CAPITOLO DODICESIMO
L'ALIBI INFORMATICO
ASPETTI TECNICI E GIURIDICI

Vincenzo Calabrò – Gerardo Costabile – Stefano Fratepietro
Mario Ianulardo – Giuseppe Nicosia

1. PREMESSA

Il ricorso sempre più massiccio all'uso di strumenti elettronici, informatici e telematici per lo svolgimento di attività lavorative e ricreative, ha determinato una enorme produzione di dati digitali. La pervasività della tecnologia elettronico-informatica ha comportato, pertanto, un sensibile aumento dei casi in cui i computer e gli apparati di comunicazione digitali vengono utilizzati come mezzo per commettere reati e, nel contempo, vengono sottoposti, anche in casi di commissione di reati non prettamente informatici, ad analisi forense al fine di trovare tracce utili alle indagini. Gli elementi idonei ad individuare responsabilità in ordine alla commissione di reati sono costituiti da file contenuti nella memoria di un PC, di una videocamera, fotocamera, telefoni cellulari e quindi in numerosi tipi di supporti di memorizzazione di dati digitali. Tuttavia, è accaduto, altresì, che tracce informatiche sono servite per dimostrare la totale estraneità dell'indiziato alle accuse formulate nei suoi confronti perché sospettato di essere stato l'autore di un delitto. Il presente lavoro si prefigge l'obiettivo di illustrare in quali casi l'attività informatica, svolta dall'indiziato, sia stata utile all'accertamento della verità e i casi in cui, con l'ausilio della tecnica, sia stato reso possibile precostituire artatamente un alibi ricorrendo a tecniche di anti forensics. Il termine *alibi* è un avverbio di lingua latina che significa altrove. Grazie al ricorso che ne è stato fatto, nell'intessere la trama di romanzi gialli e film polizieschi, l'alibi rappresenta l' "altro luogo" in cui si trovava l'indiziato nello stesso arco temporale in cui in altro luogo veniva commesso un delitto. Il termine, in ambito giudiziario, appare suscettibile di assurgere ad elemento di prova se corroborato da elementi di riscontro oggettivi capaci di dimostrare appunto che al momento in cui veniva commesso il reato, l'indiziato, nello stesso orario, si trovava in un luogo diverso. Pare opportuno evidenziare, in questa sede, la distinzione tra alibi e cause di giustificazione, c.d. scriminanti. Queste ultime rappresentano situazioni, al ricorrere delle

quali, il fatto, nonostante la sua conformità alla fattispecie penale astratta, risulta non punibile in concreto in quanto autorizzato o imposto da altre norme dell'ordinamento. Le scriminanti, dette anche cause di esclusione del reato, sono tassativamente individuate dalla legge ed escludono l'antigiuridicità di una condotta che, in loro assenza, sarebbe penalmente rilevante e sanzionabile. Si citano, come esempio, il consenso dell'avente diritto (art.50 c.p.); l'esercizio di un diritto e l' adempimento di un dovere (art.51 c.p.); la legittima difesa (art.52 c.p.); l'uso legittimo delle armi (art.53 c.p.); lo stato di necessità (art.54 c.p.); l'eccesso colposo (art.55 c.p.).
L'alibi, al contrario, indica la "non presenza" dell'indiziato sul luogo del delitto che quindi esclude la sua partecipazione all'azione delittuosa. In definitiva, mentre in presenza di un alibi fondato si dimostra di non aver commesso il reato, in presenza di una causa di giustificazione, invece, è data per scontata la partecipazione del soggetto agente all'azione delittuosa, tuttavia, ne viene esclusa la punibilità. Infatti, all'esito della celebrazione di un processo penale, il giudice, in presenza di un alibi di ferro dovrà emettere sentenza di assoluzione nei confronti dell'imputato "per non aver commesso il fatto"; viceversa, se si trovasse a decidere il caso giudiziario di un soggetto che ha agito in presenza di una causa di giustificazione, dovrà emettere sentenza di assoluzione "perché il fatto non costituisce reato".

2. ASPETTI GENERALI. DEFINIZIONI

Come detto per "alibi" si intende generalmente una allegazione difensiva di circostanze di fatto prospettabili a difesa dell' imputato o dell' indagato, che si pongono in oggettivo contrasto con i fatti posti a base dell' ipotesi accusatoria[1].

Tale allegazione, frequentemente (ma non unicamente) è volta a dimostrare che il soggetto indagato o imputato, al momento della commissione del reato si trovava in luogo diverso e lontano rispetto a quello ove il reato stesso sarebbe stato perpetrato o che, comunque, lo stesso non avrebbe potuto commettere quanto a lui contestato. Si tratta, dunque di una prova o dimostrazione logico-fattuale contro-deduttiva, rispetto alle tesi accusatorie, proposta dalla difesa al fine di minare elementi fondamentali della ricostruzione avversa e ciò si dice in un' ottica che, pur nella "parità " fra accusa e difesa prevista nel nostro ordinamento processuale, vede comunque solo la prima tenuta a dimostrare puntualmente tutti i suoi assunti e percorsi "oltre ogni ragionevole dubbio", essendo, invece, sufficiente, per le allegazioni difensive, che le stesse siano ragionevoli e coerenti e tali da impedire all' accusa il raggiungimento di detto

1 Sul punto vedasi Ass. App. Catania, sez. III, 15.1.2005

punto di certezza. Vertendosi in tema di prova controdeduttiva-controfattuale la stessa è intimamente legata alla ricostruzione probatoria offerta dall'accusa, alla quale dovrebbe andare a sovrapporsi con segno però opposto, ed in relazione alla quale instaura un rapporto di alternatività che può essere anche solo parziale. Il trovarsi "in altro luogo" infatti, può e deve essere inteso sia in senso letterale che nel senso figurato di *non essersi trovato in situazione tale da poter commettere il reato*; da ciò deriva logicamente una doppia proposizione da dimostrare: negativa il "non essere nel luogo" e positiva "perché si è in altro luogo". Il tutto legato dalla dimostrazione dell'impossibilità, per ragioni di spazio e di tempo, di trascendere dall' uno all' altro dei luoghi individuati al momento della commissione del fatto.
Su questi elementi si appunterà l'opera dimostrativa delle parti e quella valutativo-decisionale del giudicante, il quale dovrà verificare analiticamente tutti i passaggi dei diversi *iter* proposti. Sempre su questi elementi andrà ad intervenire l'opera ricostruttiva dei consulenti, chiamati a coadiuvare i singoli soggetti del procedimento con le loro indagini. Sarà quindi compito di detti consulenti, di concerto con i soggetti predetti:

- innanzitutto individuare le differenti ipotesi ricostruttive, sulla base dei fatti acquisiti al procedimento, delineando l'ipotesi accusatoria e quelle eventualmente alternative;
- verificare i punti di forza e di debolezza sia fattuale, sia logica che tecnica delle singole ipotesi, individuando le conferme endogene ed esogene delle stesse e, se possibile, il grado di probabilità delle medesime, anche alla luce dell' utilizzo di strumenti quali il Daubert test [2] e delle regole (best practice, regole di esperienza, stato dell' arte) eventualmente condivise dagli esperti del singolo settore. In tale maniera si verificheranno non solo i risultati, ma soprattutto il grado di affidabilità degli strumenti sia logici che tecnici utilizzati, alla luce delle migliori conoscenze scientifiche esistenti al momento;
- reperire ulteriori elementi probatori in via di integrazione sia a supporto dell' ipotesi sostenuta che a contrasto delle ipotesi avversarie, svolgendo le rispettive attività di ricerca ed indagine anche suppletiva;
- infine ricomporre gli accertamenti svolti in un unico *iter* logico-giuridico, il piu' possibile coerente e motivato, che riesca, pertanto, a dare conto del maggior numero degli elementi (di fatto) acquisiti al processo in maniera non contraddittoria.

[2] In merito al Daubert test si rinvia alla relativa voce di Wikipedia all' indirizzo http://*en.wikipedia.org/wiki/**Daubert_standard*** e alla definizione contenuta nel Free dictionary all' indirizzo http://legal-dictionary.thefreedictionary.com/Daubert+Test. Si ricordano altresì le interessanti considerazioni a tale proposito svolte da O Dominioni in La Prova scientifica Penale, Giuffre' 2005 e da Luparia e Ziccardi in Investigazione penale e Tecnologia Informatica, Giuffre', 2007

A tale proposito deve ricordarsi come la giurisprudenza abbia ritenuto che il giudicante debba (e non semplicemente possa), anche in caso di mancata diretta o di parziale allegazione, tener conto delle risultanze controfattuali, eventualmente attivando anche poteri di ufficio ex art. 507 c.p.p. (integrazione probatoria) ed ex art. 195 co. 2 c.p.p. (testimonianza indiretta) al fine della completa ricostruzione di condotte ed eventi, specialmente in ipotesi di commissione di reati di particolare gravità. [3]

Ciò vuol dire che la mera incompletezza dell' allegazione o anche la genericità (purché non tale da impedire ogni controllo giudiziario) dell' alibi non comporterà la sua irrilevanza, obbligando comunque il giudicante a tenerne conto, pena la censurabilità della decisione sotto il profilo eventuale della incongruità, incompletezza o contraddittorietà della motivazione assunta [4] e ciò anche in ipotesi di accesso a riti alternativi o di eventuale fase impugnativa, soprattutto se la prova a sostegno del prospettato alibi, e della quale si chiede l'acquisizione, si prospetti come decisiva ai sensi dell' art. 606 co. 1 lett. d) c.p.p. [5]. E' ovvio che tali ragioni e tali percorsi mutino grandemente di significato allorquando la commissione del reato avvenga (e quindi la condotta si svolga) in tutto o in parte non in un ambito meramente "fisico", ma coinvolga ambiti " virtuali" quali quelli telecomunicativi o nel Web, come anche recenti episodi balzati alle cronache nazionali hanno potuto dimostrare; oppure quando tracce ed elementi di prova attingano detti ambiti (ad esempio vedansi le indagini su supporti o sistemi informatici, collegati o meno alla rete, volte alla dimostrazione dello svolgimento di "attività informatica" in un certo luogo da parte di un certo soggetto, così come è avvenuto nel caso "Garlasco"). I fatti, le condotte, gli eventi e le relative dimostrazioni, dirette, indirette e contrarie dovranno, quindi tener conto del "luogo" ove si svolgono (o si sarebbero svolti) i fatti, sia per la loro ricostruzione, sia per la loro acquisizione processuale, sia, infine, per la loro valutazione. Deve ancora ricordarsi che la individuazione e ricostruzione di un alibi non è una scelta difensiva necessaria, visto che la giurisprudenza ha ripetutamente affermato che dalla assenza (appunto) di un alibi non possa farsi discendere le colpevolezza dell' imputato, in mancanza di elementi di prova che ne dimostrino la responsabilità al di là di ogni ragionevole dubbio. Parimenti processualmente neutra (e quindi non valutabile neppure alla stregua di mero indizio, ai sensi dell' art. 192 c.p.p., come confermato dalla giurisprudenza piu'

