ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

DIPARTIMENTO DI INFORMATICA – SCIENZA E INGEGNERIA
Corso di Laurea in Ingegneria e Scienze Informatiche

Applicazione di strumenti e metodi dell'Informatica Forense ai dati contenuti negli autoveicoli

Elaborato in
Informatica Forense

Candidato:
Paola Smakaj

Relatore:
Chiar.ma Prof.ssa Raffaella Brighi

Correlatore:
Dott. Ulrico Bardari

Anno Accademico 2019–2020

Ad Alberto, ne abbiamo passate tante insieme.
E al mio amico Federico, per lo stesso motivo.

Introduzione

Quasi tutto nella vita è collegato a un dispositivo elettronico. Ci sono fotocamere digitali all'interno dei campanelli; lo *smartphone* rileva il tragitto casa-lavoro; le telefonate, l'accesso alla banca e gli appuntamenti medici sono tutti monitorati tramite la tecnologia. Se si tiene traccia delle attività quotidiane banali, che dire di quelle criminali?

La tesi si colloca nel perimetro dell'Informatica Forense, o *Digital Forensics*, la scienza forense che «*studia l'insieme delle attività che sono rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova*». [1]

Gli oggetti e i dispositivi che utilizziamo conservano tracce che, se estratte e analizzate da un esperto informatico forense, possono aiutare nell'accertamento di un fatto giuridicamente rilevante. Tuttavia, come si vedrà, occorre operare nel rispetto di regole tecniche e norme processuali perché il risultato sia resistente dal punto di vista probatorio e al contempo garantisca il diritto di difesa. In particolare, l'elaborato prende in esame l'applicazione dei principi e metodi dell'Informatica Forense alle potenziali prove digitali memorizzate in moduli, reti e messaggi automobilistici, la c.d. *Car Forensics*; i sistemi informatici delle vetture infatti registrano e archiviano dati e, ovunque ci siano dati, c'è l'opportunità di individuarli, estrarli e analizzarli.

All'analisi teorica si è affiancato un esperimento, condotto in laboratorio, con l'obiettivo specifico di acquisire e analizzare le informazioni archiviate nell'unità di controllo motore di un'Audi A4 del 2009. Il progetto è stato realizzato presso il laboratorio del

consulente informatico forense Luca Mercuriali, con la supervisione del dott. Ulrico Bardari (Polizia di Stato), dopo aver svolto un periodo di tirocinio presso BIT4LAW, società che si occupa di consulenze tecniche nell'ambito dell'Informatica Forense. Lo scopo dell'indagine sarà quello di dimostrare come sia sempre plausibile condurre un'investigazione sul veicolo indipendentemente dal suo stato fisico, a patto che sia possibile restaurare i collegamenti tra le varie centraline e che sia preservata l'integrità delle memorie interne di queste ultime.

Il lavoro di questa trattazione è così articolato:

1. *Principi dell'Informatica Forense*: in questo primo capitolo verrà fornita la definizione della disciplina, evidenziandone le metodologie e gli standard, analizzando, successivamente, le fasi del trattamento della prova digitale. Infine, verranno proposti alcuni strumenti di analisi forense utilizzati durante il tirocinio in preparazione della tesi;

2. *Car Forensics*: il capitolo 2 tratterà l'ambito dell'Informatica Forense in cui è stato svolto l'esperimento. In particolare, si vedrà un approfondimento sui dispositivi informatici principali delle automobili, evidenziando soprattutto quelli che verranno ripresi nel capitolo progettuale;

3. *Case study*: questo spazio sarà dedicato all'esperimento e alle varie fasi legali seguite per poter identificare, acquisire e analizzare le prove digitali;

4. *Veicoli a guida autonoma da una prospettiva forense*: l'ultimo capitolo farà un balzo nel futuro, non troppo distante, affrontando le problematiche legali connesse all'*autonomous driving* e si vedrà come l'introduzione dei veicoli a guida autonoma comporti la produzione e la gestione di una quantità elevata di dati, che possono potenzialmente diventare rilevanti in un contesto giudiziario.

Indice

Capitolo 1

Principi dell'Informatica Forense

1.1 Definizione

La scienza forense, o criminalistica, è definita come la scienza applicata all'amministrazione della giustizia: la competenza è vastissima e spazia dalla chimica alla fisica, dalla medicina alla psicologia, nonché ad altri svariati campi della tecnica e dell'ingegneria. Per garantire che le prove siano ammissibili in tribunale, gli esaminatori devono seguire una procedura rigida e legale quando raccolgono e trattano i reperti. Ad esempio, durante la raccolta e l'esame di campioni di sangue, impronte digitali, e via dicendo, gli investigatori forensi documentano ogni passaggio per garantire che le prove vengano gestite in modo che non possano essere manomesse. Infine, presentano i loro accertamenti e le loro conclusioni insieme alle loro procedure in tribunale. La *Digital Forensics* o *Computer Forensics* è una branca della scienza forense che si concentra principalmente sulle prove digitali come i dati del computer di un sospettato, rete, *smartphone*, penne USB e dati GPS.
Il concetto di *Computer Forensics* emerse per la prima volta nei laboratori del *Federal Bureau of Investigation* negli Stati Uniti agli inizi degli anni '80, quando i *personal* computer iniziarono a essere sempre più accessibili ai consumatori, accrescendone al contempo l'utilizzo anche in attività criminali. Il materiale contenuto in questi sistemi informatici come file, file di log, archivi elettronici, documenti, informazioni temporanee o residuali, o celate in aree nascoste e normalmente non accessibili nei dispositivi

di *storage*, è così diventato il cuore dell'analisi effettuata dagli esperti di *Computer Forensics*. [2] L'FBI definisce la *Computer Forensics* come "*the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media*". [3]

Al giorno d'oggi, con l'esigenza di poter coprire l'indagine di tutti i dispositivi in grado di memorizzare dati digitali, si è passati a utilizzare il termine più ampio "*Digital Forensics*".

Ken Zatyko, professore alla John Hopkins University, fu uno dei primi autori ad adoperare il termine "*Digital Forensics*" piuttosto che "*Computer Forensics*", il che sembra più appropriato dato che le analisi forensi dei dati digitali riguarderanno sempre di meno il *personal* computer e sempre di più altri dispositivi (*smartphone*, navigatori satellitari, console per videogiochi, *smart* TV) o risorse *cloud*.

Dai primi anni del 2000 la *Computer Forensics* è diventata progressivamente più conosciuta anche in Italia, dove è nota sotto il nome di Informatica Forense. La prima definizione dell'oggetto dell'Informatica Forense fu sviluppata da Cesare Maioli, docente universitario e consulente, come segue: «*gli scopi dell'Informatica Forense sono di conservare, identificare, acquisire, documentare e interpretare i dati presenti su un computer. A livello generale si tratta di individuare le modalità migliori per: acquisire le prove senza alterare o modificare il sistema informatico su cui si trovano; garantire che le prove acquisite su altro supporto siano identiche a quelle originarie; analizzare i dati senza alterarli. In sintesi, di "dare voce alle prove". L'Informatica Forense comprende le attività di verifica dei supporti di memorizzazione dei dati e delle componenti informatiche, delle immagini, audio e video generate da computer, dei contenuti di archivi e basi dati e delle azioni svolte nelle reti telematiche*».

L'Informatica Forense comprende dunque l'insieme di quei casi in cui le prove sono da ricercare in strumenti informatici a fronte di reati delocalizzati come terrorismo, *cracking*, pedopornografia, truffe online, discriminazione razziale, *phishing*, violazione della privacy, *spamming*, ingiuria e diffamazione, frode informatica, furto di dati, violazioni al diritto d'autore, accessi abusivi, danneggiamenti informatici e altri reati connessi all'uso di sistemi informatici. [2]

È bene distinguere l'Informatica Forense dalla sicurezza informatica, sebbene queste due aree di attività siano strettamente correlate. Da un lato, la sicurezza informatica può essere vista come un ostacolo e, dall'altro, come una fonte di strumenti e opportunità per l'Informatica Forense. In effetti, la sicurezza informatica ha l'obiettivo finale di rendere i sistemi i più sicuri possibile; tuttavia, se questo livello di sicurezza viene aumentato (ad esempio dalla persona responsabile di un crimine), sarebbe più complicato estrarre il contenuto informativo desiderato. La raccolta di reperti informatici in questo caso richiederà la "violazione" del sistema analizzato e in quest'area la stessa sicurezza informatica sarà utile come fonte per gli studi sulle tecniche di hacking. In aggiunta, le migliori pratiche di sicurezza definiscono molti requisiti per i sistemi che, se utilizzati correttamente, possono quindi fornire una grande quantità di informazioni aggiuntive che possono essere utilizzate per l'analisi forense.
Importante sottolineare, inoltre, che l'Informatica Forense si differenzia anche dal normale recupero dei dati, il quale rinviene informazioni che sono state accidentalmente eliminate o perse, ad esempio durante un'interruzione di corrente o un arresto anomalo del server. Quando si recuperano i dati, solitamente si conosce l'oggetto della ricerca; l'Informatica Forense ha il compito di cercare quei dati che gli utenti hanno nascosto o cancellato, con lo scopo ultimo di garantirne la validità per poi essere utilizzati come prove in sede processuale.
A seconda delle peculiarità dei dispositivi oggetto di analisi o delle modalità di raccolta dei dati, l'Informatica Forense può essere meglio classificata in varie specializzazioni che potrebbero essere ripensate nel tempo in base allo sviluppo tecnologico.
Più in dettaglio le aree della *Digital Forensics* sono:

- La *Computer Forensics*, o *Disk Forensics*, che si occupa del trattamento di computer, laptop, hard disk, pendrive, DVD, CD, eccetera;
- La *Mobile Forensics* che si occupa di effettuare analisi forense di smartphone, tablet, telefoni cellulare e ogni altro dispositivo mobile;
- La *Network Forensics* che si occupa di analizzare e intercettare traffico telematico e di correlare eventi su diversi sistemi connessi in rete;

- L'*Image Forensics* che si occupa di migliorare la qualità di immagini e video al fine di estrarre informazioni da essi;
- L'*Embedded Forensics*che si occupa di dispositivi "non tradizionali" quali ad esempio antifurti;
- La *Vehicle Forensics*, o *Car Forensics*, per l'analisi forense relativa ai mezzi di trasporto, di cui parleremo ampiamente nei prossimi capitoli di questa tesi.

1.1.1 Caratteristiche della prova digitale

Più a fondo, Stephen Mason, avvocato inglese e fondatore della rivista "*Digital Evidence and Electronic Signature Law Review*", definisce le prove elettroniche come l'insieme di tutti quei dati, inclusi quelli derivanti dalle risultanze registrate da dispositivi analogici e/o digitali, elaborati, archiviati o trasmessi mediante qualsiasi apparecchio, computer o sistema elettronico, o comunque diffusi da una rete di comunicazione, rilevanti ai fini di un processo decisionale.
La caratteristica delle prove digitali è che consiste in dati digitali e viene utilizzata come prova scientifica in tribunale. Nella definizione più comune, l'evidenza scientifica è definita come qualsiasi operazione probatoria (cioè, ricerca di una spiegazione) che utilizza strumenti di informazione specifici della scienza o usa tecniche e metodi propri della scienza.
Per sua natura, il dato digitale è:

- Immateriale, per cui necessita di un supporto idoneo per contenerlo quali ad esempio CD-ROM, hard disk, chiavette USB;
- Volatile, in quanto può essere disperso abbastanza facilmente;
- Deteriorabile, modificabile in modo anche anonimo e/o involontario;
- Riproducibile in un numero potenzialmente infinito di copie.

Stephen Mason, inoltre, classifica la prova digitale in tre diverse categorie: [4]

- La prova creata dall'uomo: si tratta di qualsiasi informazione digitale che emerge come risultato dell'intervento o dell'attività umana e che, a sua volta, può essere di due tipi: *human to human* (come lo scambio di e-mail) che richiede l'interazione di due persone; oppure *human to PC*, come la modifica di un documento utilizzando un software di video scrittura. Da un punto di vista probatorio, è quindi essenziale dimostrare che il contenuto del documento non sia stato modificato e che le affermazioni in esso contenute possano essere considerate corrette.

- La prova creata automaticamente dal computer: tutte le informazioni visualizzate come risultato di un processo eseguito da un software secondo un preciso algoritmo e senza l'intervento umano (esempi possono essere i tabulati telefonici o file di log). Da un punto di vista probatorio, in questo caso, è necessario dimostrare che il software che ha generato l'attività abbia funzionato correttamente e che le prove non siano state alterate da quando sono state prodotte.

- La prova creata sia dall'essere umano che dal computer: tutti i dati che sembrano essere il frutto di un input umano e di un calcolo creato e memorizzato da un elaboratore elettronico. Da un punto di vista probatorio, è fondamentale dimostrare sia l'autenticità del contenuto scritto dall'uomo sia il corretto funzionamento dell'elaboratore.

Quanto all'ordinamento giuridico italiano, i giuristi fanno riferimento agli articoli del codice di procedura penale specificamente previste e, in mancanza a quelle che regolano le cosiddette "prove atipiche" in base alle quali le parti di un processo hanno il diritto di produrre prove, che ritengono utili per la difesa della propria posizione, purché ciò non sia vietato dalla legge e non sia manifestamente irrilevante ai fini dell'oggetto della controversia. In pratica, il giudice può rifiutare una prova o un'opinione scientifica solo se per ottenerle è stata violata la legge.

1.1.2 I fondamenti giuridici: Convenzione di Budapest

A seguito della presa di consapevolezza della necessità di una lotta internazionale contro il crimine informatico, il Consiglio d'Europa ha istituito un comitato di esperti

che, in circa quattro anni di lavoro, ha elaborato la Convenzione per la lotta contro la criminalità informatica, aperta alla firma a Budapest il 23 novembre 2001 ed entrata in vigore il primo luglio 2004. [5]

Tale atto vincolava i paesi aderenti a dotarsi di un corpus normativo che includesse le principali figure di reato, gli strumenti processuali per il loro accertamento, gli organi e le procedure di coordinamento e cooperazione transnazionale tra organi investigativi statali per rendere più efficace l'attività di contrasto. Nella fattispecie, la disposizione prevedeva anche l'adozione di strumenti tecnici, le normative e le garanzie per le parti coinvolte in procedure relative all'IT. [6]

Più approfonditamente, l'art. 1 della Convenzione definisce le nozioni di sistema e di dato informatico esprimendo il concetto: "*computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*". Si tratta di una definizione molto generale che consente di includere qualsiasi strumento elettronico, informatico o telematico, nella rete (gruppo di dispositivi) o anche in grado di lavorare in modo completamente autonomo. Questa definizione include anche dispositivi elettronici che sono forniti di un software (o anche solo un firmware) che permette il loro funzionamento elaborando delle informazioni (o comandi). Ad esempio, è possibile utilizzare questa definizione per inserire come dispositivo tutelato dalla legge un telefono cellulare, uno strumento PDA o dispositivo elettronico collocato in un impianto per la produzione industriale.

Lo stesso articolo include anche la definizione di "dato informatico" che descrive il concetto che risulta dall'uso: "*computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*". In questo caso, la definizione doveva comprendere due argomenti, il dato in senso stretto e i programmi. Entrambi sono memorizzati in forma digitale di byte all'interno di file, ma hanno due funzioni molto diverse. I primi sono i dati utente che vengono generati e archiviati utilizzando un'applicazione; per programma (o applicazione), invece, si intende il software. In questa definizione rientrano anche i sistemi operativi, i driver, firmware o un qualsiasi programma, anche di base, presenti su un computer o dispositivo elettronico

e necessari per il loro funzionamento. [7]

1.1.3 La legge di ratifica 48/2008

In Italia la legge n. 48/2008 ha ratificato le norme del Consiglio d'Europa sulla criminalità informatica. Tuttavia, non ha introdotto da zero questi principi, in quanto il codice penale italiano già prevedeva una serie di articoli introdotti dalla legge 547/1993. In particolare, la disposizione riconosce il merito di aver risolto il problema del trattamento dei dati digitali a fini procedurali e di essersi posta come obiettivo, tra i tanti, l'implementazione del principio di affidabilità della prova digitale come risultato di integrità e autenticità. Allo stesso modo, va notato come l'attenzione del legislatore si sia concentrata più sul risultato da raggiungere che sul metodo da seguire, istituendo solamente l'introduzione di tecniche per il trattamento dei dati interessati senza l'imposizione di specifiche metodologie, a condizione che l'obiettivo finale sia la corretta gestione del dato. La Convenzione, a ogni modo, non viene recepita integralmente: si noti come la legge non ne ratifica, ad esempio, l'art. 1 citato precedentemente, relativo alle definizioni tecniche.

1.1.4 Accertamenti tecnici ripetibili e non ripetibili

Tra le questioni giuridiche più rilevanti vi è quella della ripetibilità o meno delle attività tecniche a fini giudiziari.
Gli accertamenti tecnici sono collocati nel titolo V del codice di procedura penale, nella parte relativa all'attività del Pubblico Ministero nella fase delle indagini preliminari: il P.M. che conduce l'indagine deve raccogliere tutti gli elementi probatori necessari a esercitare o meno l'azione penale. Quest'ultimo può quindi dover effettuare indagini con specifiche conoscenze scientifiche, tecniche o artistiche che vanno al di là delle capacità dell'organo inquirente. In questo caso, l'articolo 359 del codice di procedura penale gli conferisce il diritto di nominare uno o più consulenti tecnici per contribuire all'attività investigativa. La nomina del consulente e la relazione tecnica da lui redatta dovrebbero essere incluse nel fascicolo del Pubblico Ministero e, di norma,

sono soggette al segreto investigativo fino al termine delle indagini preliminari (415 a c.c.p.p.).
Tuttavia, quando le valutazioni tecniche assumono il carattere dell'irripetibilità, l'articolo 360 del c.p.p. italiano prevede che il Pubblico Ministero informi tempestivamente la persona indagata, la persona offesa e i loro legali della data, ora e luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici, in modo che si proceda in contraddittorio all'accertamento, proprio come nel caso di una perizia. Il difensore e tutti i consulenti tecnici designati hanno il diritto di partecipare alla delega dell'incarico, assistere alle indagini e formulare commenti e riserve.
L'irripetibilità dell'accertamento tecnico vale sia per la verifica di cose, persone o luoghi che possono mutare nel tempo, sia per l'attività di per sé "distruttiva", proprio a causa del tipo di ispezione da svolgere. Un rapporto di valutazione tecnica non riproducibile deve essere incluso nel fascicolo per il dibattimento, ove venga disposto il rinvio a giudizio.

