Università di Catania

Dipartimento di Matematica e Informatica
Cittadella Universitaria - Viale Andrea Doria, 6 - 95125 - Catania

Relazione di consulenza tecnica

Procedimento n. 22

Committente: Prof. Sebastiano Battiato

Consulente Tecnico

Emanuel Ramaci

Matricola: 1000045322

Catania, 21 Gennaio 2025

Indice

Glossario

- **Acquisizione forense**: Processo di raccolta di dati digitali garantendo l'integrità e la conformità alle best practice della Digital Forensics, con documentazione delle operazioni.
- **FAW** (Forensic Acquisition of Websites): Software utilizzato per acquisire pagine web in formato certificato, generando copie navigabili offline e garantendo l'integrità dei dati acquisiti.
- **aTube Catcher**: Strumento per il download di contenuti multimediali da piattaforme online, utilizzato in ambito forense senza conversioni o compressioni per preservare il formato originale.
- **Bandicam**: Software per la registrazione dello schermo, utilizzato per documentare le operazioni di acquisizione e garantire la trasparenza del processo.
- **Copia forense**: Copia immutabile dei dati digitali originali, utilizzata per evitare alterazioni durante le analisi e preservare l'evidenza digitale.
- **Hash**: Algoritmo crittografico che genera un valore univoco e di lunghezza fissa, utilizzato per verificare l'integrità dei dati.
- **Frame**: Singola immagine statica che, in sequenza, compone un video; nel caso specifico, utilizzata per ricostruire eventi attraverso analisi temporali e spaziali.
- **Frame rate**: Frequenza con cui i fotogrammi sono visualizzati in un video, misurata in frame per secondo (fps).
- **Codec (h264)**: Algoritmo di compressione video utilizzato per ridurre le dimensioni del file mantenendo una qualità accettabile; comune nel formato MP4.
- **Timestamp**: Marcatura temporale sovraimpressa nei fotogrammi di un video, utilizzata per identificare eventi e sequenze temporali precise.
- **Amped FIVE**: Software avanzato per l'elaborazione, il miglioramento e l'analisi forense di video e immagini, documentando filtri e parametri utilizzati per garantire la ripetibilità dell'analisi.
- **Amped Authenticate Video**: Software specializzato per la verifica dell'integrità e autenticità dei file video multimediali, utile per individuare manipolazioni o incongruenze.
- **Compressione video**: Processo di riduzione delle dimensioni di un file video, spesso tramite codec come h264, che può alterare la qualità e l'integrità del file originale.

- **Tagli video**: Rimozioni di porzioni di video, che possono compromettere la continuità temporale e la completezza dell'evidenza multimediale.
- **Metadati**: Informazioni aggiuntive associate a un file digitale, come data di creazione, modifiche e codec utilizzati, fondamentali per analisi forensi.
- **Risoluzione spaziale**: Numero di pixel che definiscono la qualità visiva di un video o di un'immagine, espressa in termini di larghezza e altezza (ad esempio, 640x360 px).
- **Risoluzione temporale**: Capacità di un video di rappresentare gli eventi nel tempo, determinata dal frame rate, ovvero il numero di fotogrammi visualizzati al secondo.
- **File .afp**: Progetto generato da Amped FIVE che include tutte le operazioni di elaborazione effettuate su un video, garantendo la documentazione e la ripetibilità delle analisi effettuate.
- **File .aavp**: Progetto generato da Amped Authenticate contenente dettagli sull'analisi forense e sull'integrità dei file video.

1. Estremi del procedimento

Procedimento numero 22 relativo ad un duplice omicidio avvenuto la notte del 30 Agosto 2015, presso l'abitazione di una coppia di coniugi a Palagonia, Sicilia. La vicenda coinvolge l'ivoriano Kamara Mamadou, arrestato in quanto sospettato di aver compiuto il duplice omicidio. Il video oggetto di analisi, reperibile al seguente indirizzo web:

https://palermo.repubblica.it/cronaca/2015/09/04/video/omicidio_di_palagonia_livoriano_ripreso_dalle_telecamere_di_sorveglianza-422796541/,

riguarda varie riprese effettuate dalle telecamere di sorveglianza nei pressi dell'abitazione della coppia assassinata.

1.1 Incidente Probatorio

In data 21 Gennaio 2025, il Committente emetteva ordinanza di ammissione di incidente probatorio per esaminare le evidenze digitali relative all'omicidio di Palagonia, avvenuto nella notte tra il 29 e il 30 agosto 2015.

1.2 Nomina del Consulente

Il sottoscritto Emanuel Ramaci, nato a Catania il 16/06/2003, in qualità di Consulente Tecnico nominato dal Committente, Sebastiano Battiato, ha ricevuto, in data 21 Gennaio 2025, l'incarico relativo al procedimento penale n. 22.

1.3 Quesito tecnico

In data 21 Gennaio 2025 alle ore 10:30 il Committente formulava il seguente quesito: ***"Facendo riferimento al filmato video 22 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."

2. Premesse tecniche

Il Consulente, una volta accettato l'incarico, si presta a elaborare la seguente relazione tecnica sull'analisi del video fornito, dal titolo *"Omicidio di Palagonia, l'ivoriano ripreso dalle telecamere di sorveglianza"*. L'obiettivo principale di tale analisi è di esaminare la sequenza video in modo da raccogliere informazioni utili alla ricostruzione della dinamica del crimine e, in particolare, per valutare l'eventuale coinvolgimento del sospettato, Kamara Mamadou, nell'omicidio delle vittime.

Le operazioni di acquisizione, conservazione e analisi delle evidenze digitali sono state effettuate seguendo le linee guida e le best practices della digital forensics, con particolare attenzione alla preservazione dell'integrità dei dati e alla ripetibilità delle operazioni. Durante tutto il processo, si è fatto riferimento a standard consolidati del settore per garantire che le evidenze non venissero alterate, distrutte o compromesse in alcun modo, preservando così il valore legale del materiale analizzato.

2.1 Strumenti hardware e software

Il Consulente si è apprestato ad acquisire e ad analizzare le riprese video fornite, utilizzando i software *FAW*, *aTube Catcher*, *Amped Five* e *Amped Authenticate*, seguendo una sequenza ben definita per garantire la massima efficacia e conformità alle best practices forensi. Le immagini, tuttavia, risultano non integre, ma comunque autentiche, a causa della compressione del video caricato sul sito *"repubblica.it*". L'analisi si è concentrata in particolare sulle riprese che mostrano l'indagato, Kamara Mamadou, nei pressi dell'abitazione delle vittime, per accertare la dinamica dei fatti.

Ai fini di poter portare al termine il quesito proposto dal Committente, il Consulente ha fatto uso dei seguenti dispositivi hardware e software.

