



Università di Catania

Relazione di Consulenza Tecnica

Procedimento n. 4438/24

Committenti: Sebastiano Battiato e Luca Guarnera

Consulente Tecnico:

Mirko Ignazio Paolo Morana

Matricola: 1000034021

Sommario

1. Estremi del procedimento e Ruoli	2
1.1 Incidente Probatorio.....	2
1.2 Nomina perito	2
1.1 Oggetto Incarico e Quesiti	2
2. Premesse Tecniche e Metodologia di Lavoro.....	3
2.1 Hardware Utilizzato e S.O.	3
2.2 Software Utilizzati	3
2.3 Acquisizione	4
2.4 Integrità	5
2.5 Metodologie applicate.....	5
3. Analisi Tecnica	8
3.1 Analisi di integrità e autenticità del filmato	8
3.2 Individuazione dei fotogrammi rilevanti e ricostruzione degli eventi.....	9
3.3 Tentativo numero 1 di riconoscimento dei sospettati.....	11
3.4 Tentativo numero 2 di riconoscimento dei sospettati.....	13
3.5 Tentativo numero 3 di riconoscimento	15
4. Conclusioni	16
5. Allegati Tecnici	19
6. Referenze Bibliografiche	20
7. Glossario	21

1. Estremi del procedimento e Ruoli

1.1 Incidente Probatorio

Il Committente, in data 20 giugno 2024 emetteva ordinanza di ammissione di incidente probatorio al fine di esaminare le evidenze digitali che riprendono tre individui che in maniera concitata e usando un piede di porco e un martello tentano di aprire una cassaforte da parete, fino a quando non riescono nell'intento di aprirla per rubarne il contenuto.

1.2 Nomina perito

Il sottoscritto Morana Mirko Ignazio Paolo, (Matricola:1000034021) Studente di Informatica all'università di Catania, nato a Catania il 04/07/1994 e domiciliato ai fini del presente procedimento presso il Dipartimento di Matematica e Informatica dell'Università di Catania, viale Andrea Doria n°6 Ingresso Ovest via Santa Sofia n° 64, in data 20 giugno 2024 alle ore 10:35 veniva nominato, dal Prof. Sebastiano Battiato, consulente tecnico nel procedimento 4438/24.

1.1 Oggetto Incarico e Quesiti

“Facendo riferimento al filmato video 10 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 ed 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.”



2. Premesse Tecniche e Metodologia di Lavoro

2.1 Hardware Utilizzato e S.O.

Sistema Operativo: Windows 11 Pro, 64 bit, Versione 23H2, build 22631.3737

Processore: AMD Ryzen 5 5600G

Storage1: Crucial P3 Plus 500GB

Storage2: Seagate Barracuda 7200 RMP 2TB

MOBO: Asus TUF Gaming B550-Plus, Socket AM4

Tipologia di RAM: G. Skill Trident Z NEO 3200 MHz

Quantità di RAM: 2x16GB

Scheda Video: AMD Radeon RX Vega 7 (Integrata del Processore)

Storage per la consegna degli allegati: Transcend JetFlash V30 1GB USB2.0

2.2 Software Utilizzati

FAW - Forensic Acquisition Of Web Site: software utilizzato, nella la versione 11.5.10.0, per la navigazione del sito web fornito dal G.I.P. e l'individuazione del filmato, successivamente è stato utilizzato per la cristallizzazione della suddetta pagina web.

(<https://en.fawproject.com/>)

MultiHasher: software utilizzato, nella versione 2.8.2.0 compilata in data 29/02/2016, per il calcolo di diverse funzioni HASH.

(<https://www.abelhadigital.com/multihasher/>)

aTube Catcher: software utilizzato, nella versione 3.8.9991, per effettuare l'acquisizione del filmato da internet in formato originale, quindi senza conversioni.

(<https://www.atube.me/>)

AmpedFIVE: software utilizzato, nella versione con Data Build 20230511 e Revisione 28912, per effettuare l'analisi ed il miglioramento del filmato.

(<https://ampedsoftware.com/it/five>)

FTK Imager: software utilizzato, nella versione 4.7.1.2, per effettuare la copia bit-a-bit del filmato originale.

(<https://www.exterro.com/digital-forensics-software/ftk-imager>)

Wireshark: software utilizzato, nella versione Version 4.2.5, per effettuare la scansione del traffico dei pacchetti in entrata ed uscita dal computer.

(<https://www.wireshark.org/>)



2.3 Acquisizione

In data 20 giugno 2024, viene assegnata da parte del committente l'evidenza digitale, questa è fruibile sulla piattaforma YouTube all'indirizzo:

<https://www.youtube.com/watch?v=bfbL5I0SiEk>

Il filmato è stato caricato sulla piattaforma dall'utente:

- Nome Utente sulla piattaforma: Gabriele Vignolini

tramite una request http effettuata tramite script in python "richiesta_UniqueID_YT.py" abbiamo rilevato il codice univoco identificativo dell'utente:

- Codice Univoco dell'utente: UCDDdODjv6Vw6KcrQ9gDPRQYw

Dall'URL che ci reindirizza al filmato abbiamo recuperato il codice identificativo del filmato :

- Codice Univoco del filmato: bfbL5I0SiEk

Il processo di acquisizione del filmato ha avuto inizio in data 22 giugno 2024 tramite la registrazione dello schermo. Le principali fasi dell'acquisizione, visibili nella registrazione presente all'interno del file denominato "AcquisizioneSchermo.mp4" sono le seguenti:

- Avvio del registratore schermo
- Avvio di Wireshark
- Controllo orario di Inizio acquisizione, 08:40:00(hh:mm:ss) del 22 giugno 2024 (Fig. 1)
- Apertura della piattaforma Microsoft Teams
- Apertura e consultazione file "Il Prova in itinere_finale_CT2024.pdf"
- apertura e consultazione file "DF - Video da Analizzare 2024.xlsx"
- Ricerca della mia matricola che corrisponde con la riga numero 10
- Apertura del browser FAW
- Cristallizzazione della pagina internet di riferimento tramite FAW, i file che vengono prodotti vengono spostati nella cartella degli "Allegati" presenti dentro la cartella "Relazione Tecnica" che si trova sul desktop
- Visualizzazione del filmato
- Scaricamento del filmato senza modifiche tramite aTubeCatcher e salvataggio sotto il nome di "Furto 10072009 cassaforte rotta.mp4", il filmato presenta le seguenti caratteristiche tecniche: (Fig. 2)
 - Formato: mp4
 - Codice: h264
 - Dimensione: 5.823.265 byte
 - Risoluzione in pixel: 480x360
 - FPS: 25
 - Durata(hh:mm:ss: SSS): 00:02:56:494



- Confronto del filmato presente sulla piattaforma YouTube e quello presente sul computer.
- Creazione copia bit-a-bit del filmato (Fig. 3)
- Calcolo degli HASH dei file finora prodotti (Fig. 4)
- Richiesta HTTP tramite script python per arrivare al codice univoco dell'utente.
- Salvataggio del file .npcap di Wireshark come report del traffico di rete e suo calcolo dell'HASH
- Controllo Orario di Fine Acquisizione, 08:52:00(hh:mm:ss) del 22 giugno 2024 (Fig. 5)
- Registrazione fermata, denominata "AcquisizioneSchermo.mp4". Viene salvata nella sottocartella "Allegati" della cartella presente sul desktop denominata "Relazione tecnica". Denominato "AcquisizioneSchermo.mp4"
- Calcolo dei vari codici HASH, in maniera tale da cristallizzare l'integrità dei file, così se soggetti a successive modifiche vengono subito scoperte.

2.4 Integrità

Il calcolo del codice degli HASH effettuato su tutti i file permette di garantire la loro integrità, in quanto se, a seguito di modifiche al file, anche non attese, qualora si ricalcolasse il codice HASH, quest'ultimo risulterebbe differente

2.5 Metodologie applicate

Le operazioni di acquisizione, conservazione e analisi delle evidenze digitali sono state effettuate con l'obiettivo di preservare la loro integrità e favorire la ripetibilità delle operazioni, tenendo in considerazione e applicando i principi e le best practice della Digital Forensics. Si sono seguite le seguenti linee guida ISO:

- ISO-27037 per l'identificazione, l'acquisizione e la preservazione delle evidenze.
- ISO-27041 per l'analisi e l'interpretazione delle evidenze

Le operazioni di Acquisizione del filmato sono state effettuate tenendo aperto il software Wireshark per l'acquisizione dei pacchetti in entrata ed in uscita dal computer utilizzato.

Le operazioni di Analisi Tecnica sono state effettuate sul file "**Furto 10072009 cassaforte(Copia).mp4**". Questo file è una copia bit-a-bit del filmato originale creata con FTK Imager. Confrontando i codici HASH dei due filmati, nell'allegato "TabellaHASH.xlsx"



notiamo che digest del filmato originale e della copia combaciano, quindi possiamo affermare che la copia bit-a-bit è avvenuta correttamente.