[3] In merito App. Terni 11/2/2008, in Corriere del merito 2008,6,708 con interessante nota di Foladore

[4] Nuovamente vedasi Ass. App. Catania, sez. III, 15.1.2005. Si ricorda altresì Cass. Sez. II, 30/1/13552 ove la Corte ha annullato con rinvio per mancanza di motivazione l'ordinanza del Tribunale del Riesame, il quale, a fronte di dichiarazioni assunte ex art. 391 bis c.p.p. prodotte dalla difesa a conferma di un alibi, aveva omesso la loro valutazione ai fini del decidere, unitamente a tutte le altre risultanze del procedimento, limitandosi ad osservare che la loro effettiva attendibilità avrebbe dovuto essere verificata dall' A.G. Procedente

[5] Vedasi Cass. Sez. I, 08/01/2002, n. 4495 ove si conferma la necessità (e non la mera opportunità) che il giudice di merito valuti, con valutazione ex ante, la potenzialità della prova di alibi, di sovvertire il valore degli altri elementi probatori utilizzati o utilizzabili ovvero che la stessa " abbia l'attitudine ad infirmare i dati favorevoli dell' accusa".

recente) [6] è l'eventualità per cui non si giunga alla dimostrazione dell' alibi prefigurato (c.d. fallimento dell' alibi) e questo sempre per il medesimo motivo, ovvero perché nessun obbligo ha l'imputato di dimostrare la propria innocenza di contro, invece, all' obbligo che spetta alla pubblica accusa, di dimostrare la di lui colpevolezza. Di segno diverso è, invece, la conseguenza che le giurisprudenze di merito e di legittimità fanno discendere dalla dimostrazione della falsità dell' alibi proposto e ciò deve dirsi anche in considerazione del tema della presente ricerca.

Rilevata la presenza di differenti opinioni giurisprudenziali in merito, deve considerarsi che generalmente il rilievo della falsità dell' alibi, come la dimostrazione del fatto che lo stesso era stato artatamente preordinato o si è dimostrato puramente mendace, può essere (ma non deve, mancando una *regula iuris* in proposito) "posto in correlazione con altre circostanze di prova a carico e valutato come indizio, nel contesto delle complessive risultanze probatorie, se appaia finalizzato alla sottrazione del reo alla giustizia" [7]. Da ciò deriva, secondo la giurisprudenza, che l'alibi " falso" o "mendacemente ricostruito" non possa costituire prova a carico dell' imputato ma possa essere valutato contro l'imputato solo se inserito in un piu' ampio quadro probatorio sfavorevole allo stesso, come ulteriore elemento di valutazione del comportamento del medesimo e quindi dell' elemento soggettivo, e solo se vi sia sicurezza della sua falsità o della sua mendace ricostruzione.[8]

A dire il vero detto indirizzo, anche alla luce delle norme e dei principi costituzionali e del giusto processo, non convince completamente e ciò non solo perché si viene a toccare il delicato tema del c. d. diritto dell' imputato di difendersi mentendo (da ritenersi intangibile e del quale il falso alibi risulta essere una estensione), ma soprattutto perché si pone una commistione logica, fra elementi fattuali ed elementi soggettivi che invece debbono restare distinti.

La mera allegazione di un alibi, poi risultato falso, sotto il profilo meramente fattuale è assolutamente irrilevante (a meno che non si provi che la falsa predisposizione sia risalente al momento precedente o coevo alla commissione del reato, potendo, ad esempio, questo costituire elemento da valutare al fine della contestazione della premeditazione) in quanto inidoneo ad influire sulle ricostruzioni degli eventi. D'altro canto la predisposizione di un falso alibi può testimoniare la scorrettezza del soggetto, ma nulla prova circa la sua reale responsabilità e colpevolezza (non è, né può essere, equiparata ad una ammissione o una confessione anche implicita, essendo, peraltro diversa la direzione della volontà) stante il fatto che il comportamento processuale successivo non può

[6] In proposito Cass. Sez. II 04/02/2001 n. 11840 in Riv. Pen., 2005, 368:" il fallimento dell' alibi non può essere posto a carico dell' imputato come elemento sfavorevole, non essendo compito di quest' ultimo dimostrare la sua innocenza ". E precedentemente Cass. Sez. I, 23/01/2001 n. 12921.

[7] Così Cass. Sez. II, 04/02/2004, n. 11840. Vedasi anche Cass. Sez. II, 15/12/2005 n. 5060 in Riv. Pen. 2006/12/1363

[8] Sempre vedasi Cass. Sez. II, 15/12/2005 n. 5060 in Riv. Pen. 2006/12/1363

dire nulla sugli elementi probatori attinenti alla commissione del fatto ed essendo, le scelte difensive, frutto di comportamenti e considerazioni non solo, come detto, successive al fatto stesso e alle condotte contestate e poste in essere, ma spesso oggetto e frutto di considerazioni altre e diverse.
Il tutto per tacere del fatto che il confine fra alibi fallito ed alibi falso può risultare, in taluni casi, vago ed indeterminabile, potendo essere molteplici, ed esterni alla vicenda, i motivi per i quali lo stesso è stato speso (vedasi il caso, ad esempio, in cui l' allegazione sia stata fatta per evitare di far conoscere al coniuge l'esistenza di una relazione extraconiugale). Deve ancora ricordarsi che nella letteratura di settore esiste una sorta di "schema di valutazione dell'alibi", per aiutare a codificare quello che può dirsi un alibi credibile. Tale schema deve combinare (e separare) molteplici variabili. Vale a dire prove "fisiche" o elettroniche (pensiamo alle prove scientifiche, ovvero a video, cellulari, computer, telepass, fino ad arrivare a scontrini, biglietti aerei, etc.) e prove testimoniali (qualcuno che possa garantire).
L'alibi si scompone, pertanto, essenzialmente in due elementi che vengono sottoposti a valutazione. Vale a dire: l' accertamento della presenza dell'indiziato nello spazio e nel tempo da lui indicati e la constatata impossibilità fisica di coprire, nell'arco temporale in cui si è svolta l'azione delittuosa, la distanza che lo separa dal *locus commissi delicti.*
In un maggior dettaglio ed in chiave psicologica, possono essere distinti due "domini" all'interno del quale il processo di determinazione dell' alibi opera: il dominio di creazione e quello della credibilità (e accertamento/verifica). Il primo include al suo interno problemi di memoria autobiografica del soggetto, così come i ricordi delle persone che sono invitati a confermare un alibi.
Questo dominio è diviso in due fasi:

- Fase 1: dichiarazione di quanto ricorda l'indagato;
- Fase 2: ricerca di ulteriori informazioni a sostegno dell'alibi. Tale fase può essere curata sia dallo stesso indagato che dagli investigatori.

Il processo si sposta, successivamente, nel dominio della "credibilità" che riguarda come le persone accertano e valutano alibi:

- Prima fase di valutazione: è svolta, come detto, nella fase preliminare delle indagini, da chiunque ne abbia necessità (investigatori, parti offese, avvocati);
- Seconda fase: finalizzazione della fase di valutazione: un alibi non sempre arriva a questa fase. Si tratta del caso in cui la valutazione sia stata costruita da chi ne abbia avuto interesse e quindi ora tale analisi è rimessa al dibattimento e alla decisione del Giudice. In questa delicata fase si ricostruirà quanto studiato nelle fasi precedenti e si verificherà la consistenza dell'alibi all'interno di un più ampio contesto investigativo.

Venendo, dunque, al piu' stretto tema del presente lavoro, ovvero la costruzione e/o ricostruzione dell' alibi ed alla sua elaborazione, conferma e verifica mediante strumenti tecnologici ed informatici, deve dirsi come tutto parta dalle scelte difensive a fronte delle contestazioni operate e operabili. Il team difensivo, quindi, individuate le tesi ricostruttive in fatto, dovrà trovare gli elementi di prova a sostegno delle stesse. Dovrà tenersi altresì conto del fatto che potrebbe darsi che l' impossibilità di procurarsi una certa prova (ad esempio la morte di un teste oculare che non ha rilasciato alcuna dichiarazione, la distruzione di un computer, l'irrimediabile perdita di dati) imponga "mutamenti di rotta ed adeguamenti", per cui, in realtà, l'elaborazione dell' alibi non risulterà esser una scelta ricostruttiva definitiva ed originaria, ma dovrà essere costantemente verificata ed adeguata, soprattutto in fase di indagini preliminari, rispetto alle singole emergenze probatorie ed indiziarie.
Indispensabile è peraltro che per detta attività vengano utilizzate piu' tecniche e conoscenze, in maniera coordinata e coerente. A tale proposito deve dirsi ancora una volta che è fondamentale l' interazione fra i diversi soggetti del team difensivo (cliente – avvocato – consulenti) per la individuazione delle strategie e dei temi probatori, tenendo ben presente che la molteplicità delle tracce effettive o anche solo rilevabili, non fa che aumentare l' ambito e le modalità di ricerca e quindi la necessità di una competenza interdisciplinare per i soggetti responsabili di dette attività.

Basti pensare alle possibilità di accedere a dati informatici e telematici e alle opportunità di incrocio, ad esempio di dati informatici, con altri tipi di dati (biologici, biometrici, telefonici etc.).

In questa vasta ed articolata operazione dovrà altresì riflettersi anche sulla necessità di valutare costantemente il grado di attendibilità dei dati ottenuti e la adeguatezza delle metodologie utilizzate, ricordando che l' utilizzo di piu' metodiche contemporaneamente può portare ad un ampliamento e non alla riduzione degli ambiti di errore o di incertezza per cui l'alibi risultante ne potrebbe risultare indebolito piuttosto che rafforzato. Alla luce di queste considerazioni e senza entrare nelle difficili problematiche in merito all'affidabilità delle persone, in particolare per gli aspetti motivazionali che portano un testimone a mentire o più semplicemente a sbagliare o confondersi, in questo scritto ci limiteremo alla trattazione del cosiddetto alibi informatico, ovvero alla discussione delle metodiche e delle elaborazioni delle informazioni digitali e telematiche che possono aiutare l'indagato, gli investigatori ed il giudicante a definire e verificare la prova d'alibi. Lo studio presenterà alcuni case study, frutto dell'esperienza investigativa, e valuterà, infine, la possibilità di falsificazione le fonti di prova digitali in un notebook nel corso di un'

indagine su reato di omicidio. Le definizioni e deduzioni menzionate potranno trovare applicazione anche in quei procedimenti penali, civili ed amministrativi, relativi alle fattispecie riconducibili ai cosiddetti reati informatici per le analogie già diffusamente trattate in altri testi giuridici. Infatti, si ribadisce, che le principali differenze che qualificano i "computer crime", rispetto ai reati comuni, consistono nella peculiarità del bene giuridico tutelato dalla norma e/o del mezzo o del luogo (sistema informatico, rete di comunicazione) ove essi vengono commessi.