Hardware:

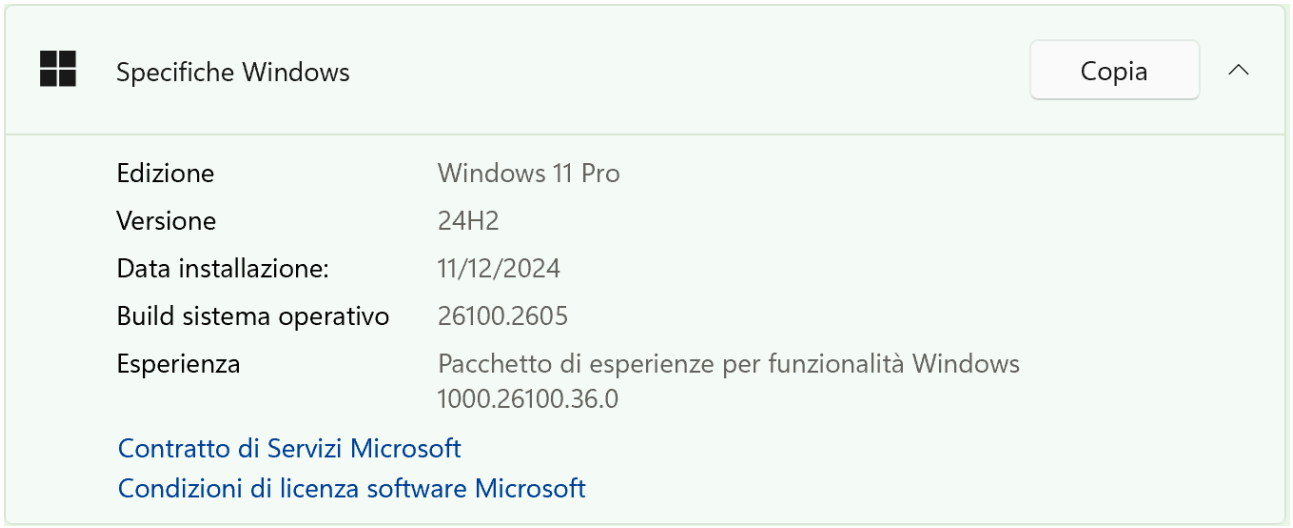
- **Host fisico**: MacBook Pro M2
    - Processore: Apple M2 (8 core CPU, 10 core GPU)
    - Memoria RAM: 8 GB
    - Sistema Operativo: macOS Sequoia 15.2
    - Storage: SSD 256 GB
    - Interfacce di rete: Wi-Fi 6, Bluetooth 5.0, USB-C / Thunderbolt 3, Ethernet (via adattatore USB-C)

Il MacBook M2 è stato utilizzato come host fisico per l'intera operazione. Tuttavia, l'analisi forense è stata eseguita su una macchina virtuale *"Windows 11 Pro"*, poiché alcuni strumenti software essenziali per l'analisi, come Amped Five e Amped

Authenticate, non sono compatibili con macOS. L'uso della macchina virtuale ha quindi garantito l'accesso a tali strumenti specialistici senza la necessità di un hardware aggiuntivo o di un sistema dual-boot.

- **Macchina Virtuale**: Windows 11 Pro
    - Software di virtualizzazione: VMware Fusion (Versione 13.0)
    - Sistema Operativo virtuale: Windows 11 Pro 64-bit, Versione 24H2
    - Memoria RAM allocata: 4 GB
    - Storage: 52 GB SSD dedicato alla macchina virtuale
    - CPU allocata: 4 core della CPU Apple M2

La macchina virtuale Windows 11 Pro è stata configurata su VMware Fusion, un software di virtualizzazione che permette di eseguire macchine virtuali come Windows 11 Pro in modo fluido su macOS. Questo ambiente è stato scelto per permettere l'esecuzione di strumenti specifici per l'analisi forense che non sono compatibili nativamente con macOS, come Amped Five e Amped Authenticate, utilizzati per l’elaborazione e la validazione delle evidenze video.



Software:

- **VMware Fusion** (Versione 13.0): Software di virtualizzazione utilizzato per creare l'ambiente Windows 11 Pro all'interno del sistema operativo macOS. VMware Fusion permette di eseguire applicazioni Windows su macOS senza compromettere le performance, consentendo l'uso di strumenti specialistici per l'analisi digitale.

- **Bandicam** (Versione 8.1.0.2516): Software di registrazione dello schermo utilizzato per acquisire il video che mostra la pagina web dove il video risiede, il processo di acquisizione tramite FAW, e il successivo download del file utilizzando aTube Catcher. Bandicam è stato impiegato per documentare e registrare il flusso completo di acquisizione e verifica del file, includendo il calcolo dell'hash SHA-256 tramite PowerShell e la creazione di un pacchetto zip contenente tutti gli elementi acquisiti da FAW, sul quale anche su questo è stato calcolato l'hash SHA-256.

- **FAW** (Forensic Acquisition of Websites - Versione 11.5.13): Software per l'acquisizione forense di contenuti web, utilizzato per raccogliere prove da siti web correlati all'indagine. FAW è stato utilizzato nelle prime fasi del procedimento per raccogliere informazioni e prove digitali provenienti da fonti online.

- **aTube Catcher** (Versione 10.8.9): Software che consente il download di video da diverse piattaforme online, inclusa YouTube. Inserendo l'URL del video, il software permette di scaricarlo nel formato originale, evitando qualsiasi tipo di compressione aggiuntiva che potrebbe compromettere la qualità del file. Questo strumento è utile per acquisire contenuti multimediali in modo diretto e senza alterazioni.

- **PowerShell** (Versione 5.1.26100.2161): Shell a riga di comando sviluppata da Microsoft, utilizzata per calcolare gli hash dei file e verificare l'integrità dei dati durante le fasi di acquisizione e analisi. È stato utilizzato per generare e verificare gli hash dei file di video e di altre evidenze digitali, garantendo l'autenticità del materiale esaminato.

- **Amped Five** (Versione 3.55.17.0): Software utilizzato per l'enhancement e restoration di immagini e filmati. Amped Five è uno strumento riconosciuto in ambito forense per la sua capacità di applicare filtri e miglioramenti video, migliorando la visibilità delle scene riprese dalle telecamere di sorveglianza e permettendo un'analisi dettagliata dei filmati.

- **Amped Authenticate Video** (Versione 3.60.33.0): Software forense utilizzato per l'autenticazione dei file video. In particolare, questo strumento è stato utilizzato per verificare l'integrità del video fornito dal Committente, analizzando i metadati e le informazioni di codifica per garantire che il file non fosse stato alterato o manipolato.

ER

3. Acquisizione

In data 21 Gennaio 2025 alle ore 10:30 viene assegnata, da parte del Committente, l'evidenza digitale sulla quale il CT dovrà eseguire le indagini.

L'evidenza è disponibile sul sito web *"repubblica.it*" al seguente link:

https://palermo.repubblica.it/cronaca/2015/09/04/video/omicidio_di_palagonia_livoriano_ripreso_dalle_telecamere_di_sorveglianza-422796541/

Il titolo del video in esame è: "*Omicidio di Palagonia, l'ivoriano ripreso dalle telecamere di sorveglianza"*.