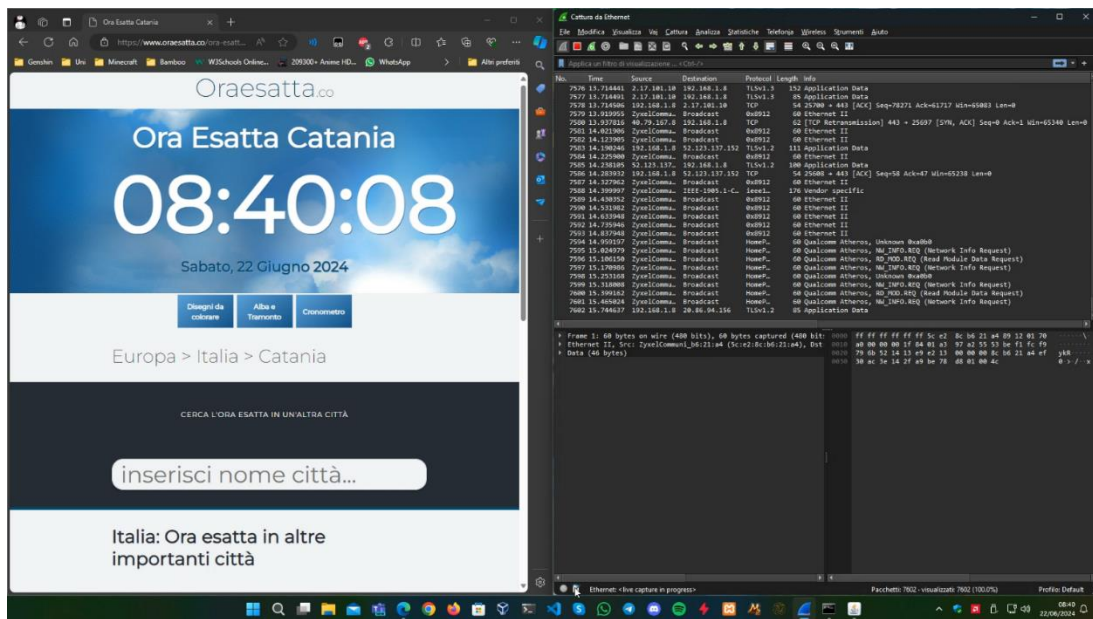


Figura 1: Ora Inizio Acquisizione e Wireshark

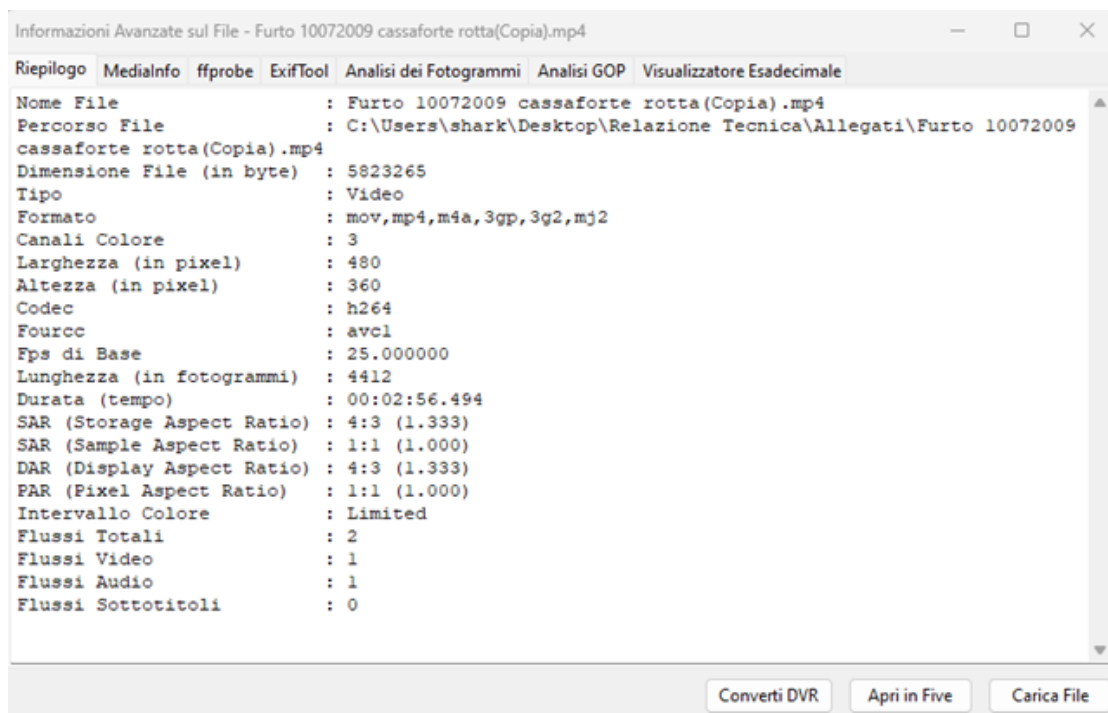


Figura 2: Caratteristiche Filmato

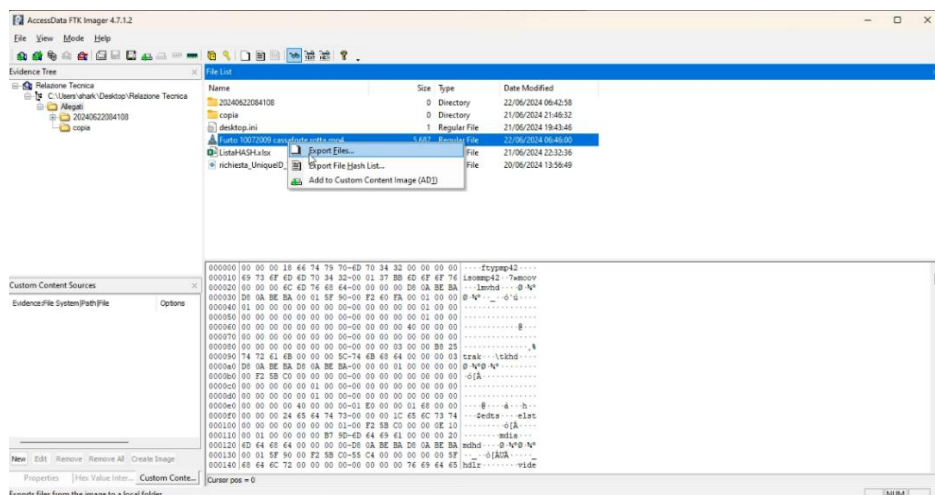


Figura 3: Clonazione del Filmato

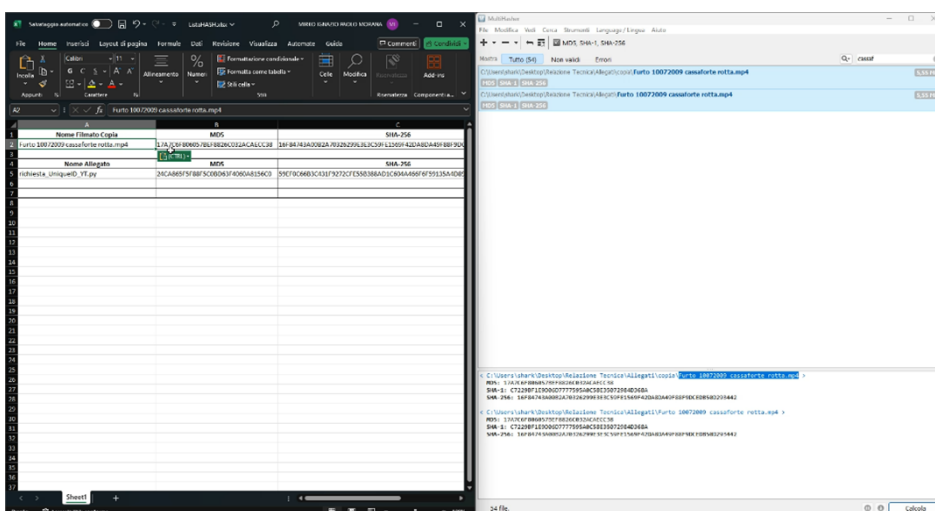


Figura 4: Calcolo degli HASH

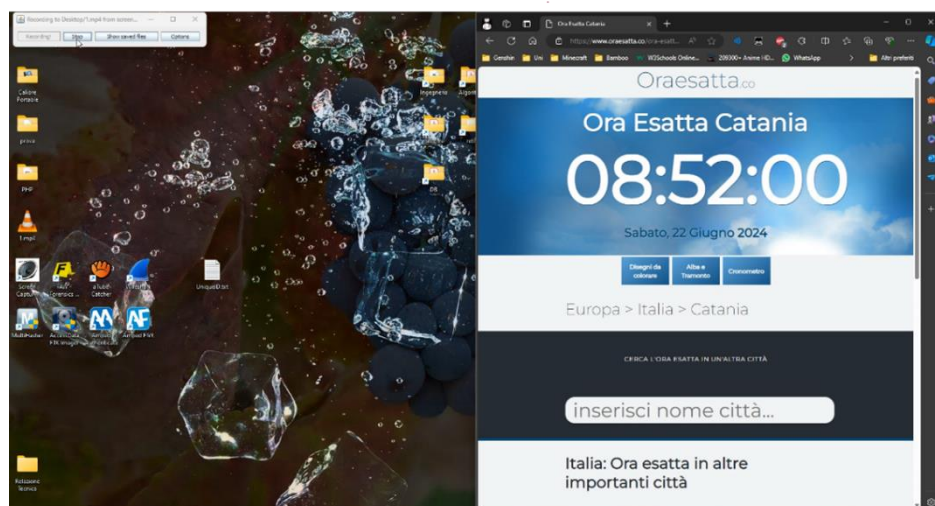


Figura 5: Fine Acquisizione

[Handwritten signature]

3. Analisi Tecnica

In data 20 giugno 2024 alle ore 17:36 il CT inizia ad analizzare il filmato fornito dal committente.

La fase di analisi è stata effettuata tramite l'ausilio del software Amped FIVE, il primo passaggio da effettuare è quello di aprire le "Informazioni Avanzate sul File" (Fig. 2) direttamente dal software, in questa maniera andremo a raccogliere ulteriori dettagli tecnici sul filmato. Altri dettagli quali dati Exif, MediaInfo e ffprobe sono consultabili tra gli allegati per conoscere i permessi del file, la creazione del file sulla piattaforma ed altre informazioni tecniche. Durante tutto il processo di analisi sono state create una serie di catene di filtri per l'analisi selettiva dei singoli sospettati.

3.1 Analisi di integrità e autenticità del filmato

