Università di Catania

Relazione Tecnica

DIGITAL IMAGING FORENSICS
CASO ID #CT003181

REPERTI IN ESAME:

- N. 3 IMMAGINI IN FORMATO JPG

Zerbo Marco

31/05/2011

ANALISI FORENSE

Allegati:

Immagini postprocessate:

- *20110522_033-postprocess.bmp,*
- *20110522_034-postprocess.bmp,*
- *20110522_034-Ingrandimento.bmp*
- *20110522_036-postprocess.bmp,*
- *20110522_036-ELA.jpg*

Report Amped Five

- *20110522_033-AmpedReport.htm*
- *20110522_034-AmpedReport.htm*
- *20110522_036-AmpedReport.htm*

Report JPEGSnoop

- *20110522_033-JPEGSnoop.txt*
- *20110522_034-JPEGSnoop.txt*
- *20110522_036-JPEGSnoop.txt*

Università di Catania

RELAZIONE TECNICA

* * *

Il sottoscritto, Zerbo Marco, laureando in Informatica presso l'Università di Catania, facoltà di Scienze MM.FF.NN, amministratore di sistema presso Foo inc., amministratore di sistema presso l'Università di Catania, in ordine all'incarico conferito dal dott. Sebastiano Battiato in data 30/05/2011

RILEVA ED ESPONE

Il presente elaborato, con riferimento ai reperti di seguito identificati, si pone l'obiettivo di documentare:

- **la presenza di elementi rilevanti nelle immagini digitali oggetto di analisi.**
- **documentare le attività eseguite**

Premessa

Le attività che sono state svolte per la redazione di tale documento sono state eseguite in concordanza con le metodologie di indagine e di trattamento dei reperti informatici, consolidate e riconosciute a livello nazionale ed internazionale dalla comunità scientifica e dalle forze dell'ordine, aventi ad oggetto le procedure relative al trattamento dei reperti informatici.

Tali linee guida sono state seguite scrupolosamente nell'ambito dell'accertamento tecnico in parola, inoltre verranno forniti puntuali riscontri di quanto svolto.

Strumenti e procedure utilizzate

I reperti soggetti ad analisi sono stati preventivamente copiati in copia conforme all'originale in maniera da mantenere il reperto originale nel caso in cui si richiedano eventuali analisi più intrusive che potrebbero alterare anche solo temporaneamente il contenuto dei reperti.

Di seguito viene esposto l'ambiente informatico con la quale sono state espletate le attività di analisi sui reperti.

> Sistema Windows XP Professional Edition SP2 come ambiente operativo per l'uso dei seguenti software: Amped Five, JPEGSnoop, Adobe Photoshop CS4 , Error Level Analysis di http://errorlevelanalysis.com

Il sistema è stato virtualizzato utilizzando con VMWare Workstation 7 su Windows7 64bit e non presenta ulteriori software di terze parti installati al di fuori di quelli sopraelencati.

Acquisizione

In data 31/05/2011 il sottoscritto viene incaricato di prelevare un archivio ZIP denominato *caso81.zip* contenete i reperti da sottoporre a perizia. L'indirizzo da cui prelevare l'archivio è il seguente:

http://www.dmi.unict.it/~battiato/CF1011/prova/caso81.zip

Tale indirizzo risulta essere identificato correttamente come di proprietà dell'Università di Catania.

L' archivio quindi ottenuto viene identificato in un (1) archivio ZIP denominato **"caso81.zip"**.

Tale archivio risulta contenere in formato compresso i seguenti tre file:

20110522_033.JPG	Immagine formato JPG
20110522_034.JPG	Immagine formato JPG
20110522_036.JPG	Immagine formato JPG

Considerato il carattere di ripetibilità che deve avere tale perizia ai sensi di legge; considerato che la consegna dei reperti è avvenuta tramite un canale non sicuro (internet), si è pertanto resa necessaria l'identificazione univoca dei reperti, così da poterne certificare l'integrità al momento dell'acquisizione.

Di seguito sono indicati degli identificativi univoci ottenuti mediante l'algoritmo hash md5 (cfr. voci Glossario) applicato ai file jpg. L'uso di questi algoritmi è consigliato dalle *best practice* di informatica forense riconosciute a livello internazionale[1].