Il processo di acquisizione del filmato ha avuto inizio alle 19:33 del 21 Gennaio 2025 con l'avvio della registrazione schermo, intitolata *"ProcessoAcquisizioneVideo.mp4"*, tramite il software **Bandicam**. Le principali fasi dell'acquisizione, visibili nella registrazione schermo, sono le seguenti:

- **Avvio del software FAW**, con la creazione di un nuovo caso nel quale è stato ricercato il video utilizzando il numero di procedimento 22.
- **Visione del video** tramite il link fornito nel file *"DF - Video da Analizzare 2025 - Seconda prova in itinere.xlsx"* (dal canale Microsoft Teams del corso di "DIGITAL FORENSICS"), per confermare che si trattasse dell'evidenza corretta.
- **Avvio del software aTubeCatcher** per il download del filmato, al fine di acquisirlo nel suo formato originale.
- **Salvataggio del filmato** come *"Omicidio di Palagonia, l'ivoriano ripreso dalle telecamere di sorveglianza.mp4"*.
- **Acquisizione dell'intera pagina web** da FAW, cliccando l'icona *"Fotocamera"* nel menù in alto (nel video *"ProcessoAcquisizioneVideo.mp4"* il click avviene al minuto 00:01:31). Questo genererà una cartella chiamata *"22"*, che verrà poi compressa in un pacchetto zip, calcolandone infine l'hash SHA-256.
- **Calcolo dell'hash** del filmato *"Omicidio di Palagonia, l'ivoriano ripreso dalle telecamere di sorveglianza.mp4"* e del pacchetto zip *"22.zip"* tramite **PowerShell**, utilizzando la funzione di hashing SHA-256, per garantire l'integrità del file.

Il comando di base per calcolare l'hash di un file con algoritmo SHA-256 tramite PowerShell è il seguente:

Get-FileHash -Algorithm SHA256 <FilePath>

- **Stop della registrazione** schermo da Bandicam, al termine dell'acquisizione, salvando il file come *"ProcessoAcquisizioneVideo.mp4"*.

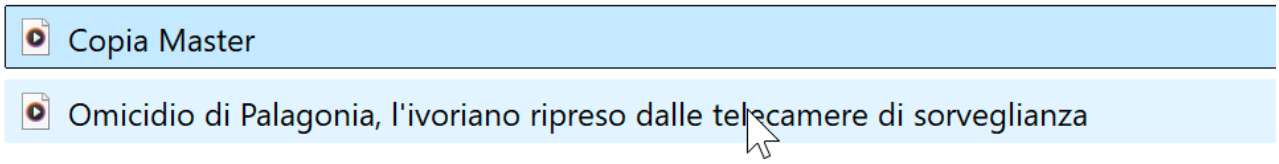
Il calcolo del codice hash, o "digest", su ciascun file serve a verificarne l'integrità. Questo perché, se il file subisse delle modifiche, anche involontarie, e venisse ricalcolato l'hash, il nuovo valore risultante sarebbe diverso da quello originale. In questo modo, si può facilmente identificare qualsiasi alterazione nel file, garantendo che esso sia rimasto invariato rispetto alla versione originale.

4. Analisi tecnica

La metodologia adottata per l'analisi del video include tecniche di esame dei file digitali per determinare la loro autenticità, identificare eventuali manipolazioni, e verificare la corrispondenza temporale con gli altri elementi di prova presenti nel fascicolo. In particolare, il video in oggetto è stato sottoposto a una verifica della sua integrità, attraverso l'analisi dei metadati e l'utilizzo di strumenti forensi avanzati per il controllo dei segnali video e audio.

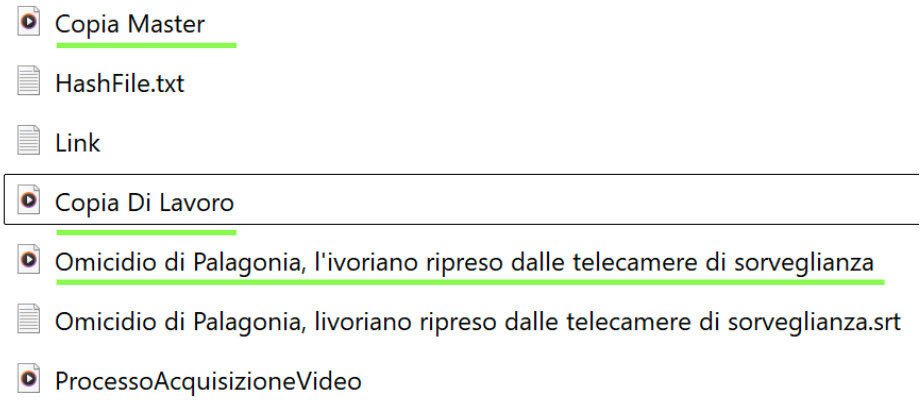
4.1 Creazione di copie forensi del filmato

Conformemente alle best practices del settore, prima di eseguire qualsiasi analisi sul filmato, è stata effettuata una copia forense del file originale. La copia forense è denominata *"Copia Master.mp4"*, ed è stata successivamente verificata mediante calcolo dell'hash per assicurare l'integrità del file.



