



UNIVERSITÀ
degli STUDI
di CATANIA

CONSULENZA TECNICA

Corso di Digital Forensics 2020/2021

Prof. *Sebastiano Battiato*

Consulente: Dott. Ing. *Calogero Lentini* (1000029092)

Procedimento n° 92/021

INDICE

1.	PREMESSE	1
1.1.	Procedimento.....	1
1.2.	Incidente probatorio	1
1.3.	Nomina perito	1
1.4.	Quesito	1
1.5.	Hardware utilizzato	2
1.6.	Software utilizzati.....	2
1.7.	Modus operandi	4
2.	ACQUISIZIONE.....	5
3.	ANALISI.....	9
3.1.	Verifica integrità.....	9
3.2.	Informazioni tecniche sul filmato	10
3.3.	Descrizione degli eventi e della scena	11
3.4.	Miglioramento del video	16
3.5.	Risultati ottenuti	16
4.	CONCLUSIONI.....	22
5.	ALLEGATI TECNICI	24
6.	REFERENZE BIBLIOGRAFICHE	26
7.	GLOSSARIO.....	27

1. PREMESSE

1.1. Procedimento

Procedimento penale n°92/021 RGNR relativo al furto di un'automobile.

1.2. Incidente probatorio

Il G.I.P. presso il tribunale di Catania, dott. Sebastiano Battiato in data 03/06/2021, emetteva ordinanza di ammissione di incidente probatorio al fine di esaminare le evidenze digitali che riprendono il furto di un autoveicolo, procedendo a perizia diretta ad accertare la dinamica del furto dell'autoveicolo.

1.3. Nomina perito

In data 3 giugno 2021 il sottoscritto, Calogero Lentini, dottore in Ingegneria informatica, nato a Leonforte il 12/07/1998 viene nominato consulente tecnico (CT). Il consulente tecnico designato ha giurato nell'udienza preliminare di giorno 3 giugno 2021.

1.4. Quesito

Nell'udienza di giorno 3 giugno 2021 il quesito formulato al CT è il seguente:

“Facendo riferimento al filmato video 92 il CT proceda all'acquisizione forense del filmato e all'analisi del contenuto; si proceda utilizzando tecniche di

image/video forensics al fine di verificarne l'integrità (ed autenticità) per poi estrarre tutte le informazioni utili per l'individuazione di luoghi, veicoli e eventuali soggetti presenti nella scena. Si ricostruiscano inoltre le dinamiche degli eventi. Riferisca il CT ogni altra circostanza utile ai fini di giustizia. Proceda il consulente a depositare relazione scritta accompagnata da filmati esplicativi e dalle immagini più significative a sostegno delle conclusioni raggiunte."

Si autorizza il CT all'utilizzo di software di terze parti al fine di acquisire ed analizzare le evidenze digitali pervenute.

1.5. Hardware utilizzato

Le componenti hardware utilizzate per eseguire acquisizione e analisi sono le seguenti:

- **Laptop** HP FE4MIQHK;
- **Processore** Intel Core i7-7500U;
- **RAM** 12Gb;
- **Pendrive** 1Gb filesystem FAT.

1.6. Software utilizzati

Sono stati utilizzati i seguenti software di terze parti volti all'acquisizione e all'analisi delle evidenze digitali.

- **Sistema operativo Windows 10 Home, versione: 2004, build: 19041.985.**
- **LegalEye¹**, dal sito web di LegalEye il servizio viene descritto come:
"servizio web per la cristallizzazione delle prove online. Consente di

¹ <https://www.legaleye.cloud/public>

acquisire in maniera semplice, sicura, documentata e legalmente corretta qualsiasi contenuto presente in Rete... Essendo un flusso informatizzato e totalmente automatizzato, sconsiglia il rischio di errore nelle procedure manuali.” Si tratta di un browser virtuale che viene reso disponibile all’utente, consente di navigare per una durata pari a 20 minuti; tutta la navigazione viene registrata e consente di scaricare dati ed effettuare screenshot. Il materiale scaricato e/o screenshottato e la registrazione della navigazione sono marcati temporalmente e resi disponibili all’interno di un archivio cifrato la cui password è a conoscenza solo dell’utente che ha effettuato l’acquisizione. L’utente non ha la necessità di installare alcun software, il tutto può essere svolto online mediante un qualsiasi browser su ogni dispositivo. La navigazione avviene tramite un browser su un’apposita macchina virtuale che viene creata ex-novo ogni qualvolta un utente richieda una nuova acquisizione. Alla fine dell’acquisizione viene, inoltre, reso disponibile un report generato da LegalEye con l’elenco di tutti i file scaricati e/o screenshottati e relativo hash in modo tale da preservare la catena di custodia.

