

**Corso di Digital Forensics**

**Num Crediti : 9CFU**

**Nome : Andrea Filippo**

**Cognome: Salemi**

**Anno di Corso: 3° In corso**

**Matricola: 1000012617**



Università  
degli Studi di Catania

*Data Inizio Prova in itinere 12 Giugno 2020*

*Data Inizio dell'analisi 12 Giugno 2020*

*Data Fine Prova in Itinere 18 Giugno 2020*

# Sommario

- I. *Premessa*
- II. *Metodologia Di Lavoro, Mezzi e Dati utilizzati*
- III. *Analisi Video, Acquisizione e Analisi Tecnica*
- IV. *Conclusione*
- V. *Glossario*

# I. Premessa

*Il sottoscritto Andrea Filippo Salemi, Studente di Informatica, nato a Catania il 15/09/1995 e domiciliato ai fini del presente procedimento presso il DMI dell'Università di Catania, in data 12/06/2020 ore 11:00 veniva nominato, dal Prof. Sebastiano Battiato Ph. D, consulente tecnico nell'anno accademico 2019/2020- II° Prova in Itinere con il seguente quesito tecnico:*

*“Facendo riferimento al filmato video 17(<https://www.youtube.com/watch?v=moyJnx0Ial0>) il CT proceda all'acquisizione forense del filmato e all'analisi del contenuto; a tal fine si proceda utilizzando tecniche di image/video forensics al fine di verificarne l'integrità ed 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.”*

## II. Metodologia Di Lavoro, Mezzi e Dati utilizzati

*Il tecnico ha utilizzato il seguente hardware e software:*

*Hardware*

*Processore: Intel Core i5-4460 clock : 3.2GHZ x 4 col turbo boost fino a 3.4 GHZ*

*RAM : 16GB di ram DDR3 2400MHZ*

*SSD : 240GB*

*Hard disk : 2TB + 500GB*

*Lettori Ottici: Lettore DVD LG*

*Scheda Grafica : GTX 1050 Ti 4GB di vram.*

*Software :*

*- Sistema Operativo Windows 10 a 64 bit Pro Versione 1909*

*- Amped FIVE Data Build 20200306 Revisione 16112*

*- Legal Eye*

*- HashTab*

***Panoramica Del Software Utilizzato:***

Amped FIVE è un software a pagamento la quale il suo sito web è: <https://ampedsoftware.com/> questo software è spesso usato per il miglioramento delle immagini a fini forensi la quale possiamo estrapolare dei dati importanti che ci consentirà di trovare il colpevole.

LegalEye è un software a pagamento la quale il suo sito web è: <https://www.legaleye.cloud>  
Esso ci consente di catturare attraverso una macchina virtuale in cloud delle informazioni che possono essere utili ai fini legali con i vari codici hash, con le varie firme e così via.

Hash Tab è un software di cui abbiamo la possibilità di scaricare anche una copia gratuitamente, il suo sito è : <http://implbits.com/products/hashtab>.

In poche parole questo software ci consente di trovare gli hash in diversi formati la quale in md5, sha-1 e CRC32 e quindi ci consente di verificare l'integrità effettiva del file.

## HASH

Praticamente è un insieme di tecniche che generano un codice alfanumerico che consente di identificare un singolo file con una chiave univoca, basta cambiare un solo bit in un file per poter avere un hash totalmente differente.

## *III. Analisi Video, Acquisizione e Analisi Tecnica*

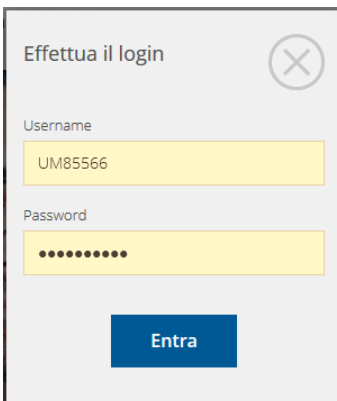
### **Analisi Video**

Il video è stato ripreso dalle telecamere il 20 febbraio del 2016 di notte, all'incirca dal 1:52 fino alle 2:16, dunque l'evento è durato intorno ai 25min .

