiudizievoli, infatti, possono rimanere a disposizione di chiunque ben oltre i limiti temporali dettati dal principio di finalità del trattamento dei dati. Appare evidente, quindi, come la relazione funzionale tra anonimato e privacy si ripete anche nel rapporto tra anonimato e diritto all'oblio. Ogni utente deve avere il "diritto a essere dimenticato", cioè avere la possibilità di cancellare, anche a distanza di molti anni, dagli archivi online, il materiale che può risultare sconveniente e dannoso per sua la personalità. In particolare, ogni individuo della Rete deve poter [15]:

"*controllare le informazioni in qualunque momento: avere accesso ai dati e poterli modificare o cancellare sono diritti fondamentali nel mondo digitale (..). I cittadini dovrebbero essere in grado di fornire il proprio consenso per la gestione dei dati personali, ad esempio quando si ritrovano a navigare online e dovrebbero anche avere il diritto di essere dimenticati, quando i loro dati non sono più necessari o magari quando sono gli stessi cittadini a volere la rimozione delle informazioni*[28]."

Dunque, al tradizionale concetto di privacy (diritto ad essere lasciati soli, inteso come diritto esclusivo di conoscenze delle vicende relative alla propria vita privata), oggi viene affiancato quello relativo alla tematica dei computer crimes, inteso come diritto-interesse al controllo dei propri dati personali.

La consapevolezza di questo nuovo diritto-necessità ha avuto l'effetto di spingere gli individui a tutelarsi nei confronti delle nuove tecnologie digitali, dando così vita alle prime tecniche di anonimato in rete.

4.2 Cosa si intende per "navigazione anonima"

L'anonimato su Internet è una proprietà comunemente identificata come la privatezza della comunicazione elettronica [16]. Da un punto di vista più ampio, le comunicazioni anonime sono studiate nell'ambito della sicurezza informatica, quando un utente tenta di proteggere la propria riservatezza da coloro che vogliono scoprire certe informazioni. Infatti, quando si naviga su

[28] Viviane Reding, Commissaria UE per la Giustizia.

Internet, ogni sito web visitato lascia la propria traccia di passaggio sul proprio pc, tramite *cookie*[29], cronologia e così via sul server web tramite log con indirizzo *IP*[30]. Esistono però diverse ipotesi nelle quali l'utente ha interesse a conoscere se e quali dati vengono raccolti sul suo conto (e con quali finalità). Si può essere, infatti, interessati alle cosiddette *"tracce di navigazione"* lasciate nel corso dell'esplorazione in rete, attraverso le quali è possibile ricostruire non solo l'indirizzo di navigazione dell'utente (TCP/IP), ma anche tempi e modalità di consultazione dei siti visitati e, quindi, acquisire informazioni attinenti a preferenze, gusti e attitudini che risultano assai utili per ricostruire profili di consumo. Esistono poi quelle informazioni che sono inviate in occasione di una visita da un sito web al programma di navigazione (browser) e impresse e memorizzate nel disco fisso dell'utente, destinate ad essere rilette in occasione di ogni visita successiva. Nell'ambito delle risposte possibili ai problemi di riservatezza e di sicurezza, è decisiva da tempo proprio la parte svolta dai progettisti di hardware e di software. Alcuni browser, ad esempio, consentono all'utente un maggior controllo sull'ambiente e la scelta di rendersi o meno identificabile. Non rimangono salvate né le pagine e le immagini né le parole cercate sui motori di ricerca o la lista dei siti visitati e le sessioni terminano alla chiusura del browser. In sostanza, una volta chiu-

[29]Il Cookie è una sorta di promemoria della pagina internet visitata: contiene brevi informazioni che possono essere salvate sul computer dell'utente quando il browser richiama un determinato sito web.

[30]Internet Protocol address, un'etichetta numerica che identifica univocamente un dispositivo (host) collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di comunicazione.

sa la scheda/finestra in modalità riservata di tutto quello che è stato fatto sul computer non resterà traccia perchè tutto è gestito dalla memoria RAM. Ma questo è solo un aspetto della navigazione in rete: se invece si vuole navigare anonimamente senza lasciare tracce sui siti che si stanno visitando, è necessario cambiare o mascherare l'indirizzo IP. Per ragioni di gestione e sicurezza, infatti, i web server mantengono tracce del nostro indirizzo IP, che abbinato con data/ora fornisce la certezza dell'utenza che è transitata per un determinato sito.

Più precisamente, quando un computer si collega a internet viene identificato con un numero chiamato indirizzo IP, ossia uno standard utilizzato per identificare vari computer in una rete informatica. Tale indirizzo è formato da una serie di numeri, (un esempio IP è 194.112.213.122) e viene assegnato in modo univoco dal provider ad ogni connessione. Per cui, mascherare un indirizzo IP è sicuramente uno degli aspetti fondamentali della navigazione anonima a tutela della privacy in rete. A tal proposito, un contributo importante al miglioramento dei prodotti e delle pratiche a difesa della navigazione anonima viene dalle cosiddette *Privacy Enhancing Technologies* (PET) [17], tecnologie o prodotti software utili per rafforzare o migliorare la protezione della privacy. Rientrano nelle PETs, ad esempio, i dispositivi per bloccare i cookies, i sistemi di cifratura ed i software a supporto delle diverse tecniche di navigazione anonima[18, 19].

4.3 Strumenti per l'anonimato

Al momento attuale esistono numerosi sistemi che concorrono all'ottenimento di un certo grado di anonimato e protezione dei dati riservati.

I più diffusi sistemi PET[20] possono essere così catalogati:

- **software per cifrare i dati**. Sono strumenti che permettono di creare dischi fissi crittografati in modo da renderne accessibile il contenuto solo agli utenti autorizzati che conoscono la password o detengono il *token* per cifrare.

- **Server Proxy**. Un proxy è fondamentalmente un intermediario che si pone tra il pc di un utente e la Rete, inoltrando per conto dell'utente tutte le richieste. I proxy garantiscono un minimo grado di anonimato, rispetto ad altri sistemi.

- **Distribuzioni LIVE** (insieme di ambiente operativo e applicazioni). Sono strumenti pensati per fornire un ambiente il più sicuro e anonimo possibile per l'utilizzatore. La distribuzione può risiedere su una chiavetta, un CD o un DVD; il computer dell'utente viene avviato (boot) da questo supporto e lavora completamente ed unicamente in memoria RAM, senza utilizzare il disco ed il sistema operativo del computer ospitante.

- **Darknet.** Una darknet è una rete virtuale privata, del tutto separata da Internet. Nel suo significato più generale, una darknet può essere

qualsiasi tipo di gruppo chiuso e privato di persone che comunicano tra loro, ma il nome spesso è usato nello specifico per reti di condivisione di file, dette P2P. Solamente all'interno di questa rete viene garantito anonimato e privacy.

- **Mix Network.** Questi sistemi creano tra il pc di un utente e la Rete una catena di proxy, attraverso la quale vengono inviati i dati. In aggiunta ogni messaggio inviato viene criptato da ogni proxy, il quale conosce solamente il nodo da cui il messaggio è arrivato e quello a cui deve essere trasmesso. Le mix network permettono di raggiungere un buon livello di anonimato.

- **Web browser portable**. Quasi tutti i principali browser (Internet Explorer, Firefox, Google Chrome, Safari e Opera) includono ora una navigazione in modalità privata e portable. Sono applicazioni (ad esempio: per scrivere, gestire la posta elettronica, cifrare i dati, chattare, navigare, cancellare informazioni) che sono, appunto, portable, ossia non hanno bisogno di essere installate in un sistema operativo ma possono "vivere" tranquillamente su una chiave USB abbastanza capiente o su un disco esterno. Lasciano tracce minime sul sistema operativo che le ospita [18].

4.4 Anonimato in rete sotto il profilo giuridico

Nella società dell'informazione di oggi, in cui raccogliere dati o catalogare informazioni è divenuta ormai un'attività molto diffusa, la descrizione del quadro normativo relativo all'anonimato assume sempre più una notevole importanza. Non esiste nell'ordinamento giuridico italiano un diritto generale all'anonimato, ma esso è collegato a particolari esigenze di tutela[21].

Il quadro che si prospetta al giurista italiano è frammentario ed è difficile da ricondurre in una categoria specifica. Se ne parla, infatti, in diversi settori:

- **diritto civile** (diritto d'autore, protezione dei dati personali, anonimato della madre);
- **diritto penale** (aggravante per minacce);
- **diritto amministrativo** (anonimato in concorsi);
- **diritto costituzionale** (libertà di manifestazione del pensiero).

4.4.1 Anonimato nel codice in materia di protezione dei dati personali

Quando si parla di anonimato in rete, però, tale tema rappresenta sempre più uno strumento di protezione e di tutela del soggetto al quale si riferiscono i dati, tanto da costituire l'inevitabile punto di riferimento nell'applicazione della normativa sulla protezione dei dati personali. Ne forniscono conferma

i numerosi articoli del Codice in materia di protezione dei dati personali che richiamano direttamente o indirettamente l'anonimato, quali:

- **Il diritto alla protezione dei dati personali**. È sancito dall'art.1 del Codice della Privacy, secondo il quale:

  "Chiunque ha diritto alla protezione dei dati personali che lo riguardano."

In altre parole, si riferisce al diritto di soggetto di esercitare il controllo sulle informazioni che lo riguardano, come quelle riguardanti le modalità e le finalità di trattamento dei propri dati e la loro origine.

- **Il principio di necessità nel trattamento dei dati**. È sancito dall'art.3 del Codice in materia di protezione dei dati personali, stabilisce che:

  "I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità."

Tale articolo introduce nell'ordinamento giuridico italiano il principio di necessità nel trattamento dei dati personali e l'obbligo, dove previsto, di ridurre

al minimo l'utilizzazione dei dati identificativi, di trattare tali dati solo quando necessario, e quindi imponendo, in capo al fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica, di rendere anonimi i dati non più necessari all'effettuazione della comunicazione.

- **Le disposizioni in materia di dati relativi al traffico.** Sono sancite dall'art.123 del Codice in materia dei dati personali, in materia di dati relativi al traffico, secondo il quale:

  "I dati relativi al traffico riguardanti contraenti ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica."

Tale art. impone ai fornitori di reti pubbliche di comunicazione che i dati relativi la traffico vadano cancellati o resi anonimi quando non più necessari ai fini della trasmissione della comunicazione elettronica, evidenziando così l'illegittimità di una conservazione indiscriminata dei dati di traffico.

4.4.2 Anonimato nella Costituzione

Nel panorama giuridico l'anonimato viene delineato secondo molteplici aspetti ed è per questo che sono numerose le norme che lo racchiudono.

Un'ulteriore fonte è indubbiamente la Costituzione. È possibile analizzare, infatti, almeno due articoli che al loro interno comprendono il diritto all'anonimato:

- **l'art.2** che riconosce i diritti inviolabili dell'uomo.

Attraverso l'art.2 della Costituzione, il concetto di "*anonimato in rete*", viene delineato dalla lettura combinata dei diritti alla riservatezza, all'identità personale ed il già citato diritto di protezione dei dati personali. Infatti, mentre il diritto alla riservatezza tutela l'esigenza ad avere una sfera personale dalla quale si può escludere chiunque dalla sua conoscenza, il diritto all'identità personale ed il diritto alla protezione dei dati personali rappresentano il modo in cui una persona sceglie di rappresentarsi agli occhi del pubblico, effettuando un controllo sulle informazioni che la riguardano.

- **l'art.21** che riconosce la libertà di manifestazione del pensiero.

Nell'art.21 della Costituzione il diritto all' anonimato si afferma come "mezzo" di libera manifestazione del pensiero, ossia come espressione libera di proprie opinioni, senza il timore di eventuali ripercussioni. Tale diritto, dunque, garantisce alla "*persona interessata di avere la possibilità di conservare l'anonimato, in particolare quando partecipa ai gruppi di discussione*[31]", pubblicando commenti ad articoli, post (ossia aggiornamenti di blog), filmati ed in qualsiasi altro contenuto informativo pubblicato in rete.

[31]Gruppo ex art.29. Tutela della vita privata su Internet

Vi sono, però, situazioni in cui l'anonimato su Internet, come mezzo di espressione, viene inquadrato come elemento di disturbo della personalità e, come tale, limitato dal diritto. È il caso della diffamazione on-line, dei reati pedo-pornografici e degli attacchi terroristici. Perciò, se da un lato, l'anonimato, attraverso il diritto mette in gioco importanti beni giuridici, come la riservatezza e le libertà dell'uomo, dall'altro evidenzia la necessità di limitare i danni derivanti dalla diffusione dei comportamenti illeciti e dannosi per la Rete.

4.4.3 I dati anonimi nel Codice della Privacy

Nell'Unione Europea il concetto di dato anonimo continua ad essere costruito in modo da riflettere un dato che non è collegato ad una persona identificata o identificabile. È in questo senso, infatti, che la definizione viene adottata dal legislatore italiano[32]:

> *"dato anonimo, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile."*

Analizzando tale definizione, risulta chiaro che sono tre gli elementi chiave a cui si riferisce la definizione: *il dato, il collegamento e l'identificabilità*. In particolare, il "dato" citato dal decreto si deve intendere in senso ristretto, in quanto fa riferimento al "dato personale[33]". Il dato, inoltre, può essere

[32] Art. 4 comma 1 lett. n) del Codice della Privacy
[33] Decreto leg 196/2003 art 4 comma 1 lettera b)

considerato anonimo non quando è criptato o nascosto, ma quando "non può essere associato" alla persona che lo ha prodotto o meglio al soggetto a cui si riferiscono le informazioni. La giurisprudenza definisce questa associazione come criterio di collegamento. Il collegamento può operare a diversi livelli e dipende da più fattori. In generale, si distinguono tre grandi categorie di collegamento: *provenienza, destinazione e pertinenza.*

Quando l'anonimato è riferito all'autore del documento, si fa riferimento al rapporto di provenienza; quando copre i contenuto dell'informazione ma non la sua provenienza, si parla di rapporto di pertinenza; ed infine, quando riguarda il destinatario si tratta di rapporto di destinazione. Le indicazioni più esplicite, per chiarire meglio questo aspetto, sembrano essere quelle fornite dal Consiglio d'Europa[34] e del Gruppo di lavoro ex art.29[35], sulla nozione di dato personale. Secondo la normativa europea[36] infatti, una persona:

> *"può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale."*

Il criterio secondo il quale un dato è personale o anonimo è la collegabilità ad un soggetto e questa associazione potenziale varia a seconda delle circostanze.

[34] Organizzazione internazionale il cui scopo è promuovere la democrazia, i diritti dell'uomo, l'identità culturale europea e la ricerca di soluzioni ai problemi sociali in Europa

[35] Il gruppo, istituito dall'art. 29 della direttiva 95/46/CE, è un organo comunitario indipendente, avente carattere consultivo con riguardo alla tutela dei dati e della vita privata.

[36] Direttiva 95/46/CE sulla Protezione dei dati personali, Art.2 lett. a)

Si pensi, ad esempio, a dati raccolti in forma anonima in una classe, che chiedano opinioni sulla qualità della didattica. Una domanda sul sesso del soggetto che compila il questionario può non permettere alcuna collegabilità dei dati ad un soggetto specifico, ma non se nella classe vi fosse un solo studente di sesso femminile. In questa eventualità, i dati non sarebbero dati anonimi per quello studente.