1.2 Tecniche e metodologie

La nuova normativa, come già sottolineato, non ha indicato nel dettaglio le modalità di acquisizione della prova informatica, ma il legislatore si è focalizzato, perlopiù, sul risultato che deve essere ottenuto evitando, così, una scelta tra gli innumerevoli protocolli soggetti a frequentissimi aggiornamenti in conseguenza dell'evoluzione tecnologica.
L'attività tecnica forense deve soddisfare alcune esigenze specificamente individuate dal legislatore, che possono essere così riassunte:

- Non alterazione o danneggiamento del dispositivo originale durante la fase di acquisizione della prova;
- Autenticazione del reperto e dell'immagine acquisita;
- Garanzia di ripetibilità dell'accertamento;
- Non modificazione dei dati originari;
- Massima imparzialità nell'agire tecnico.

1.2.1 Metodologia tecnica

Per poter procedere all'acquisizione di materiale informatico, è necessario effettuarne la copia forense.
Una copia *bitstream* è una copia bit a bit (chiamata anche "copia forense") del drive originale o del supporto di memorizzazione e si tratta di un duplicato esatto di quest'ultimo.
Una copia *bitstream* è diversa da una semplice copia di backup di un disco rigido. Questa, infatti, si differenzia da una copia normalmente effettuata dall'utente di un sistema operativo in quanto con essa:

- È possibile copiare anche i dati dello spazio cancellato;
- È possibile copiare anche i dati dello *slack space*;
- Si preservano le date dei file;
- Si ha una copia integra e completa, senza rischi di perdere dati importanti perché inizialmente ritenuti meno significativi.

Poiché nella maggior parte dei *filesystem* la rimozione di un file comporta solo l'eliminazione dell'indice che contiene la posizione del file su disco, l'accesso alle aree non allocate consentirebbe, dunque, di recuperare file o informazioni non più disponibili all'utente.
Difatti, l'evento di eliminazione di solito provoca lo spostamento della voce di directory del file in un'area riservata, la cartella identificata come cestino, mentre i cluster che compongono il file non sono né sposati né eliminati. Quando avviene uno svuotamento del cestino o una cancellazione diretta, il file viene eliminato dal sistema ma continua a rimanere memorizzato sul disco: perde semplicemente il proprio identificativo a livello di indice, ma la propria allocazione rimane integra e il record originario resta esattamente dove è stato creato. Solo quando i cluster del file vengono sovrascritti il contenuto del vecchio file diventa irrecuperabile (nella maggior parte dei casi). Per questo motivo, ripristinare i file che sono stati eliminati dai sistemi Microsoft è generalmente un processo semplice e ci sono migliaia di strumenti per perfezionare l'azione

di ripristino. Infine, la copia forense è realizzabile in due modi: tramite clonazione o tramite creazione di un file immagine.

Figura 1: Una copia *bitstream* raccoglie ogni singolo bit di ogni byte su un dispositivo. Non viene eseguita sui file (al livello dei file), bensì sul drive (al livello del drive), ignorando il marker di *end of file*.

1.2.2 Clonazione

Prevede una copia bit a bit del dispositivo di origine su quello di destinazione, senza riorganizzare o comprimere i dati scritti. Più esatta è la copia, maggiori sono le possibilità di recuperare le prove necessarie dal disco. Ciò implica che le dimensioni di origine e di destinazione saranno le stesse e conterranno gli stessi identici bit. L'unico vantaggio di questo metodo è che il disco di destinazione è identico a quello sorgente, il che in alcuni casi significa avere un duplicato esatto avviabile direttamente sulla macchina da cui è stato estratto il disco originario. Tuttavia, sul disco di destinazione è possibile copiare soltanto un disco sorgente ed è necessario utilizzare un *write blocker* per accedere ai dati della copia, poiché l'accesso senza precauzioni comporterebbe un'alterazione immediata dei dati e dell'integrità del supporto. Una copia bit-*stream* è diversa da una semplice copia di backup di un disco: il software di backup può solo

copiare file compressi archiviati in una cartella o di un tipo di file noto. Non è in grado, dunque, di copiare file cancellati o recuperare frammenti di file

1.2.3 Immagine

Questa metodologia comporta, invece, la copia del disco di origine in un file all'interno del *file system* del disco di destinazione. Quando si crea un file di immagine, quindi, i byte che compongono il disco di origine vengono archiviati in un file sul disco di destinazione con dimensione variabile che dipende dal tipo di codifica scelto. Nel caso di immagine chiamata *raw*, il file e il disco sorgente avranno le stesse dimensioni poiché i bit verranno copiati uno alla volta senza compressione o organizzazione dei dati, in modo simile alla clonazione. In questo caso, la differenza sta nel fatto che si sta scrivendo su un file all'interno del *file system* del disco di arrivo anziché direttamente sul disco. Esistono molti modi per codificare l'immagine sul disco di destinazione, che prevedono diversi tipi di compressione e organizzazione dei dati. Le modalità di acquisizione delle immagini più comuni, spesso utilizzate in alternativa alla modalità *raw* per risparmiare spazio di archiviazione, sono *Expert Witness Format* (EWF) e *Advanced Forensics Format* (AFF). Un vantaggio importante di questo tipo di copia forense è la possibilità di memorizzare varie immagini dei supporti di origine sul disco di destinazione, poiché ogni immagine corrisponderà a un file (o a più file di dimensione ridotta, in caso di suddivisione). Inoltre, non sarà necessario utilizzare alcun *write blocker* per accedere ai vari file.

1.2.4 Algoritmi di *hash*

Nel mondo dell'Informatica Forense, gli algoritmi di *hash*, in particolare *Message Digest 5* (MD5) e *Secure Hash Algorithm* (SHA), vengono spesso utilizzati per convalidare e firmare digitalmente i dati acquisiti. Infatti, la recente legislazione richiede una catena di custodia che consenta di preservare i reperti informatici da possibili modifiche post-acquisizione: i codici *hash*, in questo caso, possono essere utilizzati per verificare se il contenuto è rimasto invariato nel tempo. Se i codici *hash* corrispondono, entrambe le parti in un procedimento giudiziario hanno la garanzia di lavorare sulla stessa versione

dei risultati, garantendo in tal modo un'analisi coerente. I risultanti dei codici *hash* sono ormai calcolati di default dalla maggior parte dei software di rilevamento forense e allegati alle copie forensi salvate.

La maggior parte dei requisiti per l'*hashing*, in Informatica Forense, può essere soddisfatta con un set di *hash* senza chiave: il risultato di tali funzioni produrrà una stringa univoca, come il comando md5sum di Linux. Il vantaggio di questo tipo di *hashing* è che rende possibile l'identificazione di file noti, come programmi eseguibili o virus, anche nel caso in cui essi vengano nascosti tramite il cambiamento del loro nome o dell'estensione. Ad esempio, molte persone che visualizzano o trasferiscono materiale pornografico cambiano i nomi dei file e le loro estensioni per poter nascondere la natura del contenuto; tuttavia, il loro valore di *hash* non verrà modificato, rendendone possibile l'individuazione.

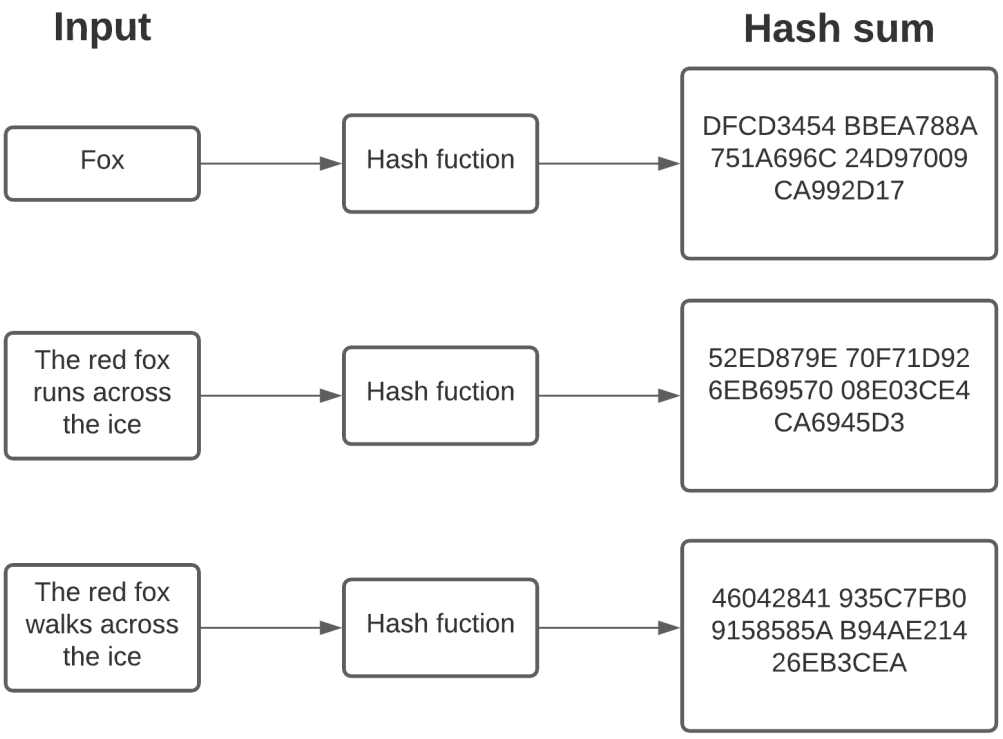

Figura 2: La funzione crittografica SHA1.

1.3 Standard internazionali e *best practice*

1.3.1 Gli standard ISO

Poiché il ricorso all'evidenza digitale solleva le problematiche che emergono dall'evidenza scientifica, si rende necessario costruire un quadro epistemologico attraverso il quale occorre definire standard metodologici e strumenti tecnici idonei a garantire la certezza procedurale e la trasparenza per far fronte alla crescente complessità dei servizi nel settore delle tecnologie dell'informazione e della comunicazione, nonché l'internazionalizzazione delle indagini sui dati digitali. [8]
ISO (l'Organizzazione Internazionale per la Standardizzazione) e IEC (la Commissione Elettrotecnica Internazionale) formano il sistema specializzato per la standardizzazione a livello mondiale. Gli enti nazionali che sono membri dell'ISO e dell'IEC partecipano allo sviluppo degli standard internazionali attraverso commissioni tecniche istituite dalle rispettive organizzazioni per occuparsi di campi specifici dell'attività tecnica.
In particolare, gli standard ISO/IEC rilevanti per il trattamento della *digital evidence* sono i seguenti:

- ISO/IEC 27037 "*Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence*" (Linee guida per l'identificazione, raccolta, acquisizione e conservazioni delle prove digitali);
- ISO/IEC 27041 "*Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method*" (Linee guida sulla garanzia di idoneità e adeguatezza dei metodi di investigazione);
- ISO/IEC 27042 "*Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*" (Linee guida per l'analisi e l'interpretazione di prove digitali);
- ISO/IEC 27043 "*Information technology – Security techniques - Incident investigation principles and processes*" (Principi e processi per l'investigazione di incidenti informatici).

1.3.2 Standard ISO/IEC 27037

Il presente standard internazionale offre le linee guida per le attività specifiche nel trattamento delle prove digitali; questi processi sono: l'identificazione, la raccolta, l'acquisizione e la conservazione. Tali attività sono necessarie in un'indagine per poter mantenere l'integrità delle prove digitali: una metodologia adeguata contribuirà alla loro ammissibilità nelle azioni legali e disciplinari, così come negli altri casi necessari. [9]

Data la grande eterogeneità della preparazione informatica degli agenti di polizia, inoltre, il dato standard definisce due categorie, il cui scopo è fornire una differenziazione sulla base della formazione e dell'esperienza dei funzionari: un *Digital Evidence First Responder* (DEFR), che ha l'abilità e l'addestramento per poter giungere sulla scena dell'incidente, valutare la situazione e prendere precauzioni per acquisire e conservare le prove; e un *Digital Evidence Specialist* (DES), il quale ha la capacità di analizzare i dati e determinare quando un altro specialista debba essere chiamato per assistere con l'analisi.

Grazie alle linee guida offerte, costoro saranno facilitati durante l'investigazione riguardo i dispositivi e le prove digitali in maniera sistematica e imparziale, preservandone al contempo l'integrità e l'autenticità.

1.3.3 *Digital Forensics Expert*: ruolo e competenze

Gli standard internazionali e le migliori pratiche sottolineano l'importanza di un'adeguata formazione e selezione del personale tecnico nelle attività di *Digital Forensics*, sia dal punto di vista giuridico che tecnico. Tali standard definiscono percorsi e preparazione, quindi ogni giurisdizione descrive come stabilire le competenze dei ruoli tecnici.

La formazione e la verifica delle competenze sono possibili quando i tecnici sono interni alle autorità procedurali, tuttavia risultano di difficile applicazione in sistemi come il nostro, dove i *digital forenser* sono spesso fuori dal mondo della giustizia, come ad esempio i consulenti del Pubblico Ministero o gli ausiliari della Polizia Giudiziaria. I

dati ONIF (Osservatorio di Informatica Forense) affermano che nel 72,6% dei casi il consulente tecnico possiede una laurea ma solo nel 40,3% delle volte sono in informatica, il 45% non ha completato alcun corso specifico e il 75% non ha certificati. [8]

1.3.4 Laboratori di Informatica Forense

Risulta fondamentale per le indagini digitali che siano istituiti laboratori specializzati in cui è possibile gestire le prove digitali. Ciò include la capacità di creare ambienti virtuali lontani dai luoghi in cui vengono condotte le indagini e che consentono anche di automatizzare alcune fasi del processo forense di gestione, archiviazione, analisi e interpretazione dei dati. Questi laboratori possono archiviare grandi quantità di dati, effettuare comunicazioni protette, eseguire autenticazioni su più livelli e controllare l'accesso in base al proprio ruolo. Un laboratorio centralizzato fornisce agli investigatori gli strumenti avanzati di cui hanno bisogno per il loro lavoro, utilizzando al meglio risorse e competenze e abbattendo il costo delle indagini. Inoltre, nessun *device* originario deve lasciare il laboratorio, ma solo copie forensi in dispositivi crittografati; in aggiunta, le workstation sono tenute a essere crittografate e bloccate quando il DES non opera, per evitare l'accesso a dati sensibili da parte di persone estranee. [8]

1.4 Le fasi di trattamento della prova digitale

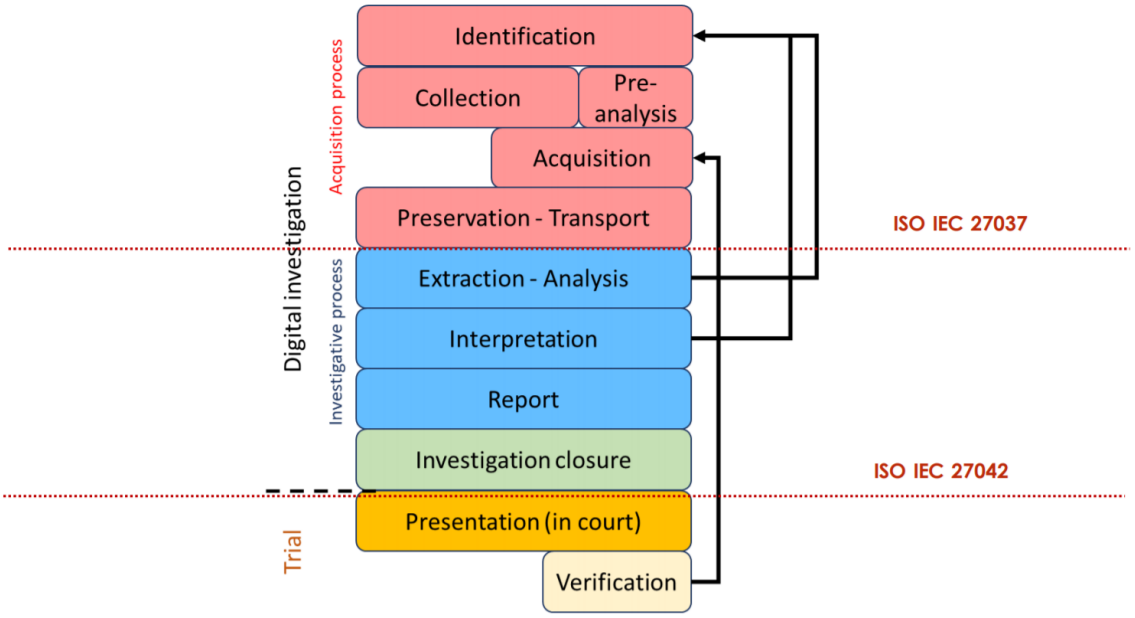

Figura 3: Ogni fase è composta da passaggi che devono essere seguiti in sequenza in ogni indagine digitale. [8]

1.4.1 Identificazione

Nella fase di identificazione l'obiettivo è la ricerca, ricognizione e documentazione di potenziali prove in formato digitale, ovvero dei dispositivi di memorizzazione di bit che possono essere rilevanti ai fini dell'indagine, individuando, ove possibile, anche i dati che si possono trovare all'esterno o in spazi virtuali come ad esempio i sistemi *cloud*. [9]

Le prove digitali soggette a questa fase sono rappresentate in forma fisica e logica. La forma fisica comprende la rappresentazione di dati in un *device* tangibile. La forma logica, invece, fa riferimento alla rappresentazione virtuale di dati all'interno di un *device*.