Nel video si può osservare come l'automobile un "Audi S4" viene rubata da due ladri forzando la serratura del cancello dell'officina.

### **Acquisizione**

Per poter acquisire il video bisogna collegarsi su LegalEYE, inserendo le opportune credenziali associate all' account .



Questa immagine contiene il seguente HASH code:

CRC32: 90892181

MD5: E783FBC6F668330E29BA12C0DCAA2EA9

SHA-1: EA19C953D2B34675154FAC1F1E92B4444563C0E6

andando su inizia una nuova acquisizione si dovranno inserire i vari dati



Codici Hash di questa immagine:

CRC32: 41266A36  
MD5: 6DECC01160875DE687EC5263C5E7A2E6  
SHA-1: 9C12AD5576D810EB420C4E1C13BB8F55FB77DA8C

inserendo dei dati analoghi all’evento negli opportuni campi, il programma ci aprirà una macchina virtuale con una versione di windows server 2012 e con una versione modificata di Firefox.

Una volta finita l’acquisizione , genererà queste informazioni:

Descrizione: Furto di un automobile

Procedimento / Pratica: prova n17

Acquisizione iniziata : 13/06/2020 09:54:46 UTC+2

Acquisizione terminata : 13/06/2020 10:04:38 UTC+2

Durata : 10 minuti

Scadenza : 11/09/2020

Hash: a4bf0eafc1c67160ac7eecf0ba27cd939b7ed81d5dfcde364ad22cfaa137d3ab

ID : 8700d8df-b3b3-4b88-80f5-59965cb8c195

Queste sono tutte le informazioni utili associati all’acquisizione sull’account del tecnico forense.

Il software ci avrà generato un file “.zip” (compresso) chiamato :

legaleye\_andrea-filippo-salemi.zip con codice hash :

CRC32: A461ED99

MD5: F9D49DF6B58A233D294C45257062E3CF

SHA-1: 4ABE6096818920CBF2D46074FC4BA0EFDE864E3A

Estraendo il file compresso troveremo alcuni file :

legaleye_materiale_scaricato_andrea-filip...	13/06/2020 11:45	Cartella di file	
legaleye_screenshot_andrea-filippo-s	13/06/2020 09:53	Cartella di file	
legaleye_copiaforense_andrea-filippo-s.7z	13/06/2020 11:45	Archivio WinRAR	461.370 KB
legaleye_report_acquisizione_andrea-filip...	13/06/2020 11:45	PDF-XChange Vie...	336 KB
legaleye_report_acquisizione_andrea-filip...	13/06/2020 11:45	File TSR	3 KB
legaleye_video_andrea-filippo-s.mp4	13/06/2020 10:06	MP4 Video File (V...	201.736 KB

In cui abbiamo una copia forense in un file 7z (7zip), un fie TSR (presunto file di log), la

registrazione dello schermo in un formato mp4, un pdf in cui abbiamo l'intero report dell'uso del programma.

Il codice Hash del contenuto della cartella è :

-legaleye\_video\_andrea-filippo-s.mp4

CRC32: 298F8FF2

MD5: D9DDC765AFB2975535E11900752D2D3B

SHA-1: B6978623362C7303B418E7267E6416F4C2BB3381

- legaleye\_report\_acquisizione\_andrea-filippo-s.pdf.tsr

CRC32: D2942BE6

MD5: FB71F5883F3D32ED1280F6CA3287CC71

SHA-1: A28E5B020DFB7736D74FD5C7EB5A94424A15F3C6

-legaleye\_report\_acquisizione\_andrea-filippo-s.pdf

CRC32: 071E7724

MD5: D69C8DCBE36953F6E60F21E42A6D4A42

SHA-1: 90DB16380DDB63AB1E46D35F2C96866A1C6C71A8

-legaleye\_copiaforense\_andrea-filippo-s.7z (per motivi forense è protetta da password)

CRC32: 33441062

MD5: 3E8C294D68468DB9BDDF13672858979B

SHA-1: 63C0C214C85942C07127B7C7A509987FC0DCD2FF

bisogna escludere le due cartelle poiché essi non hanno alcun valore rilevante poiché essi sono vuote.