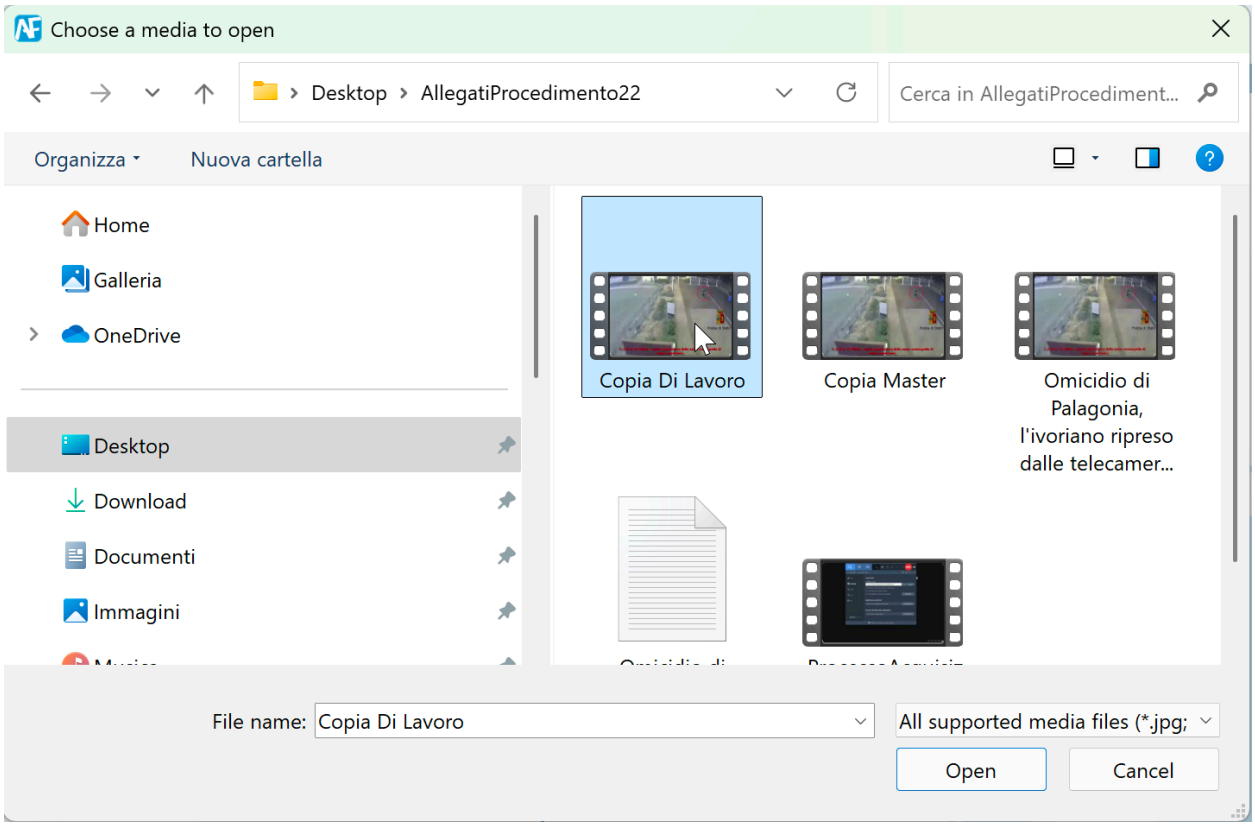

```
PS C:\WINDOWS\system32> Get-FileHash -Algorithm SHA256 "C:\Users\emanuelebay\Desktop\AllegatiProcedimento22\Omicidio di
Palagonia, l'ivoriano ripreso dalle telecamere di sorveglianza.mp4"

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          35CCA15AB9F3F2AF086185330438D686569FAFFC62D0DDEFE7DF5CE537FEFB14       C:\Users\emanuelebay\Desktop\...


PS C:\WINDOWS\system32> Get-FileHash -Algorithm SHA256 "C:\Users\emanuelebay\Desktop\AllegatiProcedimento22\Copia Master
.mp4"

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          35CCA15AB9F3F2AF086185330438D686569FAFFC62D0DDEFE7DF5CE537FEFB14       C:\Users\emanuelebay\Desktop\...
```

Una seconda copia, denominata *"Copia di Lavoro.mp4"*, è stata generata per eseguire le operazioni di analisi, riducendo il rischio di alterazioni accidentali al file originale. Entrambe le copie hanno restituito valori di hash identici, confermando la correttezza del processo di duplicazione.




```
PS C:\WINDOWS\system32> Get-FileHash -Algorithm SHA256 "C:\Users\emanuelebay\Desktop\AllegatiProcedimento22\Omicidio di
Palagonia, l'ivoriano ripreso dalle telecamere di sorveglianza.mp4"

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          35CCA15AB9F3F2AF086185330438D686569FAFFC62D0DDEFE7DF5CE537FEFB14       C:\Users\emanuelebay\Desktop\...


PS C:\WINDOWS\system32> Get-FileHash -Algorithm SHA256 "C:\Users\emanuelebay\Desktop\AllegatiProcedimento22\Copia Master
.mp4"

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          35CCA15AB9F3F2AF086185330438D686569FAFFC62D0DDEFE7DF5CE537FEFB14       C:\Users\emanuelebay\Desktop\...


PS C:\WINDOWS\system32> Get-FileHash -Algorithm SHA256 "C:\Users\emanuelebay\Desktop\AllegatiProcedimento22\Copia Di Lav
oro.mp4"

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          35CCA15AB9F3F2AF086185330438D686569FAFFC62D0DDEFE7DF5CE537FEFB14       C:\Users\emanuelebay\Desktop\...
```

Il file *"Copia Di Lavoro.mp4"* è stato quindi importato in un progetto denominato *"OmicidioPalagonia.afp"* all'interno di **Amped Five** per l'analisi.