Il processo di identificazione comprende anche un'attività di attribuzione della priorità nella raccolta delle prove basata sulla loro volatilità, che dovrà essere accertata per assicurare l'ordine corretto dei processi di acquisizione e raccolta per minimizzare il danno alle potenziali prove.

In questa fase si redige la catena di custodia, un documento che tiene traccia della vita di un supporto informatico, rendendone così possibile l'identificazione degli accessi e dei movimenti delle potenziali prove digitali in ogni momento.

1.4.2 Raccolta, acquisizione e conservazione

Una volta identificati i *digital device* che possono contenere le potenziali prove, il DEFR e il DES dovranno decidere se procedere alla raccolta o all'acquisizione. La decisione dovrà essere basata sulle circostanze.
La raccolta è il processo in cui i *device* scelti sono trasferiti dalla loro posizione originale a un laboratorio o altro ambiente controllato per la successiva acquisizione e analisi. Tali *device* possono trovarsi in uno dei due stati: sistema accesso (*live forensics*) e sistema spento (post mortem *forensics*). Prima del 2008, le forze dell'ordine in genere seguivano il processo di togliere la spina dalla corrente per conservare prove digitali non volatili su un computer sospetto e si concentravano principalmente sull'acquisizione dell'immagine del disco. Con la crittografia avanzata e *malware*, i dati volatili presenti solo nella memoria fisica diventano cruciali per il recupero delle chiavi di crittografia e il rilevamento di software dannosi a fine delle indagini.

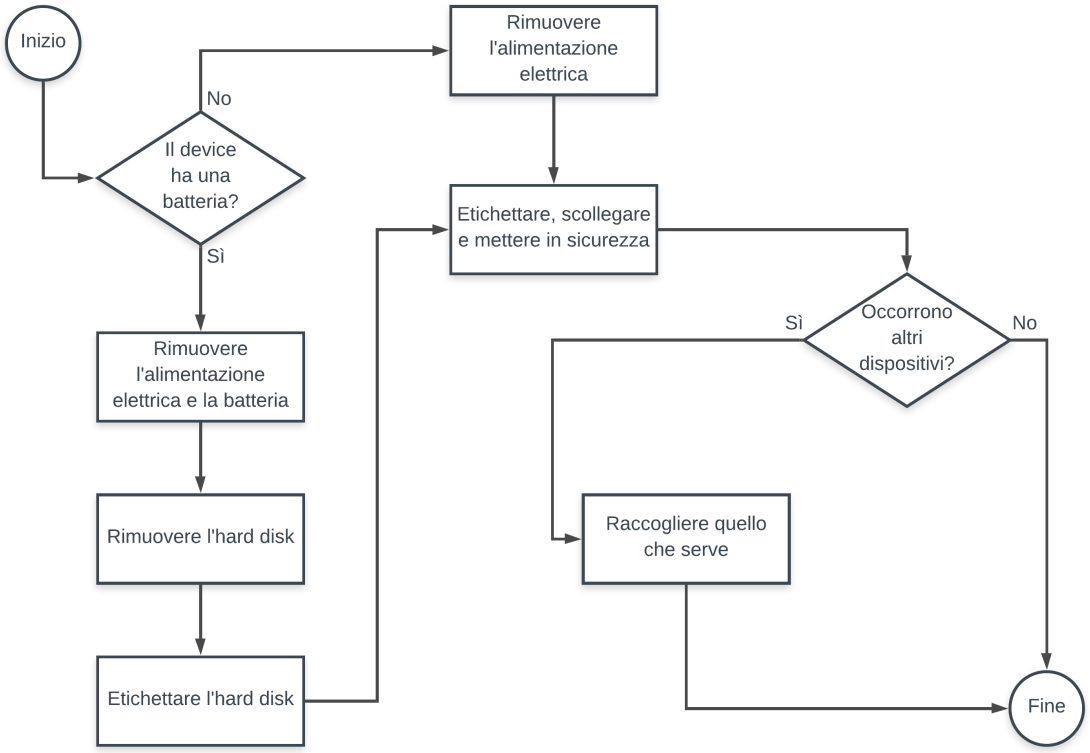

Figura 4: Linee guida per la raccolta di dispositivi digitali spenti [2]

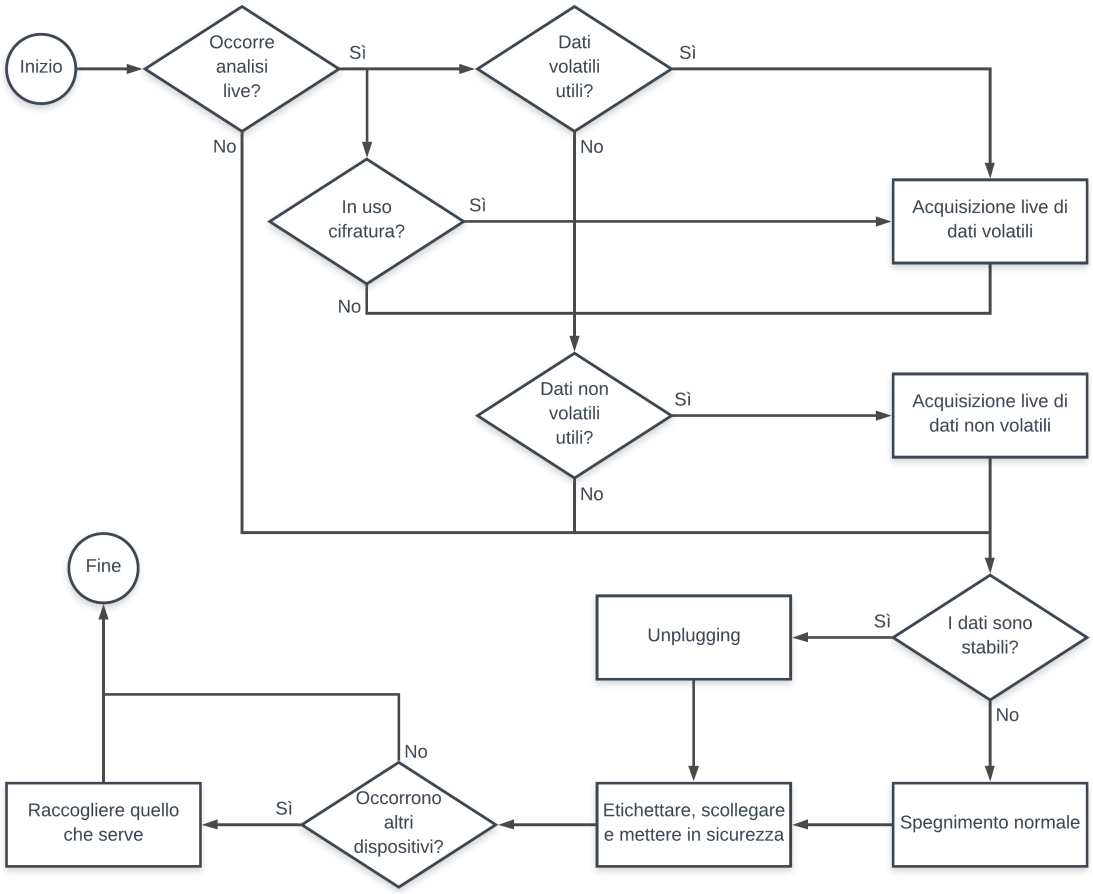

Figura 5: Linee guida per la raccolta e acquisizione di dispositivi digitali accesi [2]

Questa fase include la documentazione dell'intero metodo, compreso l'imballaggio dei *device* prioritario al trasporto. È importante per il DEFR e il DES raccogliere ogni materiale che potrebbe essere relativo a potenziale informazione digitale (ad esempio carte con password annotate, connettori e alimentatori per *system device* incorporati). Il processo di acquisizione implica la produzione di una copia delle prove digitali e la documentazione dei metodi utilizzati e delle attività svolte. Il DEFR dovrà adottare un metodo di acquisizione idoneo basato su situazione, costi e tempi. L'acquisizione deve essere svolta nella maniera meno invasiva in modo da evitare di produrre cambiamenti ove possibile; se il processo ha come risultato un'inevitabile alterazione dei dati digitali, le attività svolte dovranno essere documentate per rendere conto delle modifiche apportate.

Alcune sotto-funzioni nella categoria di acquisizione includono:

- Copia fisica dei dati;
- Copia logica dei dati;
- Formato di acquisizione dei dati;
- Acquisizione da riga di comando;
- Acquisizione tramite GUI;
- Acquisizione remota, *live* e di memoria.

La norma ISO 27037 afferma che i fattori chiave nella raccolta dei dati sono la competenza del DEFR e l'uso di strumenti validi. Contiene inoltre linee guida su come acquisire in diverse situazioni. La cosa più importante è documentare cosa e perché è stato fatto.
La maggior parte dei software di acquisizione offre la possibilità di eseguire il backup di un'intera unità fisica o solo di una partizione logica. In genere, la situazione dipende dal fatto che si stia eseguendo un'acquisizione fisica o logica. Un motivo per scegliere un'acquisizione logica è la crittografia del drive: con la crescente enfasi sulla sicurezza dei dati, la crittografia viene ora utilizzata più spesso e l'acquisizione fisica di un drive con crittografia completa del disco può causare dati illeggibili. Ovviamente, questo metodo richiede un'acquisizione *live* perché è necessario accedere al sistema.
L'acquisizione di file remoti è ampiamente utilizzata nelle organizzazioni più grandi: le imprese a livello aziendale sono geograficamente distanziate, quindi gli investigatori potrebbero non avere accesso fisico ai sistemi senza dover percorrere lunghe distanze.
Le potenziali prove digitali dovranno poi essere conservate per assicurare la loro utilità nelle indagini. Il processo di conservazione, dunque, implica la salvaguardia delle potenziali prove e dei *digital device* da manomissioni e alterazioni. Il DEFR, infine, dovrà essere in grado di dimostrare che le prove non sono state modificate da quando sono state raccolte o acquisite.

1.4.3 Analisi

Durante la fase di analisi si procederà sui dati acquisiti, ovvero su una copia forense dei dati.
Si presuppongono approfondite nozioni di architettura degli elaboratori e di sistemi operativi, ma anche di reti, di protocolli di comunicazione, di amministrazione di sistemi e un'attitudine investigativa da parte dell'esaminatore che avrà il compito di cercare e trovare il materiale rilevante ai fini dell'indagine. [2]
L'esame e l'analisi delle prove digitali dipendono dal tipo di investigazione e dalla quantità di dati da elaborare. Le indagini penali si limitano a trovare i dati specificati nel mandato di perquisizione e le indagini civili sono spesso limitate da ordini di accertamento giudiziario. Le indagini del settore privato possono ricercare violazioni delle politiche aziendali che coinvolgono solo determinati elementi, quali ad esempio le e-mail. Pertanto, gli accertamenti comportano spesso la ricerca e il ripristino di alcuni elementi specifici, semplificando e accelerando in tal modo l'elaborazione. Tuttavia, in un ambiente privato, l'avvocato dello studio spesso incarica l'investigatore di recuperare quante più informazioni possibili, soprattutto se si tratta di un processo o di un processo imminente.
Ai fini probatori, l'operazione di analisi dovrà essere riproducibile e ogni singola operazione eseguita dovrà produrre sempre lo stesso risultato. L'obiettivo è quello di identificare e trasformare il dato dell'analisi in prova digitale in modo che dimostrino eventi o fatti utili in sede processuale.
L'investigatore dovrà prestare attenzione allo spazio non visibile all'utente comune, in quanto è in quelle zone che spesso risiedono i dati più utili ai fini forensi. Alcuni di essi sono:

- E-mail;
- File di *peer-to-peer*;
- File temporanei di navigazione web;
- File temporanei di applicazioni;

- File di installazione;
- File di stampa;
- File parziali.

1.4.4 Valutazione

Il processo di valutazione è fondamentale per poter ricostruire i dettagli in grado di determinare le circostanze in cui un reato è stato commesso e le modalità dello stesso. Difatti i dati emersi dall'analisi sono spesso privi di senso: i dati evidenziati in questa fase dovranno essere interpretati per sostenere, sia a favore che a sfavore, le proprie tesi.
In particolare, un altro motivo per duplicare un drive sospetto è fare una copia per altri investigatori digitali che potrebbero aver bisogno di una copia completamente funzionale dell'unità in modo che possano acquisire, testare e analizzare i dati loro stessi.

1.4.5 Presentazione

Le citate attività tecniche trovano sfogo unico e sostanziale nell'esposizione dibattimentale. Lo scopo della presentazione è quello di trasmettere a tutte le parti del processo i fatti accertati secondo tecniche e metodologie scientifiche di cui si dovranno illustrare le fasi percorse. Una valida e completa relazione tecnica di un'attività forense dovrebbe contenere:

- La sintesi dei principi scientifici accademicamente riconosciuti su cui l'analisi si basa;
- La catena di custodia dei reperti e la loro accurata descrizione;
- La descrizione delle operazioni svolte in laboratorio e l'esito finale.

Molti strumenti forensi possono generare un report dei log che registra le attività di un investigatore e incorpora le prove che sono state aggiunte ai segnalibri o taggate

durante l'estrazione. Quindi, viene creato un report in vari formati utilizzando un generatore integrato. È possibile aggiungere un report dei log alla relazione finale come documentazione dei passaggi eseguiti durante l'esame: ciò risulterà utile se sarà necessario ripetere l'esame. Per un caso che richiede la revisione tra pari, i report dei log confermano quali attività sono state eseguite e quali risultati sono stati trovati nelle analisi e nelle revisioni originali. Si noti che i report generati dagli strumenti forensi non sostituiscono un report di indagine, gli investigatori devono essere in grado di spiegare le loro decisioni e il risultato in modo più dettagliato di quanto sia possibile con un rapporto generato dallo strumento.

1.5 Gli strumenti

Per poter condurre indagini e analisi forensi, è necessario disporre di un PC appositamente configurato chiamato anche *forensic* workstation, ovvero un computer con *drive bay* e software forensi aggiuntivi.
In primo luogo, gli strumenti forensi devono condurre un'operazione forense, cioè non modificare le prove; inoltre, gli strumenti di analisi del sistema di solito possono funzionare sia con immagini acquisite che con sistemi *live* prendendo una partizione o l'immagine del disco come input. Questi strumenti sono in grado di elaborare la struttura dei dati, aggirando il supporto del kernel perché ci si aspetta che mostrino i contenuti eliminati e altri dati che sono in genere nascosti.
Per quanto riguarda il processo di acquisizione di dati volatili e non volatili, le prove volatili sono quelle con la probabilità di essere modificate maggiore. Se la macchina sospetta è attiva e connessa, prove volatili come processi in esecuzione, *dump* della memoria, connessioni di rete e gli utenti che hanno effettuato l'accesso sono ancora una variabile da raccogliere. Ogni *dump* della memoria sarà diverso poiché la stessa è in costante cambiamento, per questo motivo si dovrebbe prima acquisire i dati più volatili. Un possibile ordine di raccolta dalla più volatile alla meno volatile è la memoria; *swap space*; stato della rete; le connessioni; processi in esecuzione; file aperti; unità e supporti rimovibili. Dato che si stanno raccogliendo direttamente prove volatili da

una macchina sospetta, si stanno inevitabilmente cambiando i dati. Per garantire la minima alterazione dei dati originali, si dovrebbero sempre usare strumenti a basso impatto e documentare tutte le procedure.