Deve in fine ricordarsi che non tutte le persone che ne hanno bisogno (e ciò per i più diversi motivi), però, possono avere le potenzialità creative ed organizzative per la creazione di un alibi "credibile", ed è proprio per questo motivo che in Italia, così come nel resto del mondo, da circa 10 anni sono nate vere e proprie aziende che forniscono servizi di enterprise, anche a costi contenuti, per la creazione di alibi (e non solo per finalità giuridiche!). La tipologia dell'alibi spazia dal convegno in Islanda, che non esiste, con tanto di corrispondenza inviata alla propria abitazione contenente l'invito all'evento, alla simulazione di hotel o aziende che non sono mai esistite.

Nella maggior parte dei casi, questi servizi vengono offerti da agenzie investigative che applicano il background dell'investigatore privato per creare scenari credibili e interattivi, con vere e proprie persone che possono simulare, per un arco temporale ben definito dal contratto, di essere ad esempio la reception dell'hotel "non esisto" di Parigi che risponde al telefono in un perfetto francese e che inoltra la chiamata, effettuata su un numero con prefisso francese, alla camera d'albergo virtuale, rendendo così credibile il tipico scenario della compagna che chiama il proprio compagno in albergo. Al ritorno dal finto viaggio di lavoro il soggetto avrà a disposizione un kit completo che potrà contenere, a seconda del budget, gadget rigorosamente made in france, memoria sd da inserire nella propria macchina fotografica digitale con fotografie della città scattate virtualmente nella data del periodo della trasferta, regali comprati ai magazzini Lafayette da donare alla propria compagna e tutto ciò che possa rendere credibile la bugia raccontata.

Il costo della prestazione fornita parte dai 200 euro ed aumenta a seconda dei rischi che si corrono, della durata temporale della farsa, da quanti scenari e da quante persone si necessita coinvolgere e dal valore dei regali che si vogliono donare al ritorno dalla propria trasferta.

Delineati i contorni della problematica passeremo ora ad esaminare alcuni casi che sono assurti agli onori della cronaca e nei quali l'esistenza di un Alibi ha avuto grande rilevanza ai fini della risoluzione della vicenda.

3. CASI NOTI E NOTEVOLI

Di seguito vengono illustrati alcuni dei più noti casi in cui l'alibi informatico è risultato determinante ai fini della scarcerazione o assoluzione del soggetto posto sotto indagine con l'accusa di aver commesso un delitto. Non sono mancati, tuttavia, casi in cui l'alibi non è stato ritenuto attendibile e quindi l'indiziato è stato ritenuto responsabile, e dunque autore, del delitto contestato.

- IL CASO GERI - Particolare interesse mediatico ha suscitato il caso "Geri". Alessandro Geri, ritenuto "il telefonista" delle Brigate Rosse coinvolte nell'omicidio del Prof. Massimo D'Antona, viene scagionato grazie ad una consulenza tecnica espletata su alcuni file. Tali file, presenti su un floppy disk acquisito dagli investigatori, hanno fornito l'alibi già nella prima fase delle indagini. Nella memoria principale del dischetto i tecnici rinvennero e sottoposero ad esame una ventina di lavori; mentre nella memoria secondaria ne furono rinvenuti soltanto cinque. Il primo file risultava salvato alle 18.03 mentre l' ultimo alle 19.32. La rivendicazione dell'attentato, da parte dei terroristi al Corriere della Sera, risultava essere avvenuta alle 19.04. I magistrati requirenti, in possesso anche di altri elementi di prova utili a ricostruire l'attività svolta dall'indiziato in concomitanza con le fasi dell'agguato, hanno ritenuto attendibile l'alibi informatico sebbene i file *de quibus* recassero la data del 20 maggio 1990 anziché la data del 20 maggio 1999, giorno in cui si erano verificati i gravi fatti di sangue. Da notare che la data del salvataggio dei file coincideva sì con il giorno e l'orario della brutale esecuzione, ma con uno sfasamento di ben nove anni. Tale circostanza è stata comunque oggetto di chiarimenti da parte dell'indiziato il quale ebbe modo di chiarire che aveva retrodatato i file per evitare i noti problemi da Millenium Bug.[9] Il Gip presso il Tribunale ordinario di Roma, su concorde richiesta, inoltrata dai pubblici ministeri impegnati nelle difficili indagini, motivata da "mancanza assoluta di indizi", emise, in data 27 maggio 2000, provvedimento di scarcerazione nei confronti di Geri. La parte motiva del provvedimento di scarcerazione riportava testualmente:"Sussistono alcune non rilevanti incertezze circa data, orari e modalità degli incontri. Inoltre, devono essere accertate mediante consulenza di una certa complessità le operazioni compiute sul disco rigido del computer del Geri, essendo lo stesso stato resettato e non fornendo lo stesso prova affidabile dell' orario e data dei file su floppy."

[9] Conosciuto anche come Y2K *bug*, è il nome che è stato attribuito ad un potenziale difetto informatico *(*bug*)* che avrebbe dovuto manifestarsi al cambio di data dalla mezzanotte del 31 dicembre 1999 al 1º gennaio 2000 nei sistemi di elaborazione dati, sia personal computer che grandi elaboratori *(*mainframe*)* e controllori di processo dedicati embedded.

- IL CASO BRADFORD - Questa vicenda ha assunto grande notorietà, oltre che per il risultato giudiziario favorevole ottenuto, anzitutto perché legato al''uso del social network Facebook.
Rodney Bradford, un diciannovenne newyorkese, veniva arrestato per rapina aggravata commessa il 18 ottobre 2009 a Brooklyn.
L'alibi fornito, sin dalla prima fase delle indagini, ha dimostrato che l'indiziato, al momento della rapina, si trovava nella casa del padre nel quartiere di Harlem.
E' stato sostenuto dalla difesa che la pagina di Facebook dell'indiziato era stata aggiornata alle 11.49, esattamente un minuto prima dell' orario coincidente con l'orario di esecuzione della rapina, con un messaggio alla fidanzata *"On the phone with this fat chick... where my IHOP."* Dall'analisi forense espletata dai tecnici è emerso effettivamente che l'aggiornamento del messaggio era stato fatto attraverso una connessione da un appartamento al 71 West, 118th Street di Manhattan (New York), ovvero la casa del padre, distante oltre 13 miglia dal luogo del reato. Ciò è stato possibile accertarlo anche perché Facebook rende nota la data e l'orario esatto dell'inserimento, da parte dei propri utenti, dei contenuti inseriti sul sito. La Corte, dopo attenta valutazione delle prove offerte e dopo soli 12 giorni scontati nella prigione di Rikers Island, provvide a rilasciare Rodney e ad archiviare la sua posizione. Alle osservazioni mosse alla difesa di Rodney - nel senso che chiunque, amico o parente, al suo posto avrebbe potuto aggiornare il suo profilo dietro disposizioni impartite dallo stesso Rodney - l'avvocato difensore ha risposto che sebbene teoricamente possibile, nel caso di specie tale possibilità andava esclusa in quanto l' attività informatica preparatoria avrebbe connotato un livello di genio criminale inusuale in un ragazzo così giovane.

- IL CASO STASI - Altro caso giudiziario, noto come il caso "Garlasco", estremamente interessante sotto il profilo della valutazione dell'alibi informatico, si è concluso con l'assoluzione di Alberto Stasi, principale indiziato dell' omicidio della propria fidanzata Chiara Poggi. *''Non ho ucciso Chiara. Io era a casa a scrivere la tesi al computer, mentre lei moriva".* Questa la frase ripetuta in più occasioni dall'imputato il quale, sin dall'inizio, ha proclamato la propria innocenza adducendo un alibi informatico. Tale caso giudiziario è caratterizzato da un serrato confronto tra risultati di analisi effettuati su ogni tipo di reperto: dal DNA su tracce ematiche alle *digital evidence* sui PC in uso alla vittima e all'indiziato. A tali accertamenti si sono affiancate anche tecniche tradizionali di ricerca di mezzi di prova consistiti nella raccolta di informazioni e testimonianze rese da soggetti informati sui fatti. Quattro i tipi di accertamenti peritali - una perizia tecnico/informatica, una medico/legale, una chimico/sperimentale e la quarta definita come "semi-virtuale" - ai quali si aggiungono le consulenze tecniche disposte dalle altre parti processuali.

L'attenzione comunque si è focalizzata sull'accertamento dell'alibi digitale fornito da Stasi il quale ha dichiarato, offrendo agli inquirenti il proprio computer portatile affinché venisse analizzato, di essere stato a casa sua, distante circa 2 km dal luogo del delitto, a scrivere sul computer la tesi di laurea proprio nell'orario in cui Chiara sarebbe stata uccisa nonché di aver effettuato alcune telefonate sull'utenza telefonica mobile della fidanzata. Peculiare appare la circostanza che il giudice, pur constatando la presenza di errori commessi dagli esperti nella fase di repertamento ed analisi delle *digital evidence,* giunge comunque ad emettere sentenza di assoluzione così motivando:"Partendo da questo dubbio di fondo e tenuto conto della grave anomalia rappresentata dalle alterazioni del contenuto informativo dovute agli accessi dei carabinieri che ben potevano avere determinato la cancellazione delle normali evidenze presenti all'interno del sistema operativo, il collegio peritale (con la collaborazione dei consulenti tecnici delle parti) ricercava delle particolari informazioni che si trovano fuori del sistema operativo (i c.d. metadati). Questa ricerca dava esito positivo: questi metadati ed il loro contenuto attestano con certezza (e questo è un'evidenza probatoria non contestata dalle parti) l'interazione diretta e sostanzialmente continuativa dell'utente con il computer dalle ore 10.17 fino alle ore 12.20 del giorno 13 agosto". Ciò significa che l'alibi digitale, sebbene minato da errori e sebbene si fosse reso necessario il ricorso all'analisi dei metadati per ricostruirne le parti compromesse, sembra aver fornito al giudice la chiave per "collocare" l'indiziato al lavoro davanti al suo computer portatile in quel lasso di tempo critico correlato all'omicidio della sua fidanzata.