Il CT dopo aver terminato la fase di acquisizione del filmato dalla piattaforma YouTube si appresta a verificare l'integrità e l'autenticità, al fine di rispondere alla prima parte del quesito tecnico.

L'unica informazione fornita dal committente è un link alla piattaforma YouTube, NON si hanno informazioni riguardo il sistema di videosorveglianza.

Considerando che il filmato è stato caricato sulla piattaforma YouTube, possiamo già affermare che il filmato non sia integro, in quanto la suddetta piattaforma in fase di caricamento modifica i codec originali del video con quelli di suo gradimento, che solitamente sono i codec h264. Questo codec applica una codifica di tipo Lossy, per tanto ci saranno perdita di informazioni rispetto al filmato originale del circuito di videosorveglianza.

Possiamo dunque affermare che il filmato risulta NON essere integro.

Per quanto riguarda l'autenticità, possiamo notare che il video non presenta manipolazioni, in quanto è presente anche la data e l'ora in cui il circuito di videosorveglianza ha ripreso l'accaduto e possiamo notare che non ci siano salti nel tempo trascorso nella registrazione, oltre che il filmato sembra rappresentare coerentemente le varie fasi del furto.

Pertanto, possiamo affermare che il filmato mostri in maniera autentica le varie fasi del reato, ribadendo però come il filmato in sé non sia integro.