È stata acquisita anche il video usando un estensione esterna di Firefox chiamata download Helper, poiché ha consentito di recuperare il video in un formato più vicino a quello presente sul sito di youtube, consentendo di avere un video meno deteriorato, il video è il seguente:

ORDERZO NARDER Autoveicoli FURTO AUDI S4 20 02 2016 .mp4

CRC32: B0A28B38

MD5: 4DE9713D3678FE2ED8389264CD4C367D

SHA-1: EC6F88A38A137ABA73CB37FE695751885D6504F9

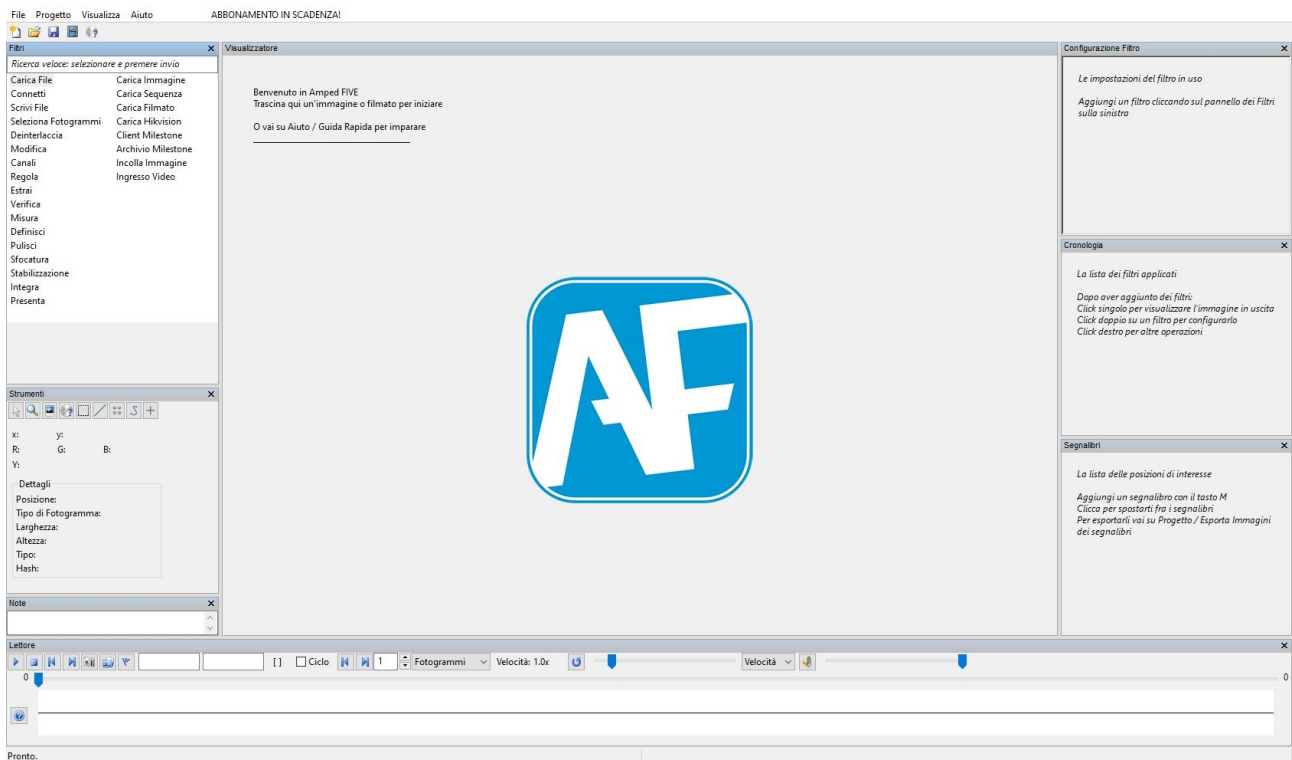
Con questo si sono presi tutti le possibili acquisizioni.