- **Free Make YouTube Downloader²**, sito web che consente il download dei video presenti su YouTube in formato mp4.
- **Amped FIVE³, data di build: 20210415, revisione: 20532**, permette l’enhancement dell’immagine mediante un insieme di filtri consentendo l’analisi su immagini di qualità aumentata e permettendo l’effettuazione di misurazioni. Molto utilizzato in ambito forense, non altera in alcun modo la copia originale, crea alla fine delle procedure di enhancement e/o misurazione un report che elenca e spiega in maniera approfondita ogni filtro utilizzato. Ogni tipo di analisi effettuata mediante Amped FIVE è di tipo ripetibile.

² www.freemake.com/it/free_video_downloader/

³ ampedsoftware.com/it/five

- **HashMyFiles⁴ v.2.38**, software molto leggero che consente il calcolo di svariati tipi di Hash.
- **SunCalc⁵**, servizio online che permette di calcolare i movimenti del sole in un dato giorno e in un dato luogo, si possono, inoltre, ricavare gli orari di alba e tramonto.

1.7. Modus operandi

Il sottoscritto CT subito dopo aver ricevuto l'evidenza digitale consistente nel video caricato sulla piattaforma YouTube intitolato "Reggio Calabria – Furto di auto in diretta nel centro storico (15.10.13)" riconducibile al seguente link <https://www.youtube.com/watch?v=89zzF8Nnlww>, si appresta ad acquisirlo con metodo forense mediante il software LegalEye, dopo aver ottenuto la copia Master dall'archivio cifrato, esegue le opportune copie e ne calcola l'hash. In seguito, analizza il filmato nella sua interezza cercando di ricavarne quanti più dettagli possibili mediante il software Amped FIVE e di ricostruire le dinamiche dell'evento.

Si è operato seguendo le Best Practices stipulate dalla legge n.48 del 18 marzo 2018 che disciplina modalità e limiti dell'attività investigativa, della quale regola i mezzi di ricerca delle prove, allargandone l'oggetto attraverso il riferimento a sistemi informatici o telematici, ed assicurando altresì che per mezzo di tali operazioni sia preservata la conservazione e la non alterabilità dei dati originali.

⁴ hashmyfiles.soft112.com/

⁵ www.suncalc.org

2. ACQUISIZIONE

In seguito all'assegnazione dell'incarico è stata cura dello scrivente CT quella di acquisire in data 03/06/2021, secondo le Best Practices sancite dalla legge n.48 del 18 marzo 2008, le evidenze digitali.

In particolare, il CT ha prelevato il link del filmato⁶ da acquisire dal file "DF – Video da Analizzare.xls" in corrispondenza della riga 92 (ultime due cifre del numero di matricola). Il link in questione porta ad un video sulla piattaforma YouTube⁷, adibita al caricamento e alla fruizione di video caricati da utenti provenienti da tutto il mondo. Il video è denominato "Reggio Calabria – Furto di auto in diretta nel centro storico (15.10.13) ", il canale sul quale risulta essere effettuato il caricamento del suddetto filmato è "Pupia Crime" riconducibile, mediante link presente in descrizione, al sito www.pupia.tv ovvero un sito di informazione che fornisce notizie su svariati temi e avente sede presumibilmente in Campania, infatti, accedendo al sito si può notare una sezione dedicata interamente alla regione Campania.

Il file in esame contiene una ripresa video di una telecamera fissa di videosorveglianza.

Si nota, ad una prima visione, che la piattaforma YouTube consente solo la visualizzazione del filmato senza permetterne il download; si decide di ricorrere allora ad un servizio online, il sopracitato "Free Make YouTube Downloader" che consente, mediante l'utilizzo del link del video, il download dello stesso in formato mp4. Il filmato consiste nella registrazione di una telecamera posta in centro città presumibilmente a Reggio Calabria; non avendo la possibilità di fare l'acquisizione direttamente dal DVR di interesse ci si limita ad acquisire in maniera forense ciò

⁶ <https://www.youtube.com/watch?v=89zzF8Nnlww>

⁷ <https://www.youtube.com/>

che è condiviso sulla piattaforma YouTube. Le informazioni andate perdute a causa del mancato accesso al DVR sono: il CoDec utilizzato per la compressione del video, il clock del sistema, i file di log e la cache.

Il sottoscritto CT per effettuare un'acquisizione legale, marcata temporalmente e preservare i dati garantendo la catena di custodia ha utilizzato il servizio online LegalEye che alla fine del processo di acquisizione genera un archivio cifrato con password a conoscenza solamente dall'utente che ha svolto l'acquisizione.