3.2 Individuazione dei fotogrammi rilevanti e ricostruzione degli eventi

Dal video “**Furto 10072009 cassaforte(Copia).mp4**”, nonostante la bassa risoluzione, è stato possibile ricostruire come sia avvenuto il furto. Tre individui maschi sono entrati in quello che per l’arredo sembra essere un ufficio(Fig. 6), nel filmato sono le 03:58:38 del mattino di giorno 10 luglio 2009, inizialmente era solo un individuo che ha spostato il tavolo(Fig. 7). Successivamente ad un’analisi del canale YouTube(Fig. 8) possiamo notare che l’utente “Gabriele Vignolini”, oltre a pubblicare filmati che non sono rilevanti per le nostre indagini, ha pubblicato più volte furti avvenuti in un paesino in provincia di Firenze quindi possiamo presumere che anche questa volta siamo in provincia di Firenze. Una volta dentro, i tre individui hanno fatto diversi tentativi di scasso della cassaforte, nei primi istanti usavano solo una mazza con testa in ferro da 5Kg (Fig. 7), successivamente hanno introdotto anche un piede di porco sulla scena(Fig. 9, Fig. 10, Fig. 11), i colpi alla cassaforte sono stati inferti fin quando questa non ha ceduto rompendosi, infine, sono riusciti a impossessarsi della refurtiva(Fig. 12), un oggetto che sembra una valigetta nera e dei fogli(Fig. 13, Fig. 14) scappando via.



Figura 6: Frame 0 Interno dell'Ufficio



Figura 7: Spostamento del Tavolo

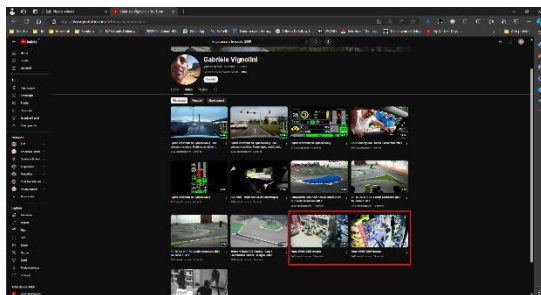


Figura 8: Canale YT



Figura 9: Assenza Piede di Porco

A handwritten signature or scribble in black ink, consisting of several overlapping loops and lines.



Figura 10: Introduzione del piede di porco



Figura 11: Dettaglio Piede di Porco



Figura 12: Cassaforte Aperta



Figura 13: Valigetta Nera



Figura 14: Fogli

3.3 Tentativo numero 1 di riconoscimento dei sospettati

Come primo tentativo di riconoscimento tenteremo di trovare qualche informazione sul tipo di forma della testa, orecchie, attaccatura dei capelli, Naso. Questo nel tentativo di effettuare un identikit facciale. Abbiamo preso in considerazione il frame 749(Fig. 15) ed il frame 2342(Fig. 16). Sono stati applicati quattro filtri di deblocking e quattro maschere di contrasto differenti per migliorare i bordi delle teste (Fig. 17 e Fig. 18). Infine, di questo frame migliorato abbiamo creato una copia bit-a-bit in maniera da assegnare ad ogni sospettato un numero di riconoscimento(Fig. 19)

Dai frame 749 e 2342 frame possiamo descrivere i seguenti aspetti dei sospettati :

Soggetto numero 1: presenta una conformazione della testa con occipite sporgente ed un Trichion Largo. Carnagione della pelle chiara olivastra.

Soggetto numero 2: presenta una conformazione della testa con vertice posteriore, non abbiamo informazioni se il sospettato ha il Trichion oppure no e del tipo di attaccatura di capelli che dovrebbe avere in quanto porta un passa montagna o comunque qualcosa che ne copre il capo. Vista la scarsa qualità dell'apparecchiatura di videosorveglianza e visto che il soggetto indossa quello che sembra un passa montagna non si riescono ad ottenere informazioni in merito alla sua carnagione

Soggetto numero 3: presenta la conformazione della testa detta testa di fronte curva, anche qui non abbiamo informazioni sull'attaccatura di capelli e l'eventuale Trichion. Carnagione della pelle chiara olivastra.



Figura 15: Frame di Riferimento 749



Figura 16: Frame di Riferimento 2342



Figura 17: Miglioramento bordi teste riferimento Frame 749



Figura 18: Miglioramento bordi della teste riferimento Frame 2342



Figura 19: Identificazione individui

A handwritten signature or mark, possibly a stylized 'A' or a similar symbol, located in the bottom right corner of the page.

3.4 Tentativo numero 2 di riconoscimento dei sospettati

In questo secondo tentativo proveremo un altro approccio, cercheremo di stimare l'altezza per ognuno dei tre sospettati, come riferimenti prenderemo la distanza che abbiamo con la maniglia della porta ed il suolo, solitamente sono misure standard, nello specifico per le porte da interno la maniglia si assesta a 90 cm dal pavimento.

Prenderemo in considerazione il frame 321 (Fig. 20), per stimare l'altezza del Sospettato numero 1, mentre per il sospettato numero 2 prenderemo in considerazione il frame 341 (Fig. 21) e per il terzo sospettato prenderemo in considerazione il frame 890 (Fig. 22).