In altre parole, l'anonimia del dato va valutata caso per caso a seconda dei mezzi e delle situazioni reali, dal momento che potenzialmente moltissime informazioni possono essere dati personali.

La caratterizzazione di un dato come anonimo ha una notevole importanza, nel senso che le informazioni che non sono suscettibili di essere collegate ad una persona identificata o identificabile possono, invece, indurre la non-applicazione delle norme in materia di protezione dei dati o eventualmente la sua applicazione in modo individualizzato. Diversi ordinamenti giuridici prevedono, per esempio, una procedura di anonimizzazione del dato personale in relazione al soggetto corrispondente come requisito per il libero trattamento di questo dato in determinate circostanze.

4.5 Anonimato e sicurezza in rete

Quando si parla di anonimato su Internet non si può non parlare anche di sicurezza informatica. Se da una lato, infatti, anonimato e sicurezza relativi

alla navigazione in Internet rappresentano due concetti opposti, dall'altro vengono spesso implementati con i medesimi metodi e strumenti tecnologici.

Quando si pensa alla sicurezza informatica, il primo riferimento è sicuramente quello legato alla disciplina della privacy. I dati personali oggetto di trattamento, infatti, devono essere custoditi e controllati in modo da ridurre al minimo i rischi di distruzione e perdita, di accesso non autorizzato o non conforme alle finalità di raccolta. Ciò è reso possibile con l'adozione di misure di sicurezza dei dati in rete. In attuazione della direttiva europea in materia di sicurezza e privacy, infatti, nel settore delle comunicazioni elettroniche, il Garante per la privacy ha fissato un primo quadro di regole in base alle quali le società di tlc e i fornitori di servizi di accesso a Internet saranno tenuti a comunicare, oltre che alla stessa Autorità, anche agli utenti le "violazioni di dati personali" che i loro database dovessero subire a seguito di attacchi informatici o di eventi avversi, quali incendi o altre calamità.

Uno dei principali argomenti usati contro la possibilità di mantenere l'anonimato online, però, è rappresentato dalla necessità di perseguire gli autori dei reati commessi attraverso Internet. A causa delle caratteristiche fondamentali della rete, che rende spesso problematica l'identificazione dell'autore, i reati commessi attraverso Internet sono difficilmente perseguibili. Quando si parla di reati universalmente considerati gravi, come il terrorismo o la pedopornografia, individuare l'autore del reato diventa, invece, una priorità a cui risulta arduo contrapporre altri interessi ed altri valori.

Davanti all'esigenza di porre fine all'utilizzo della Rete per sfruttare i minori, l'importanza dell'anonimato e dei valori che vi sono sottesi sembra svanire e cedere inevitabilmente il passo a forme di identificazione, monitoraggio e registrazione sempre più invasive.

Il fenomeno della pedofilia è venuto prepotentemente alla luce perché la garanzia dell'anonimato semplifica la ricerca di materiale pornografico, reperibile con minore facilità. Perciò, se da un lato vi è la libertà di manifestazione del pensiero, dall'altro, vi è l'esigenza di una adeguata tutela dei diritti inviolabili dell'uomo ed, in particolare, della tutela dei minori e del loro sano sviluppo sessuale, garantiti dall'art.2 della Costituzione, dalla Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali. Fortunatamente, i circuiti anonimi seri, pur garantendo la possibilità di ogni utente di comunicare su argomenti che possono essere ritenuti immorali da parte della popolazione, sono aperti alla lotta contro il terrorismo e la pedofilia, ponendo filtri o agevolando eventuali indagini delle forze di polizia contro coloro che hanno sfruttato il circuito in modo non lecito.

L'attenzione ai temi della sicurezza delle informazioni sembra, quindi, essere assai alta sia da parte degli utenti che da parte delle istituzioni. Tuttavia, la percezione comune è che si sia ancora molto lontani dal raggiungere una condizione di sicurezza soddisfacente.

4.6 Considerazioni sulla navigazione anonima

La rete offre numerosi strumenti per navigare in completo ed assoluto anonimato, dipende solo dalle proprie capacità tecniche e dal livello di tecnologia conosciuta o conoscibile.

É opportuno affermare anche che l'anonimato non sempre viene utilizzato per commettere reati. Anzi, rispetto alla molteplicità degli usi, dai più semplici ai più lodevoli, l'uso criminale della Rete è comunque marginale.

Il desiderio di anonimato di un utente solitamente nasce da motivi perfettamente legittimi che trovano la loro spiegazione nella vasta e complessa natura umana.

Oggi è difficile fare una scelta netta tra libertà e sicurezza rappresentata dalla navigazione anonima. La possibilità di rimanere anonimi è importante per garantire nella Rete il rispetto dei diritti fondamentali alla riservatezza e alla libertà di espressione, ma è altrettanto importante controllare il traffico dei dati per evitare abusi ed illeciti. Tuttavia, trattandosi di una forma di esercizio del diritto alla protezione dei dati personali e alla riservatezza, come questi è destinato ad un continuo bilanciamento con altri diritti fondamentali. Perciò, in questo scenario i governi e le istituzioni internazionali sono impegnati a trovare il giusto equilibrio per garantire la tutela della privacy degli utenti senza danneggiare le logiche di una economia Internet in forte espansione.

Si è discusso e si discuterà ancora se sia giusto o meno un diritto all'anonimato in rete, e questo fa intendere la complessità della problematica ed i molteplici profili che debbano essere tenuti in considerazione quando si parla di anonimato.

4.7 Browser portable

Le applicazioni di cui viene resa disponibile una versione "portable" sono sempre più numerose, tanto che si sta difondendo la tendenza di progettare le applicazioni in questo modo sin dall'origine. In tal modo, nel computer ospitante (nelle chiavi di registro e nei file di sistema) non viene registrato alcun riferimento alla presenza di questi programmi, potendo eseguire tali software anche senza il godimento dei privilegi di amministratori sulla macchina ospitante: tale situazione è frequente in contesti aziendali, dove sono presenti anche policy relative al divieto di utilizzo di alcuni software in tal modo eludibili. Relativamente ai browser portable, tutte le informazioni ed i dati di navigazione (cache, cookies, cronologia) di un utente non vengono infatti salvate sul sistema informatico. Di seguito si enunciano i più diffusi web browser portable quali Google Chrome Portable, Mozilla Firefox Portable, Tor Browser che verranno poi analizzati da un punto di vista forense ai fini del presente lavoro di tesi. Tutti i test sono stati eseguiti sul sistema operativo Windows in quanto più diffuso[37].

[37]Si veda il sito http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qptimeframe=M&qpsp=133

4.7.1 Google Chrome Portable

Google Chrome Portable[38] è la versione portable del browser Google Chrome. Per utilizzarlo è necessario installarlo (dove per installazione si intende una sorta di decompressione) in una cartella a propria scelta: nell'ambito di questo test, la cartella, che occupa circa 60 MB, viene salvata sulla chiavetta USB. All'atto dell'esecuzione, il browser non presenta differenze sostanziali rispetto alla versione standard, se non un link al blog dell'autore del browser web.

4.7.2 Mozilla Firefox Portable

Firefox Portable[39] è la versione portable di Mozilla Firefox. Anche in questo caso, per utilizzarlo è necessario installarlo (dove per installazione si intende una sorta di decompressione) in una cartella a propria scelta: nell'ambito di questo test, la cartella, che occupa 35MB, viene salvata sulla chiavetta USB.

4.7.3 Tor Browser Portable

Il browser portable alla base di Tor[40] è una versione modificata di Mozilla Firefox portable. Nato come progetto della marina militare americana e ora diffuso in tutto il mondo, è un software sviluppato dal Tor Project che si

[38]Scaricabile dal sito http://www.chromeplugins.org/tips-tricks/latest-google-chrome-portable-usb-version/

[39]Scaricabile dal sito http://portableapps.com/apps/internet/firefox_portable

[40]Scaricabile dal sito https://www.torproject.org/

propone di garantire un buon livello di anonimato durante la navigazione in rete. Il suo funzionamento si basa sull'invio di pacchetti di dati che partono dal computer dell'utente e che non arrivano direttamente a destinazione (ovvero al server che ospita le pagine del sito web che si vuole consultare) ma transitano attraverso almeno tre computer che li reindirizzano, cifrati, sino al collegamento finale: dal punto di vista del server web, il richiedente della risorsa è dunque l'ultimo nodo. TOR fornisce buone performance e anche l'utente meno esperto è in grado di usare questo sistema perché è molto semplice e totalmente trasparente per l'utente.

Come mostrato nella seguente figura, Tor si preoccupa di ridurre i rischi di intercettazione distribuendo la richiesta dell'utente attraverso diversi sistemi in Rete in modo che nessun nodo possa mettere in correlazione diretta la reale sorgente dei pacchetti dati con la destinazione. Per cui, invece di collegare in modo diretto la sorgente con la destinazione dei dati, i pacchetti della rete Tor seguono un percorso casuale attraverso router che celano le tracce della comunicazione, in modo tale che nessun osservatore esterno possa stabilire da dove proviene un pacchetto e dove è destinato.

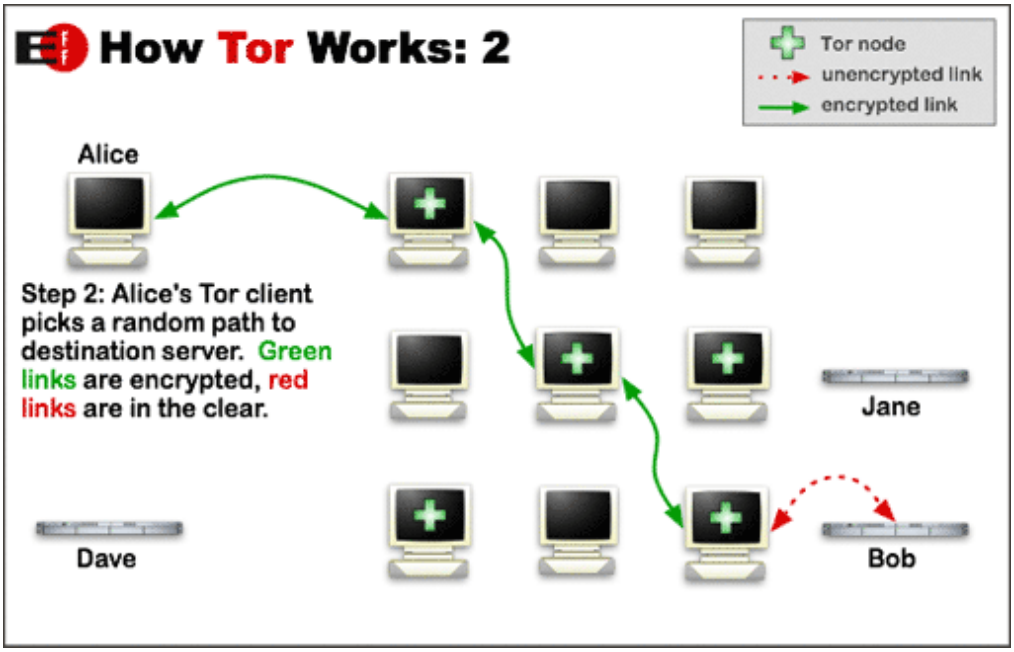

Figura 4.1: Funzionamento del browser *Tor*

Il client Tor, utilizzato per connettersi alla rete anonima, stabilisce l'intero percorso verso la destinazione basandosi su una lista di nodi disponibili. I dati inviati vengono subito incapsulati in una sequenza di messaggi criptati, una per ogni specifico nodo che verrà attraversato. Ogni nodo sarà poi in grado di aprire unicamente i propri messaggi, rendendo così possibile l'inoltro del nuovo livello criptato al router successivo. Con questa struttura di trasmissione "a cipolla"[41], quindi, il percorso e i dati rimangono anonimi e di difficile ricostruzione sia in tempo reale che a posteriori[42].

[41]La definizione "a cipolla" è presente anche nel nome TOR, acronimo di "The Onion Router", e rappresenta altresì il logo del software.

[42]Maggiori informazioni sono disponibili al sito http://www.html.it/articoli/tor-una-rete-anonima-per-navigare-sicuri-2/

Per utilizzare Tor browser è necessario installarlo (dove per installazione si intende una sorta di decompressione) in una cartella a propria scelta: nell'ambito di questo test, la cartella, che occupa 30MB, viene salvata sulla chiavetta USB.

Capitolo 5

5 Lo studio sperimentale

Questo lavoro di tesi si pone l'obiettivo di analizzare in dettaglio le tracce informatiche rinvenute su un drive USB[43] al fine di ricostruire l'attività di navigazione web effettuata con strumenti web browser portable. L'obiettivo finale è quello di comprendere che tipo di dati è possibile rinvenire in caso di analisi forense di un dispositivo di questo tipo: parallelamente, essendo il cracking dei sistemi informatici alla base dell'informatica forense, in questo contesto verranno evidenziati i livelli di riservatezza offerti da parte dei più diffusi browser portable. Il focus non sarà sulla riservatezza del dato che transita sulla rete, ma del dato residente sul dispositivo utilizzato. Inoltre non verrà preso in considerazione il sistema informatico sul quale il software viene eseguito, in considerazione del fatto che tali strumenti lavorano esclusivamente in memoria RAM[44].

Sono stati perciò ideati ed eseguiti dei test che si prefiggono lo scopo di imitare il comportamento di un utente di medio-basso livello che adoperi uno strumento web browser portable. Tale sequenza di test è stata condotta

[43] Per comodità, è stato utilizzato un drive di piccole dimensioni (128 MB)

[44] Alcune tracce potrebbero essere rinvenute negli spazi destinati a memoria virtuale e file di ibernazione. Tuttavia, essendo situazioni estremamente variabili a seconda del sistema informatico che si trova alla base, tale circostanza non verrà presa in esame in quanto non fornirebbe risultati inteeressanti.

in maniera identica 5 volte, tanti quanti sono gli scenari di partenza come di seguito dettagliato:

- **Scenario A:** utilizzo del browser portable Chrome con la possibilità di navigare sul web, attivando l'opzione di salvataggio delle password.
- **Scenario B:** utilizzo del browser portable Chrome con la possibilità di navigare sul web, disattivando l'opzione di salvataggio delle password.
- **Scenario C:** utilizzo del browser portable Firefox con la possibilità di navigare sul web, attivando l'opzione di salvataggio delle password.
- **Scenario D:** utilizzo del browser portable Firefox con la possibilità di navigare sul web, disattivando l'opzione di salvataggio delle password.
- **Scenario E:** utilizzo del browser portable Tor.

Per ogni scenario, una volta eseguito l'insieme di operazioni che compongono il test, è stata realizzata un'immagine bit-stream del dispositivo utilizzando il software *Encase*[45].

[45]EnCase Forensics è il tool più utilizzato nelle procedure di investigazione informatica da parte di organizzazioni governative e forze dell'ordine a livello mondiale. Tra le sue caratteristiche principali troviamo una evoluzione del supporto per l'analisi di email, nei formati PST, DBX, AOL , MBOX e web-mail, la possibilità di navigazione delle pagine HTML presenti nella cache e l'accesso dettagliato ai log di navigazione.