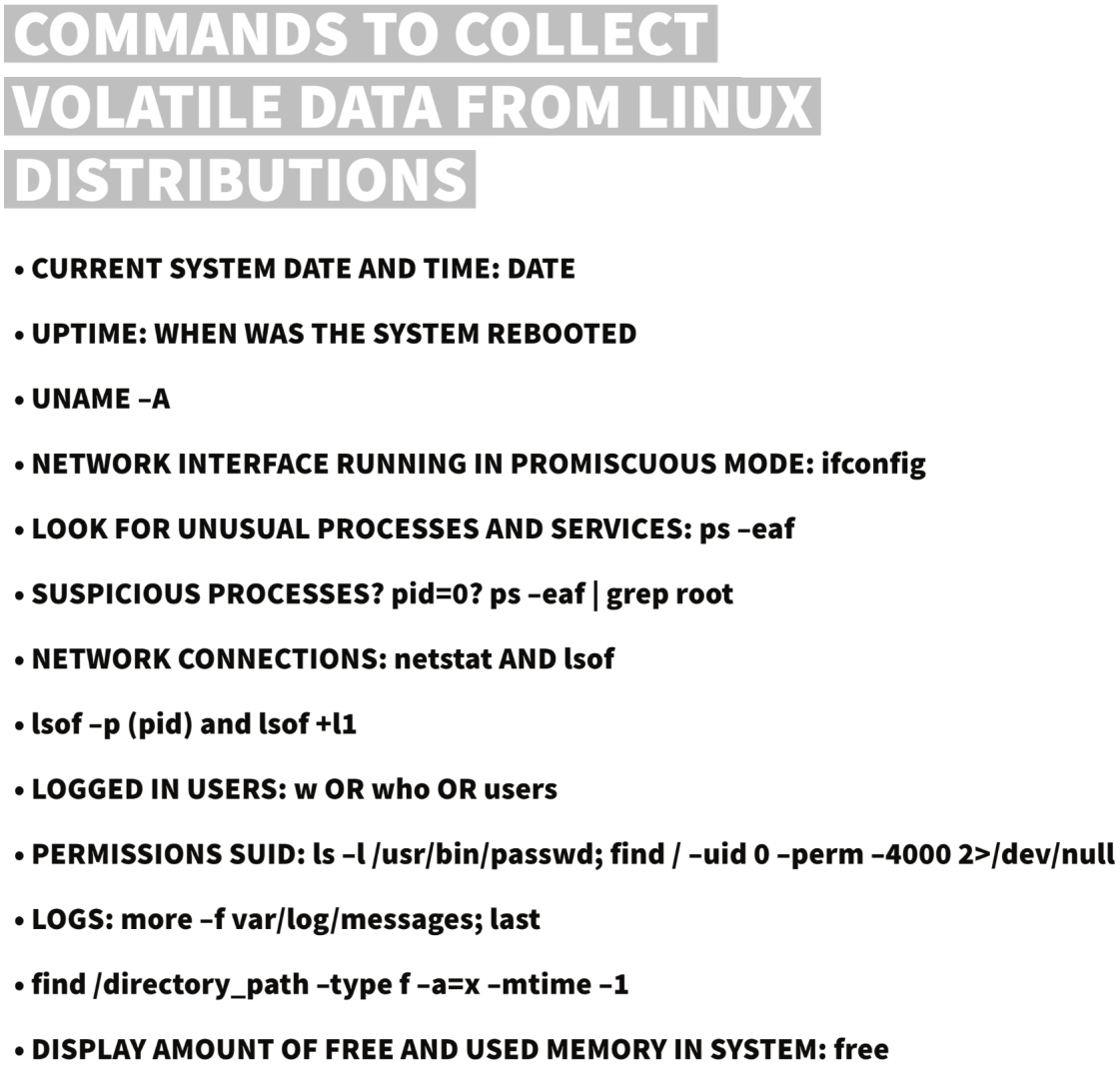

Figura 6: Alcuni esempi di comandi per la raccolta di dati volatili. (Linux)

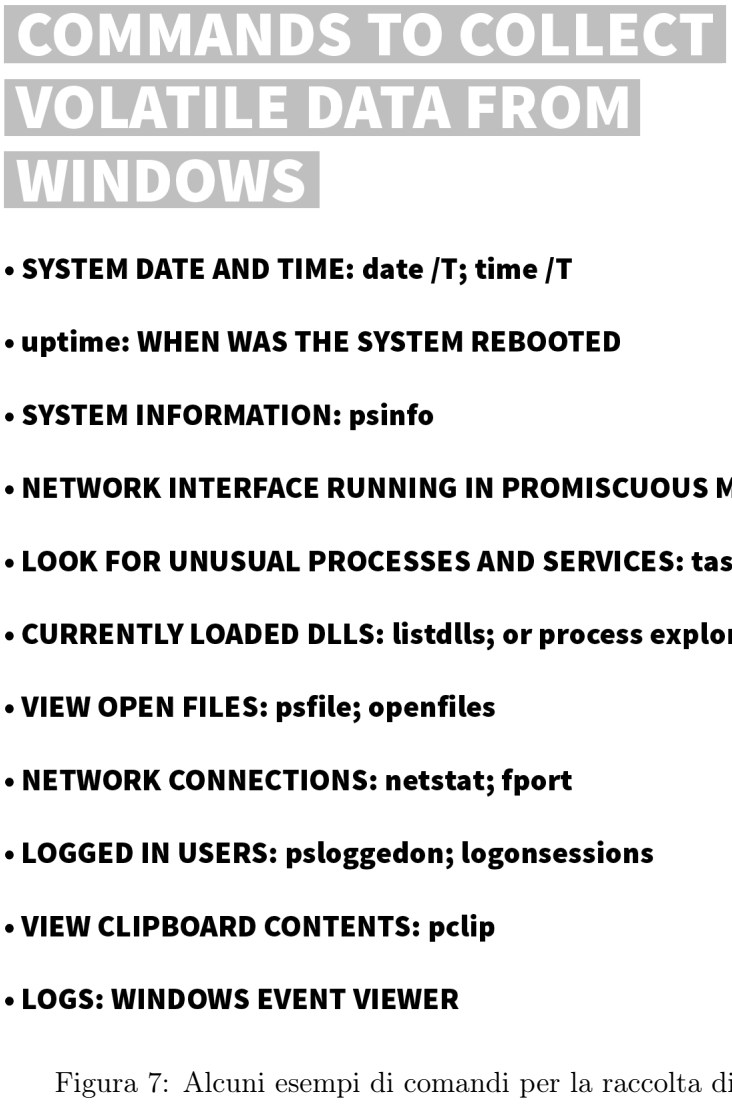

Figura 7: Alcuni esempi di comandi per la raccolta di dati volatili. (Windows)

A seconda delle esigenze, una *forensic* workstation può utilizzare uno dei seguenti sistemi operativi:

- Windows 95, 98, o Me;
- Windows NT 3.5 o 4.0;
- Windows 2000, XP, Vista, 7, 8 or 10;
- Linux;
- Mac OS X e macOS;

Se si avvia un sistema operativo mentre si sta esaminando un disco rigido, l'OS altererà il disco scrivendo i dati nel cestino e corrompendo la qualità e l'integrità delle prove da conservare. I sistemi operativi Windows più recenti registrano anche i numeri seriali degli hard disk e delle CPU in un file, rendendone così difficile il recupero. Di tutti i sistemi operativi di Microsoft, il meno invadente (in termini di modifica dei dati) è il MS-DOS 6.22.

I formati di *file system* più recenti, come NFTS, sono accessibili solo da Windows NT e versioni successive o da qualsiasi sistema operativo Linux. È possibile utilizzare uno dei numerosi *write blocker* che, come già accennato, consentono di avviare Windows senza scrivere dati sul drive. Sono inoltre disponibili *write blocker* sotto forma di software; in genere, questi writer richiedono un'unità DVD o USB *bootable* che esegue un sistema operativo a sé stante nella RAM del computer sospetto.

Si noti che nessun strumento di analisi forense è in grado di recuperare tutto. Ogni strumento e sistema operativo ha i suoi punti di forza e di debolezza, quindi è importante saper utilizzare il maggior numero possibile di strumenti per poter essere considerati un informatico forense di tutto rispetto.

Gli strumenti hardware e software necessari per un'analisi forense esauriente e approfondita possono essere suddivisi in categorie relative a ogni fase dell'investigazione, all'interno delle quali l'informatico forense dovrà essere in grado di cercare e trovare tutte le evidenze utili al caso. Nell'elenco che segue verranno proposti alcuni strumenti che sono stati utilizzati durante il tirocinio finalizzato allo sviluppo e alla stesura di questa tesi.

1.5.1 Autopsy

Autopsy è un programma *open source* e un'interfaccia grafica per The Sleuth Kit (una raccolta di strumenti da riga di comando e una libreria C che consente di analizzare le immagini del disco e recuperare i file da esse) e altri strumenti forensi digitali. Lo strumento è ampiamente gestito da Basis Technology Corp con l'assistenza di programmatori della comunità e viene utilizzato principalmente dalle forze dell'ordine, dai militari e dagli esaminatori aziendali per indagare su ciò che è accaduto su un

computer. Autopsy è stato progettato per essere una piattaforma *end-to-end* con moduli forniti immediatamente pronti all'uso e altri disponibili da terze parti. Alcuni dei moduli forniscono:

- *Timeline Analysis*, interfaccia grafica avanzata di visualizzazione degli eventi;
- *Hash Filtering*, contrassegna i file danneggiati e ignora i quelli noti.
- *Keyword Search*, ricerca per parola chiave indicizzata per trovare file che menzionano termini pertinenti.
- *Web Artifacts*, estrae cronologia, segnalibri e cookie da Firefox, Chrome e IE.
- *Data Carving*, recupera i file eliminati dallo spazio non allocato utilizzando PhotoRec
- Multimedia, estrae EXIF da immagini e guarda i video.
- *Indicators of Compromise*, scansiona il computer usando STIX.

Il browser principale può essere esteso aggiungendo moduli che aiutano a scansionare i file (chiamati "*ingesting*"), sfogliare i risultati (chiamati "*viewing*") o riepilogare i risultati (chiamati "*reporting*"). Autopsy analizza i principali file system (NTFS, FAT, ExFAT, HFS +, Ext2/Ext3/Ext4, YAFFS2) eseguendo l'*hashing* di tutti i file, decomprimendo gli archivi standard (ZIP, JAR, eccetera), estraendo tutti i valori EXIF e inserendo le parole chiave in un indice. Alcuni tipi di file come formati di posta elettronica standard o file di contatti sono anch'essi analizzati e catalogati. Gli utenti possono cercare questi file indicizzati per le attività recenti o creare un report in HTML o PDF che riassuma le attività più importanti. Se il tempo è breve, gli utenti possono attivare le funzioni di triage che utilizzano le regole per analizzare prima i file più importanti. Autopsy può inoltre salvare un'immagine parziale di questi file nel formato VHD.

1.5.2 CAINE (*Computer Aided Investigative Environment*)

È una distribuzione *live* GNU/Linux italiana con a capo, come *project* manager, Nanni Bassetti. CAINE offre un ambiente forense completo, organizzato per integrare gli strumenti software esistenti come moduli software e per fornire un'interfaccia grafica semplice. I principali obiettivi di progettazione che CAINE mira a garantire sono i seguenti:

- un ambiente interoperabile che supporta lo sperimentatore digitale durante le fasi dell'indagine digitale;
- un'interfaccia grafica e strumenti *user-friendly*.

1.5.3 UFED (*Universal Forensic Extraction Device*)

È un software capace di estrarre i dati fisici e logici dai dispositivi mobili come telefoni cellulari e altri apparati portatili, inclusa la possibilità di recuperare dati cancellati e decifrare informazioni crittografate e protette da password.

1.5.4 GuyMager

È un software che viene utilizzato per l'acquisizione di dispositivi digitali (hard disk, *memory* card, eccetera) ed è contenuto nei *repository* standard di diverse distribuzioni, ad esempio Debian (Squeeze o successive), Ubuntu (10.04 o successive) e CAINE. Tramite fdisk -lu oppure con il click sull'applicazione "*mounter*" , si individua il disco sorgente (es. /dev/sdb) e il disco destinazione, dove si andrà a scrivere il file immagine (es. /dev/sdc), infine si monta in scrittura il disco destinazione non modificando il disco sorgente. Avviando GuyMager per effettuare la copia forense, si dovranno scegliere gli algoritmi di *hash* e il formato d'uscita, *raw* (dd) o *EWF*, il primo è una copia bit a bit senza compressione, il secondo formato effettua una compressione e fa risparmiare spazio sul disco destinazione.

1.5.5 FTK Imager

È un software simile a GuyMager ma utilizzato in ambiente Windows. Poiché in un sistema operativo Windows non è possibile montare i dispositivi in sola lettura, è necessario garantirne la protezione attraverso un *write blocker* hardware o software. Durante la fase di copia forense il programma verifica che l'*hash* dell'immagine realizzata e quello dell'hard disk coincidano. Sono disponibili le due funzioni di *hash* MD5 e SHA-1. FTK Imager supporta i *filesystem* FAT12, FAT16, FAT32, NTFS, Ext2, Ext3, HFS, HFS+ e Reiser. Al termine dell'acquisizione, nella cartella di destinazione sono presenti 3 file:

- File immagine dell'hard disk in formato dd;
- File di testo contenente le informazioni di acquisizione;
- File in formato CSV contenente il *Directory Listing* del *file system* dell'hard disk.

1.5.6 Wireshark

È uno strumento utilizzato da molti investigatori e hacker forensi per analizzare il traffico di dati e manipolare i pacchetti ottenendo informazioni utili dal traffico di rete. Nella *Network Forensics*, viene impiegato anche per acquisire pagine web come fonti di prova per reati penali quali:

- Ingiurie, diffamazioni e minacce a mezzo Internet (tipicamente, mediante l'uso di *social network*);
- Frodi commesse attraverso la posta elettronica;
- Accessi abusivi a sistemi informatici, finalizzati alla distruzione di dati (danneggiamento informatico) e/o alla copia o al "furto" di dati;
- Pedopornografia.

Se si dispone di più di uno strumento di acquisizione forense, è consigliabile creare almeno due immagini delle prove digitali raccolte, una con ciascuno di essi: diversi strumenti di acquisizione utilizzano diversi metodi di copia dei dati; ad esempio, uno strumento può tentare ripetutamente di copiare aree danneggiate di un'unità.

Capitolo 2

Car Forensics

2.1 Introduzione

La *Vehicle Forensics* o *Car Forensics*, come già accennato, è una branca della *Digital Forensics* relativa al recupero di prove o dati digitali archiviati in moduli, reti e messaggi automobilistici. In particolare, il seguente capitolo avrà lo scopo di mostrare come l'Informatica Forense, applicata in ambito *automotive*, abbia la possibilità di identificare i difetti originari del veicolo o, in caso di incidente o infrazione, le cause e le possibili responsabilità che hanno portato al verificarsi di quel sinistro.
A causa dell'estrema diversità dei sistemi coinvolti, tuttavia, applicare i principi dell'Informatica Forense ai veicoli risulta talvolta complicato: si basti pensare a un ipotetico accertamento su un veicolo moderno in cui potrebbe essere necessario esaminare vari moduli elettronici, configurazioni e interazioni o addirittura rintracciare dati in sistemi che non comunicano direttamente con il componente informatico dell'automobile. Inoltre, non aiuta il fatto di avere a disposizione solamente pochi strumenti analitici, che sono comunque limitati nelle loro funzioni.

2.1.1 I sistemi informatici delle autovetture moderne

La grande rivoluzione di Internet permette alle auto di offrire ai conducenti un'esperienza di viaggio migliore e più sicura, rendendole parte di un sistema eccezionale. Grazie ai moderni sistemi di *infotainment* e all'uso di sensori, le automobili più moderne forni-

scono agli utenti una varietà di strumenti avanzati che permettono di controllare tutti i parametri del veicolo, le informazioni sul percorso, le condizioni del traffico e un'intera gamma di dati che aiutano il conducente a scegliere il miglior tragitto possibile.
Di seguito, si elencano i principali sistemi informatici presenti: [10]

- Diverse unità di controllo, tra cui unità di controllo del motore (ECU), unità di controllo della trasmissione (TCU), sistema di frenata antibloccaggio (ABS), moduli di *Body Control Module* (BCM);
- Sistema di intrattenimento, tra cui radio digitale, lettore audio (CD, MP3, USB o *Bluetooth*), lettore DVD, televisore;
- Sistema di connettività *Bluetooth* che permette il collegamento dei dispositivi mobili al sistema di intrattenimento e ciò consente lo scambio di dati relativi a rubrica, messaggi, chiamate, eccetera;
- Sistema di navigazione satellitare (GPS), integrato oppure esterno;
- *Hotspot* Wi-Fi, ovvero l'accesso a Internet per consentire la navigazione web per più passeggeri tramite una connessione integrata e può anche fornire aggiornamenti sul traffico in tempo reale per i sistemi di navigazione;
- Telecamere, una serie di telecamere che assistono durante il parcheggio o che riprendono l'interno e/o l'esterno del veicolo;
- Scatola nera, un dispositivo installato allo scopo di registrare alcune informazioni da utilizzare in caso di incidente; le compagnie assicurative negli ultimi anni invogliano l'installazione a fronte di forti sconti sul prezzo di polizza.

Nei veicoli odierni i numerosi moduli elettronici sono collegati e controllati da diversi dispositivi informatici che interagiscono tra loro grazie alle informazioni trasmesse tramite i bus di connessione. I suddetti moduli comprendono, oltre ai sistemi di intrattenimento e navigazione, l'unità di controllo elettronico, l'unità di controllo della trasmissione, il sistema di frenata antibloccaggio e il *Body Control Module*.

2.1.2 Le unità di controllo elettronico

Nell'elettronica automobilistica, un'unità di controllo elettronico (*Electronic Control Unit*) è un sistema di controllo software incorporato, cioè direttamente integrato nel componente elettrico, che controlla uno o più sistemi o sottosistemi elettrici di un veicolo.
I diversi componenti che controllano i vari aspetti del veicolo possono essere raggruppati in tre categorie: [10]

- Sensori che misurano quantità fisiche come accelerazione, velocità delle ruote, temperatura, esalazioni;
- Elementi di calcolo che, esaminando i dati raccolti dai sensori, eseguono calcoli e decisioni sulle azioni da adottare senza doverle direttamente intraprendere;
- Attuatori, ovvero dispositivi installati vicino agli apparati fisici in grado di controllare ed eseguire attività.

Analizzando ad esempio il sistema ABS, un'unità di controllo elettronica integrata con i sistemi di frenata assistita che impedisce il bloccaggio delle ruote (di solito quando il fondo stradale è scivoloso e garantisce prestazioni di frenata), si può notare come il sistema si basi su quattro sensori, un elemento di elaborazione e un attuatore.
Su ciascuna ruota del veicolo è presente un *encoder* costituito da un trasduttore e una ruota fonica (una ruota dentata simile a un ingranaggio) che gira con la ruota del veicolo, e un sensore di prossimità induttivo fisso che rileva il passaggio dei denti di tale ruota. L'unità di controllo elettronica, contando il numero di denti che passano in una determinata unità di tempo, calcola così la velocità della ruota. Se rileva che una o più ruote sono bloccate durante la frenata, esso abbassa la pressione sui freni tramite un attuatore per ridurre lo spazio di arresto del veicolo, rendendo l'autovettura manovrabile.