Adesso si è pronti per poter fare una analisi tecnica del video con Amped 5.

## -Analisi Tecnica Del video

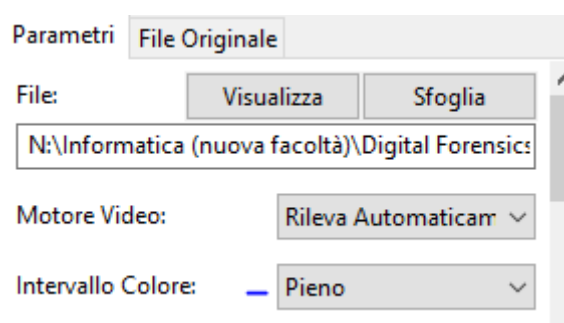
Nell'analisi tecnica bisogna trovare delle informazioni utili ai fini legali con amped FIVE.

Adesso bisogna aprire il programma citato in precedenza ed adesso :



L'interfaccia si presenta in modo molto semplice con la possibilità di caricare un video o un'immagine, per fare ciò bisogna caricare andando nell'icona dove è indicata la pellicola . 

Adesso, dopo aver aperto il video, troviamo la scena clou in cui i criminali mostrano involontariamente il loro volto e cercando di ricavare dalle immagini notturne i loro lineamenti facciali.



Dopo aver caricato il video su Amped Five viene inserito l'intervallo dei Colori "Pieno" così si avrà una gamma dei colori completa anche se in questo caso la situazione non cambia moltissimo poiché il video sostanzialmente essendo di notte è in scala di grigi (Prodotto dalle telecamere a infrarossi in scarsità di luce o con una luce notturna).

Al minuto 1:45.172 e al 3152 esimo fotogramma del video riprodotto, possiamo notare che uno dei due criminali guarda la telecamera quindi sembrerebbe la posa perfetta per riuscire a catturare qualcosa.



L'immagine in figura è "ODERZO NARDER Autoveicoli FURTO AUDI S4 20 02 2016 - 200614134037.jpg" con i relativi HASH:

CRC32: 76B5672B

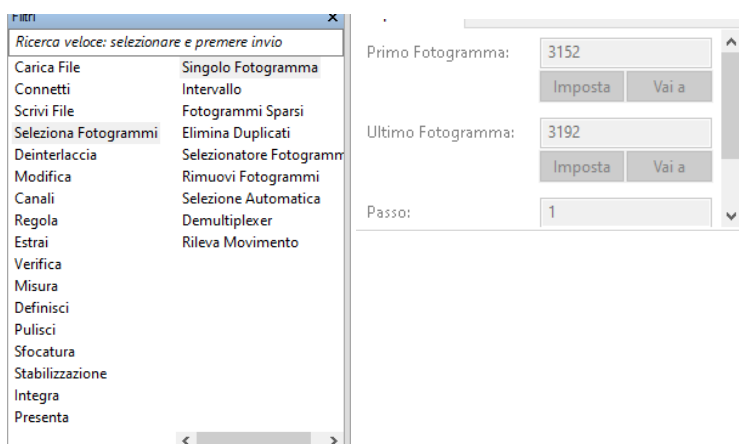
MD5: 969EDA0B4CBBB7ADBC1CAFBEC9D5710C

SHA-1: 528F606BAE979A4977EAFD2290169E24024FDFCB

Bisogna tagliare l'intervallo del video così da isolare la parte interessata:

Tagliamo il video utilizzando lo strumento intervallo:

Selezionando in filtro, la prima voce Seleziona Fotogrammi e poi su intervallo come è indicata in figura, per poi selezionare l'intervallo, in questo caso visionando il video sembra che l'intervallo ideale del primo criminale sia dal 3152 al 3192 (40 fotogrammi).