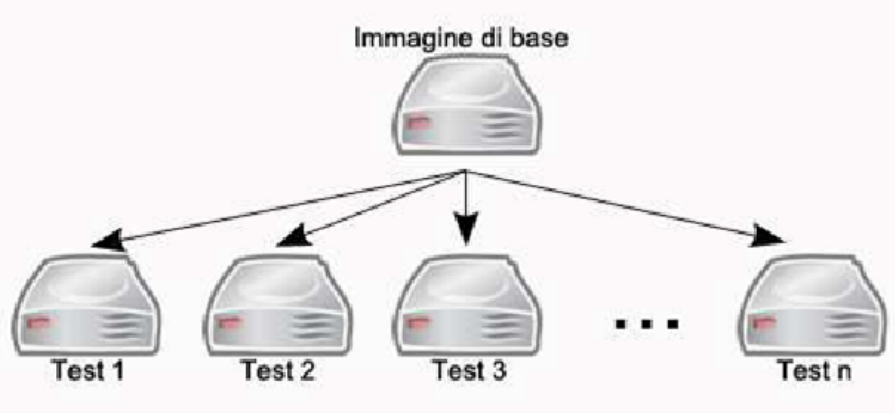

Figura 5.1: Rappresentazione di immagini forensi della USB

Una volta completato il test e l'acquisizione del device, prima di eseguire il nuovo test la chiavetta usb è stata sottoposta a operazione di wiping, mediante la quale tutti i bit sono stati posti al valore 0 al fine di non contaminare il test dello scenario successivo con dati dei test precedenti. Questa operazione è stata eseguita in ambiente linux con il comando

dd if=/dev/zero of=/dev/sda

Tenendo fede alle best practice utilizzate in un'indagine reale di informatica forense, l'analisi è stata condotta sull'immagine forense, evitando in tal modo di modificare dei dati in caso di attività improprie[46]. A tale scopo sono stati utilizzati alcuni software per analisi forense, commerciali (in versione demo), freeware e opensource, quali:

- Encase

[46]Banalmente, l'apertura di un file modificherebbe la data di ultima lettura.

- FTK Toolkit
- Autopsy
- ChromeHistoryView
- MozillaHistoryView

5.1 Definizione dei test effettuati

La prima operazione è il wiping del dispositivo al fine di cancellare completamente e definitivamente i dati contenuti precedentemente sul dispositivo di memoria di massa ed evitare che l'analisi successiva venga compromessa. La cancellazione di un file con le classiche operazioni fornite dal sistema operativo non garantisce infatti l'effettiva pulitura del settore, per cui risulta necessaria una cancellazione irreversibile dei dati, rendendo di fatto il drive USB "come nuovo", privo cioè di qualsiasi traccia di passati utilizzi, impostando tutti i bit a 0. Come tutte le operazione descritte in seguito, l'operazione di wiping è stata ripetuta all'inizio dello svolgimento di ogni scenario delineato nel corso del progetto(Pagarafo 5.2.1).

Successivamente, sulla chiavetta USB "sterilizzata" è stato salvato il browser portable necessario per svolgere la navigazione in rete. Il test prevede una sequenza di visite e interazioni con alcuni siti web. Dopodichè è stata creata una copia bit-stream del drive USB che è stata poi analizzata al fine di esaminare e quantificare le attività web memorizzate dai diversi browser. Le

prove e le analisi si concentrano sulle tracce relative alle pagine visitate, dove per tracce si intendono gli URL, le pagine memorizzate nella cache, parole chiave utilizzate nei motori di ricerca e qualsiasi altro elemento utile per la ricostruzione della navigazione web.

5.1.1 La navigazione in rete

La navigazione sui vari siti web è avvenuta attraverso la lettura di articoli di cronaca ed informatici, attraverso la ricerca e la visualizzazione di video, lettura e scambio di email e navigazione su alcuni dei più famosi social network. In particolare, per tutti i tipi di browser sono stati siti esplorati i seguenti siti web:

- *www.gmail.com*: un servizio gratuito di posta elettronica via web gestito da Google.
- *www.libero.it*: un portale italiano che tra i numerosi servizi offre la possibilità di creare e gestire gratuitamente una casella di posta elettronica.
- *www.repubblica.it*: un quotidiano online con notizie in tempo reale.
- *www.punto-informatico.it*: un quotidiano italiano online di informazione su Internet, tecnologie, innovazione e next economy.
- *www.facebook.com*: uno dei più famosi social network a livello mondiale.

- *www.twitter.com*: un servizio gratuito di social network e microblogging.
- *www.tgcom.it*: un sito di informazione online.
- *www.youtube.com*: il più famoso sito web che consente la condivisione e visualizzazione di video.

Inoltre, l'accesso all'interno dei principali gestori di posta elettronica e dei social network è avvenuto attraverso la creazione di due differenti profili utente con le seguenti credenziali:

Utente 1

- **UserID:** testif2012user@gmail.com
- **Password:** psw1475xyz

Utente 2

- **UserID:** testif1999user@libero.it
- **Password:** psw4954abc

Tali profili utente sono stati utilizzati per poter poi successivamente effettuare ricerche per parola chiave (utilizzato come chiave di ricerca l'indirizzo email e la password).

5.1.2 Configurazione dei browser portable

Come accennato in precedenza, si sono voluti ricreare cinque possibili scenari per effettuare la navigazione anonima sul web. Per questo motivo sono state realizzate altrettante diverse immagini della pendrive *USB*, che differiscono tra di loro o per il browser installato o per le configurazioni di quest'ultimo.

- **Img1**

Dopo l'avvio del browser *Google Chrome Portable* dal drive *USB* e lo svolgimento della navigazione web con attiva l'opzione "*salva password*", l'immagine è stata "congelata" per poter essere utilizzata per i test.

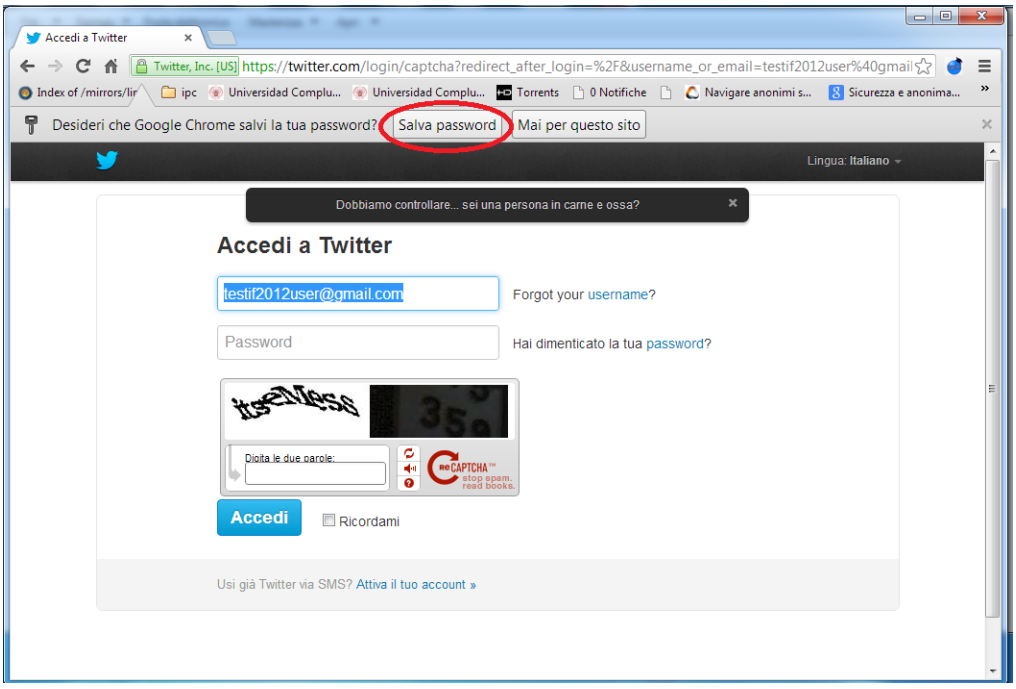

Figura 5.2: *Google Chrome Portable* con salvataggio password

- **Img2**

Lo stesso browser di *Img1* è stato utilizzato anche per eseguire il secondo test, con l'unica differenza che la modalità di navigazione avviene senza il salvataggio delle password. Anche questa immagine è stata congelata dopo la sua preparazione.

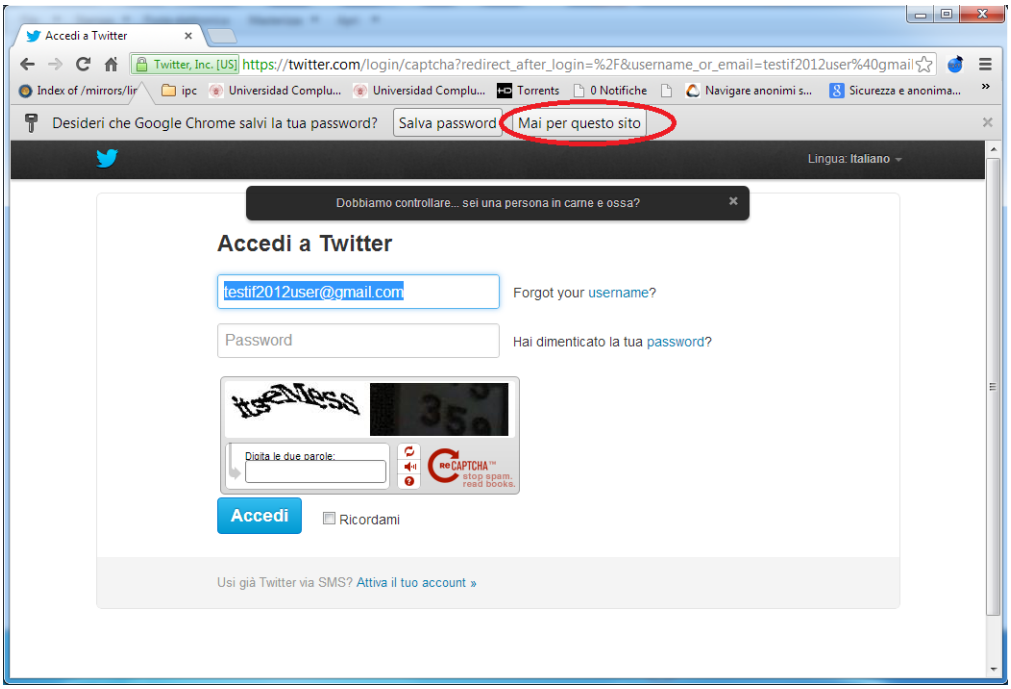

Figura 5.3: *Google Chrome Portable* senza salvataggio password

- **Img3**

Questa immagine del drive USB contiene i dati di navigazione relativi all'utilizzo del browser Firefox Portable con attiva l'opzione "*salva password*".

Come per i casi precedenti, questa immagine è stata congelata dopo la navigazione sul web.

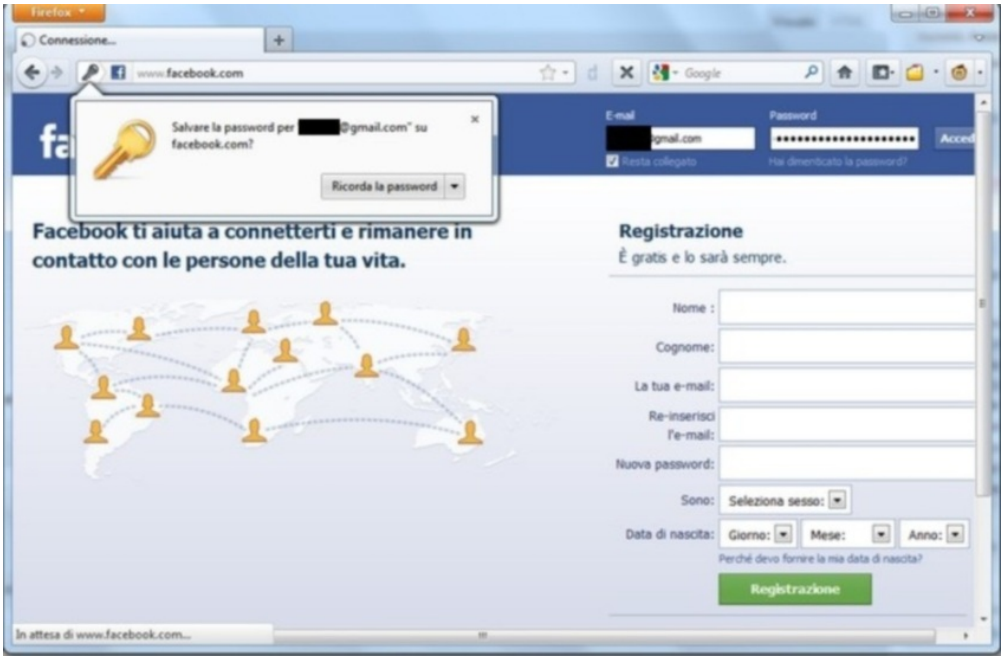

Figura 5.4: *Mozilla Firefox Portable* con salvataggio password

- **Img4**

Anche questa immagine presenta una singola differenza rispetto all'*Img3*, poiché qui è stato utilizzato il browser Mozilla Firefox per la navigazione sul web, ma non è stata attivata l'opzione di salvataggio password.

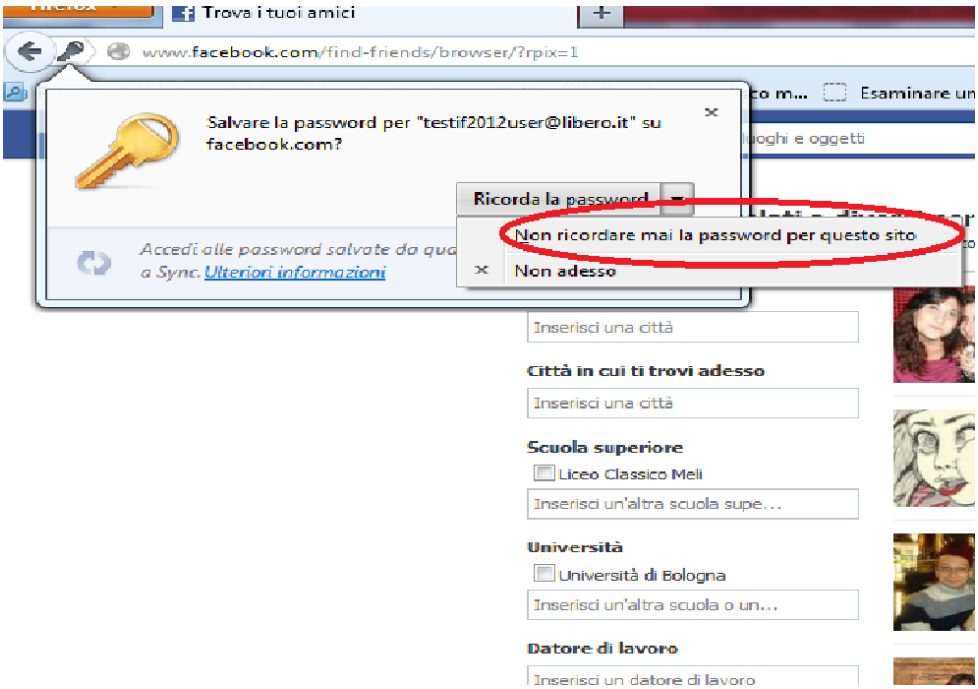

Figura 5.5: *Mozilla Firefox Portable* senza salvataggio password

- **Img5**

In questa immagine, invece, è racchiusa la navigazione web effettuata mediante il browser Tor, che a differenza degli altri non permette di attivare un'opzione di salvataggio delle password digitate durante la navigazione.