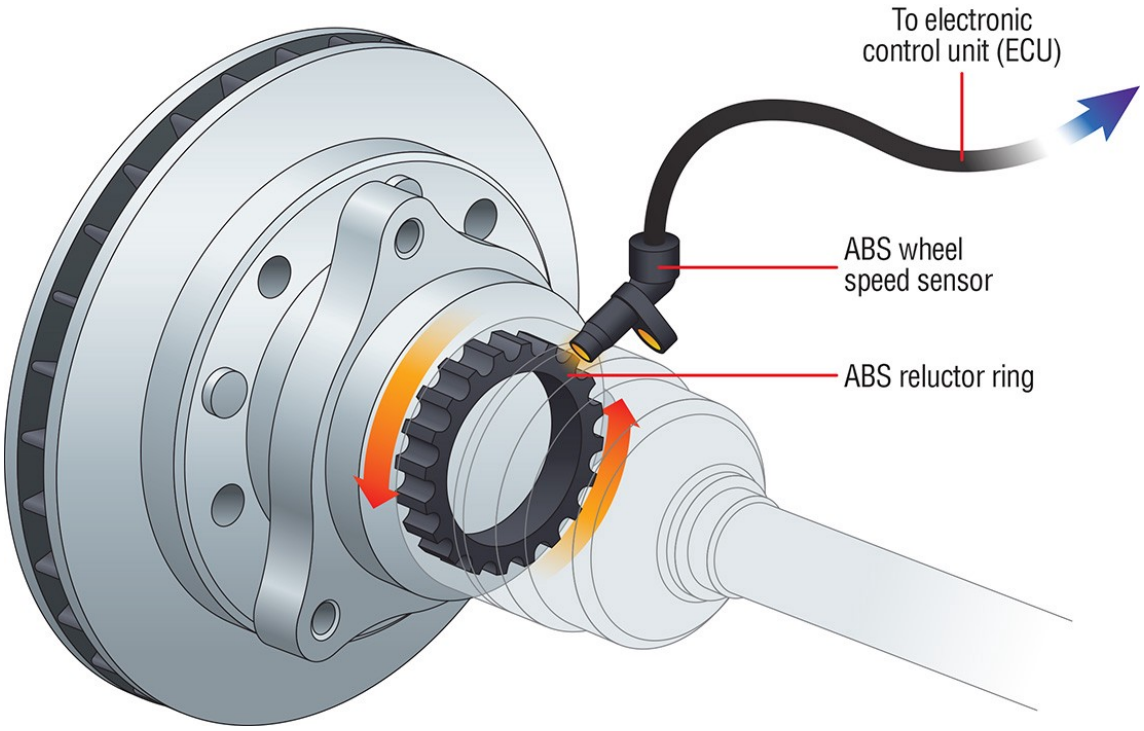

Figura 8: Figura 7. Rappresentazione del sensore di velocità e della ruota fonica in un sistema ABS.

2.1.3 L'unità di controllo motore

L'unità di controllo del motore (*Engine Control Unit*), indicato anche come modulo di controllo del gruppo propulsore, è un tipo di dispositivo di controllo elettronico che monitora un certo numero di attuatori di un motore a combustione interna (*Internal Combustion Engine*). Per essere ancora più dettagliati, la centralina decide, ad esempio, l'anticipo dell'accensione nei motori a benzina, l'attivazione e la durata delle fasi di iniezione, il funzionamento del variatore di fase e la pressione del turbo. Inoltre, stabilisce l'attivazione del sistema start-stop, l'interruzione dell'iniezione durante la fase di rilascio e imposta una diversa modalità di funzionamento nel caso in cui il motore sia alimentato con benzina ad alto numero di ottani tramite il sensore di battito in testa. In più, varia continuamente i parametri in base alle condizioni di guida, alla temperatura dell'aria ambientale e del motore, al carico sul pedale dell'acceleratore, eccetera, per garantire le migliori prestazioni in termini di consumi ed emissioni. [11]

In parole povere, l'unità di controllo motore è il cervello dell'auto. Una volta, prima dell'introduzione della centralina motore, la miscela aria/carburante, la fasatura d'accensione e il regime di minimo erano regolati meccanicamente e controllati dinamicamente con mezzi meccanici e pneumatici. Quei giorni sono ormai alle nostre spalle.

2.1.4 I bus di collegamento

Le varie centraline presenti nel veicolo sono collegate tra di loro in modo da potersi scambiare messaggi e dati attraverso reti interne costruite da protocolli di bus che regolano il trasferimento dei pacchetti. Ciascun produttore può decidere quali bus e quali protocolli utilizzare ma il CAN-bus (*Controller Area Network*) è presente su tutti i veicoli e consente l'interrogazione attraverso il connettore OBD. Più a fondo, il CAN-bus è un protocollo piuttosto semplice utilizzato nella manifattura e nell'industria automobilistica: esso è uno standard per le auto e i camion leggeri statunitensi dal 1996, ma non è stato reso obbligatorio fino al 2008 (2001 per i veicoli europei).
Il CAN-bus funziona grazie a due canali: CAN *high* (CANH) e CAN *low* (CANL). CAN utilizza la tecnica di segnale differenziale (a eccezione del CAN a bassa velocità) il che significa che quando arriva un segnale in ingresso, CAN aumenta la tensione su una linea e la diminuisce sull'altra di uno stesso valore assoluto. Il segnale differenziale viene normalmente utilizzato in ambienti che devono essere resistenti ai guasti.

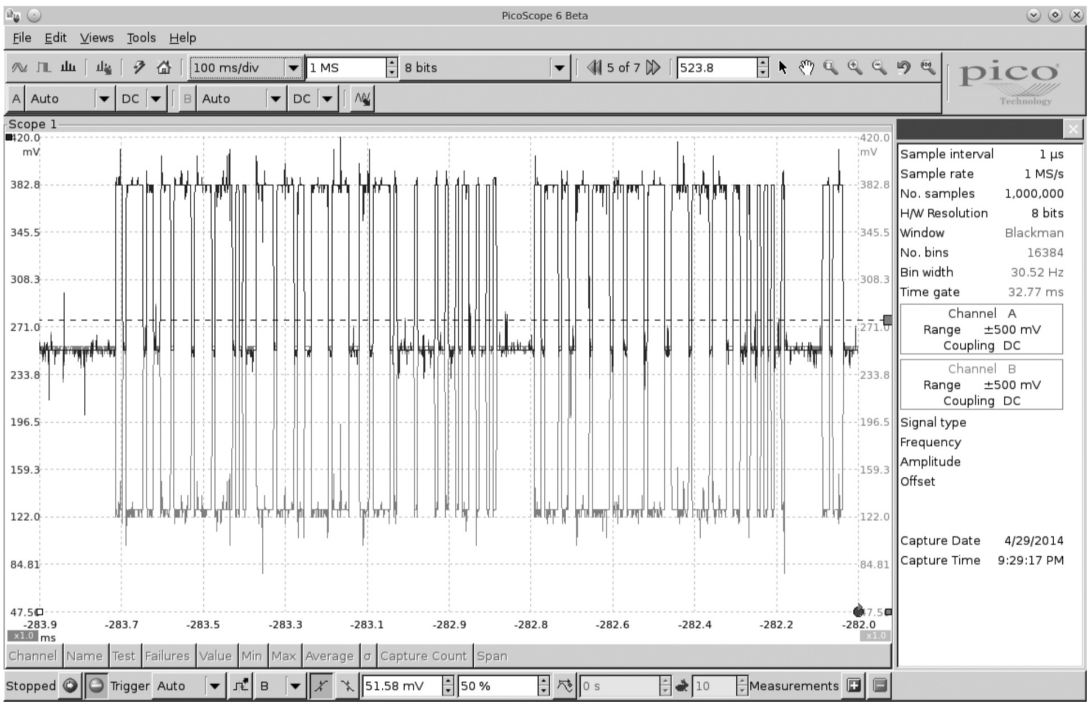

Figura 9: Figura 8. Segnale differenziale del CAN bus. [12]

La Figura 8 mostra un segnale acquisito utilizzando il software PicoScope, che ascolta sia CANH (linee più scure nella parte superiore del grafico) sia CANL (linee più chiare nella parte inferiore del grafico). Notare che quando un bit viene trasmesso sul bus CAN, il segnale trasmetterà simultaneamente 1V sia in alto che in basso. I sensori e le centraline dispongono di un ricetrasmettitore che verifica che entrambi i segnali siano attivati; in caso contrario, il ricetrasmettitore rifiuta il pacchetto come rumore.
In queste reti, le comunicazioni in transito sono in chiaro e quindi il rischio di interventi di tipo *man-in-the-middle* (MITM) che possono interferire con la trasmissione è elevato. Il motivo di questa scelta sta nel fatto che questi sistemi nascevano chiusi e non collegati all'esterno, utilizzando componenti a bassa capacità di calcolo e costi ridotti.

2.1.5 La diagnostica di bordo

OBD (*On-Board Diagnostic*) è un termine usato nel settore automobilistico per riferirsi alla funzione di autodiagnostica e di segnalazione di un veicolo; in particolare, i sistemi OBD consentono di accedere allo stato dei vari sottosistemi. La quantità di

informazioni diagnostiche disponibili tramite OBD è cambiata radicalmente dalla sua introduzione nelle versioni dei computer di bordo dei primi anni '80: le prime versioni di OBD avrebbero semplicemente acceso un indicatore di guasto o una spia luminosa se fosse stato rilevato un problema, ma non avrebbero fornito informazioni sulla sua natura. Le moderne implementazioni OBD utilizzano una porta di comunicazione digitale standardizzata per generare dati in tempo reale, nonché codici diagnostici standardizzati (DTC) che consentono a una persona di identificare e risolvere rapidamente i malfunzionamenti del veicolo.

Allo stato attuale lo standard di riferimento è OBD-II: esso specifica il tipo di connettore diagnostico e la relativa piedinatura, i protocolli di firma elettrica disponibili e il formato del messaggio. Il connettore si autoalimenta tramite la batteria del veicolo, eliminando la necessità di un collegamento separato alla fonte di alimentazione. Tuttavia, alcuni tecnici potrebbero comunque collegare lo strumento a una fonte di alimentazione ausiliaria per proteggere i dati nel caso insolito in cui un veicolo subisse una perdita di energia elettrica dovuta a un malfunzionamento. Infine, lo standard OBD-II fornisce un elenco estensibile di DTC (*Diagnostic Trouble Codes*). I codici diagnostici di errore OBD-II sono composti da 4 cifre precedute da lettere: P per motore e trasmissione, B per carrozzeria, C per telaio e U per rete. OBD-II fornisce l'accesso ai dati dell'unità di controllo del motore procurando una preziosa fonte di informazioni per la risoluzione dei problemi del veicolo.

In commercio sono disponibili diversi strumenti che si collegano alla porta OBD per accedere alle sue funzioni. Questi vanno dai semplici strumenti di scansione manuale, adatti alle autodiagnosi e usati anche dai tecnici riparatori, agli strumenti sofisticati per i rivenditori OEM, ai dispositivi telematici dei veicoli. I dati che possono essere acquisiti forniscono tra le altre le seguenti funzionalità: monitoraggio del motore e del veicolo durante il normale funzionamento; dati di scatole nere; comportamento del conducente; test sulle emissioni; dati su strumentazione supplementare (ad esempio navigazione GPS).

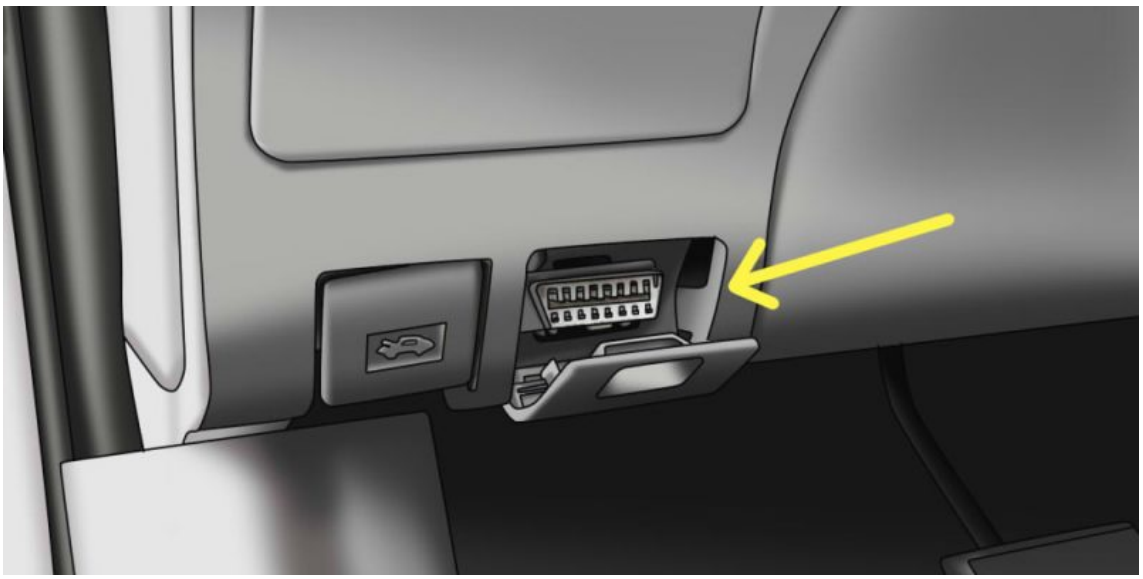

Figura 10: Esempio di connettore OBD femmina su un'auto.

2.2 Identificazione delle minacce sui veicoli

Nel corso del tempo, i veicoli hanno progressivamente sviluppato tecnologie più complesse basate su elettronica, software e connettività; contemporaneamente, tuttavia, sono state identificate varie vulnerabilità sui sistemi informatici, alcune delle quali consentono anche il controllo remoto del veicolo, rendendolo estremamente pericoloso. In sintesi, le possibili superfici possono essere esterne o interne al veicolo. Nella prima categoria vi sono: [12]

- Rete mobile;
- Rete *wireless*;
- KES (*Keyless Entry System*, sistemi per apertura e chiusura del veicolo con telecomando)
- TPMS (*Tyre Pressure Monitoring System*, sistemi di monitoraggio della pressione degli pneumatici).

Nella seconda categoria troviamo:

- I sistemi di *infotainment*;
- L'USB;
- OBD (*On-Board Diagnostic*);
- CAN-bus (*Controller Area Network*).

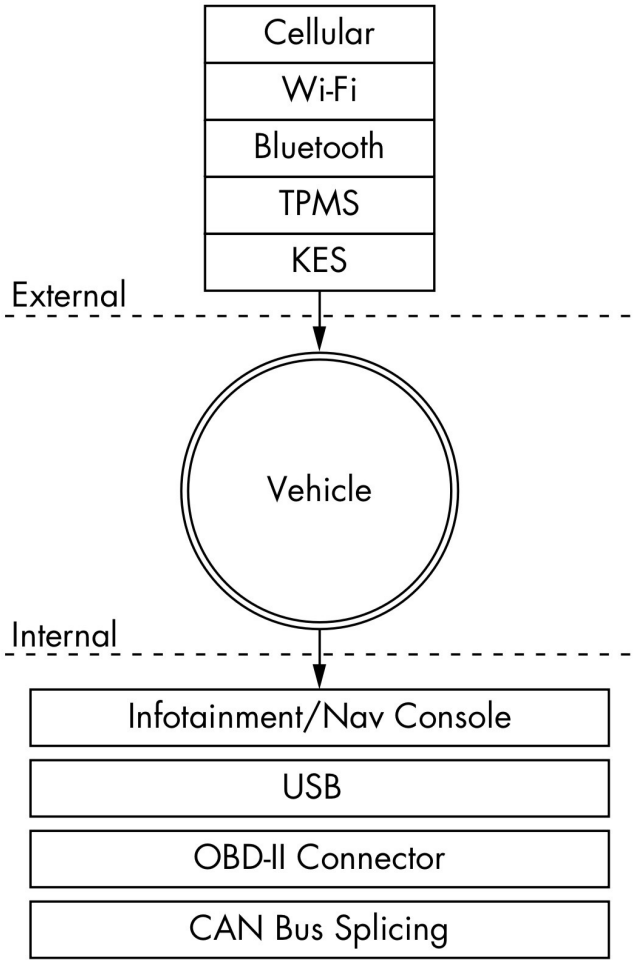

Figura 11: Le caselle rettangolari sono gli input e il cerchio al centro rappresenta l'intero veicolo. Per raggiungere l'automobile, gli ingressi attraversano due linee tratteggiate, che rappresentano minacce esterne e interne. [12]

Per determinare le potenziali minacce che possono interessare un veicolo, è necessario innanzitutto considerare quali comportamenti ad alto livello possono essere intrapresi

da un attaccante. Le eventuali azioni da considerare sono: assumere il controllo del veicolo da remoto, spegnere il veicolo, spiare le persone a bordo, sbloccare il veicolo, rubare il veicolo, tracciare il veicolo, aggirare i sistemi di sicurezza, installare *malware*.