Adesso dopo questo , bisogna andare su: modifica → ritaglia esso è un normale filtro di “ritaglia” , ritaglia la parte dell’immagine che ci interessa, in questo caso il volto dell’uomo e aumentiamo la risoluzione con “Super Risoluzione” esso cattura i dettagli mancanti da più fotogrammi creando un immagine con una risoluzione più alta che comprende tutti i dettagli.

In questo caso purtroppo dopo numerosi tentativi non si è riusciti a migliorare l’immagine per poter ottenere delle immagini decenti da poter vedere un volto quando meno riconoscibile, è stato applicato anche il filtro “Gaussiano”.

La migliore immagine che possiamo ottenere è questa :



L’immagine ha dei difetti che non possono essere rimossi per trovare dei lineamenti facciali.

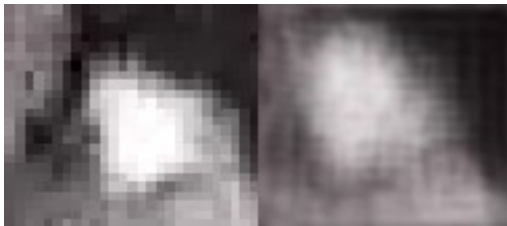
Informazioni immagine:

Nome Immagine: ODERZO NARDER Autoveicoli FURTO AUDI S4 20 02 2016 -200614142312.jpg

CRC32: 1FA3668D

MD5: 0D4DC4D2B7E0C36F4131BA7B87F66077

SHA-1: 05B4DB22850AB64E0DD1EE7F63202C8D3B6D2BF9



Questo è un confronto con l’immagine originale e quella modificata.

ODERZO NARDER Autoveicoli FURTO AUDI S4 20 02 2016 -200614155428.jpg

CRC32: 6B64325F

MD5: E42C2A5B90C25CDD745001ED53C8223B

SHA-1: C1D57FB736BF28229C036E96B0798DABECFBE63D

Un’altra cosa utile ai fini dell’investigazione è quella di calcolare l’altezza del criminale.

Creando una seconda catena copiando solamente l’intervallo precedente, torneremo all’immagine iniziale quella presa in precedenza, dovremo calcolare l’altezza del soggetto.

Per calcolare l’altezza del soggetto si usa, in questo caso, uno strumento che si trova in misura e si chiama, misura 1D, esso ha un funzione molto simile a quella del righello che consente di misurare il soggetto interessato attraverso una misura approssimativa di un oggetto.

In questo scenario, si potrà sapere dell’altezza del ladro misurando come punto di riferimento una sezione di muretto accanto al cancello che misura all’incirca 60cm (0.60m), utilizzando questo metodo e misurando il criminale si potrà notare un altezza molto approssimativa di 1.84m.



Nome File: ODERZO NARDER Autoveicoli FURTO AUDI S4

20 02 2016 -200614182015.jpg

CRC32: E54B129B

MD5: B6F77C0CD1682434AE7194288450B80A

SHA-1: 6EA31CE320E2D6F3C4C49CAE5A96A2230A92E393

NB: le misure con alta probabilità sono molto approssimative.

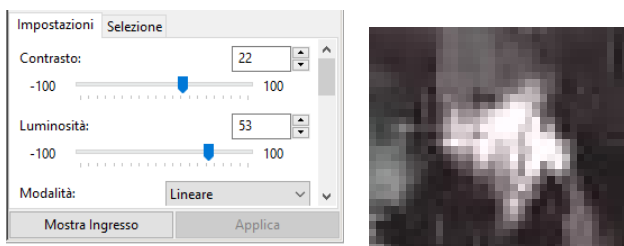
Adesso bisogna occuparsi del secondo criminale.



Il secondo criminale si volta verso la telecamera alle ore 1:53:39 per qualche secondo, si può provare quindi ad estrarre qualcosa utilizzando dei filtri.

Ritagliando la parte interessante come abbiamo fatto in precedenza così da concentrarci solo nel viso del 2° terminale.