Non in tutti i casi l'alibi informatico risulta determinante ai fini della esclusione di responsabilità dell'indiziato. In molti altri casi, l'analisi digitale ha dimostrato, invece, l'inattendibilità dell'alibi informatico offerto ed i risultati sono stati tutt'altro che favorevoli all'indiziato.
Si pensi al caso "Sollecito", relativo all' omicidio della studentessa inglese Meredith Kercher uccisa a Perugia in data 1 novembre 2007, conclusosi con sentenza di condanna emessa dalla Corte di Assise di Perugia che ha comminato la pena di anni 25 di reclusione a Raffaele Sollecito, imputato del reato di omicidio in concorso con Amanda Knox, condannata a 26 anni di reclusione.
Sollecito, arrestato perché sospettato di essere l'autore materiale del delitto, aveva addotto un alibi sotteso a dimostrare che era al computer a vedere un film sin dalle ore 18,30 della data dell'omicidio e che pertanto non poteva aver partecipato all'azione delittuosa.
I tecnici di computer forensics, escussi nella fase di istruttoria dibattimentale, pur confermando che il filmato era stato realmente visionato all'orario indicato delle 18,30 hanno messo in debita evidenza che l'ultima delle attività svolte sul notebook in data 1 novembre 2007 si era manifestata alle ore 21,10 e che il

portatile era rimasto inattivo fino alle 05,32 del 2 novembre 2007.
In effetti hanno sostenuto che non era stata riscontrata "alcuna traccia di interazione umana" sul computer di Sollecito nell'arco temporale, compreso tra le 21,10 e le 05,32 della mattina successiva, coincidente con l'arco temporale in cui risulta essere stata barbaramente accoltellata la studentessa inglese nel suo appartamento di Perugia.
In tale caso la inattività del PC, ovvero la mancata interazione tra l'utente ed il PC, ha dato al giudice la possibilità di ritenere inattendibile l'alibi informatico addotto dalla difesa dell'indagato e di ritenere la sua presenza sul luogo dell'omicidio perfettamente compatibile con altre risultanze d'indagini.

Altra situazione, analoga alla precedente, è rappresentata dal caso "Douglas Plude". Quest'ultimo, cittadino americano accusato dell'omicidio della propria moglie Genell, trovata morta per soffocamento nel bagno di casa, ha offerto alla Corte un alibi informatico non prima di aver mosso pesanti critiche nei confronti dell'autorità giudiziaria americana che non aveva provveduto a mettere, sin dalla prima fase delle indagini, a disposizione dei propri consulenti tecnici i computer da analizzare.
Egli ha comunque sostenuto che era estraneo ai fatti contestati e che la moglie si era suicidata ingerendo eccessive dosi del farmaco Fioricet.[10]
L'analisi forense appurava che nella tarda serata del 21 ottobre 1999, poco prima della morte di Genell, entrambi i computer erano attivi. Il notebook di Genell dimostrava che alle ore 22,00 l'utente aveva condotto ricerche online per informazioni sul Fioricet; il notebook di Plude dimostrava attività in Internet e l' utilizzo di un programma di fotoritocco dalle ore 22,00 alle 22,30.
L'alibi fornito tendeva a dimostrare che la moglie, la sera stessa del decesso, aveva navigato sul suo notebook ed aveva aperto la pagina web dedicata a tale farmaco per verificare gli effetti mortali che derivavano dall'assunzione di dosi massicce e quindi col chiaro intendo di suicidarsi. Tutto ciò avveniva nello stesso momento in cui l'indiziato era impegnato ad editare foto sul proprio portatile. Ebbene il giudice non ha ritenuto degno di credibilità l'alibi argomentando: che risultava visionata la sola pagina relativa al farmaco e non erano state consultate le parti di essa che trattavano del dosaggio; che, tutto sommato, lo stesso indiziato avrebbe potuto usare entrambi i computer, visto che erano portatili e facilmente collocabili in prossimità dell'operatore.
In definitiva la Corte, nell'emettere sentenza di condanna per il reato di omicidio premeditato, ha ritenuto che artatamente Plude aveva effettuato l'accesso alla pagina web attribuendo, così, scarso valore al risultato dell'analisi forense che aveva riscontrato tracce di attività sul notebook di proprietà della consorte Genell. In tale caso le tracce informatiche sono state comparate con elementi di

[10] Farmaco utilizzato per i forti mal di testa e forti contratture muscolari. Preso in dosi elevate risulta velenoso.

indagini acquisiti in maniera tradizionale, ed hanno prodotto un ottimo risultato. Infatti, da indagini condotte parallelamente, era emerso che l'indiziato, la mattina precedente la morte della moglie, aveva contattato i colleghi di ufficio per sapere se era ancora attiva l'assicurazione sulla vita della moglie.
I casi citati, oltre che interessanti sotto il profilo giudiziario, fanno riflettere circa la reale attendibilità dei dati digitali oggetto di analisi forense e soprattutto sul loro significato probatorio, e ciò sia nel caso in cui vengano acquisiti dagli inquirenti, sia nel caso in cui vengano offerti dall' indiziato.
Non sempre, infatti, è possibile sapere chi fosse realmente e con certezza dietro la tastiera.

4. METODI D'ANALISI

Come detto al pari della prova di colpevolezza, l'alibi rappresenta uno degli argomenti più interessanti di un procedimento giudiziario. In presenza di un alibi si ribaltano le condotte dell'organo inquirente e dell'imputato: il primo deve dimostrare l'infondatezza della prova portata a discredito della tesi dell'accusa, mentre il secondo deve tentare in ogni modo di rafforzarne l'attendibilità.
Cerchiamo di capire come si possa dimostrare la solidità, od eventualmente l'inconsistenza, di un alibi, nella fattispecie, informatico. In questo paragrafo si vuole suggerire un metodo generale, per effettuare detta verifica, che consiste nell'applicare il seguente schema di 8 domande:

- cinque riguardano l'**oggetto:** «Chi», «Cosa», «Quando», «Dove», «Perché»[11]
- tre riguardano il **soggetto agente**: «Quanto», «In che modo», «Con quali mezzi»[12]

Proviamo ad analizzarle singolarmente per capirne l'utilità.
CHI (*QUIS*)

L'alibi informatico diventa, sicuramente, inattaccabile se si riesce a dimostrare scientificamente la sua paternità, viceversa se l'evidenza non riporta alcuna informazione riferibile, direttamente o indirettamente, all'imputato, rischia di diventare solo un indizio.

Per esempio produrre documentazione informatica che rivela informazioni strettamente legate alla persona (transazioni autorizzate con dati biometrici, documenti firmati digitalmente, immagini che ritraggono l'imputato, email e transazioni autorizzate da pin o password) hanno un peso specifico maggiore, rispetto a un documento anonimo o ad un log che non rileva alcun dato personale.

[11] Conosciuta nel mondo anglosassone come la regole delle 5 W (Who, What, When, Where, Why)
[12] Creato da San Tommaso D'Aquino nella sua opera più famosa, la *Summa Theologiae*, in cui, alla fine del XII secolo, il teologo individuò gli elementi fondamentali che identificano la struttura dell'azione morale

COSA (*QUID*)

La prima difficoltà che l'investigatore informatico deve affrontare è proprio l'individuazione delle tracce che possono costituire elementi di prova digitale. La singola evidenza digitale, spesso, non è sufficiente a rappresentare una prova o un alibi. Vi sono casi in cui è necessario acquisire altri elementi, anche esterni alla scena del crimine, che possono avvalorare o screditare la stessa.

Per esempio una email diventa robusta se può essere avvalorata dai log dei server su cui è transitata, oppure dal traffico di rete generato.

QUANDO (*QUANDO*)

Il tempo è, al pari del luogo, una caratteristica fondamentale per valutare l'ammissibilità di una prova. Pertanto, riuscire a dimostrare che l'ora della formazione della prova è certa ed inattaccabile, consente di confrontare, in un intervallo temporale, la simultaneità dei tempi in cui si è consumato il reato oggetto del procedimento. (Data di creazione, modifica e ultimo accesso, Log file, Temporary file).

Per esempio sarebbe utile verificare la data di sistema, i parametri di sincronizzazione, se presenti, i log di sistema per risalire ad eventuali modifche.

DOVE (*UBI*)

Anche il luogo è una proprietà fondamentale di una prova. Riuscire a dimostrare dove è stata formata una prova informatica potrebbe diventare un elemento rilevante se ad esso possa essere associata la presenza dell'imputato.

Spesso queste tracce vengono rappresentate da ulteriori dati informatici e, come tali, possono essere creati o modificati con facilità. Per esempio, per simulare la propria posizione in un determinato posto, in un determinato giorno, è sufficiente lasciare tracce informatiche (come quelle del telefonino, del telepass, della carta di credito o del navigatore satellitare) che non richiedono la presenza contemporanea del soggetto indagato.

PERCHÉ (*CUR*)

Rappresenta il movente del reato. L'alibi può solo dimostrare che il movente non sia vero attraverso il significato di ciò che rappresenta.

QUANTO (*QUANTUM*)

Al tecnico può essere richiesta la quantificazione del danno, o di facilitarne il calcolo, attraverso l'analisi dei dati e delle informazioni rinvenute. Il peso della prova può diventare elemento di giudizio a favore o contro l'imputato.

IN CHE MODO (*QUOMODO*)

La prova informatica è sicuramente un prodotto di strumenti tecnologici (Software, Computer, Palmari, Rete Dati, Apparati Elettronici). Dimostrare come è stata formata, riportando anche ulteriori prove a conferma della

propria validità (Log file, Temporary file, Backup), può incrementare o abbassare il grado di attendibilità della stessa.

CON QUALI MEZZI (*QUIBUS AUXILIIS*)

In maniera speculare al modo, è utile scoprire con quali mezzi si è formata una evidenza informatica. L'identificazione e l'analisi delle caratteristiche tecniche dello strumento utilizzato possono avvalorare o indebolire la credibilità della prova.

Difficilmente il consulente tecnico riuscirà a fornire una risposta a tutte le domande suggerite, ma tentare aiuta a rappresentare una evidenza digitale in maniera completa e consente, all'organo giudicante, di potersi determinare più facilmente circa l'eventuale ammissibilità o meno della stessa.

5. ANALISI E CLASSIFICAZIONE

Per agevolare l'analisi tecnica di un alibi informatico è utile ribadire che è, in tutto e per tutto, equivalente ad una traccia informatica (digital evidence) e, di conseguenza, ad esso possono essere ascritte le stesse peculiarità e lo stesso modus operandi, relativamente all'acquisizione, al trattamento, all'analisi ed alla conservazione, tipici della prova digitale. Dalla definizione, citata nei paragrafi precedenti, è possibile evidenziare tre qualità che qualificano la prova: la paternità, il momento ed il luogo. Focalizzando l'attenzione su queste tre caratteristiche proviamo a delineare alcune fattispecie di alibi che ci consentiranno di compiere l'analisi e la verifica di ammissibilità in un procedimento giudiziario. Se valutiamo la variabile tempo, possiamo distinguere due classi di alibi:

1. quelli generati durante, o contemporaneamente, l'evento criminoso,
2. quelli creati in un momento diverso, antecedente o seguente, dell'atto delittuoso.