Si è proceduto dunque alla generazione della macchina virtuale e al successivo utilizzo del browser forniti da LegalEye previa creazione di una password per la cifratura. All'interno del browser è stato scaricato il video mediante il sito web "Free Make YouTube Downloader" cercando di preservare la qualità del filmato, infine viene chiusa la macchina virtuale, risulta essere terminato il processo di acquisizione e viene generato l'archivio cifrato.

L'archivio cifrato contiene:

- Materiale scaricato;
- Screenshots;
- Copia forense acquisizione;
- Video dell'acquisizione;
- Report acquisizione.

I documenti contenuti nell'archivio cifrato e gli allegati num. 4-5-6 possono essere utilizzati a dimostrazione della corretta descrizione dell'acquisizione eseguita dal sottoscritto. Si riportano i controlli dell'infrastruttura LegalEye per dimostrare l'integrità dell'infrastruttura.

CONTROLLO	ORA	RISULTATO
Check iniziale infrastruttura	03/06/2021 110707 UTC+2	OK
Verifica integrità template virtuale	03/06/2021 110501 UTC+2	OK
Accesso al template	03/06/2021 110934 UTC+2	OK
Avvio acquisizione cifrata	03/06/2021 110941 UTC+2	OK

Figura 2.1. Controlli iniziali di integrità.

CONTROLLO	ORA	RISULTATO
Avvio fase di export	03/06/2021 111538 UTC+2	OK
Verifica sicurezza infrastruttura	03/06/2021 111608 UTC+2	OK
Spegnimento template	03/06/2021 112038 UTC+2	OK
Chiusura archivio cifrato	03/06/2021 111845 UTC+2	OK
Cancellazione template	03/06/2021 112142 UTC+2	OK

Figura 2.2. Controlli finali di integrità.

All'interno del report generato da LegalEye, insieme al codice hash di tutti i file presenti nell'archivio, si nota l'hash SHA-256 del video scaricato che risulta essere 1178C6982536753BC832F7C3129CD92B73D619502CC84EB7ECAE7B2B0D878CB9 ed è uguale all'hash SHA-256 del video "Reggio Calabria - Furto di auto in diretta nel centro storico (15.10.13).mp4" presente fra gli allegati. Inoltre il codice hash SHA-256 dell'archivio cifrato contenente l'intera acquisizione è il seguente: 0CCA81126CCFE233796D705D100BA5812057D264E384DB532FF31B043ED8EDF2, anche questo risulta essere uguale a quello presente fra gli allegati.

Si è allora proceduto ad effettuare una copia di: archivio cifrato contenente l'acquisizione, video scaricato, video dell'acquisizione e report prodotto da LegalEye. La copia è stata effettuata sia in locale che su pendrive usb in modo da mantenere intatta la catena di custodia ma anche per effettuare i lavori di analisi non sui file originali ma sulle copie come indicato dalle Best Practices.

Si intende precisare che la pendrive usb è stata precedentemente formattata in modo tale da escludere ogni compromissione dei dati o interazione dall'esterno.

La directory utilizzata su tale pendrive usb viene rinominata:
“consulenza_tecnica_seconda_prova”.

3. ANALISI

3.1. Verifica integrità

Il CT dopo aver terminato l'acquisizione del filmato da YouTube si appresta in primis a verificarne l'integrità. L'unico tipo di analisi a disposizione del CT per verificare l'integrità del filmato è quella visiva vale a dire verificare se siano presenti tagli, artefatti o montaggi.

Si possono notare dal fotogramma 19 al fotogramma 54 (00:00:03.167 – 00:00:09.000) del filmato: "Reggio Calabria - Furto di auto in diretta nel centro storico (15.10.13).mp4" due diciture aventi come contenuto "AUTO DEI LADRI" e "AUTO RUBATA", anche dal fotogramma 862 all'879(00:02:23.666 – 00:02:26.449) si nota la scritta "LADRO 1" e dal fotogramma 1729 al 1746(00:04:48.166 – 00:04:50.999) la dicitura "LADRO 2 LADRO 3". Queste informazioni sono aggiunte in post-produzione per identificare al meglio quale delle due auto è quella rubata e quale è invece quella di cui si servono i ladri per compiere il reato e per distinguere i vari ladri.

L'immagine risulta, inoltre, essere stata tagliata nella parte inferiore in quanto l'orario stampato a video dalla telecamera stessa non è completamente visibile.

Si può dunque affermare con ragionevole certezza che **il filmato non è integro** in quanto editato prima della pubblicazione sulla piattaforma YouTube con un software di editing non specificato.