Figura 20: Frame 3103



Figura 21: Frame 341



Figura 22: Frame 890

Da questi tre frame, tramite la misurazione 3D del software AmpedFIVE dopo aver tracciato le traiettorie, che servono a regolare la scena, possiamo stimare delle misure, nel nostro caso abbiamo stimato le altezze dei sospettati:

Soggetto numero 1: è un maschio, dall'analisi visiva del video sembra combaciare con un somatotipo Ectomorfo, ha una carnagione che sembra tendere al bianco/olivastra, tramite misurazione 3D abbiamo stimato un'altezza approssimativa di $169,56 \text{ cm} \pm 1,95 \text{ cm}$. (Fig. 23).

Soggetto numero 2: è un maschio, dall'analisi visiva del video sembra combaciare con una corporatura di tipo Endomorfo, ha una carnagione che sembra tendere all'olivastra,

tramite misurazione 3D abbiamo stimato un'altezza approssimativa di 156,56 cm \pm 2,77 cm.(Fig. 24).

Soggetto numero 3: è un maschio, dall'analisi visiva del video sembra combaciare con una corporatura di tipo Endomorfo, ha una carnagione che sembra tendere al bianco, tramite misurazione 3D abbiamo stimato un'altezza approssimativa di 164,51 cm \pm 2,06 cm(Fig. 25).



Figura 23: Altezza Sospettato 1

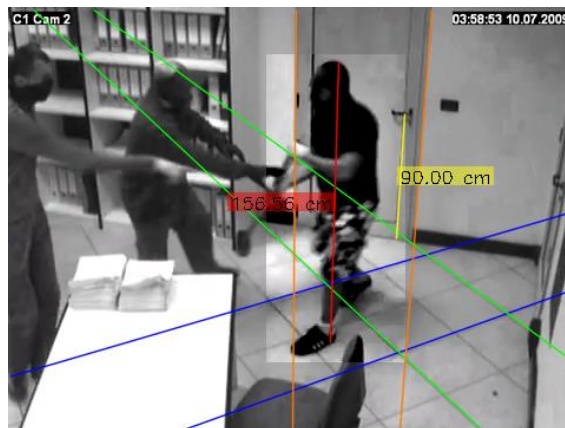


Figura 24: Altezza Sospettato 2



Figura 25: Altezza Sospettato 3

3.5 Tentativo numero 3 di riconoscimento dei sospettati

In questo terzo tentativo tenteremo di migliorare i volti, delimitare meglio il viso e cercheremo di ricavare qualche informazione in più rispetto a quelle che possiamo avere guardando il video, o rispetto a quelle prese nel primo tentativo per questo tentativo sono stati utilizzati i frame 1877(Fig. 26) e 2261(Fig. 27), il primo servirà per controllare i volti del sospettato 1 e 2, il secondo per cercare di recepire qualcosa in più sul Sospettato 3. È stato applicato un filtro di deblocking localmente intorno alle teste dei sospettati, successivamente è stata applicata una maschera di contrasto per mettere in risalto eventuali contorni degli occhi e della faccia, come possiamo notare nelle Fig. 28, Fig.29 per fattori di scarsa qualità del video originale sembra che l'applicazione dei filtri abbia addirittura peggiorato la situazione, abbiamo inoltre ritagliato(Fig. 30, Fig. 31, Fig. 32) la porzione di frame e applicato dello zoom sperando di ricavare qualche informazione in più ma per problemi di bassa qualità questo tentativo non ha portato a nulla di nuovo.



Figura 26:Frame 1877



Figura 27: Frame 2261



Figura 28: Miglioramento Frame 1187



Figura 29: Miglioramento Frame 2261



Figura 30: Primo piano Sospetto 1



Figura 31: Primo piano Sospetto 2



Figura 32: Primo piano Sospetto 3

4. Conclusioni

In data 20 giugno 2024 il sottoscritto Mirko Ignazio Paolo Morana ha accettato l'incarico da parte dei committenti, il quale formulavano al sottoscritto il seguente quesito:

“Facendo riferimento al filmato video 10 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.”

Il video è stato fornito dal committente mediante apposito link, il quale riconduce all'interno della piattaforma YouTube. Si è quindi proceduto inizialmente ad acquisire il filmato dalla suddetta piattaforma.

Durante la fase di acquisizione, le cui operazioni sono state accuratamente registrate tramite il software “Screen Capturer Recorder” della suite di programmi FAW. Successivamente il sottoscritto ha proceduto ad effettuare l'accesso sulla piattaforma Teams per andare a consultare prima il quesito tecnico proposto dal committente (Il Prova in itinere_finale_CT2024.pdf), successivamente per andare a reperire l'URL associato al nostro filmato nel file “DF - Video da Analizzare 2024.xlsx”. Successivamente questo URL è stato inserito sul browser basato su Microsoft edge della suite di programmi forensi FAW per effettuare in prima cosa la cristallizzazione della pagina e del traffico del computer, in seconda cosa FAW è stato utilizzato anche per la consultazione del filmato. Una volta finita la visione del filmato e la cristallizzazione della pagina web il CT ha proceduto ad acquisire il video mediante il software “aTube Catcher” senza applicare alcune conversioni come previsto dalle “best practice”. Quindi è stato controllato che la durata del video acquisito con quello presente nella piattaforma sia la stessa, inoltre sono stati confrontati alcuni istanti in maniera da capire se la qualità fosse la medesima dell'originale. In seguito, è stato calcolato il codice HASH del filmato acquisito e del report effettuato con FAW e sono stati trascritti nel file “ListaHASH.xlsx”. Dopo il calcolo iniziale degli HASH tramite script python “richiesta_UniqueID_YT.py”, che troverete nella cartella allegati, esegue una richiesta http, siamo andati a reperire il codice univoco dell'utente “Gabriele Vignolini” e del filmato:

- Codice Univoco Utente: UCDdODjv6Vw6KcrQ9gDPRQYw
- Codice Univoco Filmato: bfbL5l0SiEk

A questo punto l'acquisizione schermo è stata interrotta, e si è calcolato un HASH anche per quest'ultima.