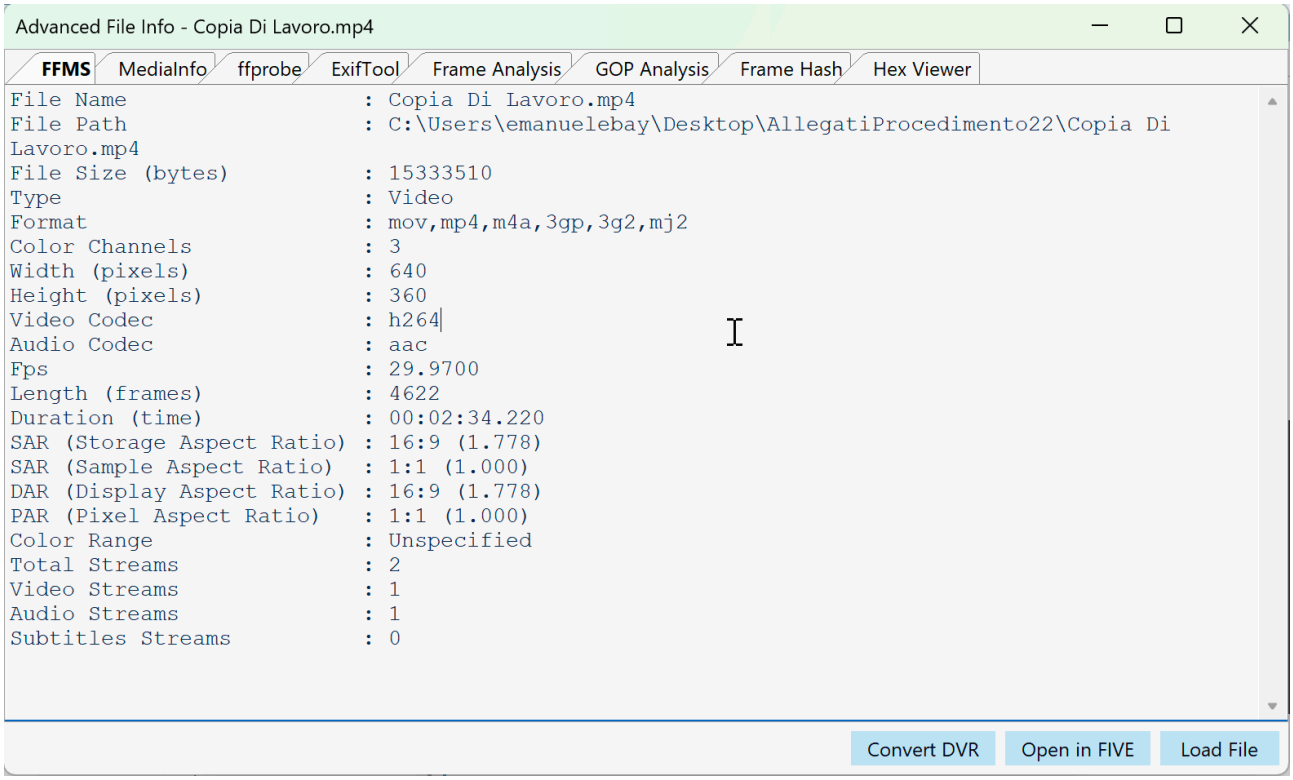


4.2 Dettagli tecnici sul file video

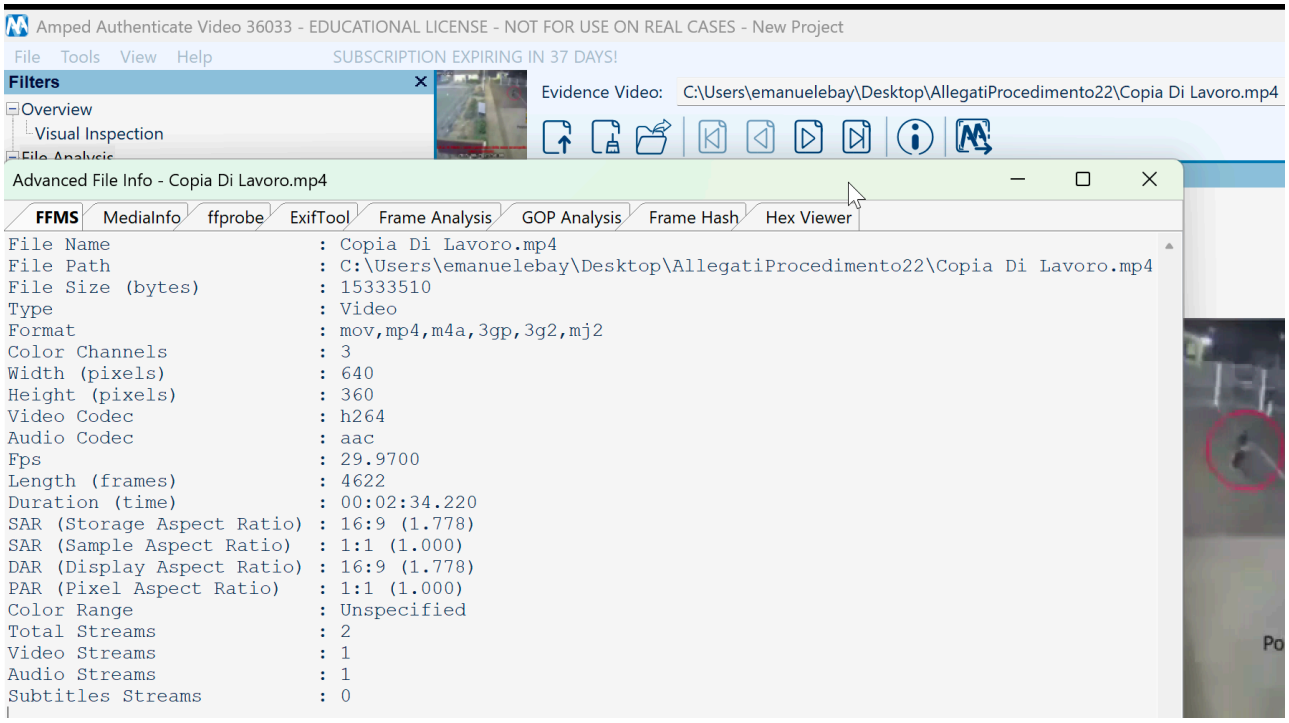
Il file analizzato, denominato *"Copia Di Lavoro.mp4"*, presenta le seguenti specifiche:

- **Dimensione**: 15.333.510 bytes
- **Formato**: mp4
- **Codec**: h264
- **Durata**: 00:02:34.220
- **Risoluzione spaziale**: 640px * 360px
- **Risoluzione temporale / Frame Rate**: 30

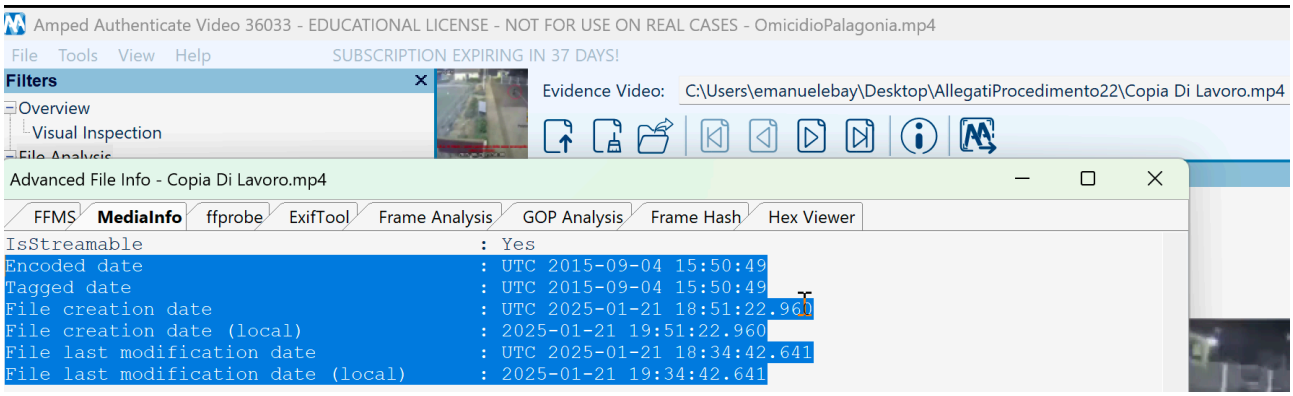
In seguito, utilizzando l'interfaccia grafica di **Amped Five**, nello specifico dal menu a tendina **Utility > Informazioni Avanzate sul File**, è stato possibile estrarre ulteriori dettagli sulle caratteristiche tecniche del file:



È possibile vedere le stesse informazioni sul progetto **Amped Authenticate** allegato (*"OmicidioPalagoniaAA.aavp"*)



Inoltre, sempre su Amped Authenticate, è possibile vedere le date originali rispetto alla codifica e tag del video e informazioni riguardanti la data di creazione e ultima modifica, andando su **Advanced File Info > MediaInfo**:



4.3 Analisi di integrità e autenticità del filmato

Il CT, dopo aver acquisito il filmato dalle telecamere di videosorveglianza, si è occupato di verificarne l'integrità e l'autenticità, in conformità al quesito tecnico.
Dai dati forniti dal Committente risulta che il filmato è stato estrapolato direttamente dal sistema di videosorveglianza installato nei pressi dell'abitazione dei coniugi Solano. Tuttavia, non sono state fornite ulteriori informazioni riguardanti il modello del sistema di sorveglianza, le specifiche tecniche dei dispositivi utilizzati, né le modalità di estrazione del file.

Dal filmato analizzato non è possibile determinare con assoluta certezza la frequenza originaria dei fotogrammi né la risoluzione iniziale, in quanto i metadati presenti risultano parziali o modificati. È importante sottolineare che eventuali alterazioni potrebbero essere avvenute durante le fasi di estrazione o trasferimento del file da parte delle autorità competenti.