2.3 Acquisizione forense di dati dai veicoli

I software per l'uso nel settore forense automobilistico sono progettati per fornire soluzioni integrate per l'identificazione, l'acquisizione e l'analisi dei dati raccolti nei sistemi di informazione dei veicoli. A seconda del veicolo e dello sviluppo tecnologico, la quantità e la qualità dei dati memorizzati nei veicoli determineranno cosa è successo, quando, chi è stato coinvolto e quale responsabilità dovrebbero essere assunte.
Nei casi giudiziari che coinvolgono veicoli, i sensori e i dati di eventi registrati sul modulo di controllo elettronico o sull'unità elettronica di controllo (EMC/ECU) si trovano a dover essere esaminati sempre più spesso. Questi dati, d'altronde, contengono elementi rilevanti che possono aiutare a definire con maggiore precisione l'incidente o il malfunzionamento; essi devono pertanto essere raccolti conformemente allo standard ISO/IEC 27037. Al momento, non esiste una grande varietà di strumenti per la raccolta dei dati sui veicoli, ma è ovvio se si considera che la *Vehicle Forensics* è appena apparsa sulla scena.
Un esempio di procedura può essere attuata avendo cognizione del fatto che la comunicazione attraverso la porta OBD avviene tramite adattatori che consentono il collegamento attraverso la rete, di solito via Wi-Fi o *Bluetooth*. In entrambi i casi, infatti, la comunicazione segue la logica del protocollo TCP/IP e il flusso di dati trasmessi (invio e ricezione) può essere acquisito tramite le pratiche di *Network Forensics*. In poche parole, registrando il flusso di rete generato dal computer che comunica con l'adattatore collegato alla porta OBD, è possibile effettuare un'acquisizione forense che risponde positivamente a tutti i requisiti dello standard ISO/IEC 27037, con una pratica simile a quella dell'acquisizione di pagine web. Se non è possibile raccogliere i dati da OBD, è possibile lavorare in modo simile alle tecniche di *Mobile Forensics* e utilizzare la tecnica *chip-off*, un procedimento in cui i chip di memoria sono dissaldati dal lettore

dei singoli bit in modo da poter effettuare una copia forense integrale. Questo processo richiede conoscenze e strumenti: se il modulo non viene rimosso correttamente, i dati andranno persi. [10]

2.4 Gli accertamenti tecnici

Per la ricostruzione di un incidente, è necessario continuare con l'ispezione di luoghi e veicoli: l'ispezione dei luoghi permette di individuare la configurazione del manto stradale, gli elementi che hanno influenzato il corso degli eventi, le condizioni meteo, i punti usati dai verbalizzanti per le misurazioni, la segnaletica orizzontale e verticale; l'ispezione dei veicoli permette di verificare la conformazione e l'entità delle deformazioni riportate.
La collisione e i successivi spostamenti sono ricostruiti sulla base dei dati raccolti: incentrandosi sulle tracce rilevate, sulle misurazioni effettuate sui veicoli, le loro posizioni, vengono ricostruite le modalità di collisione tra i mezzi e i loro movimenti, nonché la velocità. A seguito dei risultati della fase d'urto vengono registrati gli spostamenti pre-urto utili a determinare il comportamento dei conducenti e le relative responsabilità, soprattutto se l'incidente poteva essere evitato. [10]
In questo contesto, l'Informatica Forense è di solito utilizzata solamente per facilitare la ricostruzione della scena, anche tramite l'animazione. Tuttavia, i dati digitali consentono oggi una ricostruzione molto più accurata, a condizione che i dati informatici siano trattati correttamente secondo le linee guida tecniche e le norme del codice di procedura civile e penale, a seconda dell'area in cui è necessario utilizzare i dati.
Le modalità con cui i dati e le valutazioni tecnico-scientifiche entrano in un procedimento penale sono molteplici: la polizia giudiziaria può ricorrere a persone adatte a svolgere attività che richiedono particolari competenze tecniche; le parti (il Pubblico Ministero, indagati, imputati, parti civili, eccetera) possono avvalersi di propri consulenti tecnici; il giudice può servirsi della collaborazione di un perito. I momenti in cui le conoscenze tecniche e scientifiche confluiscono nei procedimenti penali sono sia le indagini preliminari che il dibattimento.

A differenza del processo penale, in ambito civile le indagini tecniche sono allegate dalle parti della causa. Il giudice nomina un consulente tecnico che svolga le funzioni di suo ausiliario per analizzare, approfondire e valutare gli elementi di prova allegate dalle parti. Queste possono farsi assistere a loro volta da consulenti. Nel settore delle prove civili, il giudice fonda la sua decisione sulle prove presentate dalle parti nel corso della causa; solo in rari casi può disporre l'assunzione di prove di propria iniziativa. Nel caso in cui l'assunzione delle prove avvenga prima dell'inizio della causa, in presenza di determinate situazioni, allora si avrà un accertamento tecnico preventivo.

Capitolo 3

Case study: accertamento tecnico su un veicolo incidentato

3.1 Introduzione

Il capitolo che segue descriverà un esperimento, condotto in laboratorio, il cui obiettivo specifico è quello di acquisire e analizzare le informazioni archiviate nell'unità di controllo motore di un'Audi A4 del 2009. Il progetto è stato realizzato presso il laboratorio del consulente informatico forense Luca Mercuriali, con la supervisione del dott. Ulrico Bardari (Polizia di Stato).

La presenza di sistemi informatici nei veicoli richiede il ricorso a consulenti tecnici d'ufficio e a esperti in Informatica Forense per raccogliere e studiare i dati digitali. In particolare, è necessario:

- Identificare i dati di interesse o capire dove si possono trovare i dati digitali;
- Acquisire i dati digitali identificati per congelare la prova e consentire il successivo test;
- Analizzare i dati registrati per provare la presunta carenza e valutare la sua significatività.

Le valutazioni tecniche sui veicoli sulla base dei dati digitali rappresentano un'area sottosviluppata che è indubbiamente emergente, ma che attualmente manca di linee

guida specifiche. Tuttavia, il trattamento di reperti informatici rientra nella categoria più ampia descritta e regolamentata dalla comunità scientifica a livello nazionale e internazionale, in particolare lo standard ISO/IEC 27037:2012, che fornisce linee guida per l'identificazione, la raccolta, l'acquisizione e l'archiviazione delle prove digitali. Tali principi e *best practice* verranno applicati durante lo svolgimento di tutto l'esperimento di questa trattazione, il quale mira a essere una proposta metodologica dell'esame, dell'indagine e della diagnosi di un'auto, un'Audi A4 del 2009, utilizzando i dati presenti nella centralina motore: le tecniche adoperate saranno, dunque, quelle associate all'Informatica Forense in modo da garantire che i risultati abbiano valore di prova in un procedimento giudiziario. In particolare, verrà effettuata un'acquisizione forense e, dopo aver cristallizzato la prova, si proseguirà con l'analisi/diagnosi ricordando che, se gli step fossero stati invertiti, si sarebbero inevitabilmente modificati i dati sporcando così il reperto. In questo modo verrà dimostrato come, a prescindere dalla gravità dell'incidente stradale e supponendo che le memorie interne delle centraline siano integre, è sempre possibile ottenere dati preziosi per le indagini.

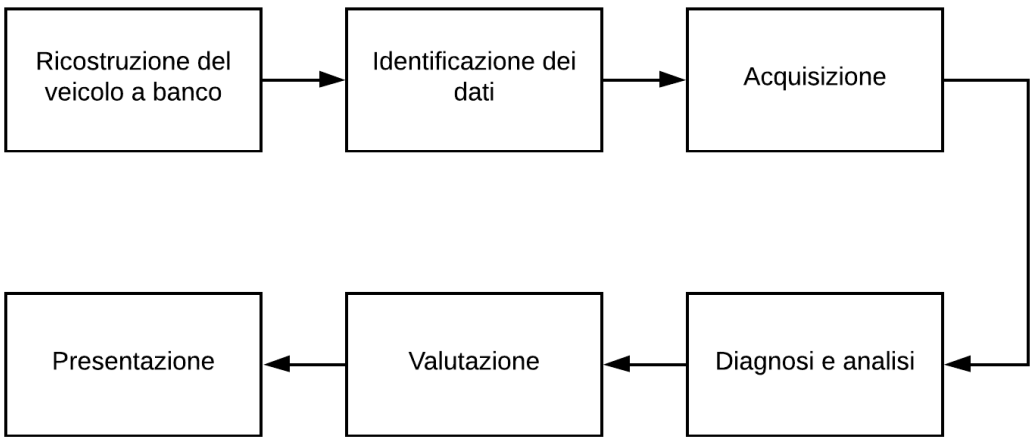

Figura 12: Diagramma di flusso dell'esercitazione.

3.2 Qualificazione dell'accertamento tecnico

I consulenti tecnici sono invitati a fornire pareri di natura tecnica e scientifica volti a colmare le inevitabili lacune cognitive di un giudice, specializzato in un campo completamente diverso. Il Pubblico Ministero nomina un consulente tecnico selezionando, di regola, una persona iscritta all'albo dei periti art. 73 disp. att. del codice di procedura penale. Quando il P.M. conduce le normali indagini e accertamenti a cui si fa riferimento all'art. 359 (accertamento ripetibile), non deve coinvolgere il sospettato e la persona offesa; le valutazioni tecniche non ripetibili, invece, sono l'eccezione in cui la stessa attività è in grado di determinare cambiamenti di cose, luoghi o persone. Data la non riproducibilità di tali valutazioni, esse sono chiaramente destinate ad avere valore probatorio, motivo per cui ai sensi l'art. 360, l'indagato, la persona lesa e gli avvocati devono essere informati senza indugio della data dell'indagine in modo che possano assistere.

Secondo la giurisprudenza consolidata, l'estrazione dei dati (ad esempio, quelli memorizzati su un computer) non dà luogo a un accertamento tecnico irripetibile, poiché si tratta di un'operazione puramente meccanica che può essere ripetuta indefinitamente. Tuttavia, l'accesso diretto al supporto informatico può compromettere i dati se il metodo utilizzato non è corretto. Di conseguenza, nell'esperimento descritto in questa trattazione, l'acquisizione dei dati potrà risultare in un primo momento ripetibile, ciononostante l'effettiva verifica dell'atto può essere effettuata solo a posteriori, assicurandosi, per quanto possibile, che le procedure tecniche seguite prevedano un margine di riscontro per le parti coinvolte. In conclusione, per quanto riguarda la ripetibilità/non ripetibilità del processo di acquisizione, è preferibile collocarlo tra le valutazioni non riproducibili.

In aggiunta, al contrario delle analisi di dispositivi tradizionali come gli *smartphone* o dei dati ottenuti da terze parti come gli elenchi telefonici, una buona scelta per l'analisi forense di questa tesi è quella di orientarsi sul procedere, nuovamente, a una valutazione tecnica non ripetibile. Le attrezzature e l'impossibilità di conoscere preventivamente lo stato di operatività e l'effettiva disponibilità dei dati, che potrebbero essere l'unico

elemento di prova utile alla difesa, richiedono il maggior coinvolgimento possibile degli interessati. [10]

3.3 Ricostruzione del veicolo a banco

Al fine di meglio comprendere il funzionamento di un veicolo dal punto di vista elettronico, il modo ottimale è quello di ricostruire l'impianto elettrico contenente le principali componenti dell'auto. In sintesi, occorre assemblare una macchina banco ripristinando sia le linee elettriche, sia i bus che collegano tra di loro le varie centraline. In questo modo si avrà la ricostruzione di un'autovettura che ne simula il funzionamento e, in caso di incidente, gli eventuali malfunzionamenti antecedenti a esso e la telemetria (cioè la pressione sul pedale del gas, sul pedale del freno, la velocità e l'angolo di imbardata, i quali vengono memorizzati al momento del sinistro).
Sarà dunque possibile verificare ipotetici difetti occulti del veicolo, difetti diretti e difetti riflessi (ovvero un guasto meccanico che si traduce in errore elettronico), determinando così se la natura del *crash* registrato sia da attribuire a una condotta non corretta di chi era alla guida oppure a un difetto dell'autoveicolo.
Il banco più semplice da realizzare è formato dal dispositivo scelto come target e un alimentatore. Quando si fornisce a una centralina la giusta quantità di energia, è possibile iniziare a eseguire test sui suoi ingressi e comunicazioni; tuttavia, spesso è necessario aggiungere almeno alcuni componenti o porte per rendere il banco più facile e intuitivo da usare e operare. Una porta OBD consente agli strumenti meccanici specializzati di comunicare con la rete del veicolo e, affinché la medesima funzioni completamente, si dovranno esporre i cavi di rete della vettura dall'unità di controllo motore alla porta. Una volta che si hanno tutti i pezzi necessari, si dovrà utilizzare lo schema elettrico dell'unità di controllo motore per determinare quali cavi collegare per farlo funzionare e, dopo aver ottenuto le informazioni sul cablaggio del connettore, sarà il momento di assemblare il tutto.
Nel caso specifico, è stato costruito un banco avanzato in grado di simulare i segnali del motore, al fine di indurre i componenti a pensare che il veicolo sia presente. In

particolare, vengono combinati la centralina motore con il modulo di controllo della carrozzeria in quanto contiene anche le chiavi originali per avviare l'automobile.
Affinché i moduli vengano rimossi senza danneggiarli o alterare i dati, è frequente che gli informatici forensi lavorino a fianco di persone con le giuste competenze nel campo, come i meccanici: la ricostruzione a banco analizzata è stata infatti resa possibile grazie all'aiuto di un tecnico meccanico.

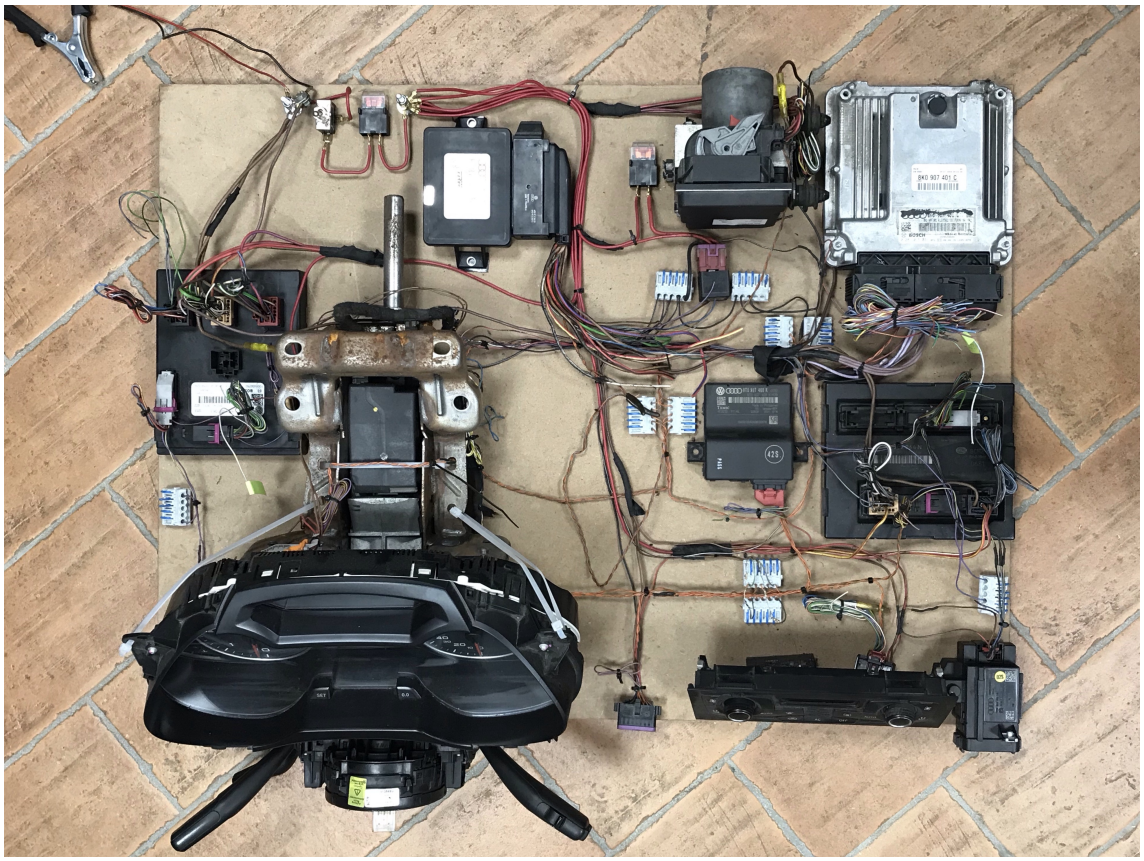

Figura 13: Fotografia della macchina ricostruita a banco utilizzata per il progetto di tesi.

3.4 Identificazione dei dati

Ci sono tre principi base nelle principali organizzazioni e giurisdizioni che governano le prove digitali: rilevanza (il materiale acquisito è rilevante per l'investigazione), affidabilità (le metodologie utilizzate nella gestione delle prove digitali devono essere controllabili e ripetibili) e sufficienza (il materiale raccolto deve essere sufficiente a consentire l'esecuzione di un'indagine corretta). Questi tre punti sono importanti

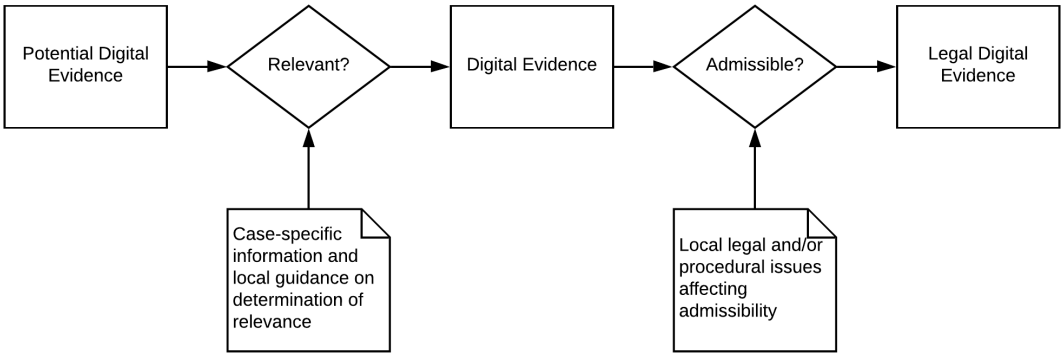

Figura 14: Transizioni dello stato delle prove digitali. [13]

per qualsiasi indagine, non solo per quelle in cui le prove digitali siano consentite in aula. Le evidenze digitali sono rilevanti se sono rivolte a comprovare o a confutare un elemento del caso specifico sottoposto a indagine. Di conseguenza, non è sempre importante che l'informatico forense raccolga tutti i dati o faccia una copia completa delle prove digitali originali; spesso, il concetto di sufficienza esprime la necessità di collezionare solamente quelle (potenziali) prove idonee a consentire che gli elementi del caso siano correttamente esaminati o investigati.

L'identificazione è dunque la fase in cui il consulente deve ricercare, individuare e documentare tutti i dati dai *device* che possono contenere possibili prove rilevanti per l'incidente riconoscendo anche i luoghi in cui sono immagazzinati. Le principali domande da porsi potrebbero essere le seguenti: quali sono i tipi di componenti e dispositivi elettronici di interesse, dispositivi integrati e autonomi, e come possono essere raccolti in modo forense? Quali sono invece i tipi di informazioni personali che sono archiviati nei veicoli, come vengono memorizzati? Ci sono ulteriori fonti di prova esterni all'automobile (ad esempio CCTV in una città)? [14] Una volta identificati tutti i sistemi rilevanti, è necessario procedere a repertare tutti i componenti, inclusi i dati di identificazione del veicolo, i dati interni delle unità di controllo del veicolo e così via.

Essendo quello della presente trattazione un esperimento, verranno documentate l'acquisizione e l'analisi dei dati memorizzati nell'unità di controllo motore, scelta per la

sua importanza e per il suo ruolo come "cervello dell'auto".