Applicando il filtro del contrasto/luminosità, si otterrà questo risultato:



dove sembra difficile che il soggetto possa essere riconoscibile in modo coerente.

L'istantanea dopo aver applicato il filtro della luminosità/contrasto avrà i seguenti valori:

ODERZO NARDER Autoveicoli FURTO AUDI S4 20 02 2016 -200615100705.jpg

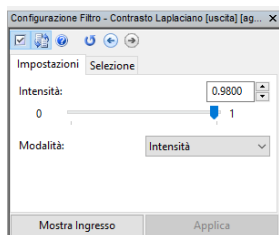
HASH:

CRC32: 7CC21BD9

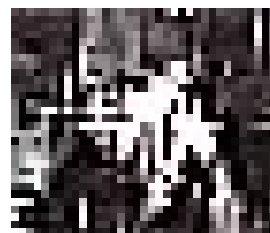
MD5: 49C852D85A656D6AF81FCBE072277A18

SHA-1: 0D77F95A96897E6B49A483682A0EB9C51F6866D5

Si può cercare di applicare il filtro Contrasto Laplaciano, così da migliorare leggermente la nitidezza dell'immagine:



con questi parametri si otterrà la seguente immagine :



Con le seguenti caratteristiche del codice hash :

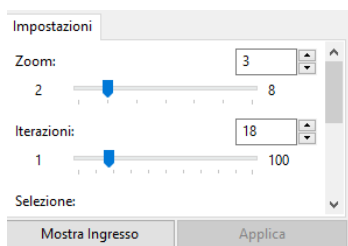
ORDERZO NARDER Autoveicoli FURTO AUDI S4 20 02 2016 -200615103502.jpg

CRC32: EDD7ADF7

MD5: 303E53096357EDB7E8B4EFC6CFA8CBC5

SHA-1: 3755B763E9B444F4833B34A335F0734605E01A78

Possiamo notare che pur applicando questo filtro è impossibile ottenere un volto visibile , quindi la soluzione sarebbe il filtro della super risoluzione , quindi, una volta applicato i filtri precedenti dovremo aggiungere il filtro della super risoluzione per poter aumentare la risoluzione ottenendo apparentemente una risoluzione più alta e quindi ottenere più dettagli ottenuti da fotogrammi simili.



Con questi parametri della super risoluzione si otterrà questa immagine:



L'immagine del soggetto riquadrato ha le seguenti caratteristiche:

ORDERZO NARDER Autoveicoli FURTO AUDI S4 20 02 2016 -200615105216.jpg

codici Hash

CRC32: BAB5859B

MD5: ED6592E334A5289FECC76F3AD2813283

SHA-1: B54C38ACF85D9505CB4AB15263B43F91536EE4C0

Sfortunatamente non si è potuto ricavare il volto neanche del secondo criminale, ma, si può provare in qualche modo a ricavare l'altezza anche del secondo criminale utilizzando le stesse e identiche tecniche del primo criminale, quindi, utilizzando il "misurazione 1D" , ed si otterrà, questa immagine:

Il soggetto è leggermente più basso rispetto al primo.



L'immagine ha le seguenti caratteristiche :

ORDERZO NARDER Autoveicoli FURTO AUDI S4 20 02 2016 -200616103635.jpg

Codice Hash:

CRC32: 0E51C7BD

MD5: CB1207483CC362D365FC7D9DBDFFB4A5

SHA-1: 9F0407DAAF845540B70CD71E54ABE113A6C2531F

## IV. CONCLUSIONI

In data 12/6/2020 è stato sottoposto al sottoscritto consulente tecnico dal Prof. Sebastiano Battiato il seguente quesito tecnico:

**“Facendo riferimento al filmato video 17 il CT proceda all’acquisizione forense del filmato e all’analisi del contenuto; a tal fine si proceda utilizzando tecniche di image/video forensics al fine di verificarne l’integrità ed estrarre tutte le informazioni utili per l’individuazione di luoghi, veicoli e identificazione di 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 tecnico forense ha effettuato l’acquisizione e l’analisi video dell’indirizzo :

<https://www.youtube.com/watch?v=moyJnx0IaI0>

seguendo le linee guida dettate dalle “best practices” forensi.