Il filmato analizzato, inoltre, presenta alcuni tagli e sovraimpressioni (come cerchi rossi attorno ai soggetti di interesse), presumibilmente aggiunti dalle autorità o dagli operatori che hanno elaborato il video per scopi investigativi. Nonostante tali modifiche, non sono emerse evidenti manipolazioni maliziose volte a falsare il contenuto del filmato.

In conclusione, il filmato risulta **non integro** a causa delle alterazioni descritte, ma conserva una **autenticità** sufficiente per rappresentare fedelmente gli eventi avvenuti tra il 29 e il 30 agosto 2015.

4.4 Individuazione dei fotogrammi e ricostruzione degli eventi

Dal video denominato *"Copia Di Lavoro.mp4"*, nonostante la qualità non ottimale, è stato possibile identificare i fotogrammi rilevanti per la ricostruzione degli eventi accaduti. Il CT ha proceduto a una prima visione integrale del filmato, acquisendo diversi "Snapshot" tramite l'interfaccia di **Amped Five**, utili per identificare i momenti chiave.

I frame selezionati sono stati salvati in una cartella chiamata *"Frames"* e possono essere restituiti come parte integrante del report generato da Amped Five, così da poter essere analizzati in dettaglio.

È importante sottolineare che, in questo caso, il report generato da Amped Five non è disponibile per la licenza istituzionale. I frame e i relativi filtri applicati possono comunque essere visionati estraendo dallo zip *"Frames.zip"*, presente tra gli allegati, la cartella *"Frames"*. Inoltre, alla visione di ogni singolo file del formato *"frame.jpg.afp"*, se richiesto da Amped Five, bisogna aprire il file video *"Copia Di Lavoro.mp4"*, sempre presente in allegato.

Durante la visione del filmato, i seguenti orari, corrispondenti ai timestamp sovraimpressi, sono stati individuati come significativi:

- **23:58**: al *frame 0* il soggetto si dirige verso l'uscita dal C.A.R.A. di Mineo in bicicletta, con uno zaino mono spalla di colore arancione.

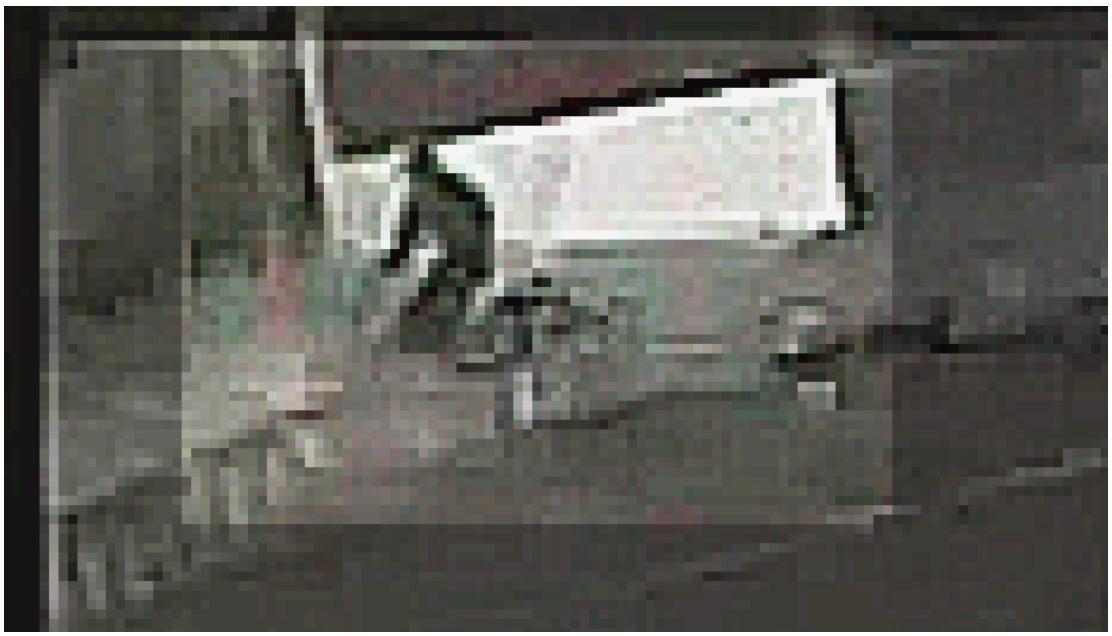
Per migliorare la qualità del frame 0 e rendere il soggetto cerchiato più visibile sono stati applicati i seguenti filtri:

- *Deinterlacciamento*;
- Correzione del *contrasto* e della *luminosità*;
- Riduzione del *rumore* tramite filtro media;
- *Nitidezza*;
- *Zoom* e *Cropping*;
- *Equalizzazione* automatica del colore.

- **02:13** (ORARIO REALE): Al *frame 436* il soggetto si trova a Palagonia, in via Palermo, con transito in direzione dell'abitazione delle vittime (da notare il particolare dello zaino).

Tramite l'applicazione dei seguenti filtri è stato possibile migliorare e rendere più evidente il soggetto in bici davanti l'abitazione dei Solano.

- *Contrasto Laplaciano*;
- Miglioramento del *contrasto* e della *luminosità*;
- Regolazione dei colori tramite *equalizzazione* automatica del colore;
- *Ritaglio* ed *evidenziamento* zona d'interesse.



- **02:16**: Al *frame 638* il soggetto percorre una stradina che conduce esclusivamente a Villa Solano. Nei fotogrammi successivi, si vede passare qualcuno dal retro dell'abitazione della famiglia Solano, prima del delitto.

- **05:14 - 05:15**: Nel range di *frame 1128-1804* il soggetto percorre la strada adiacente al retro dell'abitazione della famiglia Solano, dopo il delitto.

- **05:22**: Dal *frame 1985* al *frame 2167* è in transito in direzione della S.S. 417 e C.A.R.A. di Mineo. In particolare, è possibile notare che viene trasportata una sacca appesa alla bicicletta.

Frame 2043 - Evidenziamento soggetto, tramite l'applicazione dei seguenti filtri:

- *Contrasto Laplaciano*;
- Filtro di *media*;
- *Equalizzazione cromatica*;
- *Aggiungi* forma, per l'evidenziamento della zona d'interesse.

- **06:20**: Al frame 2504 rientra e viene sottoposto al controllo al C.A.R.A. di Mineo.

Gli orari menzionati si riferiscono ai timestamp visibili nelle immagini, che sono parte integrante del sistema di videosorveglianza. Tuttavia, si precisa che il filmato presenta tagli che rendono impossibile determinare con precisione la continuità temporale tra un fotogramma e l'altro.

Questi elementi sono stati fondamentali per ricostruire i movimenti di Kamara Mamadou e la sequenza degli eventi che lo collocano nei pressi del luogo del delitto.