Nella prima classificazione rientrano le tracce informatiche prodotte nello stesso istante in cui si consuma il reato. In questa categoria possiamo distinguere quattro fattispecie:

a. l'imputato ha generato direttamente tracce informatiche su dispositivi distanti dalla scena del crimine;
b. un sistema informatizzato ha eseguito "automaticamente" azioni ed eventi pianificati che, producendo tracce informatiche, simulano la presenza e l'interazione dell'imputato in un luogo diverso dalla scena del crimine;
c. un terzo, persona fisica o sistema automatico, ha registrato tracce che potrebbero giustificare la presenza dell'imputato in luoghi diversi dalla scena del crimine;
d. un terzo, un complice, ha eseguito azioni, per nome e per conto dell'imputato,

che producono tracce informatiche su dispositivi distanti dalla scena del crimine.

Nella seconda classificazione rientrano quelle tracce informatiche, evidentemente false, che vengono prodotte in momenti diversi, precedenti o successivi, da quello dell'evento criminoso. In questa categoria possiamo distinguere altre due fattispecie in aggiunta alle precedenti:

e. l'imputato (o chi per lui) realizza una prova ex novo, facendo attenzione che gli elementi caratterizzanti il tempo rivelino la contemporaneità con l'azione criminale.
f. l'imputato (o chi per lui) riutilizza una traccia informatica già esistente, alterando gli elementi utili a dimostrare la correlazione temporale tra il momento della produzione e l'evento criminoso.

Analizziamo più nel dettaglio le varie ipotesi per cogliere gli elementi tecnici che ci possano aiutare a valutare la veridicità, o meno, dell'alibi informatico.

Ipotesi A - L'imputato ha generato direttamente tracce informatiche a distanza.

E' nota la facilità con cui sia possibile utilizzare dispositivi o elaboratori elettronici attraverso l'uso di tecnologie di controllo a distanza. Ricorrendo, infatti, all'utilizzo di programmi di accesso remoto, quali ad esempio ssh, vnc e remote desktop, risulta possibile interagire a distanza ed effettuare operazioni che registrano l'attività sul sistema remoto oppure eseguire programmi che generano azioni di simulazioni d'uso della postazione.

In questa fattispecie il focus dell'indagine consiste nel rilevare la presenza e l'utilizzo di eventuali dispositivi di controllo remoto, quindi tecnologie, software o hardware, che consentono l'interazione a distanza direttamente su un dispositivo remoto tanto da far ritenere che dette attività fossero state svolte personalmente dall'utente.

Esistono due categorie di dispositivi di controllo remoto:

1. hardware, che si collegano esternamente al dispositivo e non interferiscono con l' apparecchiatura controllata. p.e. le KVM over IP;[13]
2. software, che si installano e si configurano sul dispositivo da controllare.

Nel primo caso le verifiche che il tecnico potrà effettuare per rilevare eventuali falsi alibi sono le seguenti:

a. rilevare la presenza di tali apparecchiature;
b. analizzare la configurazione di eventuali router o firewall che permettono l'accesso da remoto;
c. analizzare i tabulati ed i log di connessione del fornitore di connessione;

[13] Console, che attraverso un collegamento telefonico o tcp/ip, consentono il controllo a distanza della tastiera, del video e del mouse di un sistema informatico.

d. analizzare gli indirizzi di destinazione con quelli dei dispositivi presenti;
e. confrontare eventuali log di connessioni presenti sul dispositivo;
f. incrociare le suddette informazioni con i dati estrapolati dall'evidenza.

Nel secondo caso il tecnico potrà acquisire ulteriori informazioni:

a. rilevare la presenza di tali software, la loro installazione e/o disinstallazione;
b. cercare ed analizzare tracce utili a svelarne l'esecuzione (p.e. file prefetch, chiavi di registro, file di configurazione);
c. cercare ed analizzare eventuali log degli stessi software rilevati;
d. analizzare la configurazione di eventuali router o firewall che permettono l'accesso da remoto;
e. analizzare i tabulati ed i log di connessione del fornitore di connessione;
f. analizzare gli indirizzi di destinazione con quelli dei dispositivi presenti;
g. confrontare tutti i suddetti log e lo storico delle connessioni presenti sul dispositivo;
h. incrociare le suddette informazioni con i dati estrapolati dall'evidenza.

E' da notare come nel primo dei casi illustrati, se non si trova il dispositivo collegato al computer, risulta difficile dimostrare la falsità dell'alibi. Lo stesso può affermarsi in relazione al secondo dei casi, se ci si trova in presenza di software portatili[14].

Ipotesi B – Un sistema automatizzato ha simulato un utilizzo in presenza.

Esistono molteplici soluzioni, commerciali o gratuite, che consentono la simulazione dell'utilizzo di determinate apparecchiature. La maggior parte sono nate per coadiuvare la didattica a distanza attraverso la rappresentazione di simulazioni o esercitazioni interattive.

Per esempio è possibile programmare in modo semplice alcune applicazioni, come Word o Excel, ad effettuare automaticamente operazioni, come il trasferimento di caratteri da un file ad un altro, decidendo il tempo e la velocità; oppure vi sono in commercio programmi che permettono di simulare l'utilizzo di tastiera e mouse (i c.d. auto-typer e auto-clicker) a partire da file predefiniti; ovvero programmi che registrano intere sessioni di utilizzo di personal computer e riescono a replicarle in momenti preferiti.

Per simulare l'utilizzo di un personal computer vi sono varie soluzioni,

[14] Un' applicazione portabile è generalmente costituita da uno o più eseguibili binari a cui possono essere associati altri file e cartelle necessarie al funzionamento del software. Quando il software è costituito soltanto dall'eseguibile principale si parla più propriamente di programma Stand-alone.Per applicazione portabile si intende un software che non necessita di installazione all'interno del sistema operativo su cui viene eseguito. Programmi di questo genere possono essere memorizzati su supporti rimovibili come Cd-rom, memorie flash o Floppy disk.
Un' applicazione portabile può indistintamente essere eseguita su qualsiasi computer in cui si dispone di un sistema operativo compatibile con l'applicazione stessa. Il vantaggio per l'utente è quindi quello di poter utilizzare la medesima applicazione su macchine diverse mantenendo le impostazioni personalizzate nell'uso dell'applicazione. Un secondo vantaggio delle applicazioni portabili deriva dal fatto che non richiedendo installazione possono spesso essere eseguite anche in ambienti in cui non si dispone dei diritti di amministrazione sul sistema operativo.

proviamo a elencarne alcune:

1. Script. Alcuni programmi quali Word, Excel, ecc., consentono di realizzare mini programmi, che sfruttano le funzioni offerte dagli stessi software, per automatizzare alcune operazioni di routine. La stessa tecnologia potrebbe essere utilizzata per riprodurre una intera sessione di utilizzo del programma stesso.
2. Macro Recorder. Sono programmi che registrano su un file, in modo automatico ed indipendente, una sessione di lavoro, comprese le digitazioni e l'utilizzo del mouse e riescono a riprodurla automaticamente con l'indicazione del momento di startup.
3. Auto Typer e Auto Clicker. Sono programmi che riproducono automaticamente la digitazione di tasti e l'utilizzo del mouse a partire da file che contengono sequenze di caratteri e comandi predefiniti.

In questa fattispecie il focus dell'indagine consiste nel rilevare la presenza e l'utilizzo di eventuali file di comandi e/o programmi di riproduzione come quelli sopraelencati.

Per cui si può tentare di trovare:

α. software che rientrano nelle categorie suddette;
β. operazioni pianificate nell'intervallo di tempo in cui è stato commesso il reato;
χ. l'elenco dei file aperti nell'intervallo di tempo da esaminare;
δ. connessioni di periferiche esterne;
ε. connessioni da e verso l'esterno;
φ. file temporanei e cancellati.

E' da evidenziare come l'analisi forense potrebbe risultare particolarmente difficile in quanto alcuni di questi software sono portabili. Essi, infatti, non si installano, non lasciano tracce nel file di registro e non si appoggiano a librerie esterne. Le uniche tracce potrebbero essere rinvenute tra le operazioni pianificate, nella cartella dei file di prefetch, nell'elenco degli ultimi file aperti e nella cartella dei file temporanei di internet.

Ipotesi C – Un terzo, persona fisica o sistema automatizzato, ha registrato tracce informatiche.

In questa fattispecie si fa riferimento alle tracce informatiche che, in maniera diretta o indiretta, potrebbero costituire una prova della presenza fisica di una determinata persona, indicando nel contempo il luogo ed il momento dell'evento.

Alcuni esempi:

- i sistemi di video sorveglianza;
- gli accessi controllati;

- i tabulati telefonici;
- le tracce di spostamento del telefonino;
- il telepass;
- gli sportelli bancomat ed i pos;
- i rilevatori ed i navigatori gps;
- l'applicazione google latitude; ecc.

In questi casi il tecnico può solo verificare l'attendibilità dell'evidenza, accertandosi che il sistema di rilevazione non abbia evidenziato falle tecnologiche tali da rendere non ammissibile giuridicamente la prova informatica.
Si evidenzia che mentre alcune di queste tracce possono essere considerate prove a tutti gli effetti, come un'impronta digitale od una traccia di dna, in quanto possono dimostrare scientificamente l'associazione indissolubile con l'individuo, al contrario una foto digitale, una ripresa video, una lettura biometrica, e altre, seppur riconducibili ad una determinata persona, non sono strettamente legate ad essa, in quanto le caratteristiche tecniche dei sistemi coinvolti possono solo svelare che un dispositivo, pur sempre di proprietà dell'imputato, è stato utilizzato in un determinato contesto, ma non da chi. Di conseguenza sminuiscono il valore della prova stessa.

Ipotesi D – Un complice ha eseguito azioni per conto dell'indiziato.

Un complice, che finge di essere l'indiziato, può utilizzare apparecchiature e dispositivi elettronici per mettere insieme informazioni, anche personali, tali da giustificare la presenza e l'attività di una persona in un determinato luogo e periodo.
Alcuni esempi: consegnare il cellulare a qualcuno chiedendogli di spostarsi e di utilizzarlo, oppure prestare la propria vettura, dotata di antifurto satellitare e telepass, invitandolo a dirigersi in un luogo distante, oppure fornire le proprie credenziali di accesso e il proprio notebook raccomandandosi di adoperarlo.
Appare evidente che ci si trovi di fronte a vere prove informatiche, e di conseguenza per il consulente tecnico sarà difficile, se non impossibile, dimostrare che siano false. In tale situazione il tecnico può, e deve, porre in debito risalto che chiunque, e quindi non solo l'indiziato, in possesso della medesima tecnologia, avrebbe potuto generare le stesse tracce informatiche. In questo caso sarà cura degli investigatori rinvenire ulteriori informazioni che dimostrino il falso.