A quest’ultimo è stata scaricata e calcolata il codice hash in diversi formati:

ODERZO NARDER Autoveicoli FURTO AUDI S4 20 02 2016 .mp4

CRC32: B0A28B38

MD5: 4DE9713D3678FE2ED8389264CD4C367D

SHA-1: EC6F88A38A137ABA73CB37FE695751885D6504F9

Risoluzione: 854x480 durata complessiva : 6:47 min , bitrate di 15kb/s, frequenza fotogrammi : 29.97fps , dimensione video: 46,1 MB

*in modo tale da avere una prova legale del video.*

Il video riporta di due criminali, due ladri, che forzano la serratura del cancello di una presunta officina per rubare un’auto situata all’interno dell’edificio, dunque i due criminali durante l’analisi video. Il tecnico ha provato ad eseguire varie operazioni utilizzando Amped5 per estrapolare dei volti visibili ma a causa della scarsa qualità delle camere durante la visione notturna e a causa della compressione video avvenuta su youtube, le immagini risultano assai confuse, rendendo ciò (quasi) impossibile da estrarre.

È stato possibile, però , fare delle misure, anche se molto approssimative dei soggetti in quadrati nella camera, preso in riferimento a una sezione di un muretto, più vicino a ogni singolo soggetto così da non poter variare di molto dalla prospettiva dei fotogrammi.

Le rispettive altezze dei soggetti sono :

Criminale 1: 1.84m ;

Criminale 2: 1.81m;

Con Amped Five è stato generato un report con tutte le operazioni fatte sulle immagini, il report è stato generato in un formato pdf:

ODERZO NARDER Autoveicoli FURTO AUDI S4 20 02 2016 -200615105216.jpg.pdf

Con gli opportuni HASH:

CRC32: 2E19D82D

MD5: CF519A2E28C067FC8703C672E3025D1B

SHA-1: 62C3A79C4445B75EB974A3E35D029881302CF549

## V. Glossario

In questo glossario sono inserite tutte le parole tecniche che non facilmente comprensibile dai “non-tecnici” .

HASH: é un codice univoco che consente di identificare un file, cioè ogni file ha un singolo codice, basta anche solamente modificare un singolo carattere in un file per poter cambiare radicalmente il codice generato, che quindi consente di verificarne l'integrità.

Esistono vari algoritmi di hash e in questa relazione ne sono stati utilizzati tre :

MD5, SHA-1 e CRC 32.

Risoluzione: Un insieme di punti rettangolari (chiamati spesso anche pixel) inseriti in una matrice, l'insieme di questi pixel accesi formano un'immagine, più pixel ci sono in un'immagine e più l'immagine sarà fedele alla realtà, quindi in breve a livello matematico possiamo dire che è la moltiplicazione delle righe e delle colonne (RxC) che vanno a formare il numero totale di pixel in un'immagine, quindi, di conseguenza, più pixel abbiamo più la risoluzione sarà alta.

SuperRisoluzione: è un filtro che consente di ottenere più dettagli e un'immagine più grande facendo la media di tutti i fotogrammi simili tra loro, spesso escono fuori immagini molto più nitide rispetto a quella di partenza, soprattutto nell'ambito investigativo, grazie alla super risoluzione spesso si possono ricavare targhe, volti, etc, anche se non è sempre efficace.

Filtro Gaussiano: è un filtro simile alla mediana che consente di preservare di più le forme riducendo il rumore.

Filtro mediano: è un filtro che consente di eliminare i rumori salii e pepe (il rumore che veniva causato ad esempio nella connessione TV analogica quando il segnale non era ottimo).

Nel file Hash.xls (file apribile con Excel) sono stati inseriti tutti gli hash.

Catania, 17 Giugno 2020,

Il CT,  
Andrea Filippo Salemi