3.2. Informazioni tecniche sul filmato

Si riportano alcune informazioni sul filmato acquisito ricavate dai metadati EXIF mediante Amped FIVE:

- **Nome file:** “Reggio Calabria - Furto di auto in diretta nel centro storico (15.10.13).mp4”;
- **Formato:** mp4 (Il sito “Free Make YouTube Downloader” permette il download solamente in formato mp4);
- **Codec:** h264;
- **Frame per secondo:** 6;
- **Numero frame:** 3270;
- **Durata:** 00:09:04:997;
- **Dimensione del file in bytes:** 2432100.
- **Larghezza(pixel):** 514;
- **Altezza(pixel):** 360

Sono state trascritte solo le informazioni ritenute più rilevanti, queste e altre informazioni tecniche sono comunque riportate all’interno dell’allegato num.8, ovvero il report creato da Amped FIVE. Nel filmato non è presente alcuna traccia audio.

Si vuole far notare che il download mediante il servizio online “Free Make YouTube Downloader” e la non disponibilità del filmato originale potrebbero aver alterato alcune caratteristiche primitive del filmato.

3.3. Descrizione degli eventi e della scena

La descrizione degli eventi può essere influenzata dalla scarsa qualità delle immagini dovuta alla bassa risoluzione della videocamera e dalla modalità infrarossi attiva per permettere una migliore visione notturna.

Computation path of the sun for:

Reggio Calabria, Reggio di Calabria

15.Oct.2013 12:11 UTC+2 >|<

Solar data for the selected location

Dawn: 06:39:29
 Sunrise: 07:05:45
 Culmination: 12:43:09
 Sunset: 18:19:59
 Dusk: 18:46:13
 Daylight duration: 11h14m14s
 Distance [km]: 149.164.306
 Altitude: 42.65°
 Azimuth: 169.17°
 Shadow length [m]: 1.09
 at an object level [m]: 1

Geodata for the selected location

Height: 39m Set Lat/Lon
 Lat: N 38°6'45.86" 38.11274°
 Lng: E 15°39'6.3" 15.65175°
 UTM: 33S 557135 4218524
 TZ: Europe/Rome DST CEST

Figura 3.1. Pannello di *suncalc.org* ottenuto inserendo come città Reggio Calabria e come data il 15/10/2013.

La data del fatto e il luogo, indicati da coloro che hanno caricato il video sulla piattaforma YouTube, corrispondono rispettivamente al 15/10/2013 e a Reggio Calabria, non è però possibile constatarne la veridicità. Il sottoscritto CT non è a conoscenza di sufficienti dettagli di toponomastica per stabilire, eventualmente, in che via precisa di Reggio Calabria sia avvenuto il reato. Non è possibile stabilire con certezza nemmeno l'orario dell'avvenimento in quanto quello stampato a video dalla telecamera in basso a destra risulta tagliato e di cui comunque non si sarebbe potuto, anche in questo caso, verificare la veridicità. Si può supporre, se il reato è avvenuto a Reggio Calabria in data 15/10/2013, che esso sia avvenuto in un orario compreso tra le 18:46:13 (orario di tramonto calcolato mediante il servizio

online SunCalc.org⁸) e le 06:39:19 (orario di alba calcolato sempre mediante il servizio online SunCalc.org). La strada è comunque trafficata e si possono notare

⁸ <https://www.suncalc.org/#/38.1127,15.6518,11/2013.10.15/12:11/1/3>

alcune persone in fondo all'immagine, quindi si potrebbe supporre che il reato sia avvenuto in un'ora non molto tarda della notte.

Sulla scena si possono notare due file di auto parcheggiate, sulla destra risultano un'auto nera ("AUTO DEI LADRI") inizialmente non identificata con marca e modello e a seguire plausibilmente una Ford C-Max (anno 2007-2010) e una Fiat Punto Evo ("AUTO RUBATA") di colore bianco (anno 2009-2011), le successive auto incolonnate sulla destra non è possibile riconoscerle a causa della scarsa qualità del video. Sulla sinistra si può affermare con ragionevole certezza che vi sia una SMART Fortwo (anno 2007-2014) con quadro strumenti probabilmente attivato desumibile dalla luce del fanale posteriore accesa, le auto incolonnate in fila alla SMART non è possibile riconoscerle con certezza. In fondo all'immagine sulla destra si può notare un forte bagliore dovuto presumibilmente alla luce artificiale di una qualche attività aperta anche durante le ore notturne.



Figura 3.2. Scena iniziale del filmato, si può notare sulla destra il fanale retromarcia attivo nella Fiat Punto Evo e sulla sinistra la SMART Fortwo con luce del fanale posteriore accesa. In fondo a destra si nota il bagliore dovuto probabilmente ad una luce artificiale. fotogramma num. 16.