5. Conclusioni

In data 21 Gennaio 2025, il sottoscritto Emanuel Ramaci ha accettato l'incarico da parte del Committente, Prof. Sebastiano Battiato, il quale formulava al sottoscritto il seguente quesito:

"Facendo riferimento al filmato video 22 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 é stato fornito dal Committente tramite un apposito link, il quale riconduce all'interno del sito *"repubblica.it"*.
Durante la fase di acquisizione, le cui operazioni sono state accuratamente registrate tramite il software **Bandicam**, si é proceduto ad avviare il software **FAW** per l'acquisizione certificata dell'intera pagina web.

Il sottoscritto ha effettuato l'accesso al link fornito dal Committente, attraverso il browser FAW, per acquisire il filmato relativo al duplice omicidio di Palagonia. Il filmato si trova al seguente indirizzo web:

https://palermo.repubblica.it/cronaca/2015/09/04/video/omicidio_di_palagonia_livoriano_ripreso_dalle_telecamere_di_sorveglianza-422796541/,

come indicato nella riga 22 del file "DF - Video da Analizzare 2025 - Seconda prova in itinere.xlsx" sul canale Microsoft Teams "DIGITAL FORENSICS".

Una volta visionato preliminarmente il filmato, è stata avviata l'acquisizione del filmato nel suo formato originale tramite il software **aTube Catcher**, senza applicare alcuna conversione o compressione, in conformità alle best practices della Digital Forensics. Parallelamente, è stata acquisita l'intera pagina web contenente il filmato. Al termine dell'acquisizione, il software **FAW** ha generato una cartella denominata con il numero del procedimento in esame, *"22"*, che è stata successivamente compressa in un archivio zip per il **calcolo dell'hash**. I codici hash del filmato e dell'archivio sono stati quindi calcolati, e la registrazione è stata interrotta. È stato altresì calcolato l'hash relativo alla registrazione stessa.

Prima di procedere con l'analisi, sono state realizzate delle copie forensi del filmato e della pagina web acquisita, al fine di preservare l'integrità dei dati originali e di evitare di dover ripetere le operazioni di acquisizione in caso di modifiche indesiderate.

L'analisi del filmato, purtroppo, è stata ostacolata dalla qualità mediamente bassa del materiale. Il filmato ha una dimensione di 15.333.510 byte, è in formato mp4 con codec

h264, e ha una durata di 2 minuti, 34 secondi e 220 millisecondi. La risoluzione spaziale è di 640px x 360px, con un frame rate di 30 fps, per un totale di 4621 frame. Queste stesse informazioni è possibile prenderle anche dal progetto **Amped Authenticate** *"OmicidioPalagoniaAA.aavp"* allegato. In quest'ultimo è stato possibile anche consultare alcune informazioni più particolari del file, quali le date di codifica/tag e di creazione/ ultima modifica del file.

Per quanto riguarda l'integrità e l'autenticità del filmato, non essendo stato fornito alcun dettaglio sul sistema di videosorveglianza utilizzato, e considerando che il filmato è stato caricato sulla piattaforma *"repubblica.it*", è evidente che il materiale è stato sottoposto a processi di compressione, probabilmente dovuti al codec utilizzato. Inoltre, il filmato presenta diversi tagli, che, sebbene possano essere stati effettuati per mostrare scene incriminanti, impediscono di stabilire una continuità temporale precisa tra i fotogrammi. Per queste ragioni, si può concludere che il filmato non sia integro.

Tuttavia, relativamente all'autenticità, non sono stati rilevati segni di manipolazione maliziosa o artefatti evidenti, e il filmato appare coerente nelle sue fasi, rappresentando in modo verosimile gli eventi che hanno portato al duplice omicidio. Pertanto, è possibile affermare che il filmato è autentico.

Nel corso dell'analisi, sono stati individuati diversi orari significativi, corrispondenti ai timestamp sovraimpressi nelle immagini del filmato, che hanno permesso di ricostruire la dinamica degli eventi:

- **23:58 (frame 0)**: uscita dal C.A.R.A. di Mineo in bicicletta, con uno zaino mono spalla di colore arancione.
- **02:13 (frame 436)**: Palagonia, via Palermo, transito in direzione dell'abitazione delle vittime (particolare dello zaino).
- **02:16 (frame 638)**: Il soggetto percorre una stradina che conduce esclusivamente a Villa Solano. Nei fotogrammi successivi, si vede passare qualcuno dal retro dell'abitazione della famiglia Solano, prima del delitto.
- **05:14 - 05:15 (frame 1128-1804)**: Il soggetto percorre la strada adiacente al retro dell'abitazione della famiglia Solano, dopo il delitto.
- **05:22 (frame 1985-2167)**: Transito in direzione della S.S. 417 e C.A.R.A. di Mineo. Particolare della sacca trasportata sulla bicicletta.
- **06:20 (frame 2504)**: Rientro e sottoposizione al controllo al C.A.R.A. di Mineo.

Si precisa che, pur essendo visibili i timestamp, il filmato presenta dei tagli che rendono difficile determinare con precisione la continuità temporale tra i fotogrammi.

In risposta alla seconda parte del quesito tecnico, sono state effettuate ulteriori analisi utilizzando il software **Amped FIVE**. Gli specifici filtri applicati e i parametri utilizzati sono stati salvati in una cartella chiamata *"Frames"*, estraibile dal pacchetto zip *"Frames.zip"* in allegato, tramite l'acquisizione di diversi Snapshot, in modo da salvare i frame e i relativi filtri applicati dallo stesso software, garantendo la ripetibilità dell'analisi.

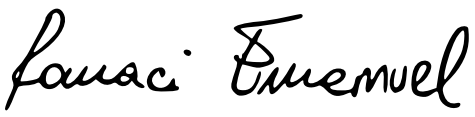
Infine, in merito al luogo del delitto, è stato confermato che l'omicidio è avvenuto a Villa Solano, e il soggetto responsabile della morte dei due coniugi è Kamara Mamadou.

Si conclude che il duplice omicidio sia avvenuto seguendo la dinamica precedentemente descritta e che i movimenti di Kamara Mamadou, nella notte tra il 29 e il 30 agosto 2015, siano stati individuati con certezza attraverso il sistema di videosorveglianza, corroborando la ricostruzione degli eventi.