Ipotesi E - L'indiziato (o chi per lui) realizza una prova ex novo.

In questo caso si ipotizza che sia stata prodotta una traccia o una prova informatica in un momento diverso rispetto a quando si è consumato il reato e

che, attraverso l'utilizzo di tool o comandi del S.O., è stato possibile modificare gli attributi temporali del sistema per farli coincidere con il momento del reato. Quasi tutti i dispositivi elettronici consentono di reimpostare la data e l'ora. In questo modo, ed utilizzando semplici tecniche di anti-forensics, è possibile utilizzare dette apparecchiature e costruire prove in tempi desiderati.
Il consulente tecnico, in questi casi, deve dapprima estrapolare ed incrociare la time-line di funzionamento della macchina con i metadati dei file e con le altre informazioni temporali presenti sul File System, includendo nell'analisi anche i file temporanei ed i file cancellati (p.e. è impossibile che una modifica di un documento di word non crei alla stessa data/ora altri file secondari) ed in seguito verificare, nell'arco temporale di riferimento, che ci siano altre tracce, quali connessioni ad internet, altri programmi o file aperti, ecc.
Vale la pena osservare che solitamente questa ipotesi è la più semplice da verificare e smascherare in quanto le informazioni sono molteplici e difficilmente armonizzabili.

Ipotesi F - L'indiziato (o chi per lui) riutilizza una traccia informatica già esistente.

In questo caso si ipotizza che siano state utilizzate prove già esistenti, i cui riferimenti temporali sono stati modificati per dimostrare la contemporaneità con l'evento criminoso. Anche in questo caso è possibile, utilizzando tools commerciali o freeware, oppure semplici comandi del S.O., modificare le date presenti sul file system o nei metadati dei file per farli coincidere con quelli desiderati. Le tecniche di analisi sono simili a quelle dell'ipotesi precedente.

6. TIME LINE

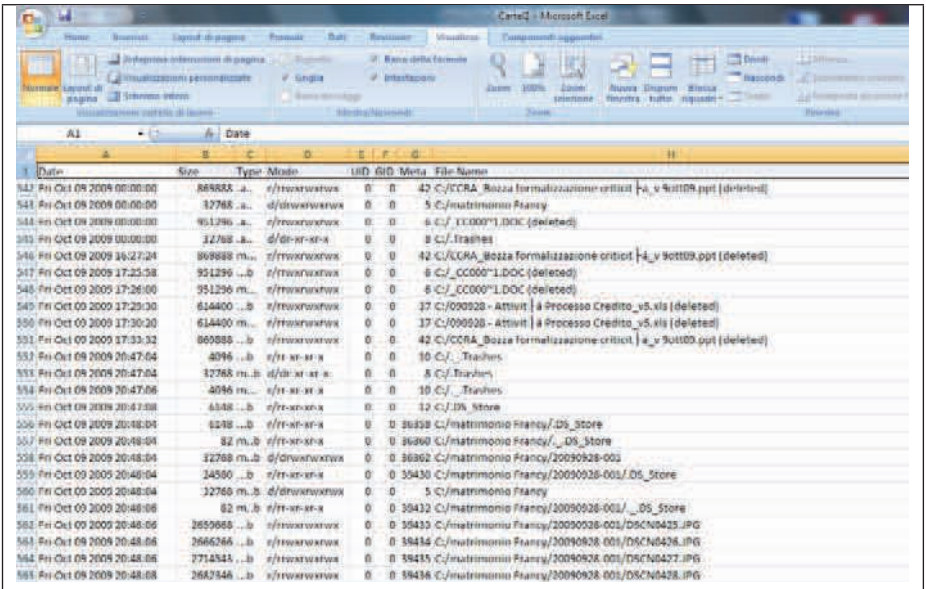
Nell'informatica forense per time line si intende una fotografia di tutti gli eventi di creazione, ultimo accesso ed ultima modifica a file o directory contenuti all'interno di una memoria informatica di un determinato sistema. La time line viene creata mettendo in ordine cronologico tutti gli eventi successi in un determinato tempo di vita delle memorie del sistema posto ad analisi. Possiamo quindi affermare che, metaforicamente parlando, una time line ci permette di viaggiare nel tempo potendo così risalire ad ogni singola azione avvenuta in un arco di tempo definito dall'analista creatore della time line. C'è però da precisare che una time line viene creata a seconda della data del sistema, pertanto se, ad esempio, il proprietario del pc che stiamo analizzando non si è mai posto il problema di impostare correttamente i riferimenti temporali

del sistema operativo mediante protocollo NTP[15] o impostazione manuale, i riferimenti temporali potrebbero essere completamente inattendibili. Pertanto, prima di dare per attendibile una time line bisognerebbe assicurarsi che il sistema, sin dalla sua prima accensione, abbia sempre avuto i riferimenti temporali corretti. Tali accertamenti devono essere eseguiti o al momento del sequestro del materiale informatico o come accertamento da eseguire prima di qualsiasi altra attività di analisi.

Creazione di una timeline

Uno degli strumenti più noti per la creazione di time line è mac-time, tool della suite di utility Sleuthkit realizzata da Brian Carrier[16] presente in tutti i live cd Linux per la Computer Forensics. Mac-time prende in input un listato completo dei dati contenuti all'interno del file system posto ad analisi creato mediante l'utility fls. Fls, prende come input o un file raw di acquisizione di memoria di massa o direttamente il device della memoria, e restituisce come output il listato dei file, allocati e non, da utilizzare successivamente con mac-time.
Di seguito viene riportato un esempio di utilizzo sia di fls che di mac-time.
fls -z GMT -s 0 -m 'c:' -f ntfs -r /caso1/image-1.dd > /caso1/list-image1 dove con -z si specifica il time zone, -s il disallineamento in secondi dell'ora di sistema con l'ora reale, -m l'inizio di ogni path di ogni percorso di file e directory, -f il file system della memoria acquisita, /caso1/image-1.dd è l'immagine che viene data come input e /caso1/list-image1 il file restituito come output.
mactime -b /caso1/list-image -z gmt -d > /caso1/timeline.csv dove con -b si specifica il file da dare in input, -z il time zone, -d > /caso1/timeline.csv è l'output della time line in formato csv; l'export in formato csv è consigliato per una facile consultazione mediante applicativi come OpenOffice e Excel.

[15] Network Time Protocol (NTP) è un protocollo client-server utilizzato per la sincronizzazione dell' orologio di sistema all'interno di una rete a commutazione di pacchetto
[16] http://www.sleuthkit.org



Export della timeline in formato csv aperto con Microsoft Excel 2007

Di seguito viene riportata una tabella per interpretare il significato dei valori che appaiono nella colonna "Type" e che indicano le azione compiute su file e directory in un determinato acro temporale.

Legenda

File System	M	A	C	B
Ext2/3	Modificato	Acceduto	Creato	n/a
FAT	Scritto	Acceduto	n/a	Creato
NTFS	Modificato	Acceduto	MFT[1] modificato	Creato
UFS	Modificato	Acceduto	Creato	n/a

7. L'ALIBI PERFETTO

Il sogno di ogni criminale: l'alibi perfetto. Si trovano esempi di ogni genere sia nelle pagine di cronaca, che nelle trame di parecchi legal thriller[17]. E' facile immaginare come, attraverso l'uso delle tecnologie informatiche e telematiche, sia possibile costruire prove che combinano alcune, se non tutte, delle suddette proprietà. Tale facilità è strettamente correlata alle proprietà intrinseche delle

[17] Film: Un alibi perfetto (2009) di Peter Hyams con Michael Douglas

tecnologie informatiche, quali:

- IMMATERIALITÀ. Un'informazione digitale è immateriale e, di conseguenza, non contiene elementi fisici che possano caratterizzarla come il DNA, le impronte o altre tracce. Un file copiato è identico all'originale
- ANONIMATO. La maggior parte delle transazioni in rete avviene in forma anonima o, peggio, attraverso l'utilizzo di false credenziali.
- VIRTUALIZZAZIONE. E' tecnicamente possibile realizzare o modificare prove informatiche che riportano date e luoghi opportuni.
- MEDIAZIONE TECNOLOGICA. Tutte le azioni informatiche e telematiche si realizzano con l'uso di tecnologie informatiche, per cui lo strumento diventa spesso il mezzo di formazione e di conservazione della prova. Ciò può dar luogo a situazioni di auto formazione, ovvero prove che si creano automaticamente o in modo indipendente.

Proviamo a fare alcune simulazioni in laboratorio utilizzando strumenti semplici, ovvero che non richiedono conoscenze informatiche avanzate, e facilmente reperibili in rete.

Primo caso: Connessione remota tramite KVM over IP.

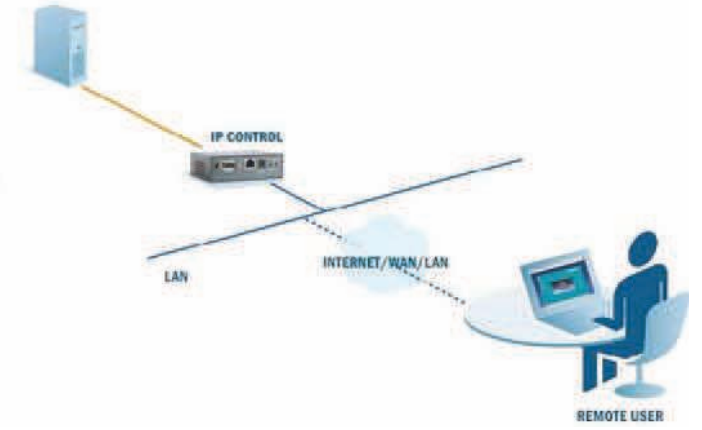
Creazione alibi:

1. Ci procuriamo una console KVM over IP;

2. Assegniamo un indirizzo IP statico alla console per evitare che il DHCP server registri il mac address della stessa;
3. Abilitiamo, sul router, il port per la connessione in entrata e la regola di inoltro specifica per la console;
4. Configuriamo il servizio DNS dinamico[18] (presente su tutti i router commerciali);

[18] Il DNS Dinamico è una tecnologia che permette ad un nome DNS in Internet di essere sempre associato all'indirizzo IP di uno stesso host, anche se l'indirizzo cambia nel tempo.