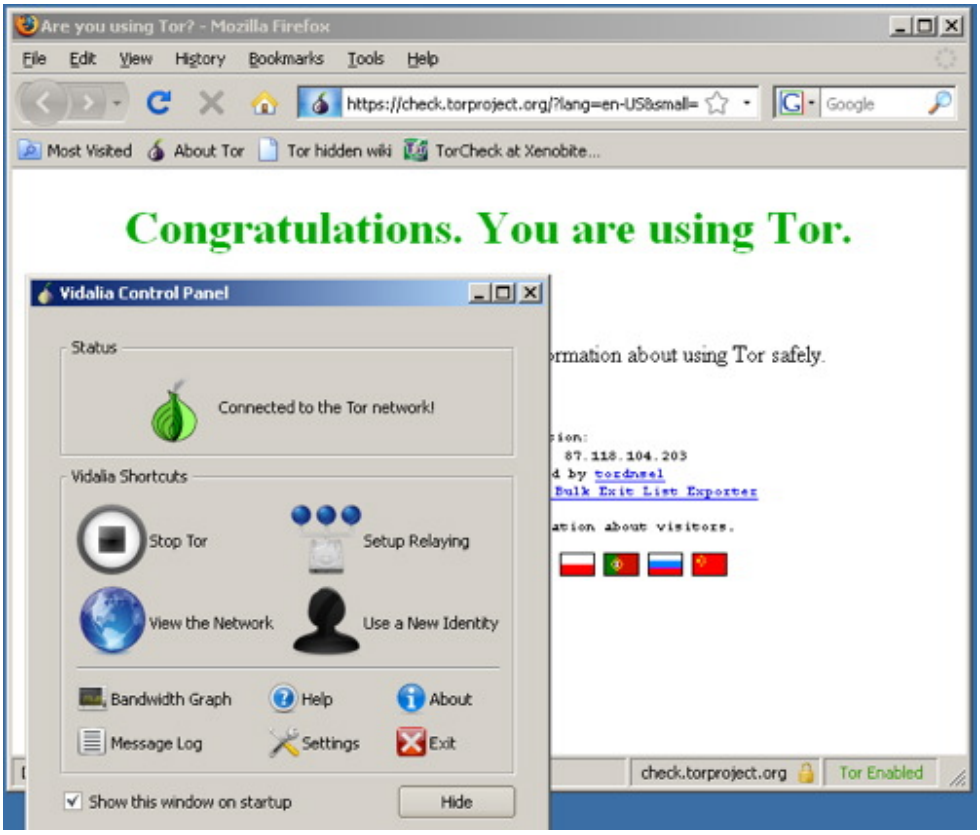

Figura 5.6: Tor Browser

Per una migliore comprensione, la seguente tabella riassume, in breve, i browser web utilizzati e le immagini forensi create durante lo svolgimento del progetto.

	Salva password	**Non salva password**
Google Chrome	*Img1*	*Img2*
Mozilla Firefox	*Img3*	*Img4*
Tor	/	*Img5*

Tabella 1: Riepilogo creazione delle immagini forensi

5.1.3 Elenco dei test

Viene di seguito riportata la lista integrale dei test eseguiti sulle diverse immagini forensi:

1. Avvio del web browser portable.
2. Connessione al sito *www.gmail.com*.
3. Richiesta di creazione casella email Utente1 su Gmail.
4. Compilazione form dei dati personali dell'Utente1 per la creazione della casella di posta Gmail.
5. Termine registrazione e disconnessione del profilo utente1 dal sito Gmail.
6. Connessione al sito *www.libero.it*.
7. Richiesta di creazione casella email Utente2 su Libero.
8. Compilazione form dei dati personali dell'Utente2 per la creazione della casella di posta Libero.
9. Termine registrazione e disconnessione del profilo utente2 dal sito di Libero.
10. Connessione al sito *www.facebook.com*.
11. Creazione profilo facebook Utente1.
12. Creazione profilo facebook Utente2.

13. Connessione al sito *www.twitter.com.*

14. Creazione profilo twitter Utente1.

15. Creazione profilo twitter Utente2.

16. Collegamento al sito *www.youtube.com.*

17. Ricerca dei video su Youtube di "*Origami cigno*" e "*Stammi vicino-Vasco Rossi*", impostando il filtro di ricerca in base al numero di visualizzazioni.

18. Visualizzazione del video "*Origami cigno*" su Youtube.

19. Visualizzazione del video *"Stammi vicino-Vasco Rossi*" su Youtube.

20. Collegamento al sito *www.repubblica.it.*

21. Visualizzazione e lettura articoli di attualità sul sito Repubblica.

22. Collegamento al sito *www.tgcom.it.*

23. Visualizzazione e lettura articoli di cronaca sul sito Tgcom.

24. Collegamento al sito *www.punto-informatico.it.*

25. Visualizzazione e lettura articoli informatici sul sito Punto-informatico.

26. Collegamento al sito *www.facebook.com.*

27. Accesso al sito di Facebook con il profilo Utente1.

28. Visualizzazione pagina personale del profilo facebook dell'Utente1.

29. Scrittura ed invio di un messaggio privato (all'interno del sito Facebook) dall' Utente1 all'Utente2.

30. Disconnessione profilo Utente1 dal sito Facebook.

31. Accesso profilo facebook da parte dell'Utente2.

32. Visualizzazione pagina personale del profilo facebook Utente2.

33. Lettura e risposta al messaggio privato ricevuto su Facebook da parte dell'Utente1.

34. Disconnessione Utente2 dal sito Facebook.

35. Collegamento al sito *www.twitter.com*.

36. Accesso al sito con profilo Utente1.

37. Visualizzazione pagina personale di profilo twitter dell'Utente2.

38. Aggiunta di *tweet* sulla pagina personale dell'Utente1.

39. Disconnessione del profilo Utente1 da Twitter.

40. Accesso al sito Twitter con profilo Utente2.

41. Aggiunta di tweet sulla pagina personale dell'Utente2.

42. Disconnessione profilo Utente2 da Twitter.

43. Connessione al sito *www.gmail.com*.

44. Accesso alla casella di posta Gmail con credenziali (email e password) dell'Utente1.

45. Lettura dei messaggi della posta in arrivo.

46. Creazione nuovo messaggio di posta elettronica.

47. Scrittura del messaggio con allegato il file "*Dar voce alle prove.pdf*".

48. Invio del messaggio di posta da parte dell'Utente1 all'indirizzo di posta elettronica dell'Utente2.

49. Disconnessione del profilo Utente1 dal sito Gmail.

50. Connessione al sito *www.libero.it*.

51. Accesso alla casella di posta libero con le credenziali di accesso dell'Utente2.

52. Lettura dei messaggi di posta in arrivo da parte dell'Utente2.

53. Apertura del file allegato presente nell'email inviata dall'Utente1.

54. Creazione nuovo messaggio di posta in risposta all'email dell'Utente1.

55. Invio messaggio e disconnessione dalla casella di posta del sito Libero da parte dell'Utente2.

56. Chiusura del browser portable.

5.2 Dettaglio sulle modalità ed esecuzione dei test

Le modalità di svolgimento dei test sono avvenute attraverso le fasi di:

1. Wiping *USB*.
2. Formattazione della chiavetta USB ed installazione del browser web.
3. Esecuzione dei test.
4. Acquisizione del disco e copia forense.
5. Analisi forense:
    - analisi della *timeline*;
    - analisi della *cronologia*;
    - analisi ricerca per parola chiave.

5.2.1 Wiping

L'operazione di wiping consente di partire ogni volta da un ambiente pulito. Pertanto la prima azione effettuata durante l'esecuzione dei test è rappresentata dall'operazione di sterilizzazione del dispositivo.

Questa operazione ha permesso la cancellazione definitiva dei files che sono stati sovrascritti una o più volte con dei dati generati in modo casuale, rendendo così impossibile, con qualunque software, il recupero delle informazioni preesistenti sulla pendrive *USB*.

In particolare, per la sua esecuzione si è scelto di utilizzare il software *CCleaner*: attivando la funzione *Bonifica Drive* è stato possibile, in pochi minuti, cancellare completamente tutti i dati presenti sul dispositivo.

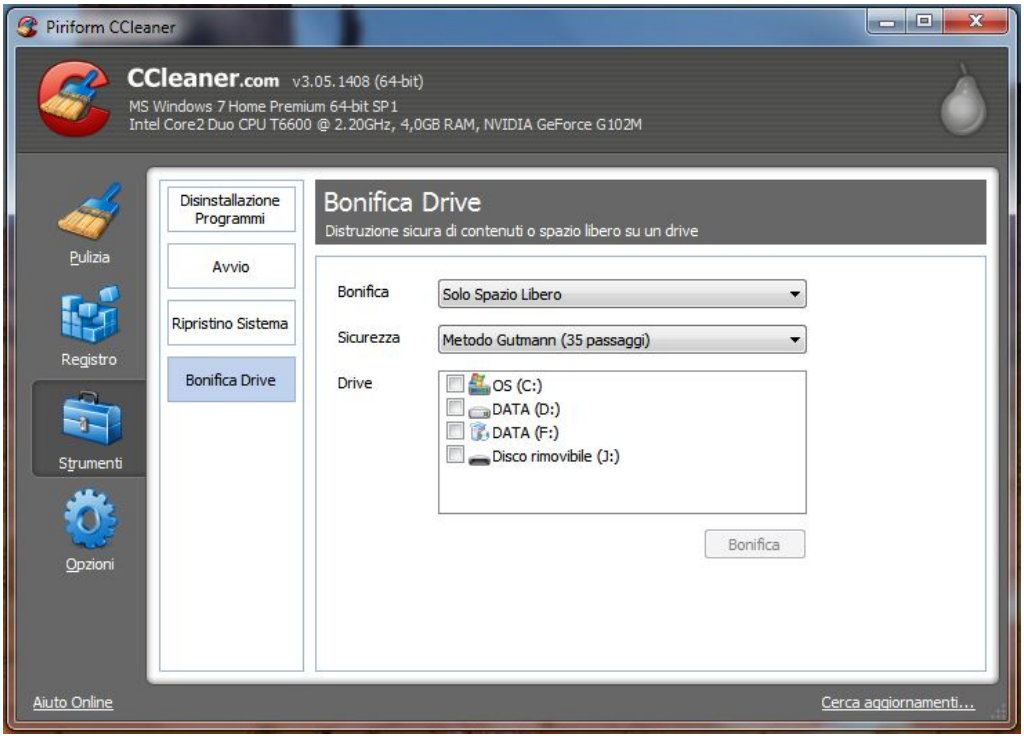

Figura 5.7: Wiping USB con il software CCleaner

5.2.2 Formattazione della chiavetta USB ed installazione del browser web

Questa fase di svolgimento del test è stata caratterizzata da un procedimento molto semplice e piuttosto simile per tutti e tre i browser. Come accennato

precedentemente, è stata eseguita l'operazione di wiping, attraverso il software *CCleaner*, che ha permesso la formazzazione della chiavetta USB, ossia la cancellazione di tutti i dati preesistenti contenuti sulla pendrive USB.

La fase successiva alla formattazione, è stata caratterizzata dall'installazione del browser web sul dispositivo USB. In particolare, dopo averlo collegato al pc, per utilizzare il browser portable è stato necessario semplicemente scaricarne dal sito ufficiale l'ultima versione disponibile e salvarla sulla pendrive. A questo punto, esplorando il dispositivo USB ed aprendo la cartella contente il browser è bastato fare click sull'icona del programma per avviarlo ed iniziare così la navigazione anonima.

5.2.3 Esecuzione dei test

La fase di esecuzione dei test è stata caratterizzata dall'attività di navigazione anonima attraverso i differenti browser web.

Per ogni tipo di browser, durante la navigazione web sono state visitate diverse pagine web e creati due profili utente (si veda il Paragrafo 5.1.1). Le pagine web esplorate ed i profili utente sono stati gli stessi sia per i browser *Mozilla Firefox* e *Google Chrome* che per *Tor*. In particolare, per quanto riguarda la visualizzazione dei siti web son stati scelti famosi social network e siti contenenti informazioni di attualità, di carattere informatico, di ricerca e visualizzazione di video e di gestione di posta elettronica, per poter esaminare

in dettaglio il tipo e la quantità di informazioni ricostruibili mediante l'analisi forense.

I profili utente sono stati creati su due diversi gestori di posta elettronica e la loro attività è stata caratterizzata da uno scambio reciproco di messaggi sia sui differenti gestori di posta elettronica che sui social newtork esplorati, in modo da analizzare se fosse possibile ricostruire eventuali parti di testo o di risalire profili e password digitate.

5.2.4 Acquisizione del drive e copia forense

La fase più delicata nell'esecuzione di un'indagine quando sono trattate informazioni digitali è quella dell'acquisizione. È indispensabile che, quando si effettua questa attività, venga assicurata l'integrità e la sicurezza dello stato del sistema in oggetto e che quindi non venga introdotta alcuna alterazione ai dati residenti nel sistema medesimo. Per creare dunque, una copia "*bit-a-bit*" del drive USB, usata per i test, è stato utilizzato *Encase*, un software proprietario che consente di reperire, analizzare e presentare dati nell'uso professionale e investigativo da parte di numerose agenzie e forze dell'ordine in tutto il mondo.

EnCase memorizza l'immagine di un disco come una serie di pagine compresse univocamente individuabili e gestibili ed ogni pagina può venire reperita in modo random e decompressa secondo le esigenze investigative.

Diversamente da quanto dovrebbe accadere in un'indagine tradizionale, per questo esperimento non è stato utilizzato un write blocker, non inficiando comunque i risultati dei test.