Consulente Tecnico

Emanuel Ramaci

Matricola: 1000045322



Catania, 24 Gennaio 2025

6. Allegati tecnici

Alla presente relazione tecnica sono allegati un totale di 12 allegati tecnici, ciascuno dei quali fornisce un ulteriore supporto e dettaglio per la comprensione e la validazione dei procedimenti descritti in questa relazione. Gli allegati tecnici sono elencati di seguito:

- **Link.txt**:
  - **SHA-256**: 243A440A898F8157C279673FBFD631FC254EF62F54CDE15F72A3A2FCC4591A35
  - **Descrizione**: File di testo contenente il link estratto dalla riga 22 del file *"DF - Video da Analizzare 2025 - Seconda prova in itinere.xlsx"* presente nel canale Microsoft Teams denominato *"DIGITAL FORENSICS"*.
- **Omicidio di Palagonia, l'ivoriano ripreso dalle telecamere di sorveglianza.mp4**:
  - **SHA-256**: 35CCA15AB9F3F2AF086185330438D686569FAFFC62D0DDEFE7DF5CE537FEFB14
  - **Descrizione**: Filmato acquisito dal sito web utilizzando il software aTubeCatcher in formato MP4, relativo al duplice omicidio di Palagonia, come descritto nella relazione principale.
- **Omicidio di Palagonia, livoriano ripreso dalle telecamere di sorveglianza.srt**:
  - **SHA-256**: D18FABC21BF20F49D4AEE05B639887D18CEC6A6E41C9A4C619AA241A823BF98A
  - **Descrizione**: File .srt generato da ffmpeg durante il tentativo di estrazione dei sottotitoli dal video acquisito. L'operazione non è andata a buon fine a causa dell'assenza di flussi di sottotitoli nel file originale.
- **Copia Master.mp4**:
  - **SHA-256**: 35CCA15AB9F3F2AF086185330438D686569FAFFC62D0DDEFE7DF5CE537FEFB14
  - **Descrizione**: Copia forense master del filmato originale.
- **Copia Di Lavoro.mp4**:
  - **SHA-256**: 35CCA15AB9F3F2AF086185330438D686569FAFFC62D0DDEFE7DF5CE537FEFB14
  - **Descrizione**: Copia forense di lavoro derivata dalla copia master.
- **22.zip**:
  - **SHA-256**: D827359835F012D718615EEAE8878F7B56282B1545B2D0C1A6100A1A77320FAF
  - **Descrizione**: Archivio generato mediante acquisizione della pagina web con il software FAW. L'archivio contiene i file necessari per la visualizzazione offline della pagina acquisita. Il percorso "22 > 00002 > Objects > [00084][WEBCL]274822-multi-auto-palagoniavideosorveglianzapalerm" consente di accedere al video, una copia del quale è allegata con il nome *"VideoScaricatoDaFAW.mp4"*.
- **VideoScaricatoDaFAW.mp4**:
  - **SHA-256**: 35CCA15AB9F3F2AF086185330438D686569FAFFC62D0DDEFE7DF5CE537FEFB14

- **Descrizione**: Copia del video scaricato come elemento della pagina web acquisita con FAW. L'hash SHA-256 calcolato è identico a quello delle copie master e di lavoro ottenute con aTubeCatcher.

- **ProcessoDiAcquisizioneVideo.mp4**:
  - **SHA-256**: B8C0BDCAEC97004860C8AAEA5BEC1663A5F275328DBB6BA46874DA19556AE185
  - **Descrizione**: Filmato registrato con Bandicam, documentante l'intero processo di acquisizione della pagina web, download del video e calcolo degli hash.

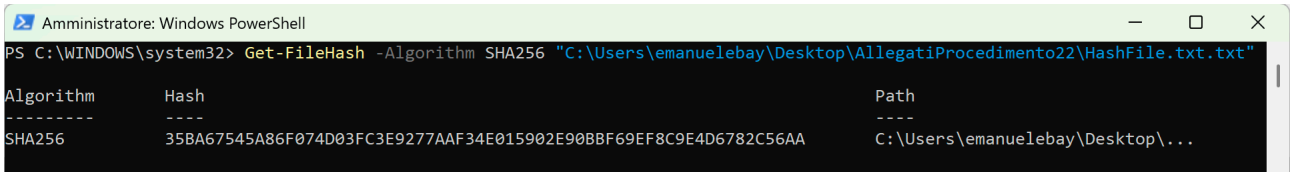
- **Frames.zip**:
  - **SHA-256**: 9999610989D744CA5ED43915E73B1E7A92EF863864B4C2B78F96622551E24F24
  - **Descrizione**: Archivio contenente i frame rilevanti del filmato analizzato acquisiti tramite l'opzione "Snapshot" di Amped Five.

- **VideoHashFramesZip.mp4**:
  - **SHA-256**: B2C6CEF4A0DBF84FD36F68FF20A7EADF287C05A46095488655F96F2388AAFE21
  - **Descrizione**: Filmato acquisito con Bandicam, che documenta il processo di calcolo degli hash dell'archivio *"Frames.zip"*.

- **OmicidioPalagonia.afp**:
  - **SHA-256**: 100A9E7A5673CBC3CDE6C7A8FCF2957A7678FE45F63797BA51324A9D646594C9
  - **Descrizione**: Progetto Amped FIVE utilizzato per le analisi forensi sul video.

- **OmicidioPalagoniaAA.aavp**:
  - **SHA-256**: 1E6CAF276F9556E9993AB7AF872846EDF38567E933A70D07B794E0B4DFAE0B58
  - **Descrizione**: Progetto Amped Authenticate Video utilizzato per le analisi di autenticità del video.

In aggiunta agli allegati tecnici sopra menzionati, è possibile consultare un file contenente i codici hash di ciascun allegato tecnico per verificarne l'integrità. Il file *"HashFile.txt"*, allegato alla presente consulenza, include un elenco completo degli hash calcolati per ogni documento e file relativo alla consulenza tecnica. Di seguito si riporta il codice hash SHA-256 relativo al file *"HashFile.txt"* per garantirne l'integrità:



Tutti gli allegati sono stati conservati e archiviati in conformità alle normative di digital forensics, al fine di garantirne la validità e la ripetibilità delle operazioni svolte. È possibile, quindi, risalire in qualsiasi momento al materiale originale e verificare la corrispondenza e l'integrità dei file acquisiti e analizzati. L'adozione di tali best practices assicura che ogni fase del processo di acquisizione e analisi sia documentata in modo chiaro e verificabile, preservando la trasparenza e l'affidabilità del lavoro svolto.

Bibliografia

[1] S. Battiato, *"Investigare su immagini e video (parte 1).pdf"*. UniCT, A.A. 2024/2025.

[2] L. Guarnera, *"DF202425 - Image Authentication.pdf"*. UniCT, A.A. 2024/2025.

[4] *Legge 48/2008 - Ratifica ed esecuzione della "Convenzione di Budapest".*

[3] Scientific Working Group on Digital Evidence (SWGDE). *"Best practices for Digital Evidence Collection".*

[4] ISO/IEC 27037:2012. *"Guidelines for identification, collection, acquisition, and preservation of digital evidence"*.

[5] Documentazione ufficiale di Amped Five e Amped Authenticate.

[6] Microsoft PowerShell: Documentazione ufficiale di Microsoft PowerShell, inclusa la guida al comando Get-FileHash.

[7] Casey, Eoghan. *"Digital Evidence and Computer Crime"*: Forensic Science, Computers and the Internet. Academic Press, 2011.

[8] Forensic Acquisition of Websites (FAW): *Manuale utente e documentazione tecnica*.

[9] *"Electronic Evidence Guide"* pubblicato da INTERPOL.

[10] European Cybercrime Training and Education Group (ECTEG). Materiale formativo su acquisizione forense e autenticazione delle prove.

[11] *Gonzalez, Rafael C., e Woods, Richard E. "Digital Image Processing". Pearson, 2018.*

[12] Khronos Group. Specifiche tecniche di codec video H.264.