Prima di iniziare la fase di analisi, seguendo le best practice del settore, sono state effettuate delle copie forensi, al fine di lavorare su queste ultime e di preservare l'integrità

del file originale, e per evitare di dover ripetere la fase di acquisizione in caso di modifiche indesiderate a quest'ultimo. Si è poi passati alla vera e propria fase di analisi, la quale è stata fortemente influenzata dalla bassissima qualità generale del filmato.

il filmato presenta le seguenti caratteristiche tecniche:

- Formato: mp4
- Codice: h264
- Dimensione: 5.823.265 byte
- Risoluzione in pixel: 480x360
- Frame Rate per Secondo : 25
- Totale Frame : 4411 frame
- Durata(hh:mm:ss:mmm): 00:02:56:494
- 1 flusso audio non udibile

Al fine di rispondere alla prima parte del quesito tecnico, si è proceduto ad un'analisi dell'integrità (e autenticità) del filmato. Poiché non sono state fornite informazioni sul sistema di videosorveglianza che ha ripreso l'accaduto, e non si conoscono informazioni riguardo risoluzione spaziale e temporale originali, e poiché il caricamento del filmato sulla piattaforma YouTube ha sicuramente previsto dei processi di compressione, anche a causa del CoDec utilizzato, è possibile concludere che il filmato non è integro.

Per quanto riguarda l'autenticità, poiché non si osservano manipolazioni o artefatti evidenti, e il video sembra rappresentare coerentemente le varie fasi del furto, è possibile affermare che il filmato sia autentico.

Dal suddetto video è stato poi possibile, come richiesto, ricostruire la dinamica degli eventi. Più nel dettaglio, è possibile assistere ad un furto avvenuto all'interno di un ufficio, senza però conoscerne luogo, il furto a quanto riportato dal sistema di videosorveglianza è durato 2 minuti, 56 secondi e 494 millisecondi, con l'entrata in scena del primo ladro alle ore 03:58:39(hh:mm:ss) della mattina del 10 luglio 2009 e la fine del furto avvenuto con successo alle ore 04:01:52(hh:mm:ss) della mattina del 10 luglio del 2009. A compiere il furto sono stati tre maschi, dalle fisicità si presume tutti maggiorenni e con volto semi-coperto

Si è proceduto poi ad effettuare analisi più approfondite per rispondere alla seconda parte del quesito tecnico, il quale chiedeva di ottenere informazioni utili per l'individuazione di luoghi, veicoli ed eventuali soggetti presenti nella scena. Per tale fase è stato fatto uso di un'ampia gamma di filtri messi a disposizione dal software Amped FIVE. Gli specifici filtri utilizzati e i valori dei relativi parametri sono presenti nel report generato da Amped FIVE stesso. Ciò garantisce la ripetibilità delle operazioni di analisi.



Per quanto riguarda il luogo, analizzando il canale dell'utente che ha pubblicato il nostro filmato possiamo notare che sono presenti altri video di furti, tutti nella provincia di Firenze, però non possiamo stabilire in che via o in che paese.


Per quanto riguarda eventuali soggetti presenti nella scena, è stato possibile contare tre diversi individui. Di questi è stato possibile misurare l'altezza ed è stato possibile reperire la carnagione ed alcune caratteristiche riguardanti il capo:

- Sospettato numero 1: da una prima analisi il CT è riuscito a reperire informazioni riguardanti la forma della testa del sospettato che è “ad occipite sporgente con Trichion Largo”. In una seconda analisi è stata stimata un'altezza approssimativa di 169,56 cm \pm 1,95 cm. La terza analisi non ha portato informazioni aggiuntive.
- Sospettato numero 2: da una prima analisi il CT è riuscito a reperire informazioni riguardanti la forma della testa del sospettato che è “con vertice posteriore”, non abbiamo informazioni se il sospettato ha il Trichion oppure no e del tipo di attaccatura di capelli che dovrebbe avere in quanto indossa qualcosa che ne copre il capo. Vista la scarsa qualità dell'apparecchiatura di videosorveglianza e visto che il soggetto indossa quello che sembra un passa montagna non si riescono ad ottenere informazioni in merito alla sua carnagione. In una seconda analisi è stata stimata un'altezza approssimativa di 156,56 cm \pm 2,77 cm. La terza analisi non ha portato informazioni aggiuntive.
- Sospettato numero 3: da una prima analisi il CT è riuscito a reperire informazioni riguardanti la forma della testa del sospettato che è “testa di fronte curva”, anche qui non abbiamo informazioni sull'attaccatura di capelli e l'eventuale Trichion. Carnagione della pelle chiara olivastra. In una seconda analisi è stata stimata un'altezza approssimativa di 164,51 cm \pm 2,06 cm. La terza analisi non ha portato informazioni aggiuntive

Successivamente alle analisi tecniche è stata effettuata un'altra analisi visiva per cercare di capire se si potessero riconoscere, marche o brand nel vestiario, in maniera tale da svolgere altre analisi tecniche, ma vista la scarsa qualità del filmato manca proprio l'informazione, sono riconoscibili una forma di cuore sulla maglietta del primo sospettato, un pattern floreale sui pantaloncini del secondo sospettato ma null'altro per tanto non sono stati eseguiti altri test.