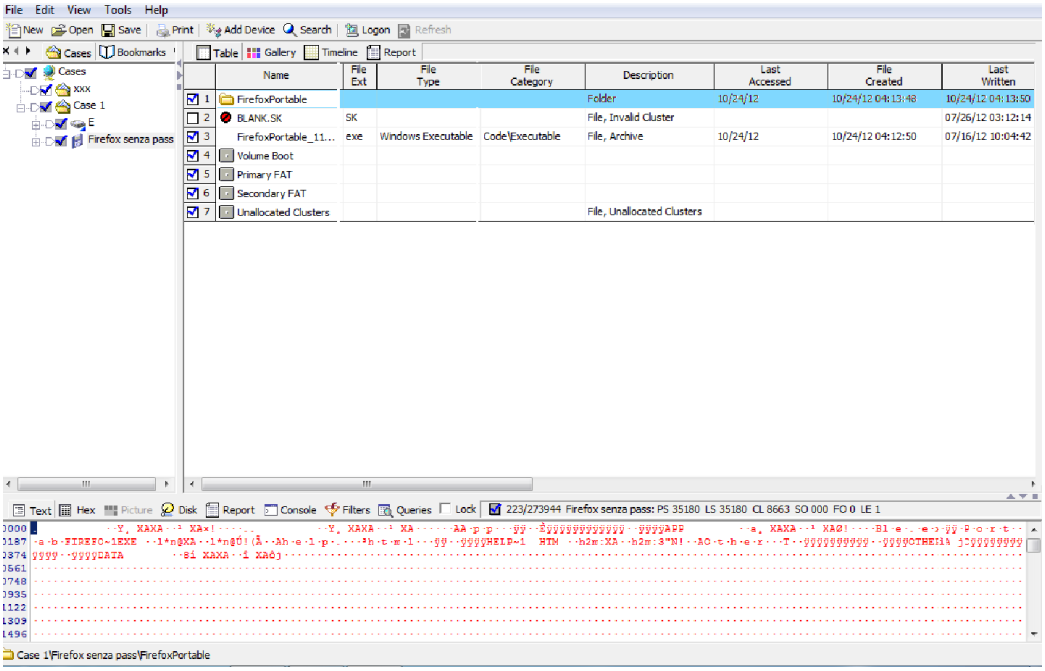

Figura 5.8: Acquisizione USB con il software Encase

5.2.5 Analisi forense

Per svolgere la fase di analisi delle diverse copie forensi, è stato utilizzato il tool *AccessData FTK Toolkit* nella sua versione demo in ambiente *Windows*, in grado di visualizzare il contenuto di tutti i file presenti, compresi i relativi metadati, e di recuperare i file cancellati o frammentati.

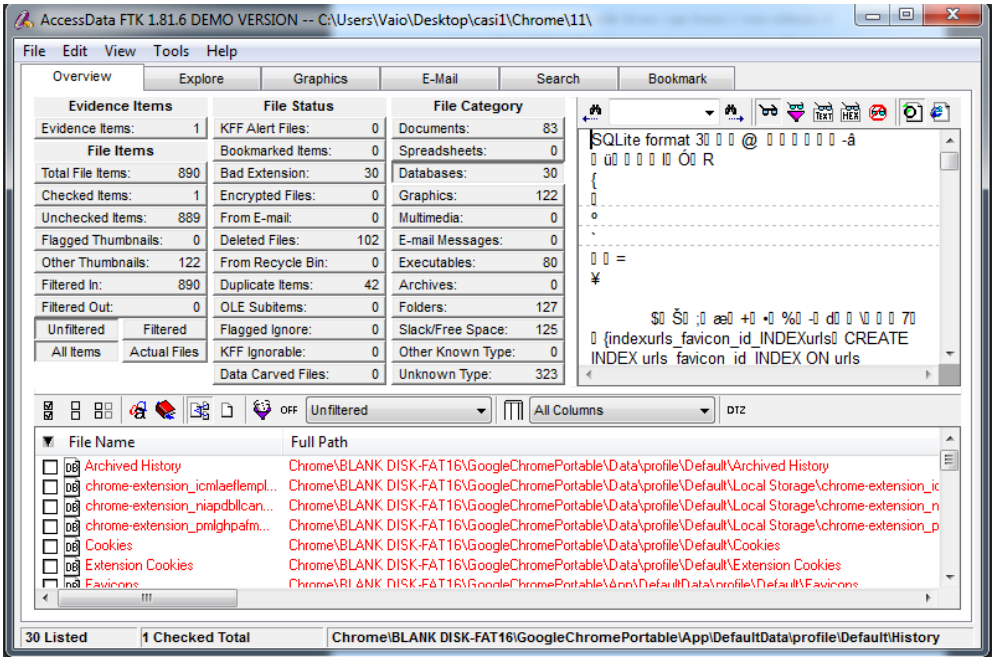

Figura 5.9: Analisi delle *Img1* con il software *FTK Toolkit*

Come mostra la figura precedente, questo software restituisce i risultati dell'analisi attraverso la visualizzazione di differenti tabelle, ognuna con una funzionalità diversa. *Overview*, ad esempio, visualizza i risultati evidenziando il numero di elementi trovati, le categorie a cui a appartengono e lo stato del file e la tabella Bookmark permette la visualizzazione e la gestione dei segnalibri. Per la nostra analisi, in particolare abbiamo utilizzato anche la tabella *Search* che ha permesso di effettuare delle ricerche sui file rinvenuti attraverso l'utilizzo di parole chiave.

Di seguito vengono descritte le tre fasi che hanno caratterizzato l'attività di analisi.

- **Analisi della timeline**

La *timeline*, intesa come sequenza degli eventi avvenuti all'interno di un sistema, è un elemento di fondamentale importanza quando si vuole comprendere ciò che è avvenuto in un sistema informatico. Infatti, tale operazione permette di visualizzare informazioni relative a data ed ora di tutte le azioni che sono state compiute e di cui vi è rimasta traccia sul dispositivo USB.

Per generare la *timeline* di ciascun test è stato utilizzato il tool *Autopsy Forensic Browser*, un software open source di interfaccia grafica basato su HTML. Mediante *Autopsy* è stato possibile acquisire ed analizzare le copie forensi della pendrive USB, recuperando così informazioni relative ai file tra cui:

- data di creazione;

- data di ultima modifica;

- tipo di operazione effettuata;

- lunghezza in byte.

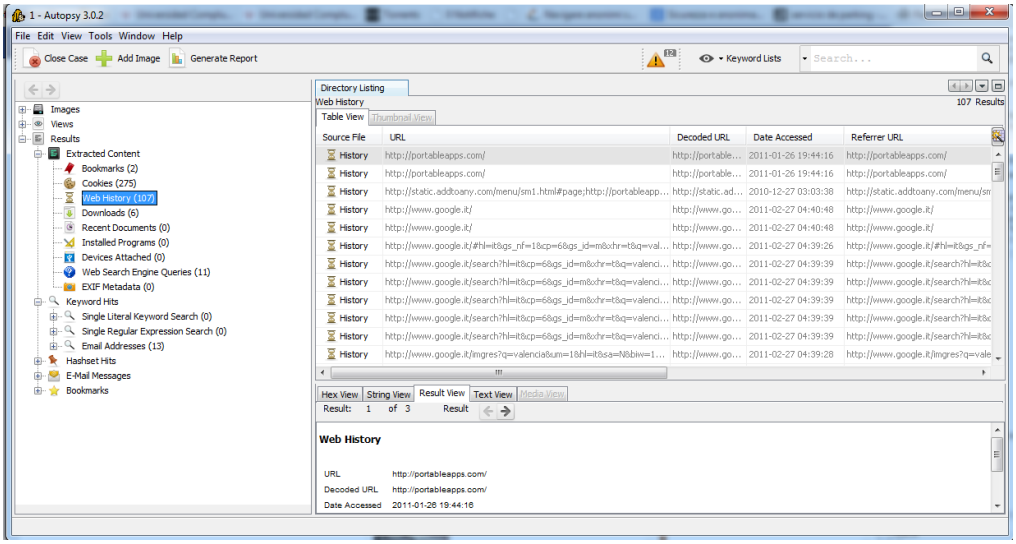

Figura 5.10: Costruzione *timeline* con Autopsy

Prendiamo la seguente voce come esempio:

2012-10-24 20:38:56	2012-10-24 20:38:54	215	r	rrwxrwxrwx

Figura 5.11: Esempio voce della *timeline* rinvenuta sull'*Img1*

dove:

- **Data e ora** dell'operazione. Nell'esempio: 2012-10-24 20:38:54.

- **Data ed ora** di modifica del file. Nell'esempio: 2012-10-24 20:38:56.

- **Dimensione** del file letto e/o modificato e/o creato. Nell'esempio: 215(kb).

- **Tipo di operazione**, è specificata da una lettera ("r", "w", "m" o "x") o una combinazione di esse che indica rispettivamente le operazioni di lettura,

scrittura, modifica o cancellazione del file. Nell'esempio il file è stato letto: "r".

- Permessi (mode), l'insieme delle operazioni consentite su quel determinato file. Nell'esempio: rrwxrwxrwx.

I dati raccolti dall'analisi della *timeline* hanno permesso di tracciare un'analisi sul numero di operazioni effettuate sui file durante la navigazione web avvenuta attraverso i diversi browser web.

	r	**w**	**m**	**x**
Firefox con password	*529*	*0*	*515*	*101*
Firefox senza password	*1078*	*0*	*755*	*231*
Chrome con password	*1079*	*0*	*652*	*132*
Chrome senza password	*1078*	*0*	*155*	*651*
Tor	*549*	*0*	*232*	*115*

Tabella 2: Riepilogo dati della *timeline*

- **Analisi delle cronologia**

Il primo passo per poter ricostruire la *cronologia* di ciascun test è stato quello di analizzare il modo in cui i tre diversi browser portable memorizzano la navigazione web. Per farlo abbiamo utilizzato rispettivamente i tools *MozillaHistoryView* per il browser Mozilla Firefox e *Chrome History View* per il browser Google Chrome. Questi software opensource, infatti, mediante una

semplice interfaccia utente, ci hanno permesso di visualizzare una vera e propria cronologia di tutto ciò che è stato rinvenuto dall'analisi del file *Sqlite*. Nello specifico, ci hanno consentito di visualizzare le informazioni relative alle operazioni eseguite dai browser web (url, download, cookie etc.) visualizzate secondo l'URL, tipo di contenuto, la dimensione del file, l'ultima volta accesso, il tempo di scadenza, nome del server, la risposta del server, ed altro ancora.

La *cronologia* di ogni test è stata creata partendo da una definizione temporale ben chiara, che comprende soltanto i movimenti avvenuti durante l'esecuzione del test. Prendiamo la seguente voce come esempio:

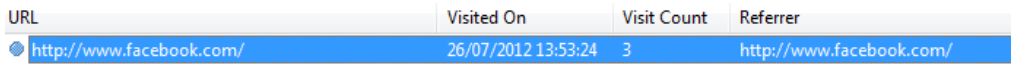

Figura 5.12: Esempio di cronologia

La struttura è di facile comprensione, dal momento che ogni sua entry rappresenta una specifica azione avvenuta durante la navigazione. In particolare, ad ogni azione avvenuta durante la navigazione web, vengono associate le seguenti componenti:

- Visit Date: descrive la data e l'ora dell'attività. Nell'esempio: 26/07/2012 13:53:24.

- URL del sito web visitato. Nell'esempio: *www.facebook.com.*

- Referrer: indica il link che l'utente ha cliccato per visualizzare la pagina web. Nell'esempio: *www.facebook.com.*

- **Visit count**: indica il numero di volte che è stata visitata la pagina web. Nell'esempio: 3.

Attraverso questi dati, è possibile tracciare un'analisi dettagliata e temporale delle operazioni di cui si è tenuto traccia sul drive USB durante la navigazione anonima.

Le seguenti figure forniscono un'immagine dei dati raccolti attraverso i tools *MozillaHistoryView* e *ChromeHistoryView* sulle *Img1*, *Img2*, *Img3* e *Img4*.