5. Colleghiamo la console al router;
6. Scolleghiamo la tastiera, il mouse ed il video da pc e connettiamo la console KVM;
7. Accendiamo il personal computer;
8. Ci connettiamo, da un luogo a distanza, attraverso un browser web, utilizzando il nome mnemonico registrato, da un'altra postazione (o con un dispositivo mobile) ed utilizziamo alcune applicazione presenti sul personal computer;



9. Ritornati a casa, spegniamo il pc, scolleghiamo e occultiamo la console KVM;
10. Resettiamo il router ripristinando le impostazioni di default.

Analisi:
Personal computer.

1. L'analisi del file di registro e del file system confermano l'utilizzo delle applicazioni e la creazione delle digital evidence che sono state esibite dall'imputato;
2. La time-line di accensione conferma gli orari di creazione e modifica dei file;
3. Viene rilevato del traffico di rete;
4. Il firewall è abilitato con tutti i port chiusi;
5. Non è presente alcun software di gestione remota.

Router.

1. E' impostato con i parametri di default;
2. Il firewall è abilitato;
3. Dai file di log si rileva che è stato riavviato in un momento successivo alla data e ora dell'alibi;

4. Non vi sono tracce di collegamenti antecedenti alla data ed ora del riavvio.

Tabulati del traffico dati.

1. Si rileva traffico entrante[19], per gran parte, coincidente con quello presente sul pc;
2. Si rileva traffico uscente, proveniente da indirizzo IP afferenti ad alcuni internet service provider, non riscontrabile sul pc.

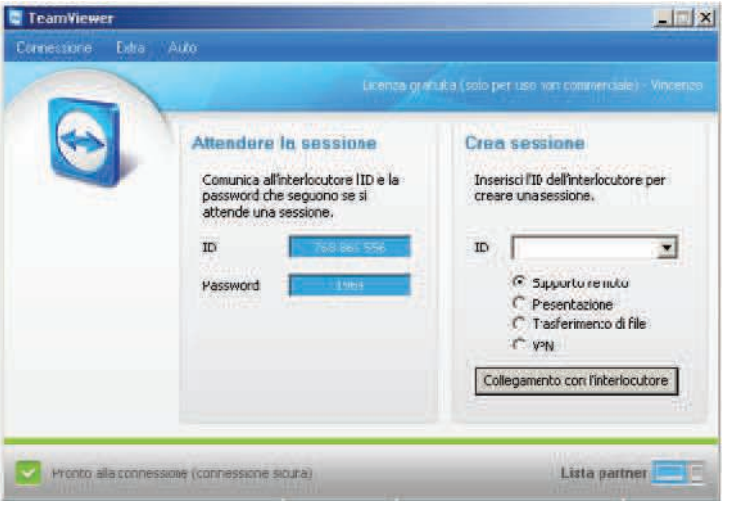
Soluzione:

In presenza di queste evidenze non si potrà affermare che l'alibi sia falso.

Secondo caso: Connessione remota tramite Software.

Creazione alibi:

1. Ci procuriamo un programma per il controllo remoto del tipo "portable", ovvero di quelli che non occorre installare e non inseriscono chiavi nel file di registro,ad esempio TeamViewer Portable (http://www.teamviewer.com), e lo salviamo su un USB drive;
2. Eseguiamo il programma, da USB drive, e ci fornirà i codici di accesso personali;



3. Ci colleghiamo a distanza, da un'altra postazione (o con un dispositivo mobile), utilizzando lo stesso software e servendoci dei codici di accesso personali, ed utilizziamo alcune applicazione presenti sul personal computer;
4. Ritornati a casa, spegniamo il pc, azzeriamo[20] e scolleghiamo la USB drive.

[19] I tabulati vengono richiesti e forniti dall'ISP (Internet Service Provider) presso cui l'utente si collega. La direzionalità del traffico, di conseguenza, è relativa al POP (Point of Presence) del provider nei confronti dell'utente.

[20] Wiping. Tecnica per la distruzione dei dati che prevede la sovrascrittura dei file eseguita più volte rendendo i file irrecuperabili

Analisi:
Personal computer.

1. L'analisi del file di registro e del file system confermano l'utilizzo delle applicazioni e la creazione delle digital evidence che sono state esibite dall'imputato;
2. La time-line di accensione conferma gli orari di creazione e modifica dei file;
3. Viene rilevato del traffico di rete;
4. Il firewall è abilitato con tutte le porte chiuse;
5. Non è presente alcun software di gestione remota;
6. Si analizza la chiave di registro "[MUICache]"[21] e si rileva la voce "X:\\ TeamViewerPortable\\TeamViewer.exe"="TeamViewer" a testimonianza che questa applicazione è stata eseguita almeno una volta all'interno di questo S.O. da una unità esterna; si controlla la cartella di sistema "prefetch"[22] e si rintraccia il file TEAMVIEWER.EXE-12345678.pf. Il risultato dell'analisi di quest'ultimo rileva che l'ultima esecuzione risale a qualche momento prima dell'ora dell'alibi.

USB drive.

1. Viene analizzata l'unità rinvenuta ed si evidenzia che è stata sottoposta ad una cancellazione sicura;
2. Sul PC è presente un programma di Wiping.

Router.

1. E' impostato con i parametri di default;
2. Il firewall è abilitato;
3. Dai file di log si rileva che è stato avviato in una data e ora precedente a quella dell'alibi e che vi sia stato del traffico entrante ed uscente.

Tabulati del traffico dati.

1. Si rileva traffico entrante[23], per gran parte, coincidente con quello presente sul pc;
2. Si rileva traffico uscente, proveniente da indirizzo ip afferenti ad alcuni internet service provider, non riscontrabile sul pc.

[21] Si trova nel file di registro e contiene il percorso dei programmi che sono stati eseguiti sul sistema in osservazione ed il corrispondente nome registrato tra le proprietà degli stessi.
Utilizzato il programma MUICacheView: http://www.nirsoft.net/utils/muicache_view.html

[22] Ogni volta che un'applicazione viene caricata in memoria il S.O. Windows crea o aggiorna un file di prefetch (.pf) contenete tutte le indicazione dei file che vengono richiamati, il numero di volte e la data e l'ora dell'ultima in cui è stata eseguita.
Utilizzato il programma Winprefectview (http http://www.nirsoft.net/utils/win_prefetch_view.html

[23] I tabulati vengono richiesti e forniti dall'ISP (Internet Service Provider) presso cui l'utente si collega. La direzionalità del traffico, di conseguenza, è relativa al POP (Point of Presence) del provider nei confronti dell'utente.

Soluzione:
In questo caso l'investigatore ha elementi sufficienti per dimostrare che vi sia stata una connessione remota e provare ad intaccare la veridicità dell'alibi, ma è anche possibile, con semplici tecniche di anti-forensics (p.e. utilizzando un programma come CCLEANER[24]), eliminare definitivamente anche queste tracce e rendere l'alibi inattaccabile.

Terzo caso: Simulare, attraverso automatismi, l'utilizzo di un computer.

Esistono molti linguaggi di scripting per ogni tipo di sistema operativo. Dal conosciutissimo linguaggio Bash Script presente nativamente nelle più note distribuzioni Linux/Unix, al VBscript nativo dei sistemi operativi della famiglia Microsoft Windows. Questi linguaggi vengono spesso utilizzati per l'esecuzione di operazioni schedulate senza l'ausilio di un operatore. Un esempio molto banale è rappresentato dall'uso di uno script che utilizza il programma ntpdate[25] eseguendolo ogni 30 minuti per il corretto allineamento dell'ora del server con l'ora reale. Oltre ai linguaggi sopra citati, esistono anche altre soluzioni, commerciali e freeware, che permettono di eseguire automatismi sempre più completi utilizzando qualsiasi componente software del nostro sistema operativo. Per la creazione dell'alibi utilizzeremo l'applicativo gratuito AutoIt[26] avente un linguaggio di scripting molto potente per sistemi operativi Windows e che interagisce con qualsiasi finestra del nostro sistema permettendo di modificare anche chiavi del registro di Windows.
Creazione alibi – scrittura di un documento word e navigazione di siti Internet in contemporanea:

```
send ("#m")
MouseClick("leA",630,250,2)
WinWaitAcIve("tesi","")
MouseClick("leA",255,120,2)
WinWaitAcIve("Doc")
send ("Testo che voglio scrivere")
send ("{Enter}")
send ("{Enter}")
send ("{Enter}")
sleep (5000)
send ("Altro testo che voglio scrivere")
run ("C:\Program Files\Mozilla Firefox\firefox.exe")
```

[24] http://www.piriform.com/ccleaner
[25] Utiliti per i sistemi operativi Linux/Unix utilizzata per la sincronizzazione dell'ora di sistema con un time server.
[26] http://www.autoitscript.com

```
send ("^t")
send ("www.google.it")
send ("{ENTER}")
send ("Notizie per la mia tesi")
send ("{ENTER}")
```

Il codice sopra riportato:

1. apre la directory tesi presente nelle coordinate del desktop 630,250,2;
2. clicca sul document Doc presente nelle coordinate della finestra 255,120,2;
3. Inizia a scrivere il testo che ho inserito tra gli apici;
4. Va 3 volte a capo;
5. Aspetta 5000 secondi (così da poter sfruttare il salvataggio automatico di Microsoft Word per la creazione del file temporaneo con la bozza dell'elaborato);
6. Scrive altro testo;
7. Esegue Firefox navigando su www.google.it;
8. Esegue una ricerca con le parole che desidero.

Soluzione:
La sola installazione o disinstallazione dell'applicativo lascia tracce facilmente individuabili sia come chiavi all'interno del registro di Windows sia come file cancellati all'interno del file system del sistema utilizzato; tutto questo è vero a meno che il creatore dello script non automatizzi anche la cancellazione delle digital evidence mediante tecniche di wiping, rendendo così visibile solo l'attività di wiping impedendo, in tal modo, di risalire alle informazioni cancellate.

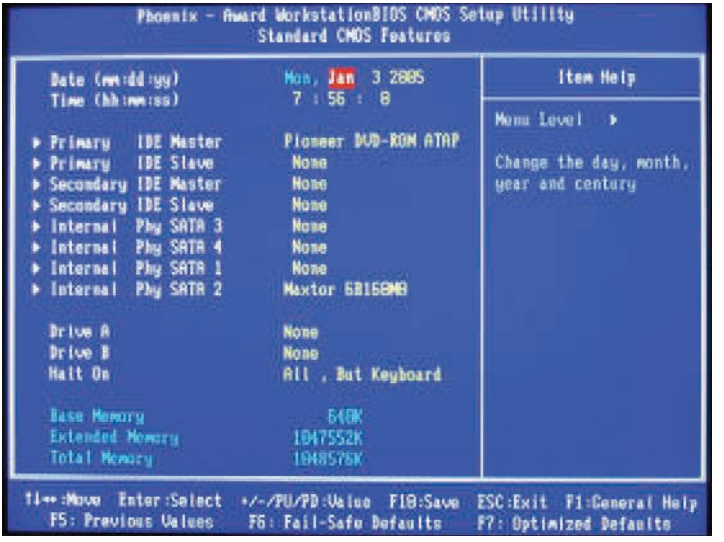
Quarto caso: Realizzare una prova ex novo, prima o dopo un determinato evento.