All'inizio del filmato si nota che la Punto Evo bianca ha la retromarcia inserita(00:00:02.67) in quanto il fanale corrispondente alla retromarcia risulta acceso, si può intravedere un uomo al suo interno infatti, dopo qualche minuto appare scendere dallo stesso(00:02:23.333), viene identificato con la dicitura "LADRO 1", compie un giro attorno al veicolo, apre la portiera lato passeggero e rientra all'interno del veicolo da quel lato, disattiva in qualche modo la retromarcia in quanto il fanale relativo alla retromarcia si spegne, effettua un'accensione di breve durata probabilmente della "segnalazione luminosa di pericolo" o più volgarmente delle "quattro frecce" e scende dal veicolo lasciando i fanali anteriori attivati.



Figura 3.3. Si possono notare le "quattro frecce" attive, fotogramma num. 997.

Mentre l'uomo identificato come "LADRO 1" scende dal veicolo una Fiat Stilo (anno 2002 – 2004) passa a fianco alla Punto Evo bianca (00:02:50.666). L'uomo appena sceso dall'auto si dirige verso la telecamera con fare guardingo e poi si allontana sullo sfondo dove si trova quell'intenso bagliore provocato molto

probabilmente da una luce artificiale. In seguito, un altro uomo (potrebbe essere lo stesso) si avvicina alla Ford C-Max, fa qualche gesto, passa davanti alla Punto Evo bianca e si allontana in fondo. Nel frattempo, passa nella strada una Ford Fiesta (00:04:21.166).

Sulla scena entrano allora due uomini identificati come “LADRO 2” e “LADRO 3” passano davanti la Punto Evo e si allontanano verso il bagliore in fondo all’immagine (00:04:48.666).

Altri due soggetti, probabilmente i due entrati precedentemente in scena (in seguito si procede a verificare se sono le stesse persone di quelle entrate in scena precedentemente), si ricongiungono con un terzo che entra nell’inquadratura (00:06:31.665). I tre sembrano discutere su qualche argomento, la mancanza dell’audio nel filmato non aiuta a capire quale sia l’argomento della discussione.



Figura 3.4. Si possono notare i tre individui discutere, fotogramma num. 2359.

In seguito, uno dei tre apre lo sportello anteriore lato passeggero della Fiat Punto Evo controlla qualcosa e torna a parlare con gli altri due. Dopo un breve colloquio i tre si dividono nuovamente, uno si accomoda nel sedile guidatore dell'auto scura in primo piano, il secondo esce dalla scena mentre il terzo che era colui che aveva controllato qualche istante prima qualcosa all'interno della Punto Evo bianca si dirige prima verso l'auto scura, identificata all'inizio del filmato come "AUTO DEI LADRI", confabula qualcosa con i passeggeri al suo interno, poi va verso la Punto Evo bianca e prende posto dal lato guidatore.

L'auto nera in primo piano viene messa in moto (00:07:25.332), si sposta, rivelandosi essere una Lancia Ypsilon e si ferma subito dietro la Punto Evo bianca. Sulla Punto Evo probabilmente viene schiacciato il pedale del freno in quanto si accendono sia i fanali posteriori di stop che il fanale di stop centrale posto sul lunotto posteriore. La Lancia Ypsilon spinge ripetutamente la Punto Evo bianca (00:08:22.665) fino al momento in cui questa si sposta e riesce ad uscire dallo stallo in cui era parcheggiata ed escono entrambe dalla scena ripresa dalla telecamera.



Figura 3.5. La Lancia Ypsilon spinge la Punto Evo fino a farla partire, fotogramma num. 3173.

3.4. Miglioramento del video

In data 06/06/2021 il sottoscritto CT si appresta ad utilizzare il software Amped FIVE, già ampiamente descritto, per ricavare dei dettagli che a causa della scarsa qualità del video non vengono a prima vista distinti. I filtri maggiormente utilizzati sono “*Super Risoluzione*” utile ad unire un insieme di fotogrammi per migliorare la risoluzione, il “*Filtro mediano*” utilizzato per rimuovere il rumore impulsivo, la “*Blocchettatura*” che riduce gli artefatti da blocchettatura e “*Misurazione 3d*” volta ad eseguire delle misurazioni mediante delle ricostruzioni 3D. Sono stati selezionati alcuni fotogrammi ritenuti fondamentali ai fini dell’indagine. Si riportano di seguito le varie catene prodotte:

- Automobili parcheggiate;
- Individuazione LADRO 1;
- Misurazione altezza LADRO 1;
- Confronto num.1;
- Confronto num.2;
- Identificazione tre uomini;

Tutti i filtri e i parametri utilizzati sono ampiamente documentati nel report di Amped FIVE. Per una più precisa descrizione delle tecniche di miglioramento e misurazione e dei filtri utilizzati nelle varie catene si rimanda al suddetto Report. All’interno dello stesso sono riportati i vari codici Hash SHA-256 relativi alle sei catene così da verificarne l’autenticità.