In generale, a causa della scarsissima qualità del filmato non è stato possibile individuare ulteriori dettagli rilevanti per l'identificazione dei sospettati.

Si conclude tale perizia potendo affermare che il fatto, ovvero il furto in ufficio, sia avvenuto con la dinamica precedentemente descritta, ed è stato possibile individuare solo la zona presunta del furto, ma non è invece stato possibile identificare con certezza i veicoli usati, in quanto mai inquadrati.



5. Allegati Tecnici

Sono allegati alla presente relazione n. 152 (centocinquatadue) file, questo forma gli allegati tecnici, elencherò di seguito le cartelle con una loro piccola descrizione ed i file generali. **È possibile consultare gli HASH di TUTTI gli allegati tecnici all'interno del file "ListaHASH.xlsx", anch'esso allegato alla presente consulenza tecnica.** Al fine di assicurare l'integrità di quest'ultimo file, è fornito di seguito il relativo codice HASH SHA256:

016B48C6047E63A03FB981E80B8ABE0D6EFCACF2FA7F8F80C21C1A827A71D15C

N. Allegato	Nome File	Dimensione(byte)	Descrizione
1	Furto 10072009 cassaforte rotta.mp4	5.824.512	File originale del Filmato
2	Furto 10072009 cassaforte rotta(Copia).mp4	5.824.512	Copia Bit-a-Bit del filmato originale
3	ImmaginidiSupporto.rar	9.883.648	Immagini usate per l'analisi per un totale di 35 file
4	ReportAmped.rar	20.480	Report effettuato tramite la funzione di report del programma
5	ReportFAW.rar	16.445.440	Report della cristallizzazione della pagina web con HASH dei file creati
6	Furto 10072009 cassaforte rotta(Copia).afp	53.248	File di progetto per salvare, aprire e chiudere le modifiche
7	richiesta_UniqueID_YT.py	4.096	Script Python per la richiesta http per ricevere ID Univoco dell'utente
8	ListaHASH.xlsx	24.576	Lista di tutti gli HASH dei file, meno di quelli di FAW che sono nel report di FAW
9	AcquisizioneSchermo.mp4	162.340.864	registrazione dello schermo avvenuta durante l'acquisizione del filmato
10	ReportRete.pcapng	70.930.432	Registrazione del traffico di rete durante l'acquisizione



6. Referenze Bibliografiche

Sono di seguito riportate alcune referenze bibliografiche riguardanti le **best practice** del settore della Digital Forensics, scrupolosamente seguite durante la realizzazione della presente relazione tecnica:

1. Legge 48/2008 – Ratifica ed esecuzione della “Convezione di Budapest”:
<https://www.parlamento.it/parlam/leggi/08048l.htm>
2. ENFSI, “Best practice manual for forensic image and video enhancement”:
<https://enfsi.eu/wp-content/uploads/2017/06/Best-Practice-Manual-for-Forensic-Image-and-Video-Enhancement.pdf>
3. S. Battiato, “Investigare su immagini e video (parte 1)”, PDF fornito durante il corso di Digital Forensics dell’Università di Catania, A.A. 2022/2023
4. ISO Guidelines:
 - ISO-27037 “Guidelines for identification, collection, acquisition and preservation of digital evidence”: <https://www.iso.org/standard/44381.html>
 - ISO-27041 “Guidance on assuring suitability and adequacy of incident investigative method”: <https://www.iso.org/standard/44405.html>
 - ISO-27042 “Guidelines for the analysis and interpretation of digital evidence”: <https://www.iso.org/standard/44406.html>
5. Referenze bibliografiche presenti nel report generato da Amped FIVE



7. Glossario

- Funzione di HASH: funzione che prende in input dei dati di qualsiasi dimensione e produce un valore, solitamente una stringa, di lunghezza fissa, noto come “digest”. Le funzioni di HASH sono ampiamente utilizzate in vari campi, come la crittografia o, nel nostro caso, per il controllo dell'integrità dei dati. Una buona funzione di HASH dovrebbe essere veloce da calcolare e avere una bassa probabilità di collisioni, ovvero la possibilità che due input diversi producano lo stesso digest dovrebbe essere molto bassa.
- Frame: Ciascuna delle singole immagini che compongono il video
- Frame rate: Frequenza di riproduzione dei fotogrammi che compongono un video, viene misurata in “FPS”.
- Pixel: più piccola unità che compone un'immagine digitale
- CoDec: è un software formato da due parti: un “encoder” e un “decoder”. Esso si occupa della codifica e/o decodifica digitale di un segnale, tipicamente audio o video, perché possa essere salvato su un supporto di memorizzazione o aperto per la sua riproduzione.
- Filtro: i Filtri servono a modificare le caratteristiche di un'immagine, in modo da migliorare la qualità (“Image Enhancement”) oppure invertire il processo di degrado (“Image Restoration”)

Catania, 22/06/2024

Consulente Tecnico

Mirko Ignazio Paolo Morana