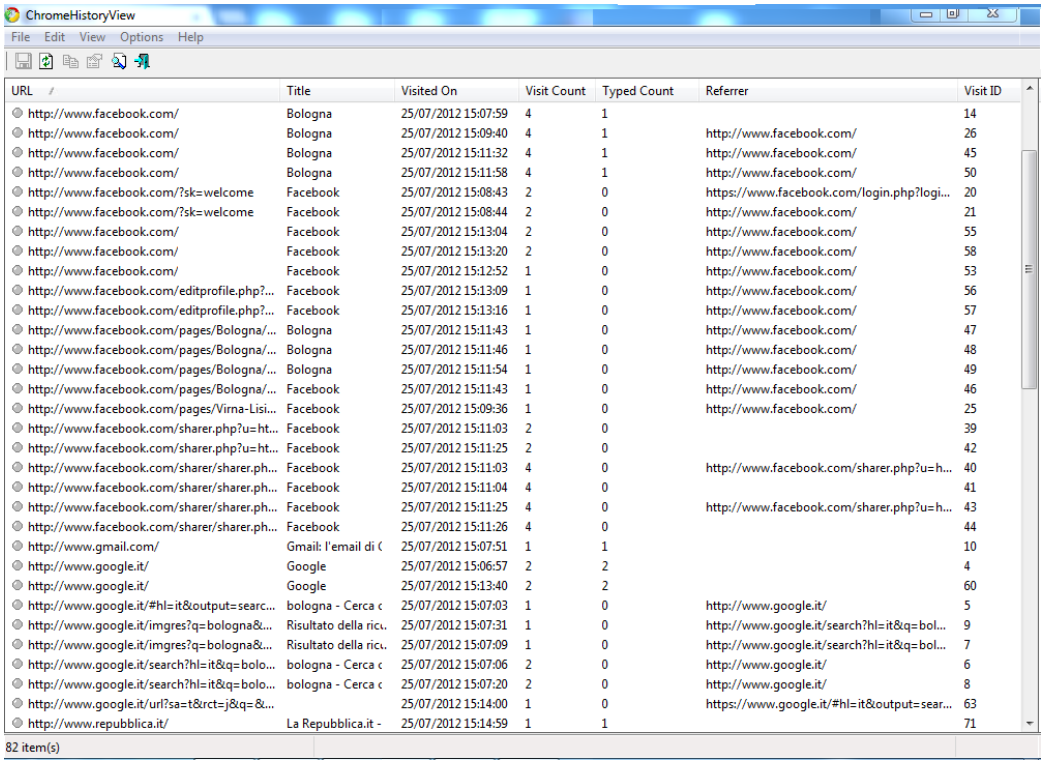

Figura 5.13: Cronologia della *Img1* con *ChromeHistoryView*

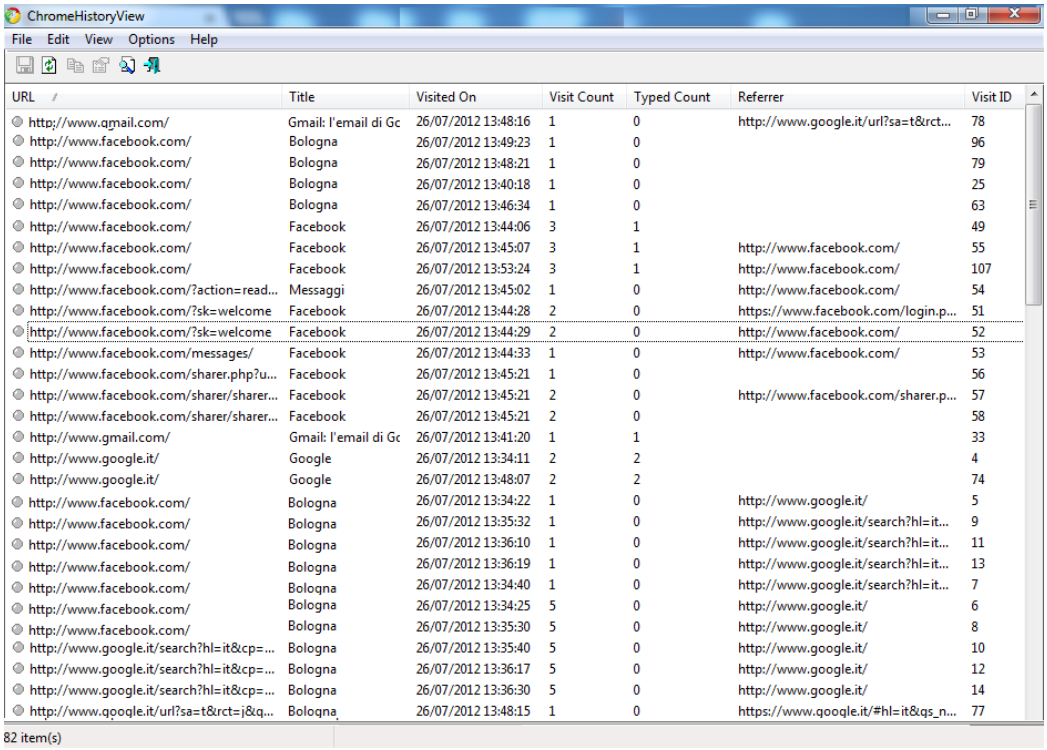

Figura 5.14: Cronologia della *Img2* con *ChromeHistoryView*

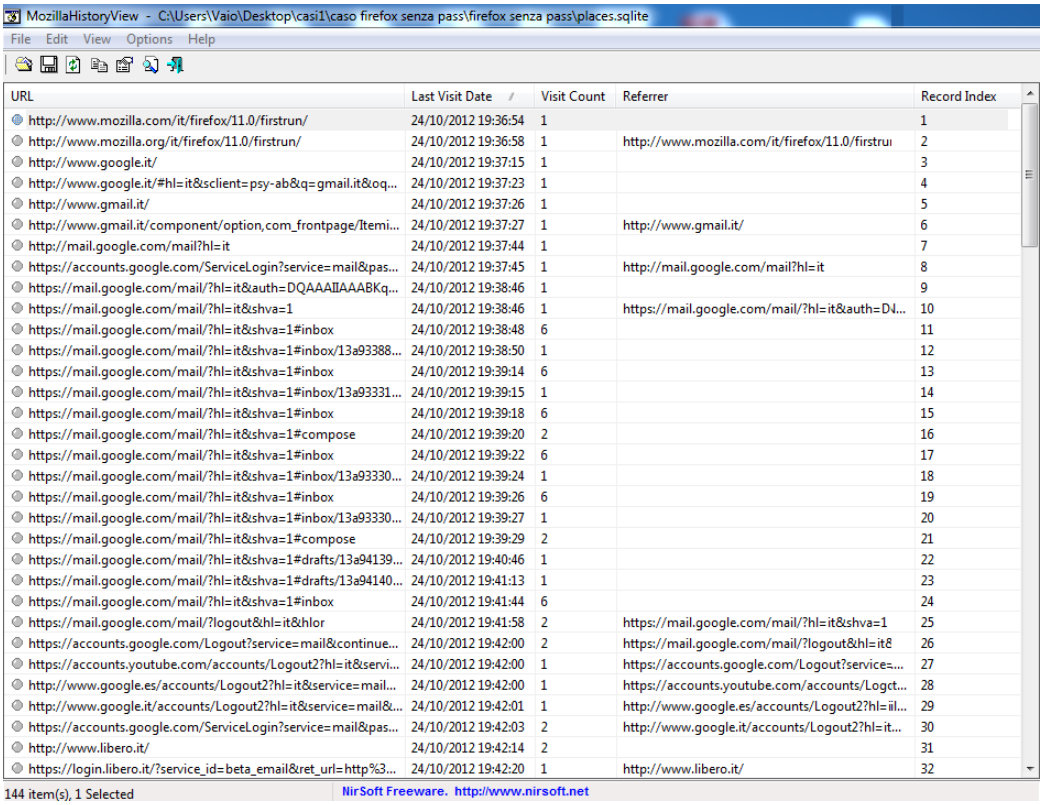

Figura 5.15: Cronologia della *Img3* con *MozillaHistoryView*

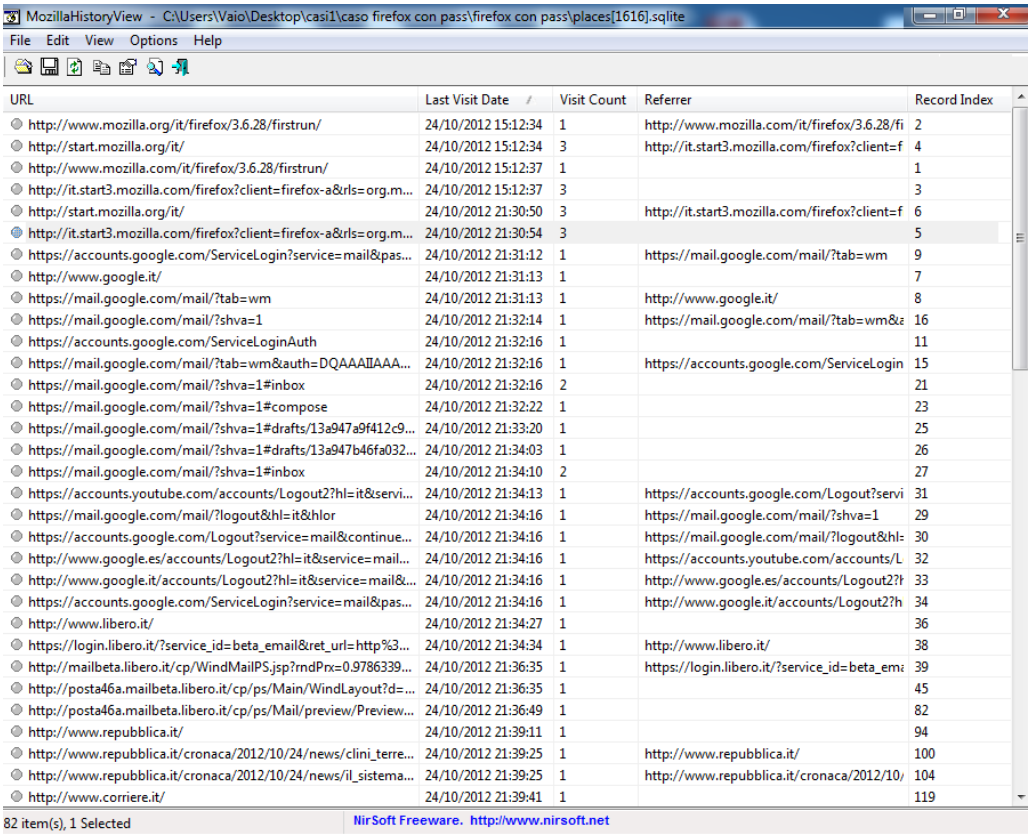

Figura 5.16: Cronologia della *Img4* con *MozillaHistoryView*

Dall'analisi delle immagini forensi realizzate con *Encase*, mediante FTK è stato possibile ricavare ed esplorare il database *SQlite* (in particolare i file *place.sqlite* ed *history.sqlite*), contenente i dati di navigazione web, come la cronologia, la cache, i cookies e tutti gli altri elementi utili alla ricostruzione dell'attività web.

Nelle figure 5.2.5, 5.2.5, 5.2.5, 5.2.5 sono mostrate rispettivamente le ricostruzioni della cronologia riscontrate sulle differenti immagini forensi create

durante i test.

Data	Evento
25/07/2012 15:06:59	L'utente1 accede al sito www.google.com
25/07/2012 15:07:15	L'utente1 visita il sito www.twitter.com
25/07/2012 15:07:59	L'utente1 accede al sito www.facebook.com
25/07/2012 15:08:43	`L'utente1 accede al suo profilo Facebook con l'account` *"testif2012user@gmail.com"*
25/07/2012 15:11:26	L'utente1 visualizza la pagina personale del suo profilo Facebook
25/07/2012 15:11:58	L'utente1 effettua il logout dal suo profilo Facebook
25/07/2012 15:14:01	L'utente1 accede al suo profilo Twitter con l'account *"testif2012user@gmail.com"*
25/07/2012 15:14:59	L'utente1 visita il sito www.repubblica.it
25/07/2012 15:15:04	L'utente1 visualizza il suo profilo Twitter
25/07/2012 15:15:59	L'utente1 effettua il logout dal suo profilo Twitter
25/07/2012 15:16:43	L'utente2 si collega al sito www.libero.it
25/07/2012 15:16:58	L'utente2 effettua il login al suo account di posta con username *"testif1999user@libero.it"*
25/07/2012 15:17:04	L'utente2 visualizza il messaggio di posta inviato dall'utente1
25/07/2012 15:17:33	L'utente2 scarica l'allegato *"Dar voce alle prove.pdf"* presente nel messaggio di posta
25/07/2012 15:17:57	Uno dei due utenti si collega al sito www.repubblica.it

25/07/2012 15:17:58	Uno dei due utenti visualizza l'articolo *"Terremoto, Clini attacca la sentenza"*
25/07/2012 15:18:06	Uno dei due utenti si collega al sito www.corriere.it ed esplora la sezione relativa agli annunci di lavoro
25/07/2012 15:18:22	Uno dei due utenti si collega al sito www.punto-informatico.it
25/07/2012 15:18:24	Uno dei due utenti visualizza l'articolo *"Apple, mini-maxi evento"*
25/07/2012 15:19:01	L'utente1 si collega al sito www.gmail.com
25/07/2012 15:19:31	L'utente1 effettua il login al suo account di posta con username *"testif2012user@gmail.com"*
25/07/2012 15:19:43	L'utente effettua il logout dal suo profilo gmail
25/07/2012 15:20:06	L'utente2 accede al suo profilo Twitter con l'account *"testif1999user@libero.it"*
25/07/2012 15:20:37	L'utente2 effettua il logout dal suo profilo Twitter
25/07/2012 15:20:45	L'utente2 accede al suo profilo Facebook con l'account *"testif1999user@libero.it"*
25/07/2012 15:20:55	L'utente2 effettua il logout dal suo profilo Facebook
25/07/2012 15:22:01	Uno dei due utenti visita la pagina www.youtube.com
25/07/2012 15:22:16	Uno dei due utenti effettua la ricerca *"Origami cigno"* e visualizza il video
25/07/2012 15:22:19	Uno dei due utenti effettua la ricerca *"Stammi vicino-Vasco Rossi"* e visualizza il video

Tabella 3: Cronologia *Img1*

Data	Evento
26/10/2012 11:06:03	L'utente1 accede al sito www.google.it
26/10/2012 11:07:07	L'utente1 accede al sito www.twitter.com
26/10/2012 11:07:36	L'utente1 accede al suo profilo Twitter con l'account *"testif2012user@gmail.com"*
26/10/2012 11:07:57	L'utente1 visualizza il proprio profilo Twitter
26/10/2012 11:08:10	L'utente1 effettua il logout dal suo profilo Twitter
26/10/2012 11:08:19	L'utente1 si collega al sito www.gmail.com
26/10/2012 11:08:54	L'utente2 si collega al sito www.libero.it
26/10/2012 11:09:09	L'utente2 effettua il login al suo account di posta con username *"testif1999user@libero.it"*
26/10/2012 11:09:42	L'utente2 visualizza il messaggio di posta inviato dall'utente1
26/10/2012 11:10:33	L'utente2 scarica l'allegato *"Dar voce alle prove.pdf"* presente nel messaggio di posta
26/10/2012 11:11:02	Uno dei due utenti si collega al sito www.repubblica.it
26/10/2012 11:11:09	Uno dei due utenti visualizza l'articolo *"Terremoto, Clini attacca la sentenza"*
26/10/2012 11:11:57	Uno dei due utenti si collega al sito www.corriere.it ed esplora la sezione relativa agli annunci di lavoro
26/10/2012 11:12:00	Uno dei due utenti visualizza l'articolo *"Apple, mini-maxi evento"*
26/10/2012 11:12:11	L'utente1 si collega al sito www.gmail.com
26/10/2012 11:12:31	L'utente1 effettua il login al suo account di posta con username *"testif2012user@gmail.com"*

26/10/2012 11:12:44	L'utente1 effettua il logout dal suo profilo gmail
26/10/2012 11:13:08	L'utente2 accede al suo profilo Twitter con l'account *"testif1999user@libero.it"*
26/10/2012 11:13:08	L'utente2 effettua il logout dal suo profilo Twitter
26/10/2012 11:13:11	L'utente2 accede al suo profilo Facebook con l'account *"testif1999user@libero.it"*
26/10/2012 11:13:39	L'utente2 effettua il logout dal suo profilo Facebook
26/10/2012 11:13:58	Uno dei due utenti visita la pagina www.punto-informatico.it
26/10/2012 11:14:04	Uno dei due utenti visita la pagina www.youtube.com
26/10/2012 11:14:08	Uno dei due utenti effettua la ricerca *"Origami cigno"* e visualizza il video

Tabella 4: Cronologia *Img2*

Data	**Evento**
24/10/2012 19:36:08	L'utente1 si collega al sito www.mozilla.com
24/10/2012 19:36:54	L'utente1 si collega al sito www.google.com
24/10/2012 19:37:04	L'utente1 effettua il login al suo account di posta con username *"testif2012user@gmail.com"*
24/10/2012 19:37:38	L'utente1 visualizza la posta in arrivo nella propria casella email
24/10/2012 19:37:47	L'utente1 compone un nuovo messaggio di posta elettronica
24/10/2012 19:37:55	L'utente1 effettua il logout dal suo profilo gmail

24/10/2012 19:38:19	L'utente2 si collega al sito www.libero.it
24/10/2012 19:39:19	L'utente2 effettua il login al suo account di posta con username *"testif1999user@libero.it"*
24/10/2012 19:39:40	L'utente2 visualizza il messaggio di posta inviato dall'utente1
24/10/2012 19:39:41	L'utente2 scarica l'allegato *"Dar voce alle prove.pdf"* presente nel messaggio di posta
24/10/2012 19:39:52	Uno dei due utenti si collega al sito www.repubblica.it
24/10/2012 19:40:03	Uno dei due utenti visualizza l'articolo *"Terremoto, Clini attacca la sentenza"*
24/10/2012 19:40:41	Uno dei due utenti si collega al sito www.corriere.it ed esplora la sezione relativa agli annunci di lavoro
24/10/2012 19:40:59	Uno dei due utenti visualizza l'articolo *"Apple, mini-maxi evento"*
24/10/2012 19:41:05	L'utente1 accede al sito www.twitter.com
24/10/2012 19:41:11	L'utente1 accede al suo profilo Twitter con l'account *"testif2012user@gmail.com"*
24/10/2012 19:41:44	L'utente1 visualizza il proprio profilo Twitter
24/10/2012 19:41:54	L'utente2 accede al suo profilo Twitter con l'account *"testif1999user@libero.it"*
24/10/2012 19:41:56	L'utente2 effettua il logout dal suo profilo Twitter
24/10/2012 19:41:57	Uno dei due utenti visita la pagina www.youtube.com
24/10/2012 19:42:03	Uno dei due utenti effettua la ricerca *"Origami cigno"* e visualizza il video
24/10/2012 19:44:19	Uno dei due utenti effettua la ricerca *"Stammi vicino-Vasco Rossi"* e visualizza il video
24/10/2012 19:44:45	L'utente2 accede al suo profilo Facebook con l'account *"testif1999user@libero.it"*
24/10/2012 19:44:54	L'utente2 effettua il logout dal suo profilo Facebook

24/10/2012 19:45:09	`L'utente1 accede al suo profilo Facebook con l'account` *"testif2012user@gmail.com"*
24/10/2012 19:45:15	L'utente1 visualizza la pagina personale del suo profilo Facebook