3.5. Risultati ottenuti

La prima catena, “***Automobili parcheggiate***” tratta il riconoscimento delle automobili in sosta, tramite l’applicazione di alcuni filtri volti ad eliminare il rumore (Filtro Mediano) e ad aumentare la risoluzione (Super Risoluzione) si cerca

di migliorare la qualità del fotogramma 16 in modo tale da riconoscere con più facilità le automobili parcheggiate ed eventualmente provare a ricavarne la targa. Purtroppo, nonostante tutti i filtri applicati non si riesce ad ottenere la targa delle auto in sosta ma si può affermare con ragionevole certezza di che marca e modello siano le auto parcheggiate.



Figura 3.6. Confronto fra input e output, catena "Automobili parcheggiate", fotogramma num.16.

Le auto parcheggiate sembrano essere sulla destra una Ford C-Max ed in seguito una Fiat Punto Evo bianca, mentre sulla sinistra è presente una SMART Fortwo. L'analisi di questo fotogramma conferma quanto già detto precedentemente nel paragrafo 3.3. I tratti distintivi delle auto come fari posteriori, posizione della targa e carrozzeria posteriore sembrano coincidere con quelli delle foto riportate di seguito



Figura 3.7. Ford C-Max.



Figura 3.8. Fiat Punto Evo.



Figura 3.9. SMART Fortwo.

Seguendo la stessa linea si è deciso di procedere per il fotogramma 1111 cercando di individuare la persona identificata con la dicitura “LADRO 1”. Nella seconda catena, “**Individuazione LADRO 1**”, sono stati applicati dei filtri per rimuovere il rumore (Filtro Mediano), rimuovere la blocchettatura ed aumentare la risoluzione (Super Risoluzione). La qualità è aumentata ma non è possibile ottenere i dettagli del volto. Si arriva alla conclusione che il cosiddetto “LADRO 1” è un uomo dalla corporatura robusta che presumibilmente al momento del furto indossava un paio di jeans, un giubbotto aperto nella zona del collo e un paio di scarpe scure.



Figura 3.10. Confronto fra input e output, catena "Individuazione LADRO 1", fotogramma num.1111.

Nella catena “**Misurazione altezza LADRO 1**” si procede con la misurazione dell’altezza dello stesso soggetto mediante il filtro “*Misurazione 3d*”, nel fotogramma num. 1130 si usa come riferimento l’altezza della Ford C-Max (anno 2010) che da ricerche sul sito della casa madre Ford risulta essere pari a 159,5 cm. Alla fine delle procedure di misurazione e dell’acquisizione dei tre assi si è arrivati alla conclusione che l’altezza del soggetto identificato con la dicitura “LADRO 1” potrebbe essere pari a 183,4 cm con un errore di misura pari a 7,15 cm. Si riportano le misurazioni effettuate.



Figura 3.11. Misurazione altezza LADRO 1, fotogramma num. 1130.

Si è in seguito proceduto con l’analisi del fotogramma numero 1447 dove si vede un uomo camminare verso la Fiat Punto Evo bianca, si prova a verificare se questi corrisponda all’uomo identificato precedentemente con la dicitura “LADRO 1”. La bassa qualità del filmato e la lontananza dalla camera, nonostante tutti i tentativi di miglioramento tramite rimozione del rumore e Super Risoluzione, non danno certezza del fatto che siano la stessa persona però si nota che anche quest’uomo

sembra essere di corporatura robusta ed avere il giubbotto aperto nella zona del collo, cosa che potrebbe portare alla conferma della corrispondenza fra i due.



Figura 3.12. Uomo di fianco alla Fiat Punto Evo, fotogramma num. 1447.

Si sono confrontati gli uomini identificati con la didascalia “LADRI 2-3” nel fotogramma 1735 con quelli che provengono dal fondo della scena nel fotogramma 2349, data anche qui la bassa qualità delle immagini non si può affermare con certezza che le due persone presenti nel fotogramma 1735 siano le stesse di quelle del fotogramma 2349. Si è attuato un miglioramento della risoluzione (Super Risoluzione), una pulizia dal rumore (Filtro mediano) e in quella a destra un aumento della luminosità. L’unico elemento che salta all’occhio è il piumino indossato da uno dei due uomini nel fotogramma a sinistra che sembra essere indossato anche da uno degli uomini nel fotogramma a destra, ma questo non certifica che la coppia di uomini sia la stessa sia nel fotogramma a destra che in quello a sinistra.



Figura 3.14. Fotogramma num. 1735.



Figura 3.13. Fotogramma num. 2349.