Ipotizziamo che la giornata odierna sia il 7 aprile 2010 e il giorno in cui compiremo il delitto sarà il 9 aprile 2010, in un arco temporale che va dalle ore 10 alle ore 13:30 dello stesso giorno.

1. A computer acceso controlliamo:
   - α se il sistema operativo non abbia alcun applicativo di sincronizzazione dell'ora tramite protocollo NTP; nel caso di controllo dell'ora attivo, disabilitarlo;
   - β. se il sistema operativo all'avvio carica programmi che effettuano accessi o log-in automatiche sulla rete; in caso positivo, disabilitare l'avvio di questi programmi.

2. Riavviamo il computer e accediamo al bios;
3. Modifichiamo la data e l'ora del bios impostandola al 7 aprile alle ore 9:40, salviamo le impostazioni e riavviamo ancora una volta il computer.

Con questa modifica il sistema operativo accederà ai dati del sistema scrivendo la data desiderata per la creazione dell'alibi.



4. Utilizziamo il computer per 4 ore circa, usando solo file locali al sistema o su memoria di massa esterna in custodia esclusiva all'utilizzatore del pc, scrivendo ad esempio un documento di testo o giocando ad un videogioco, evitando qualsiasi connessione con la rete Internet per evitare di scaricare dati che potrebbero ricondurre al riferimento temporale reale,
5. Passate le 4 ore, spegnere il computer e riaccenderlo per accedere nuovamente al bios per ripristinare i riferimenti temporali reali; una volta ripristinata l'esatta data ed ora, salvare le impostazioni e spegnere il computer senza eseguire l'avvio del sistema operativo;
6. Non utilizzare il computer sino al giorno successivo alla commissione del delitto così da evitare l'inquinamento della prova creata; eseguire almeno un avvio completo del sistema dopo l'arco temporale della creazione dell'alibi.

Soluzione: in questo caso, a meno di errori durante la creazione dell'alibi, come ad esempio l'accesso ad una pagina web di un giornale on line che riporti un contenuto in prima pagina comparso il 7 aprile 2010 e non il 9 aprile, oppure l'accesso alla propria posta elettronica on line, l'investigatore non ha elementi per poter affermare con certezza che le operazioni eseguite siano state effettuate in un arco temporale differente da quello riportato dalla time line.

Lo stesso alibi potrebbe essere realizzato in una data anteriore, ovvero dopo aver commesso il fatto, seguendo determinate accortezze:

- Il PC deve essere spento da una data anteriore al momento del reato;
- All'accensione occorre modificare immediatamente la data del BIOS;
- E' consigliabile non navigare in rete.

8. CONCLUSIONI

Sorge spontaneo a questo punto porsi le domande: "Quanto sono credibili questi alibi" e "Fino a che punto possono considerarsi veri o falsi e comunque dimostrabili ".

L'affermazione della falsità di un alibi, considerato nella sua intrinseca strutturazione in rapporto alla situazione processuale concreta, presuppone, concettualmente, che un soggetto, al quale sia contestato un fatto criminoso, si difenda dall'accusa e che la prova contraria da lui offerta mediante le dichiarazioni difensive, sottoposta a verifica, risulti falsa, non bastando la mera mancata dimostrazione. Vero o falso che sia l'alibi, la risposta ai quesiti risiede nell'espletamento di una consulenza tecnica o di una perizia capace di reperire, analizzare e valutare, facendo ricorso alle tecnologie più avanzate e alla massima professionalità, le digital evidence. Si tenga presente che la *digital forensics* è una scienza nuova tant'è che solo nel febbraio 2008 l'America Academy of Forensic Sciences (AAFS) l'ha inserita nel novero delle scienze forensi riconosciute. Tale branca cognitiva appare peculiare rispetto alle altre scienze sia perché non può considerarsi una scienza comparativa sia perché più delle altre è soggetta ad un continuo mutamento connesso all'inarrestabile e velocissimo processo di innovazione tecnologica.

Infatti, mentre tracce di DNA, sangue, impronte digitali non subiscono mutamenti essenziali nella struttura e quindi risultano soggetti a mutamento esclusivamente le conoscenze (ormai peraltro abbastanza stabilizzate) ed i tool utilizzati per l'analisi dei predetti reperti; nel caso della *computer forensics,* invece, il mutamento e l' evoluzione coinvolgono radicalmente non soltanto i tool e le metodiche necessari per l'individuazione, repertamento ed analisi delle tracce digitali ma anche le componenti strutturali ed elettroniche degli stessi "fenomeni" oggetto dell'analisi. In tale ultimo caso si appalesa evidente la necessità di ricorrere, non solo ad un costante ammodernamento degli strumenti di *forensic analisys,* ma anche ad un aggiornamento delle stesse tecniche di analisi e delle conoscenze di base in materia (ad esempio comportamento ed interazione dei programmi, etc.).

Uno dei punti deboli di queste metodiche e conoscenze, soprattutto in sede applicativa, infine, sembra essere rappresentato dalla imprescindibile necessità di una previa verifica delle capacità tecniche dei consulenti esperti di *computer forensics* chiamati a deporre dinanzi alle Corti o a svolgere accertamenti

e ricostruzioni. In USA, al fine di stabilire degli standard qualitativi per la valutazione dei consulenti tecnici si ha riguardo innanzitutto al *curriculum vitae* per verificarne l'esperienza professionale e quindi l'attendibilità mentre la *rule* n. 702 (Federal Rules of Evidence USA) indica i presupposti di ammissione ai fini del giudizio delle conoscenze esperte e quindi anche delle tecniche utilizzate per l' analisi delle prove digitali.
Secondo il già citato "Daubert test" deve trattarsi: di una procedura sperimentata; con una accertata bassissima percentualità di errori; pubblicata e recensita; ed infine generalmente accettata. E' evidente quale sia la difficoltà di applicazione di questa interpretazione normativa nel caso, come il nostro, delle prove digitali, ove la "general acceptance" per ovvi motivi non ha potuto ancora formarsi per la novità delle tecniche e dei fenomeni oggetto.
Altro problema, al quale occorre necessariamente fare riferimento al termine di questo lavoro, concerne l'influenza che il *report* del consulente tecnico può avere nella fase di convincimento del giudice chiamato ad emettere il provvedimento decisorio, problema, peraltro comune con quello, più vasto, del peso della conoscenza esperta acquisita al procedimento, nel momento decisionale.
Sarà il giudice, sebbene definito *peritus peritorum,* in grado di comprendere le risultanze della consulenza tecnica esperita e, prima, di porre i quesiti e guidare il consulente ? Vi è il forte dubbio che la risposta sia negativa nel maggior numero dei casi ed ancor più inquietante appare la risposta che potrebbe venire all'interrogativo circa il reale possesso, in capo al giudicante, delle capacità tecniche atte consentirgli di valutare approfonditamente (ed eventualmente ritenere non convincenti) le conclusioni alle quali è pervenuto il consulente tecnico chiamato a deporre nel processo.
Pare scontato che, almeno in questa fase di forte transizione che ci vede coinvolti in un inesorabile processo di digitalizzazione dei dati e dei fenomeni, nella stragrande maggioranza dei casi il giudice non sarà in grado né di comprendere il significato dei termini adoperati per indicare le varie fasi dell'accertamento né tanto meno di metabolizzare il loro contenuto ai fini decisionale. Appare ovvio, quindi, che il giudice darà ampio credito alle conclusioni alle quali è pervenuto il consulente e, in quasi totale assenza di capacità critica, egli sarà indotto a porre l'elaborato tecnico come fulcro della motivazione posta a sostegno della decisione.
Gli esempi esposti in questi paragrafi, molto probabilmente, non rappresentano in modo esaustivo tutte le casistiche annoverabili tra i possibili casi di alibi informatici, ma possono aiutare l'investigatore informatico a riflettere su un principio fondamentale dell'analisi forense:

"Una traccia informatica inizialmente deve essere trattata come (ed è) un

indizio. Se la si vuole promuovere a prova digitale è necessario raccogliere ulteriori elementi, diretti o indiretti, che possano rafforzare, o indebolire l'attendibilità, il valore probatorio, attraverso catene di relazioni".

Non bisogna dimenticare che:

- la maggior parte dei fatti ed eventi informatici, e dei dati derivanti, nascono da azioni caratterizzate dalla prerogativa dell'anonimato e comunque sono segnate della difficoltà attributiva ad un soggetto determinato, che contraddistingue le tecnologie informatiche e telematiche. Peraltro, il continuo affinamento delle tecniche di anti-forensics, facilmente reperibili in rete, accresce questa peculiarità e difficoltà;
- I riferimenti temporali in qualsiasi sistema sono governati da un orologio interno alimentato da una batteria dedicata e, in alcuni casi, allineato ad un servizio di sincronizzazione del tempo mediante protocollo NTP, pertanto se questo orologio subisce delle modifiche anche solo temporanee o ha dei malfunzionamenti, i riferimenti temporali del sistema possono subire alterazioni, scrivendo date e ore inesatte e quindi rendendo inaffidabili i riferimenti temporali stessi;
- Occorre sempre mettere in relazione le digital evidence con gli elementi indiziari e di prova acquisiti secondo una metodica di indagine, che, considerati i tempi, potremmo definire "tradizionale" ed affidata anche all'intuizione, all'acume ed alla professionalità degli investigatori ed ai riscontri esterni. Solo in tal modo si potrà giungere a delineare un quadro probatorio quanto più vicino alla realtà dei fatti evitando dichiarazioni avventate ed errori giudiziari, senza aver timore di affermare che la prova raggiungibile, anche con le tecniche piu' raffinate, non è certa o non è al di sopra di ogni ragionevole dubbio. Non bisogna dimenticare infatti che, come detto, il giudice tenderà a deciderà sulla base degli elementi forniti e sulla scorta delle valutazioni espresse dai consulenti tecnici chiamati a fornire le proprie deduzioni. Per tali motivi un consulente tecnico, capace e preparato professionalmente (il che vuol dire anche costantemente aggiornato), rappresenterà di sicuro un valido punto di riferimento per le istanze e strategie delle parti e per la decisione solo e nella misura in cui sarà in grado di "interagire e dialogare" con gli altri soggetti processuali e di integrare la propria opera e conoscenza con quanto risultante dagli atti, eventualmente stimolando alla assunzione di nuove prove o allo svolgimento di nuovi temi di indagine.