Tabella 5: Cronologia *Img3*

Data	Evento
24/10/2012 21:30:32	L'utente1 si collega al sito www.mozilla.com
24/10/2012 21:31:13	L'utente1 si collega al sito www.google.com
24/10/2012 21:32:16	L'utente1 effettua il login al suo account di posta con username *"testif2012user@gmail.com"*
24/10/2012 21:32:18	L'utente2 visualizza il messaggio di posta inviato dall'utente1
24/10/2012 21:32:22	L'utente1 compone un nuovo messaggio di posta elettronica
24/10/2012 21:34:16	L'utente1 effettua il logout dal suo profilo gmail
24/10/2012 21:34:34	L'utente2 si collega al sito www.libero.it
24/10/2012 21:34:54	L'utente2 effettua il login al suo account di posta con username *"testif1999user@libero.it"*
24/10/2012 21:34:56	L'utente2 visualizza il messaggio di posta inviato dall'utente1
24/10/2012 21:35:12	L'utente2 scarica l'allegato *"Dar voce alle prove.pdf"* presente nel messaggio di posta
24/10/2012 21:35:23	Uno dei due utenti si collega al sito www.repubblica.it
24/10/2012 21:35:46	Uno dei due utenti visualizza l'articolo *"Terremoto, Clini attacca la sentenza"*

24/10/2012 21:35:58	Uno dei due utenti si collega al sito www.corriere.it ed esplora la sezione relativa agli annunci di lavoro
24/10/2012 21:36:07	Uno dei due utenti visualizza l'articolo *"Apple, mini-maxi evento"*
24/10/2012 21:36:40	L'utente1 accede al sito www.twitter.com
24/10/2012 21:36:56	L'utente1 accede al suo profilo Twitter con l'account *"testif2012user@gmail.com"*
24/10/2012 21:37:00	L'utente1 visualizza il proprio profilo Twitter
24/10/2012 21:37:31	L'utente2 accede al suo profilo Twitter con l'account *"testif1999user@libero.it"*
24/10/2012 21:37:45	L'utente2 effettua il logout dal suo profilo Twitter
24/10/2012 21:38:56	L'utente2 accede al suo profilo Facebook con l'account *"testif1999user@libero.it"*
24/10/2012 21:39:04	L'utente2 effettua il logout dal suo profilo Facebook
24/10/2012 21:39:35	`L'utente1 accede al suo profilo Facebook con l'account` *"testif2012user@gmail.com"*
24/10/2012 21:39:46	L'utente1 visualizza la pagina personale del suo profilo Facebook

Tabella 6: Cronologia *Img4*

La lettura delle tabelle è abbastanza intuitiva: per ogni test sono elencate le ricorrenze di ogni operazione rilevata, evidenziandone in particolare la data ed il sito web visitato. Di particolare interesse, in tali ricostruzioni, sono le informazioni riguardanti gli accessi ai social network Facebook e Twitter, gli accessi alla mail ed i download effettuati, dal momento che rappresentano le informazioni più importanti per la tutela della privacy. Inoltre, per quanto riguarda in Browser Tor, l'analisi della cronologia dei siti web è avvenuta

esclusivamente utilizzando FTK Toolkit, dal momento che non sono disponibili software opensource che permettano una visualizzazione dei siti web visitati attraverso semplici interfacce utente.

- **Analisi ricerca per parola chiave**

Data la grande quantità di dati da analizzare, per rendere l'attività di analisi più efficiente sono state definite una serie di parole da utilizzare come chiavi di ricerca. All'interno della tabella *Indexed Search,* del software *FTK toolkit,* sono state digitale le parole chiave "*testif2012*" e "*testif1999*", al fine di visualizzare rapidamente elementi relativi ai due profili utente e ricostruirne l'attività sul web.

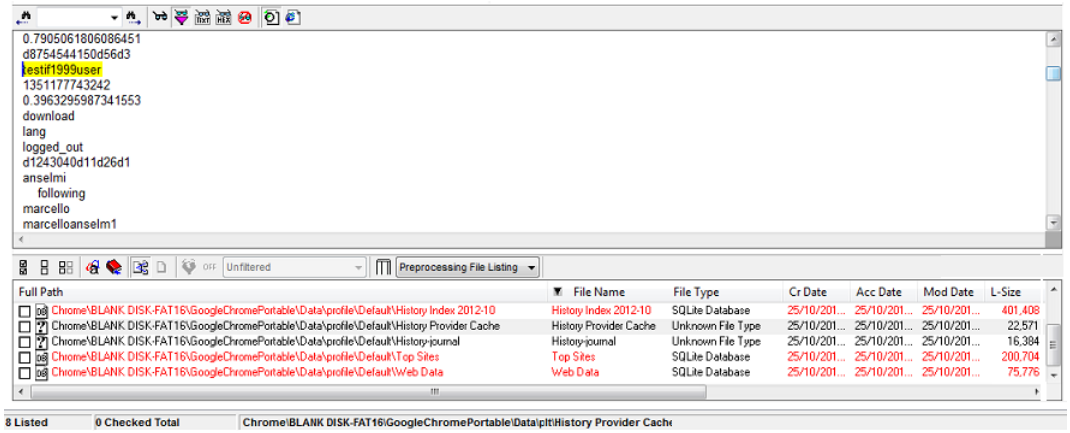

Figura 5.17: Ricerca per parole chiave

La ricerca ha permesso di esplorare i file all'interno dei quali erano state memorizzate le parole chiave e di visualizzarle in formato testuale.

5.3 Analisi dei risultati

Servendoci di alcuni grafici, ci dedicheremo ora alla comparazione dei dati raccolti. In particolare, per documentare come differiscano i tre browser, ne abbiamo testato diverse funzioni ed osservato come cambiano il tipo e la quantità di informazioni memorizzate durante la navigazione anonima.

I dati di maggiore interesse rilevati durante la navigazione anonima fanno riferimento a pagine visitate, moduli e barra di ricerca, password ed profili utente, elenco dei download, contenuti web in cache e cookies.

I risultati sono riassunti nella seguente tabella.

	Mozilla Firefox con password	**Mozilla Firefox senza password**	**Google Chrome con password**	**Google Chrome senza password**	**Tor**
Siti visitati	*96*	*144*	*82*	*104*	*0*
Cache	*0*	*0*	*0*	*0*	*0*
Cookies	*109*	*0*	*0*	*0*	*0*
Utenze	*9*	*17*	*5*	*9*	*0*
Password utente	*0*	*0*	*0*	*0*	*0*
Download	*2*	*2*	*2*	*2*	*0*

Parole ricercate	*12*	*12*	*12*	*19*	*0*

Tabella 7:Risultati dei test

dove:

- **siti visitati** sono il numero di siti rilevati durante l'operazione di analisi forense;
- **cache** è il numero di copie temporanee delle pagine visitate durante la navigazione anonima;
- **cookies** è la voce che descrive il numero di file di testo archiviati nella memoria di massa del computer dell'utente;
- **utenze** è la voce che evidenzia il numero di indirizzi email trovati mediante il processo di analisi e relativi ai due profili utente;
- **password utente** è la voce che descrive il numero di password digitate e rilevate;
- **download** è il numero di file scaricati durante la navigazione web;
- **parole ricercate** è il numero di parole digitate e rinvenute sui vari motori di ricerca.

5.3.1 Peso percentuale delle operazioni rilevate

Per rendere più evidente e chiara l'analisi dei risultati pervenuti dai test e dall'analisi condotta sui browser portable, osserviamo il peso percentuale della presenza dei dati rilevati (Hystory, Cookies, Password, query di ricerca ecc) per ogni tipo di browser utilizzato durante la navigazione. Di seguito vengono mostrati graficamente i risultati delle analisi condotte per ogni test effettuato in base al tipo di informazione memerizzata nei diversi browser (si veda la figura 5.3).

- **Analisi dei risultati del test 1**

La figura 5.18, mostra il confronto tra il numero di voci URL dei siti web rilevati nei cinque test effettuati, ossia mediante l'utilizzo dei browser Google Chrome, Mozilla Firefox e Tor con attiva o meno l'opzione del salvataggio delle password.

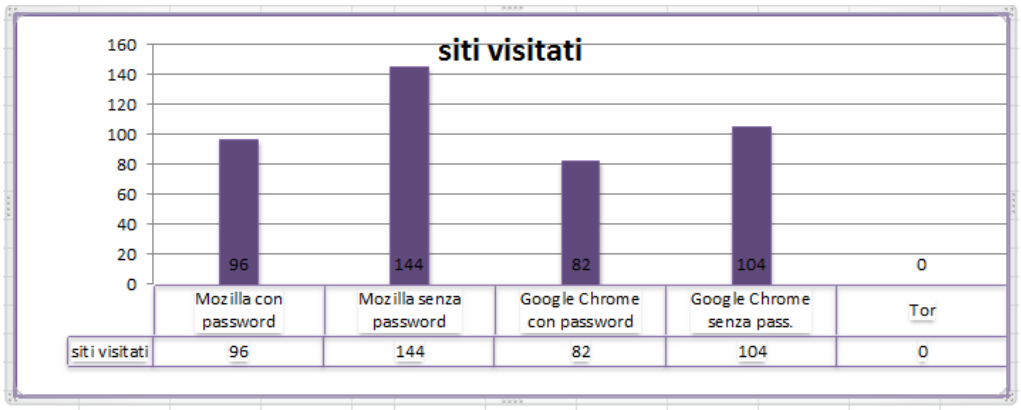

Figura 5.18: Comparazione dei siti web visitati nei diversi browser

- **Analisi dei risultati del test 2**

Come mostra la figura 5.19, il risultato del test 2 evidenzia il confronto tra il numero di elementi della cache rilevati sui diversi browser web.

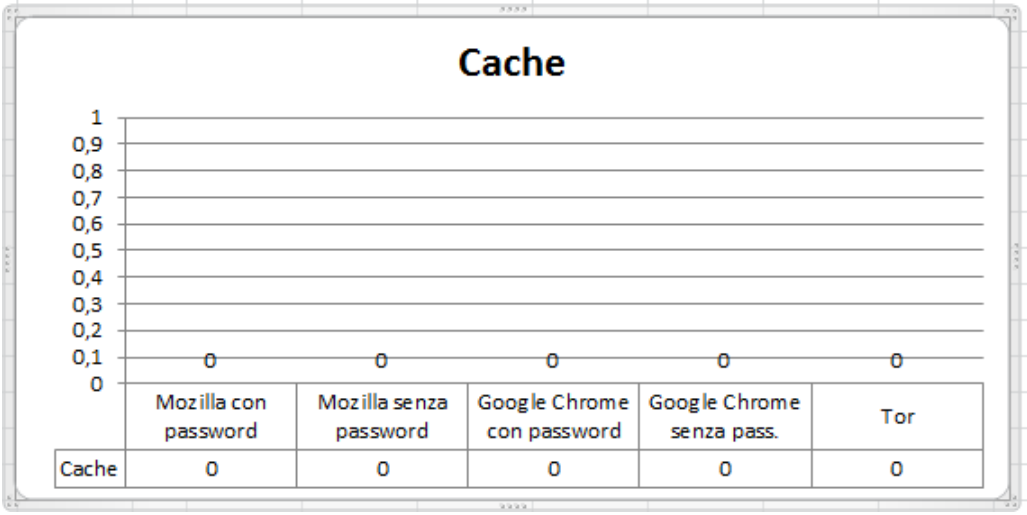

Figura 5.19: Comparazione della cache nei diversi browser

- **Analisi dei risultati dei test 3**

Il test 3 delinea il numero di cookies memorizzati nei diversi browser web durante la navigazione anonima.

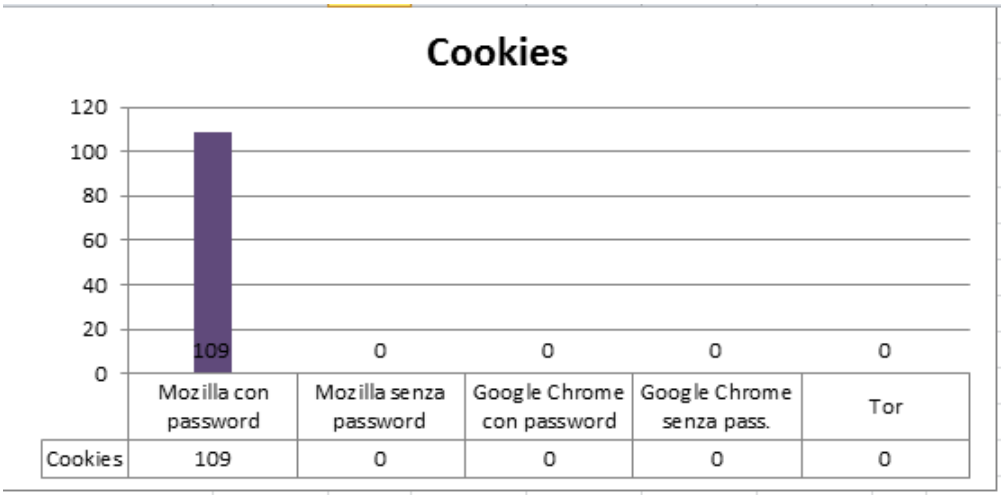

Figura 5.20: Comparazione dei cookies nei diversi browser

- **Analisi dei risultati dei test 4**

Come mostra la seguente figura, il test 4 ha evidenziato come sono state memorizzate le informazioni (email) legate ai due profili utente creati per la realizzazione dei test.

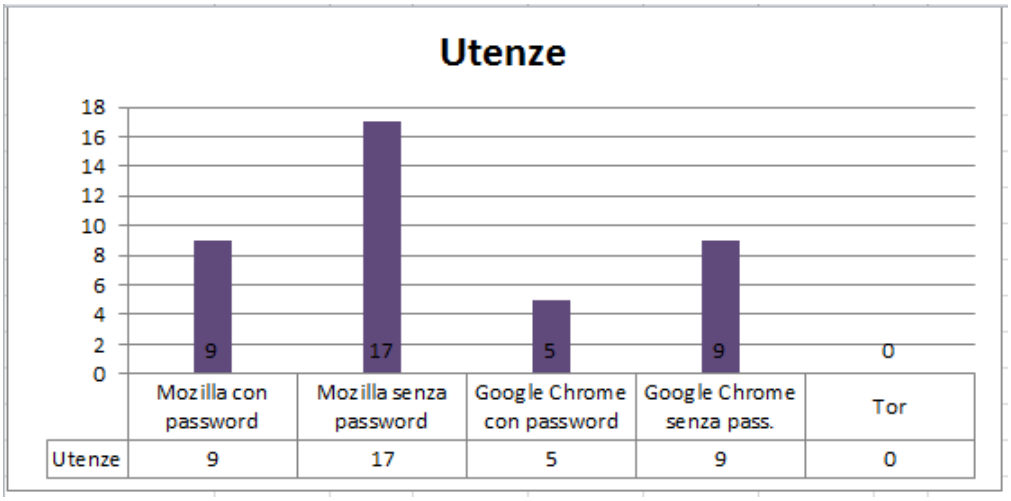

Figura 5.21: Comparazione delle utenze nei diversi browser

- **Analisi dei risultati del test 5**

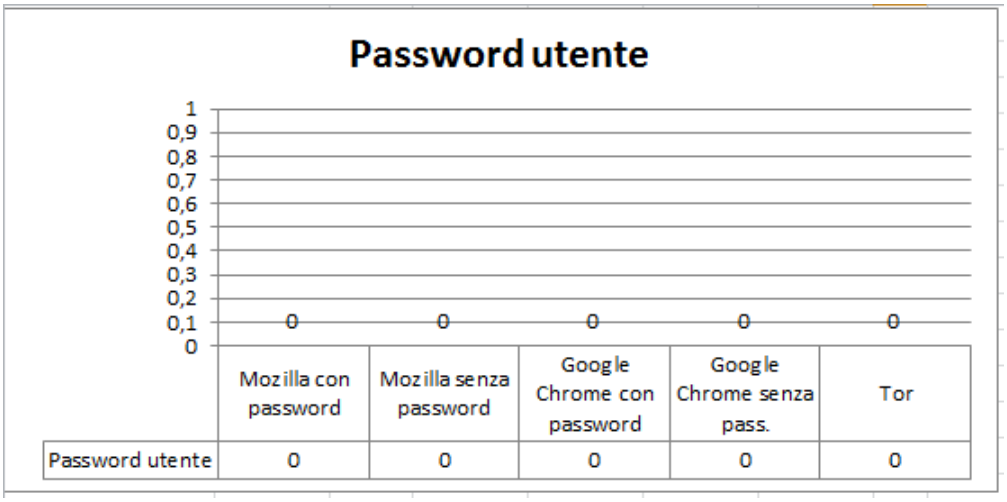

Figura 5.22: Comparazione delle password nei diversi browser

- **Analisi dei risultati del test 6**

I risultati del test 6 mettono in rilievo il numero di file scaricati durante la navigazione web e memorizzati all'interno dei browser web analizzati.