Si prova, infine, nella catena “**Identificazione tre uomini**” ad ottenere dei dettagli dal fotogramma 2358 che possano essere significativi ai fini dell’indagine a proposito dei tre uomini che discutono sul marciapiede. Nonostante i vari miglioramenti applicati non si ottengono dettagli ai fini dell’identificazione, né inerenti all’abbigliamento. L’unica affermazione che può essere fatta è che ogni uomo sembri portare un giubbotto.



Figura 3.15. Fotogramma num. 2358.

4. CONCLUSIONI

In data 03/06/2021 il sottoscritto Calogero Lentini veniva nominato consulente tecnico con l'incarico di rispondere al quesito presente nel paragrafo 1.1.3.

In sintesi, veniva fornito al CT un link che rimanda ad un video intitolato "Reggio Calabria - Furto di auto in diretta nel centro storico (15.10.13)"⁹ caricato sul canale "Pupia crime" sulla piattaforma YouTube, al CT non è stato reso possibile acquisire il video dalla fonte originale e non riceveva nessun'altra informazione riguardante il filmato.

Si procedeva, sempre in data 03/06/2021, mediante l'infrastruttura LegalEye, ad acquisire, secondo le best practices di settore, il filmato. YouTube non consente di scaricare i contenuti presenti sulla sua piattaforma quindi all'interno del browser creato da LegalEye si è optato per il download tramite il sito "Free Make YouTube Downloader". Il filmato acquisito, così come quello presente sulla piattaforma, risulta di bassa qualità e con un basso frame rate. Dal momento dell'acquisizione è stata sempre preservata la catena di custodia.

Il CT non ha potuto acquisire il filmato dal DVR originale quindi la verifica dell'integrità si è basata su dei parametri prettamente visivi. Si sono notate in primis delle diciture come, ad esempio, "AUTO LADRI" o "AUTO RUBATA" aggiunte in post-produzione mediante dei software di editing ed inoltre il filmato risulta tagliato nella parte inferiore in quanto non è possibile leggere per intero l'orario stampato a video dalla telecamera. Si è dunque arrivati alla conclusione che il filmato non è integro.

Il video, come già affermato, riprende presumibilmente una strada della città di Reggio Calabria durante le ore notturne. La risoluzione della telecamera, la

⁹ <https://www.youtube.com/watch?v=89zzF8Nnlww>

modalità infrarossi attiva e il basso frame rate fanno sì che la qualità del video sia veramente pessima, si è però riusciti a ricostruire la dinamica degli eventi.

La telecamera riprende tre uomini identificati con la dicitura “LADRO 1”, “LADRO 2” e “LADRO 3” che riescono in nove minuti circa ad appropriarsi di una Fiat Punto Evo di colore bianco. I ladri dopo alcune verifiche all’interno dell’auto da rubare, nella quale erano già riusciti ad entrare, e dopo alcuni colloqui fra di loro decidevano di portare via l’auto spingendola letteralmente fuori dallo stallo in cui era parcheggiata mediante l’ausilio di un’altra vettura.

Le fasi di analisi mediante il software Amped FIVE hanno apportato delle migliorie nella qualità delle immagini, hanno permesso il riconoscimento di alcune auto in sosta, la misurazione dell’altezza e la descrizione della corporatura e del vestiario dell’uomo indicato con “LADRO 1” ma non hanno permesso in alcun modo l’identificazione dei volti dei tre soggetti apparsi in seguito.

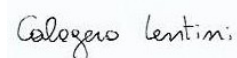
In conclusione, il consulente non è potuto risalire con certezza alla data, all’orario e al luogo. La data e il luogo indicati nel titolo sono 15/10/2013 e Reggio Calabria ma non si può constatarne la veridicità, per quanto riguarda l’orario si può invece affermare che il reato, se commesso a Reggio Calabria il 15/10/2013, sia avvenuto fra le 18:46:13 e le 06:39:19 ma non si riesce ad ottenere un range più contenuto.

Il lavoro del consulente tecnico risulta dunque terminato in data 09/06/2021.

Catania, lì 9 giugno 2021

Il consulente

Dott. Ing. Calogero Lentini



5. ALLEGATI TECNICI

La presente relazione tecnica si compone di num. 30 (trenta) pagine e di num. 8 (otto) allegati. Mediante il software “Hash my files” si è proceduto a calcolare i codici hash dei seguenti allegati.