Figura 15: Centralina motore

3.5 Acquisizione dell'unità di controllo motore

L'informatico deve prestare attenzione quando si utilizza uno strumento specifico per la raccolta o l'acquisizione dei dati digitali. La mancata osservanza di questa precauzione può comportare la perdita di una parte o di tutte le prove, pertanto i rischi necessitano di essere dichiarati per ridurre l'esposizione ad azioni di danno; per esempio, essere soggetti a campi magnetici può modificare i dati degli strumenti di archiviazione magnetica. In definitiva, l'obiettivo della *Digital Forensics* è creare un'immagine forense. [13]

I dati contenuti nella centralina motore, che dovranno essere acquisiti, si trovano nelle seguenti memorie: FLASH e EEPROM. Il chip di memoria, spesso denominato FLASH o EPROM, è la "memoria dati di gestione motore": contiene il file originale con i

parametri di calibrazione (mappe), gli aggiornamenti per il micro software (ovvero quanto necessario per una migliore gestione di un particolare motore), la decelerazione improvvisa e altri elementi come la velocità del veicolo e il regime motore. Un altro chip di memoria, di dimensione minore, è la EEPROM: è possibile chiamarla "memoria dati del veicolo" in quanto contiene una serie di informazioni sulla vettura specifica (ad esempio, numero di telaio, codici chiave, i dati di errore, eccetera) a cui spesso è possibile accedere solo utilizzando lo strumento diagnostico ufficiale del produttore.
Una volta che sono state identificate le fonti delle prove, è necessario determinare, quindi, come tali dati possono essere raccolti in modo forense.
La procedura scelta è quella di effettuare il *dump*, chiamata anche analisi *hex dump*, che altro non è che l'estrazione fisica compiuta da un informatico forense per accedere ai dati grezzi archiviati nella memoria del dispositivo. Questo tipo di acquisizione viene praticato eseguendo una copia bit a bit della memoria in questione fornendo all'operatore una vista logica della struttura; il vantaggio di questo approccio è evitare il danneggiamento dei dispositivi e di conseguenza garantire l'integrità delle prove. I software e hardware che si occupano di questa attività sono molteplici ed è compito dell'informatico saper scegliere la strumentazione giusta. Nel caso specifico di questa tesi, il *tool* utilizzato è un programmatore a banco di centraline motore e trasmissione automatica di nome K-TAG, in grado di leggere e/o scrivere direttamente il microprocessore della centralina, la memoria FLASH e la EEPROM.

Figura 16: K-TAG

Il programmatore viene semplicemente collegato alla centralina utilizzando il cablaggio in dotazione. Per sfruttare le capacità di K-TAG si utilizza il software di gestione chiamato K-Suite, che permette di realizzare il collegamento con la centralina selezionando il componente da leggere. In questo modo si estraggono i dati da tutti i chip che contengono informazioni forensi importanti. Finalmente, il *dump* viene salvato in esadecimale e può letto con un *hex editor* a piacere.

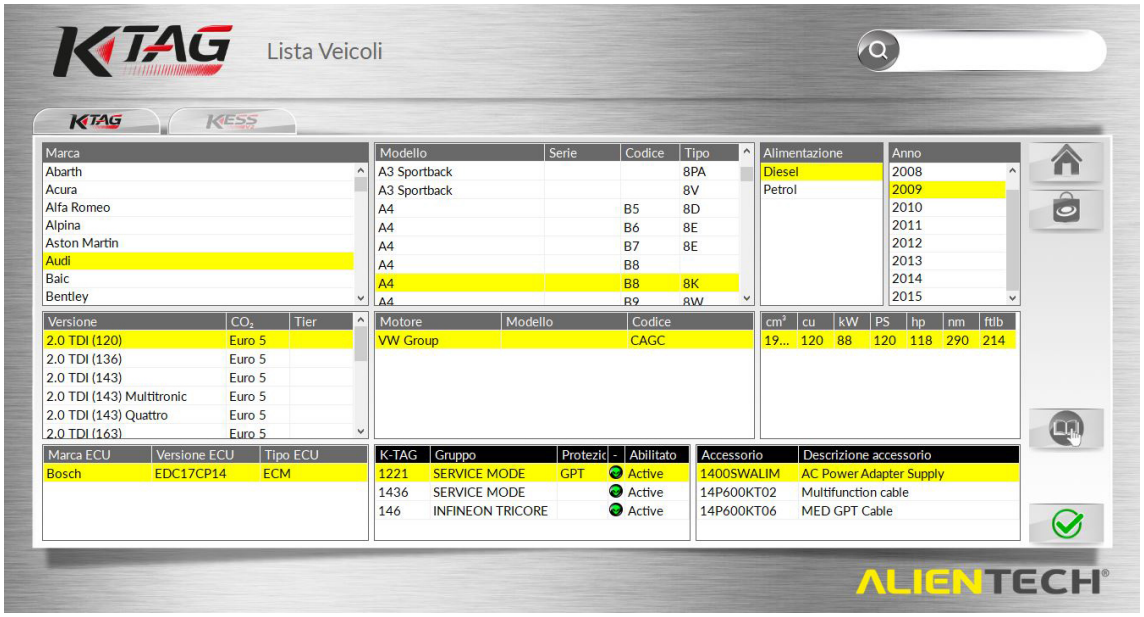

Figura 17: Software K-Suite.

Poiché i dati digitali sono estremamente facili da modificare, i sistemi giudiziari hanno richiesto un modo per garantire che i dati non cambino dopo essere stati raccolti. A tal fine, vengono utilizzati vari metodi per dimostrare definitivamente l'integrità delle potenziali prove dopo che sono state nelle mani degli investigatori. Il metodo principale utilizzato per eseguire questo controllo di integrità consiste nell'usare un *checksum*. Nel caso in esame, è stato determinato l'*hash*: immediatamente dopo aver creato l'immagine della memoria del chip, è importante calcolare la funzione (in questo caso SHA-256) e salvare il risultato in un file di testo. È stata scelta la SHA-256 poiché essa quantifica un numero univoco a 256 bit in base al contenuto dell'archivio, quest'ultimo non può essere determinato a partire dall'*hash* ed è unico per ogni file.

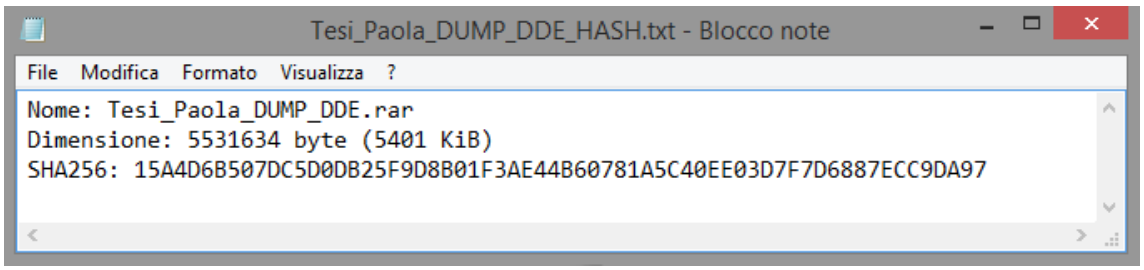

Figura 18: Funzione crittografica SHA-256 applicata al file compresso contenente l'estrazione forense dei dati della centralina.

Infine, è consigliabile effettuare un duplicato della copia forense. La ragione di ciò è che, semplicemente, si desidera una copia forense funzionante delle prove in caso di disastro: se la prima copia viene accidentalmente distrutta senza averne un'altra, si dovrà accedere ancora una volta al supporto originale e correre di nuovo il rischio di contaminare le evidenze. La procedura si rivelerà essenziale dal momento che questi saranno proprio i dati che verranno portati in tribunale. Le potenziali prove digitali devono essere preservate per tutta la loro durata, che può variare in base alla giurisdizione e alle politiche organizzative. Inoltre, tutti i dispositivi digitali raccolti devono essere adeguatamente conservati e *device* diversi possono richiedere metodi di archiviazione differenti.

Ogni situazione, scena del crimine e indagine sarà diversa, il che significa che le azioni intraprese saranno basate sulle circostanze specifiche incontrate. Le capacità di *problem-solving* e le decisioni rapide sulla base delle informazioni limitate disponibili risulteranno fondamentali.

Una volta terminata l'acquisizione, il passo successivo è quello di effettuare la diagnosi.

3.6 Diagnosi e analisi forense

Esaminare le prove elettroniche segna un passaggio dalla scienza forense all'arte dell'indagine. Non esiste tecnologia o intelligenza artificiale in grado di catturare l'odore e raccogliere indizi, testare teorie, fare ipotesi e interpretare le evidenze: nessun strumento analitico può comprendere le prove digitali o fornire gli indizi che collegano queste ultime e gli elementi di un caso.

In alcune circostanze può essere appropriato o necessario esaminare il sistema interagendo direttamente con esso o osservandolo in funzione. In questi casi, gli investigatori dovrebbero aver cura di emulare, in hardware o software, l'ambiente originale il più fedelmente possibile utilizzando macchine virtuali verificate o copie dell'hardware originale. Quando deve essere utilizzata l'imitazione, è necessario prestare attenzione per garantire che essa sia il più vicino possibile al sistema di origine. [13]

È fondamentale adottare misure per garantire che qualsiasi modifica richiesta per con-

sentire l'esecuzione della copia nell'emulatore non modifichi sostanzialmente il funzionamento del sistema e le potenziali prove digitali in analisi. Tuttavia, nell'esperimento in questione verrà effettuata una *live forensics* direttamente sull'automobile di partenza dal momento in cui sarebbe risultato dispendioso l'acquisto di una nuova vettura.

La diagnosi è lo step che farà finalmente chiarezza sulle cause dell'eventuale sinistro stradale mostrando il momento in cui è avvenuto il *crash*. Per dare un senso ai dati appena raccolti, è stato utilizzato un software diagnostico di nome AUTOCOM, uno strumento universale che soddisfa tutte le norme e i protocolli di comunicazione per accedere direttamente al fulcro del veicolo.

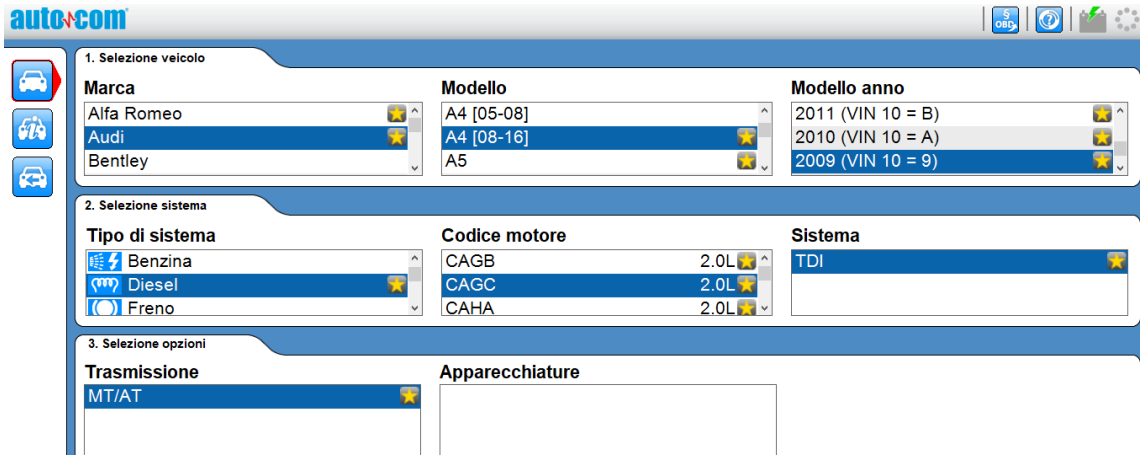

Figura 19: Software AUTOCOM.

AUTOCOM viene inizializzato sul computer mentre, a quadro spento, si collega l'automobile a banco con il software tramite OBD. Dopo aver inserito le specifiche dell'automobile come in figura 19, sarà possibile verificare quali eventi sono avvenuti prima del *crash* e di conseguenza trarre alcune ipotesi sulle cause del sinistro. Un esempio banale in cui gli errori dell'automobile risultano fondamentali potrebbe essere quello di un conducente che afferma di non essere riuscito a fermarsi a causa dei freni improvvisamente non funzionanti; se il software rivelerà effettivamente un malfunzionamento dei freni prima dell'episodio di *crash* allora la testimonianza dell'automobilista sarà in un primo momento verificata. È importante notare che un uso scorretto di AUTOCOM può provocare la corruzione dei dati nei moduli; di conseguenza, è fortemente consi-

gliato per gli investigatori una formazione adeguata sul software prima di condurre le indagini.

Conclusa l'analisi, sarà essenziale verificare che le informazioni individuate con AUTOCOM siano coerenti con l'acquisizione effettuata in precedenza; in caso di inconsistenze significa che qualcosa non è andato a buon fine. Non potendo utilizzare gli errori antecedenti all'incidente, poiché l'automobile presa in oggetto non ne ha fatti, a fini dimostrativi, la prova di verifica effettuata è stata quella di comparare il numero di telaio mostrato dal software diagnostico con quello che risiede, come già accennato, nel file in esadecimale estratto dalla EEPROM della centralina. Cercando nell'opportuna sezione relativa ai parametri in tempo reale, il software mostra la seguente informazione:

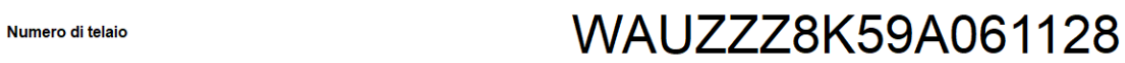

Figura 20: Numero di telaio secondo AUTOCOM.

Ora, inserendo i dati della EEPROM in un *hex editor* il *matching* dei due numeri viene facilmente verificato e la congruenza dei dati è accertata.

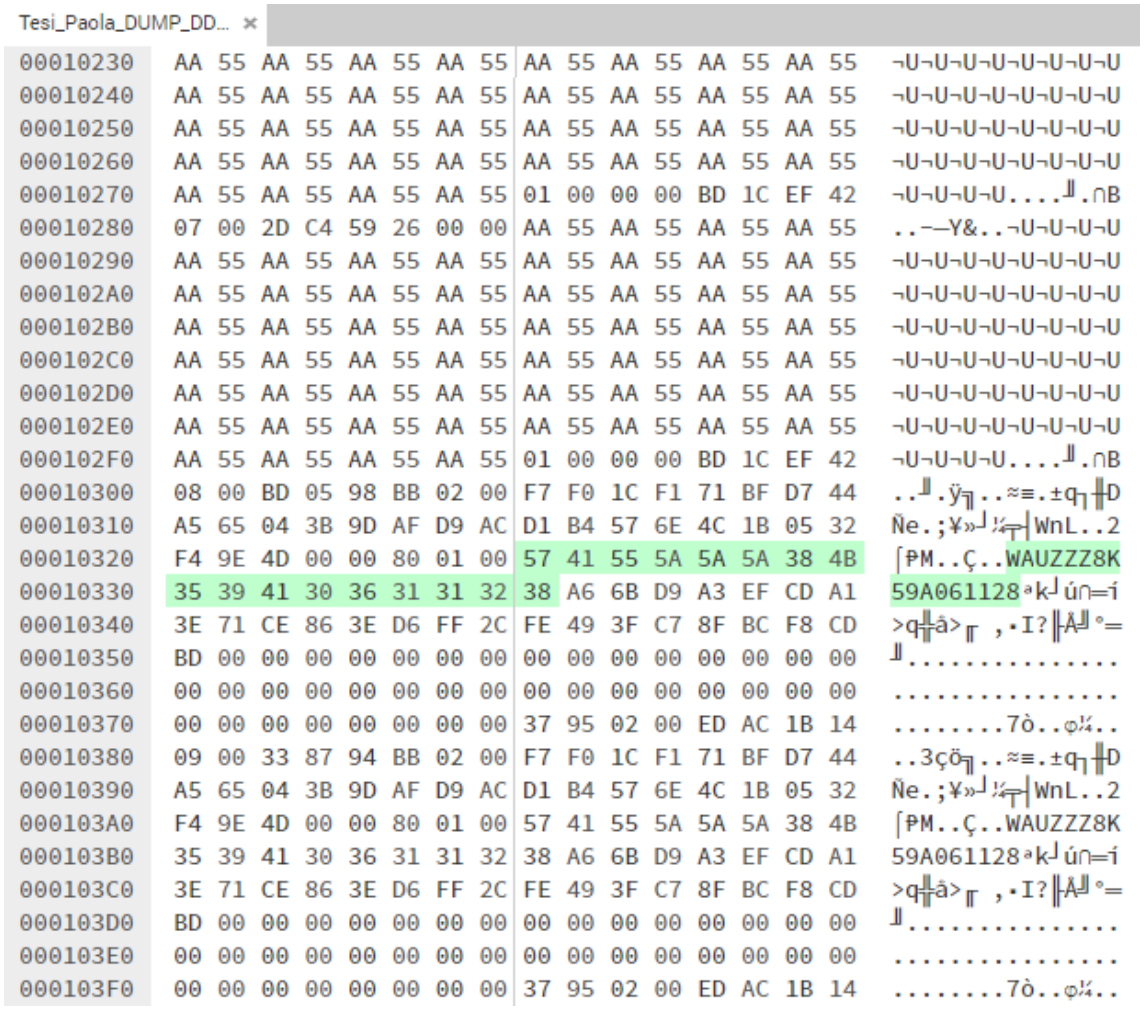

Figura 21: Numero di telaio trovato nei dati acquisiti dalla centralina motore.