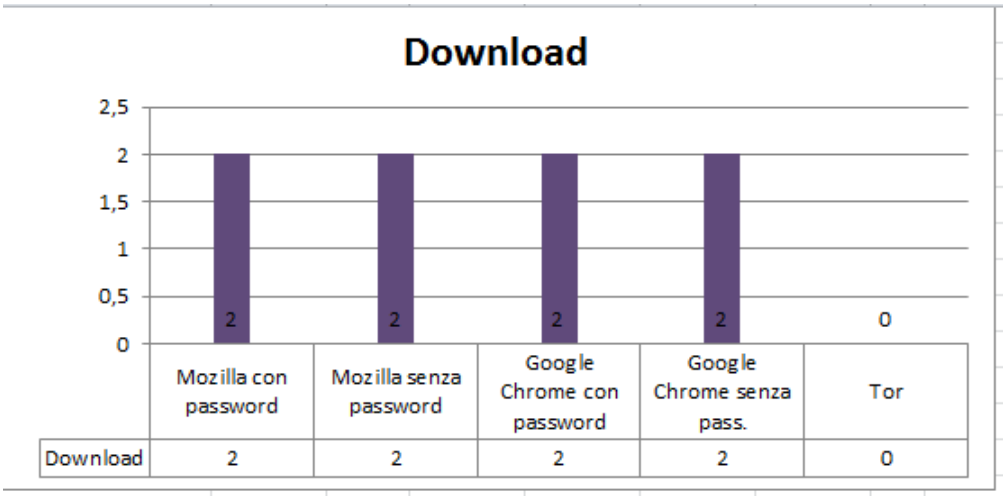

Figura 5.23: Comparazione dei download nei diversi browser

- **Analisi dei risultati del test 7**

Questo test, come mostra la figura seguente, mette in luce il differente numero di informazioni rinvenute sui diversi browser web in base ad una serie di parole utilizzate come chiavi di ricerca (si veda la figura 5.17).

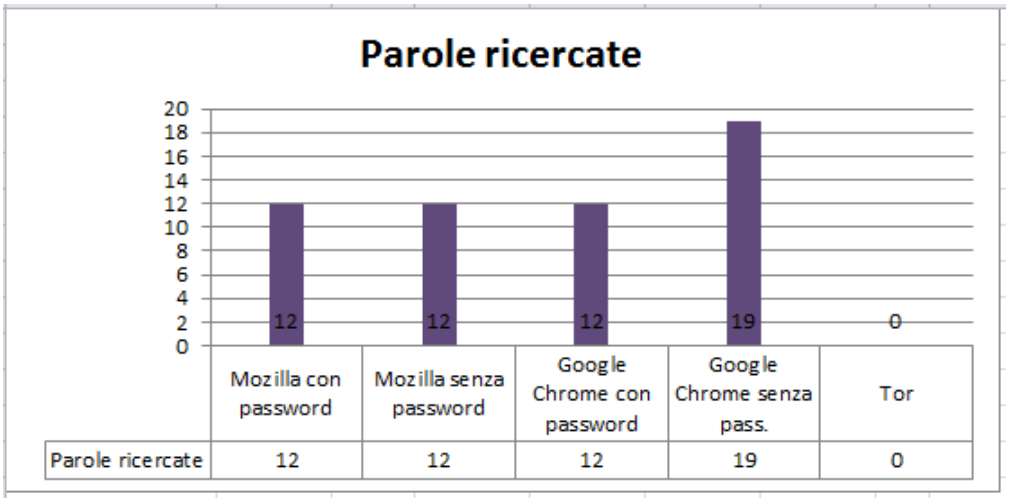

Figura 5.24: Comparazione delle parole ricercate nei diversi browser

5.3.2 Comparazione dei risultati

L'analisi dei risultati ci ha permesso di effettuare una comparazione tra i diversi servizi offerti dai browser portable.

Nel grafico seguente, vengono infatti riassunte ed evidenziate le caratteristiche di ogni browser, in base al tipo di informazioni memorizzate sul drive USB durante la navigazione web.

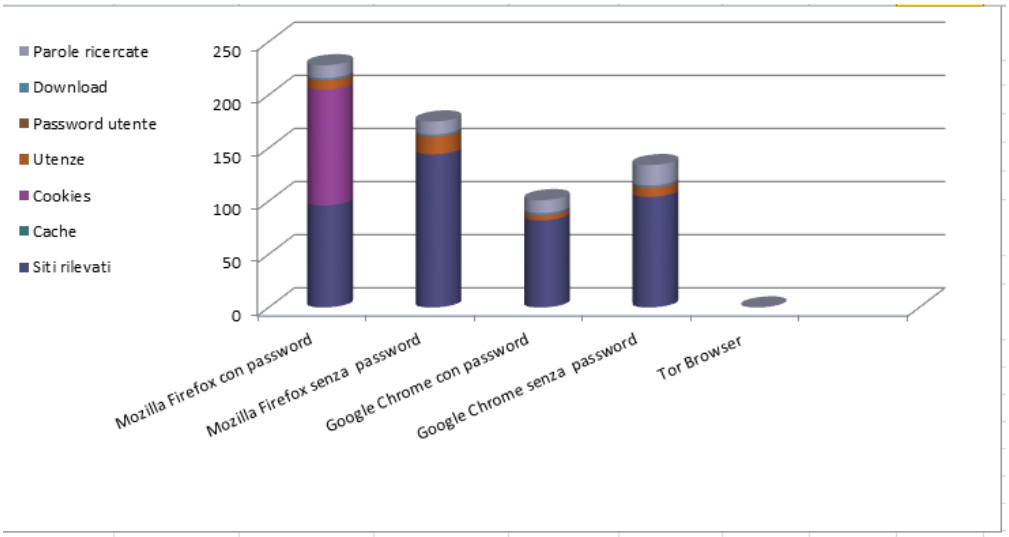

Figura 5.25: Grafico risultati

I risultati mostrano il livello di privacy fornite dai tre browser.

Confrontando i risultati (Figura 5.25) di ciascun Web Browser è facile intuire che Tor è il più sicuro di tutti, in termini di non memorizzazione di dati. Il punto di forza di questo browser è infatti, la capacità di non lasciare tracce sulla rete e pertanto non vengono memorizzate nemmeno le attività svolte durante la navigazione web all'interno del drive USB.

Rispetto al browser Tor, Google Chrome e Mozilla Firefox, invece, presentano un livello di anonimato discreto, in quanto sembrano tenere traccia della cronologia, delle parole chiave utilizzate nei motori di ricerca, di alcune informazioni relative ai profili utente ed ai file scaricati durante la navigazione. Inoltre, a seconda del tipo di configurazione Mozilla Firefox, memorizza anche i cookies. Come risultato, tutti i file risiedono sul drive USB fino a

quando non vengono sovrascritti da altri file, e questo rende facile estrarre i file e ricostruire l'attività web anche se si utilizzati strumenti portable al fine di proteggere la propria privacy.

Conclusioni

Questo lavoro di tesi si proponeva come obiettivo la misurazione di eventi generati da un utente utilizzatore di browser portable. A tal fine sono stati condotti 5 test, ognuno dei quali prevedeva una variante e al termine del quale veniva generata un'immagine forense *bit-stream* da sottoporre ad analisi:

1. browser portable Mozilla Firefox con salvataggio delle credenziali *"testif2012user@gmail.com"* e *"testif1999user@libero.it";*
2. browser portable Mozilla Firefox senza salvataggio delle credenziali *"testif2012user@gmail.com"* e *"testif1999user@libero.it";*
3. browser portable Google Chrome con salvataggio delle credenziali *"testif2012user@gmail.com"* e *"testif1999user@libero.it";*
4. browser portable Gooogle Chrome senza salvataggio delle credenziali *"testif2012user@gmail.com"* e *"testif1999user@libero.it";*
5. browser portable TOR*;*

Su ogni immagine forense è stata dunque operata un'analisi forense allo scopo di identificare tracce di navigazione, misurando in tal modo sia l'efficacia in termini di privacy e assenza di dati sulle memorie di massa, sia le risultanze ottenibili dall'informatico forense che si trova a dover analizzare tali software.

É doveroso precisare che obiettivo del presente lavoro è la misurazione delle tracce digitali lasciate dai browser portable sulle memorie di massa, tra-

lasciando gli aspetti relativi a possibili intercezioni del traffico telematico e all'eventualità di identificazione dell'utenza telefonica che ha generato il traffico di rete.

Relativamente all'assenza di eventi (cronologia, cache, cookie...) sulla memoria di massa, il sistema che è risultato migliore è TOR (test 5). Tale risultato mette in evidenza l'impossibilità di ricostruire da parte di un informatico forense l'attività dell'utente (gusti, abitudini, interessi, frequenza d'uso...).

Laddove invece sono stati identificati degli artefatti, risultano maggiormente presenti tracce di *url* visitati e *file* scaricati (lista di download), mentre risultano limitati tracce relative a *cache*, *credenziali* e *cookie*. Entrando maggiormente nel dettaglio, il test che in assoluto ha registrato il maggior numero di eventi recuperabili è il test 1, nel quale, come già testè esposto, è stato utilizzato il browser Mozilla Firefox prevedendo il salvataggio delle credenziali *"testif2012user@gmail.com"* e *"testif1999user@libero.it"*: è possibile ricostruire oltre 100 operazioni delle 144 eseguite dall'utente (come illustrato nel paragrafo 5.2.5). Gli eventi individuati in questo test sono di gran lunga superiori in termini quantitativi rispetto ai risultati degli altri test condotti.

Pertanto, da un punto di vista delle tracce rinvenibili sul sistema informatico utilizzato, le garanzie maggiori in termini di riservatezza sono offerte nell'ordine da TOR, Google Chrome e ultimo Mozilla Firefox. Da un punto di vista di informatica forense, la classifica va ribaltata se si intende classificare l'opportunità di individuare le operazioni compiute sul sistema.

Riferimenti bibliografici

[1] U.S. Department of Justice. Federal Bureau of Investigation. Laboratory Division. HANDBOOK OF FORENSIC. *Pentagon Publishing, 2011.* Url: *http://www.fbi.gov/about-us/lab/handbook-of-forensic-services-pdf* 1.3

[2] Cesare MAIOLI. *Dar voce alle prove: elementi di Informatica forense,* Franco Angeli 2004. 1.4, 1.6.4, 2

[3] Giovanni ZICCARDI. *Scienze forensi e Tecnologie informatiche: la computer and network forensics.* In "Informatica e diritto", *Volume 2*, Anno 2006, pp.103-125. 1.4

[4] Tribunale penale di Bologna sezione I monocratica. *Sentenza 21/07/2005 (caso Vierika),* 2005. 1.4

[5] Corte d'appello di Bologna sezione II penale. *Sentenza 30/01/2008 (caso Vierika),* 2008. 1.4

[6] Tribunale di Vigevano sezione penale. *Sentenza 31/10/2008, 2009.* 1.4.2

[7] WikiNotizie. Speciale Omicidio Chiara Poggi. url: *http://it.wikinews.org/wiki/Speciale_Omicidio_Chiara_Poggi* 1.4.2

[8] Svein Yngvar WILLASSEN, Forensic analysis of digital copiers, 2005. Url: *http://www.willassen.no/svein/pub/copier-en.pdf* 1.6.1

[9] Marco MATTIUCCI. *Computer Forensics*. Ultima visita: 28 febbraio 2013. Url: *http://www.marcomattiucci.it/computerforensicsarea.php* 1.6.2, 1.6.5

[10] Wikipedia. *Sequestro probatorio*. Ultima visita: 26 febbraio 2013. Url: *http://it.wikipedia.org/wiki/Sequestro_probatorio* 2.4.3

[11] Wikipedia. *Intercettazioni*. Ultima visita: 01 marzo 2013. Url: *http://it.wikipedia.org/wiki/Intercettazione* 2.4.4

[12] Crimine.it. *Accertamenti tecnici*. Ultima visita: 27 febbraio 2013. Url: *http://www.crimine.it/pagina.asp?ID=165* 2.5.1

[13] Consulenza-tecnica.lacasagiusta.it. *Consulenza tecnica d'ufficio*. Ultima visita: 23 febbraio 2013. Url:*http://consulenza-tecnica.lacasagiusta.it/consulenza-tecnica-di-ufficio/*

[14] Giusella FINOCCHIARO. *La memoria della rete e il diritto all'oblio,* Giuffrè Editore 2010. 2.6.1, 4.1

[15] Giuseppe DEZZANI e Mario Leone PICCININI. *Social Generation*, Hoepli Editore 2012. 4.1

[16] Carmelo BADALAMENTI. *Tor e la sicurezza informatica*, 2007. Url*: http://rollsappletree.altervista.org/Sicurezza/i07_Badalamenti.pdf* 4.2

[17] Wikipedia. *Privacy-enhancing technologies.* Ultima visita: 28 febbraio 2013. Url: http://en.wikipedia.org/wiki/Privacy-enhancing_technologies 4.2

[18] Marco CALAMARI (Punto-informatico.it). *Lo stato delle Pet, 2006.* Ultima visita: 25 febbraio 2013. Url:http://punto-informatico.it/1811559/PI/Commenti/cassandra-crossing-stato-delle-pet.aspx 4.2, 4.3

[19] Giovanni PASCUZZI. *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, Mulino, 2002, pagg. 1-70. 4.2

[20] Giovanni ZICCARDI. *Il giornalista hacker*, Marsilio Editori 2012. 4.3

[21] Giovanni ZICCARDI (2012). *Cyber Law in Italy*, ALPHEN A/D RIJN: Wolters Kluwer Law International (THE NETHERLANDS), 2012.

4.4