Num.	Nome file / cartella	Descrizione	Hash SHA-256
1	Analisi_video_Reggio_Calabria.afp	Progetto Amped FIVE	826C48071C5C6 162AE992C62F0 1C79CAB15C567 929EBCFFAB6BF 64E755CB0C37
2	CVCalogeroLentini.pdf	CV del consulente tecnico	AEBF99C3616D2 A6CC89C193662 9EAA29019C8D4 0DE24524812EA 48E2F3513E87
3	istantanee.zip	File zip delle istantanee prodotte	0D71A1E9F1174 99B5B417A252D E76A07E623577 FF84B03706746 F190F0D06E7C
4	legaleye_copiaforense_reggio-calabria-.7z	Copia forense archivio LegalEye	0CCA81126CCFE 233796D705D10 0BA5812057D26 4E384DB532FF3 1B043ED8EDF2

5	legaleye_report_acquisizione_reggio-calabria-.pdf	Report in pdf prodotto da LegalEye	4E80A682B5524 3D2D77C30183F 86418296CA341 17B34104ADF25 5E7B63F9139F
6	legaleye_video_reggio-calabria-.mp4	Video intera acquisizione in LegalEye	14A5A98D6EB26 88F16EB92D107 DC30C1A022A1B 7756F0B605315 2707FB692044
7	Reggio Calabria - Furto di auto in diretta nel centro storico (15.10.13).mp4	Video scaricato mediante LegalEye	1178C69825367 53BC832F7C312 9CD92B73D6195 02CC84EB7ECAE 7B2B0D878CB9
8	report- Analisi_video_Reggio_Calabria.zip	Report prodotto da Amped FIVE	0A1C2272A5B2C 6AEA0DF18B6B6 81E9CAADF209F 71C29C5E9EB95 71024D1F762F

6. REFERENZE BIBLIOGRAFICHE

Si indicano i link ai documenti riguardanti le best practices di settore:

- 1) <https://www.parlamento.it/parlam/leggi/08048l.htm>
- 2) https://www.s-five.eu/sftp/BPM/DRAFT_BPM_FIVE_20151208.doc
- 3) <https://enfsi.eu/wp-content/uploads/2021/05/MP2018-WP5-BPM-GSR-DRAFT-for-Expert-Review.pdf>
- 4) <http://enfsi.eu/wp-content/uploads/2017/06/Best-Practice-Manual-for-Forensic-Image-and-Video-Enhancement.pdf>
- 5) http://enfsi.eu/wp-content/uploads/2016/09/1_forensic_examination_of_digital_technology_0.pdf

7. GLOSSARIO

- 1) **Codice Hash:** La **funzione di hash** o **funzione hash** produce una sequenza di bit, detta digest, (o una stringa) strettamente correlata con i dati in ingresso. La lunghezza dei valori di hash varia a seconda degli algoritmi utilizzati. Il valore più comunemente adottato è di 128 bit, che offre una buona affidabilità in uno spazio relativamente ridotto. Tuttavia, va registrata la possibilità d'uso di hash di dimensione maggiore (SHA, ad esempio, può anche fornire stringhe di 224, 256, 384 e 512 bit) e minore (che però è fortemente sconsigliato). Le funzioni hash svolgono un ruolo essenziale nella crittografia: sono utili per verificare l'integrità di un messaggio, poiché l'esecuzione dell'algoritmo su un testo anche minimamente modificato fornisce un *message digest* completamente differente rispetto a quello calcolato sul testo originale, rivelando la tentata modifica.

Fonte: Wikipedia.org.¹⁰

- 2) **Best practices:** Insieme delle attività (procedure, comportamenti, abitudini ecc.) che, organizzate in modo sistematico, possono essere prese come riferimento e riprodotte per favorire il raggiungimento dei risultati migliori in ambito aziendale, ingegneristico, sanitario, educativo, governativo e così via.

Fonte: Treccani.it.¹¹

- 3) **Macchina virtuale:** In informatica il termine **macchina virtuale (VM)** indica un software che, attraverso un processo di virtualizzazione, crea un ambiente virtuale che emula tipicamente il comportamento di una macchina fisica (PC, client o server) grazie all'assegnazione di risorse

¹⁰ https://it.wikipedia.org/wiki/Funzione_di_hash

¹¹ https://www.treccani.it/enciclopedia/migliore-pratica-tecnica-della_%28Dizionario-di-Economia-e-Finanza%29/

hardware (porzioni di disco rigido, RAM e risorse di processamento) ed in cui alcune applicazioni possono essere eseguite come se interagissero con tale macchina; infatti se dovesse andare fuori uso il sistema operativo che gira sulla macchina virtuale, il sistema di base non ne risentirebbe affatto.

Fonte: Wikipedia.org.¹²

- 4) **DVR digitale**: Un videoregistratore digitale, detto anche in inglese digital video recorder (DVR) o personal video recorder (PVR) è un tipo di dispositivo elettronico che consente di programmare la registrazione automatica.

Fonte: Wikipedia.org.¹³

¹² https://it.wikipedia.org/wiki/Macchina_virtuale

¹³ https://it.wikipedia.org/wiki/Videoregistratore_digitale