3.7 Valutazione e presentazione finale

A questo punto, in un'indagine vera a propria, si ha tutto il necessario per poter interpretare i dati e fondare le proprie ipotesi sulle cause del sinistro. Se, in un certo senso, i dati digitali hanno un valore oggettivo, l'esame congiunto di più dati consente di delineare il comportamento avuto dal guidatore. Infine, tutte le prove raccolte e le conclusioni della valutazione saranno dettagliate in una relazione tecnica che sarà utilizzata in dibattimento. Dovrebbe essere possibile per un esaminatore indipendente o altre parti interessate autorizzate valutare le attività svolte dall'informatico forense. Infatti, ciò sarà possibile soltanto documentando adeguatamente tutte le azioni intra-

prese. Il consulente dovrebbe essere in grado di giustificare il processo decisionale nella selezione di una determinata linea di condotta e i processi eseguiti dovrebbero essere disponibili per una valutazione indipendente per determinare se è stato rispettato un metodo scientifico, una tecnica o una procedura appropriata. [13]
Si dovrà inoltre essere in grado di spiegare le scoperte a una persona che non sia un perito, il che significa affrontare un argomento molto tecnico e parlarne in un modo che non sia tecnico. Tutti i documenti acquisiti o creati durante l'analisi devono essere inclusi nel report che deve inoltre contenere gli argomenti scientifici sviluppati durante la fase di ricerca, i metodi usati per analizzare i dati, gli strumenti utilizzati e le scoperte fatte. Quando si esprimono le proprie considerazioni, è preferibile guardare i reperti senza pregiudizi e vedere se l'accaduto corrisponde di nuovo all'ipotesi. Anche non avere un'opinione è un'opinione. Il punto non è sempre trovare la persona colpevole: le prove devono essere fornite anche se il soggetto non ha fatto ciò di cui è accusato. Ciononostante, il consulente non può sostituire il giudice, ma deve solamente fornirgli tutti i mezzi affinché possa formulare giudizi analitici e accurati sui risultati prodotti. L'obbligo di motivare una decisione, a prescindere dalla scelta del giudice di non seguire il parere del perito o di invece accogliere la sua conclusione, sembra essere decisivo, perché garantisce l'indipendenza del giudice come esperto a supporto del controllo razionale. Questo obbligo significa che il giudice analizza e verifica le prove scientifiche e giustifica esplicitamente la sua valutazione anche quando ritiene valide e affidabili le evidenze ottenute. [15]

Capitolo 4

Veicoli a guida autonoma da una prospettiva forense

4.1 Introduzione

Un veicolo autonomo, noto informalmente come senza conducente, è un'auto autonoma in grado di imitare le capacità di gestione e controllo umane. Come veicolo autonomo è capace di percepire l'ambiente circostante e di spostarsi di conseguenza: il conducente sarà in grado di scegliere la destinazione, ma non dovrà eseguire alcuna operazione meccanica del veicolo. È importante distinguere che la guida automatizzata e la guida autonoma sono molto diverse. Attualmente non esiste un veicolo autonomo facilmente disponibile per il mercato generale e lo sviluppo di questa tecnologia è ancora in corso. Un veicolo autonomo, per definizione, non richiederebbe alcun livello di interazione umana, mentre un veicolo automatizzato, parzialmente o condizionatamente, richiederebbe comunque un input umano per funzionare.

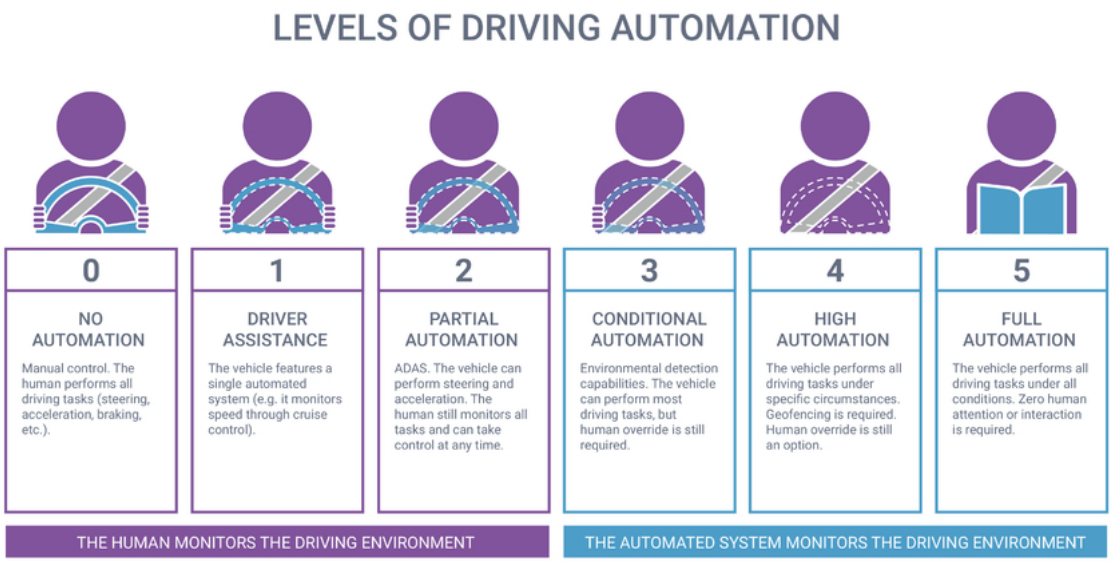

Figura 22: La scala dell'automazione basata sul controllo di un veicolo da parte del conducente.

Secondo le case automobilistiche, esistono cinque livelli di guida autonoma o tipi di veicoli autonomi.

4.1.1 Assistenza alla guida

Il primo livello è l'assistenza al conducente, *Driver Assistance*, in cui il veicolo è di ausilio al guidatore ma non assume alcun controllo in termini di guida effettiva. A questo livello sono presenti sistemi di assistenza personale che supportano i conducenti su strada, contribuendo a garantire sicurezza e comfort. Esempi di questo includono il "controllo automatico della velocità attivo" che regola in modo indipendente la distanza corrispondente all'auto che precede.

4.1.2 Guida parzialmente automatica

Il secondo livello è *Partial Automation*. A questo punto, il sistema può assumere il controllo, ma il conducente rimane responsabile del funzionamento del veicolo. Alcuni esempi sono i sistemi di assistenza semi-autonomi, come l'assistente allo sterzo,

l'assistente al controllo di corsia e l'assistente al trasporto del traffico. Può frenare e accelerare automaticamente e, a differenza del livello 1, prendere il comando dello sterzo. A questo livello, il conducente continua a mantenere il controllo dell'auto e deve sempre prestare attenzione al traffico.

4.1.3 Alta automazione di guida

Il terzo livello di questa tecnologia si chiama *Conditional Automation*. Questo livello consente al conducente di disconnettersi dalla guida per lunghi periodi di tempo. In altre parole, i guidatori possono fornire all'auto il controllo di guida completo. Con i sistemi di automazione condizionale, l'auto può guidare autonomamente su lunghe distanze, come ad esempio sulle autostrade. Questo sistema necessita comunque che il conducente assuma il controllo del veicolo su alcuni terreni come i cantieri.

4.1.4 Guida completamente automatica

Il quarto livello è *High Automation*, in cui l'auto può gestire la maggior parte delle situazioni di guida in modo indipendente; questa tecnologia è sviluppata al punto che un'auto può gestire situazioni di guida urbana molto complesse, come ad esempio la comparsa di nuovi cantieri, senza alcun intervento da parte del conducente. L'autista, tuttavia, deve rimanere vigile per riassumere il controllo se necessario. A questo livello, il guidatore ha persino la capacità di dormire durante i tratti più lunghi.

4.1.5 Automazione totale

Per quanto riguarda il livello più alto, *Full Automation*, il veicolo svolge tutte le funzioni di guida, rendendo le persone nel veicolo solo passeggeri. Questo quinto livello è dove la vera guida autonoma diventa realtà: non è necessario che i conducenti siano idonei alla guida e non devono neppure disporre di una licenza dal momento in cui l'auto eseguirà tutte le attività di guida. Le auto a questo punto dovranno soddisfare severi requisiti di sicurezza e guideranno solo a velocità relativamente basse nelle aree

popolate. Possono anche spostarsi su strada, ma inizialmente verranno utilizzate solo in aree definite dei centri cittadini.

4.2 Informatica Forense e *Autonomous Driving*

L'introduzione di veicoli a guida autonoma comporta la produzione e la gestione di una quantità ancora maggiore di dispositivi hardware, che forniscono una grande mole di dati digitali. Questi possono diventare rilevanti in un contesto giudiziario e quindi richiedere l'adozione di tecnologie informatiche forensi.

4.2.1 Le problematiche legali connesse alla guida autonoma

I vantaggi della guida autonoma sarebbero sicurezza, produttività, mobilità e riduzioni sia del traffico che delle emissioni. La capacità di rimuovere un guidatore umano non solo consentirebbe una maggiore indipendenza per coloro che non sono in grado di guidare, ma gioverebbe anche ad altri guidatori sulla strada rimuovendo l'errore umano a essi associato: infatti viene rilevato che nel 2016 il 94% di tutte le gravi collisioni negli Stati Uniti erano legate a scelte umane. I rischi connessi alla guida autonoma, tuttavia, verterebbero anche e principalmente sulla privacy e sulla sicurezza informatica, a causa dei controlli del veicolo e delle informazioni personali memorizzate. Ad esempio, i veicoli autonomi devono mappare l'ambiente circostante per comprendere le proprie circostanze, ma la mappatura della proprietà privata potrebbe essere considerata un'intrusione.

Purtroppo, ci sono già stati incidenti che hanno coinvolto veicoli che utilizzano una qualche forma di guida autonoma, cosa che spesso può accadere durante i test e le fasi introduttive della nuova tecnologia. Uno di questi incidenti si è verificato quando un veicolo si è scontrato con un pedone che attraversava la strada accompagnando la bicicletta a mano; il veicolo non è stato in grado di riconoscere il pedone dal suo database di oggetti distinti e quindi non ha determinato la necessità di frenare. È chiaro agli sviluppatori di questa tecnologia che identificare semplicemente la posizione degli oggetti non è sufficiente: il veicolo deve anche distinguere quale sia ogni oggetto,

nonché la sua probabile traiettoria. Inoltre, è possibile che il software commetta errori, sia manomesso, sia in condizioni non previste o che ci siano malfunzionamenti nella parte meccanica del veicolo; oppure, che si verifichino circostanze esterne inattese come pedoni distratti o negligenti, condizioni climatiche critiche, animali selvatici.
Il fatto che i veicoli a guida autonoma non siano immuni da incidenti pone importanti problemi civili e penali che devono ancora essere risolti. La possibilità che un veicolo senza conducente sia coinvolto in una situazione di emergenza deve essere anticipata o programmata nel codice del software al fine di rispondere con una modalità di guida appropriata in grado di ridurre al minimo i danni. Si ritiene pertanto che sia possibile progettare e produrre veicoli a guida autonoma che possono causare un minor numero di incidenti con meno danni rispetto alle auto a propulsione umana. Se i veicoli a guida autonoma causassero più incidenti o incidenti più gravi, il loro uso, oltre al fatto che è improbabile che abbiano un processo di omologazione, non sarebbe tollerato, in quanto esporrebbero utenti e case automobilistiche a danni significativi da un punto di vista economico e persino penale.

4.2.2 *Autonomous Driving Forensics*

Sebbene al momento non esista una procedura universale definita per il modo in cui gli investigatori forensi estrarranno i dati da veicoli autonomi, Ross Clarke, ingegnere e investigatore di incidenti stradali dell'ufficio di Hawkins a Londra, ipotizza che l'uso della tecnologia attuale come gli *Event Data Recorder* (EDR) possa essere fondamentale. Gli EDR su alcuni veicoli registrano già informazioni sull'incidente, come la velocità e l'occupazione del veicolo, o l'applicazione dei controlli. La maggior parte dei veicoli moderni in Europa include una qualche forma di EDR: sebbene il suo scopo principale sia quello di fornire al costruttore del veicolo informazioni critiche relative ai sistemi di sicurezza, l'accesso ai dati EDR è generalmente limitato e attualmente è fornito solo agli investigatori forensi volontariamente e da un numero limitato di produttori.
Ross ritiene che per i veicoli autonomi, gli EDR probabilmente svolgeranno le stesse funzioni, ma ci si aspetta che la quantità di informazioni memorizzate in relazione a

ciascun evento di incidente possa aumentare notevolmente.

I veicoli automatizzati attuali sono più vicini al livello 3: automazione condizionale. Questo è un enorme passo in avanti per la tecnologia, in quanto, in questo scenario, il guidatore sarebbe essenzialmente un ripiego piuttosto che il sistema di controllo primario. Le metodologie dell'Informatica Forense possono entrare in gioco per valutare il modo in cui questi veicoli sono stati progettati e costruiti e per verificare la conformità con le specifiche del costruttore.

Esaminare i dati digitali in un ambiente in cui i veicoli sono guidati da sistemi informatici piuttosto che dall'uomo diventa fondamentale in caso di incidente. La valutazione tecnica del sistema di sterzo del veicolo e dei dati raccolti aiuta a determinare tali responsabilità e richiede pertanto l'Informatica Forense per l'elaborazione dei dati digitali pertinenti.

Conclusioni

La tesi in Informatica Forense ha voluto ripercorrere le fasi del trattamento della prova digitale applicate in ambito *automotive*, dimostrando con chiarezza come sia possibile acquisire, analizzare e valutare i dati di un veicolo incidentato indipendentemente dalla gravità del sinistro stradale, purché sia fattibile riassemblare l'automobile a banco ripristinando i collegamenti delle centraline e che sia preservata l'integrità delle memorie interne di queste ultime.

A causa della fragilità dei dati informatici, è fondamentale attuare una metodologia accettabile per garantire l'integrità e l'autenticità delle potenziali evidenze digitali. I componenti chiave che forniscono credibilità nell'indagine sono la metodologia applicata durante il processo e le persone qualificate nell'esecuzione dei compiti specificati.

Un esperto di Informatica Forense ha, inoltre, la necessità di disporre di competenze trasversali in quasi tutti i campi della tecnologia dell'informazione, dai computer ai telefoni cellulari, dalle reti di telecomunicazione ai database, dai linguaggi di programmazione ai *social network*, e così via, per comprendere eventuali prove e sapere dove cercarle. Oltre a tutto questo, c'è l'esigenza di conoscere le procedure di base del diritto penale e civile, nonché gli articoli che regolano la *Digital Forensics* in Italia, come il 359 c.p.p., il 360 c.p.p., e leggi come L. 48/2008.

Gli apparati investigativi, scienziati forensi e operatori del diritto, devono quindi operare sempre più in modo sinergico, mettendo a disposizione del proprio personale figure altamente formate in grado di dare un certo contributo alla gestione di ambienti a elevato contenuto tecnologico.

Bibliografia

[1] Cesare Maioli. «Dar voce alle prove: elementi di informatica forense». In: *La sicurezza preventiva dell'informazione e della comunicazione* (2004), pp. 66–75.

[2] Michele Ferrazzano. *Aspetti metodologici, giuridici e tecnici nel trattamento di reperti informatici nei casi di pedopornografia.* ARACNE, 2018.

[3] *Recovering and Examining Computer Forensic Evidence*. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm.

[4] Giuseppe Vaciago. *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*. Giappichelli, 2012.

[5] *Convenzione di Budapest sui reati informatici.* http://www.unioneconsulenti.it/convenzione-di-budapest-sui-reati-informatici/.

[6] Antonio Gammarota. «Informatica forense e processo penale: la prova digitale tra innovazione normativa e incertezze giurisprudenziali». Tesi di dott. Alma Mater Studiorum – Università di Bologna, 2016.

[7] *La criminalità informatica.* https://www.diritto.it/la-criminalita-informatica/.

[8] Raffaella Brighi, Michele Ferrazzano. «Digital forensics: best practices and perspective». In: *Digital Forensic Evidence: Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (2021), pp. 13–48.

[9] *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.* ISO/IEC 27037:2012.

[10] Michele Ferrazzano. *Dai veicoli a guida umana alle autonomous car*. Giappichelli, 2018.

[11] *Unità di controllo motore*. https://www.quattroruote.it/guide/componenti-auto/centralina-gestione-motore.html.

[12] Craig Smith. *The Car Hacker's Handbook: A Guide for the Penetration Tester*. No Starch Press, 2016.

[13] *Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*. ISO/IEC 27042:2015.

[14] Nhien-An Le-Khac, Daniel Jacobs, John Nijhoff, Karsten Bertens, Kim-Kwang Raymond Choo. «Smart Vehicle Forensics: Challenges and Case Study».

[15] Raffaella Brighi. «Una governance integrata per nuovi modelli dell'informatica forense». In: *I-LEX* (2017), pp. 45–70.

Ringraziamenti

Finalmente, il capitolo più piacevole.

In primo luogo, desidero ringraziare di cuore la prof.ssa Raffaella Brighi, relatrice di questa tesi: sin dai primi giorni di tirocinio mi ha accolta sotto la sua ala e mi ha guidata, sia a livello accademico che personale, come una mentore. Ricorderò questo periodo per sempre.
Un grazie speciale all'Avv. Antonio Gammarota per i suoi preziosi suggerimenti in materia legale e per essere riuscito a insegnare un po' di codice di procedura penale a un'aspirante ingegnera.
Un ringraziamento doveroso va anche al dott. Ulrico Bardari, per aver seguito la tesi e soprattutto l'esperimento, per avermi intrattenuta e ammaliata con i racconti di quando era un giovane poliziotto.
Ringrazio il dott. Michele Ferrazzano e i suoi collaboratori di BIT4LAW per la disponibilità e per avermi mostrato come utilizzare i primi strumenti della disciplina.
Un GRAZIE immenso a Luca Mercuriali. Senza di lui questo progetto non avrebbe mai preso vita.

Vorrei inoltre ringraziare la mia famiglia, per supportarmi moralmente (ed economicamente) in ogni mia decisione, sin da quando ne ho memoria.
Grazie a Federico, l'altra metà della stessa mela marcia, per questi 10 anni di amicizia che spero diventeranno poi 20, e 30, e 100.
Infine, il ringraziamento più caloroso va ad Alberto, per l'amore e l'affetto, per sostenermi sempre incondizionatamente: se ho raggiunto questo traguardo lo devo soltanto a te.