Nome File	Hash md5	Data ultima modifica
20110522_033.jpg	2b9b018087a977c2b281ac8a1bf2f142	23 Maggio 2011 ore 9.12
20110522_034.jpg	38f8770aa733e79f04612ee5371d6b32	23 Maggio 2011 ore 9.12
20110522_036.jpg	dda6e56798345570ab44a407eb5ad728	23 Maggio 2011 ore 9.13

La dimensione dei file decompressi è:

20110522_033.jpg	111.038 byte
20110522_034.jpg	221.046 byt
20110522_036.jpg	182.274 byte

[1] Carrier B., File system forensic analysis , Addison-Wesley, 2005 – Cfr. "General Guidelines"

E' stata effettuata quindi una copia conforme dei tre file. Le copie sono state quindi denominate posponendo il suffisso:
- *copia* ai nomi originali dei file.

Di seguito una tabella riassuntiva che elenca i nomi delle nuove copie e la conformità ai reperti originali.

Nome File	Hash md5
20110522_033 - copia.jpg	2b9b018087a977c2b281ac8a1bf2f142
20110522_034 - copia.jpg	38f8770aa733e79f04612ee5371d6b32
20110522_036 - copia.jpg	dda6e56798345570ab44a407eb5ad728

Analisi forense delle immagini

Obiettivi

L'obiettivo primario da raggiungere è identificare eventuali informazioni rilevanti presenti nelle scene ritratte nelle foto, identificare luoghi, date ed orari.

Attività Svolte

E' stata quindi condotta un'analisi preliminare sui metadati dei file mediante il software JPEGSnoop che mostra i dati EXIF (vedi voce glossario) relativi all'immagine. Successivamente alla fase preliminare si è proceduto analizzando e processando le immagini con sia con Amped Five che con Adobe Photoshop, applicando anche dei filtri in maniera da estrapolare quante più informazioni possibili.

Analisi preliminare (JPEGSnoop)

JPEGSnoop è un software che permette di visualizzare i metadati EXIF/IPCT/XMP relativi ad un immagine, mostra inoltre altri dati relativi alla compressione JPEG, come ad esempio le tabelle di quantizzazione applicate ai livelli crominanza e luminanza, le tabelle di Huffman, e permette di riconoscere se l'immagine è stata acquisita da una determinata fotocamera ovvero è stata manipolata con un software di image editing. JPEGSnoop si avvale di un database che cataloga migliaia di fotocamere differenti, ad ognuna delle quali è associata una tabella di quantizzazione nota. Spesso, infatti molte fotocamere digitali, utilizzano per la compressione delle immagini delle tabelle di quantizzazione predefinite così da abbattere i tempi di calcolo che potrebbero essere elevati per determinare dinamicamente delle tabelle ottimali, soprattutto per dei *sistemi embeded* che hanno solitamente capacità di calcolo ridotte. In tal modo, JPEGSnoop cataloga e identifica univocamente con estrema precisione un set di fotocamere molto elevato. Tale set è correntemente aggiornato periodicamente grazie al contributo degli stessi utilizzatori del software.

In generale i metadati possono essere oggetto di contraffazione, attraverso appositi software che ne permettono la modifica, senza lasciare traccia alcuna delle avvenute operazioni. Le informazioni fornite dai metadati sono quindi in genere di limitata autorevolezza e da contestualizzare con le altre ricavabili visivamente e analiticamente dalle immagini stesse.

Riguardo le tre immagini oggetto di analisi, resta comunque plausibile la genuinità delle informazioni ottenute dai metadati EXIF mostrate da JPEGSnoop, motivazioni verranno addotte di seguito.

Come si evince dai report prodotti da JPEGSnoop le le tre immagini sono state verosimilmente acquisite tramite una fotocamera integrata su:

telefono cellulare Nokia N900,

in data **22 Maggio 2011** tra le ore **21:11** e le ore **21:13**

(vedi dettaglio in allegato A) .

Tutte e tre le foto hanno **dimensioni 2560x1440 pixel (3.5megapixel in formato 16:9).**

I metadati riportano altresì seguenti parametri di impostazione usati per la fotocamera:

- sensibilità ISO-800,
- apertura diaframma F2.8,
- tempo di esposizione 0.066 s (33/500) (1/15),
- zoom 1/1,
- distanza focale 5mm,
- utilizzo flash: no.
- risoluzione 300dpi

(Per un dettaglio più approfondito si rimanda all'allegato A che mostra i dati estratti dal software JPEGSnoop.)

Analisi immagini e postprocessing

Foto denominata 20110522_033 - copia.jpg

Sembra essere stata scattata in un luogo chiuso e molto buio, con due fonti di luci molto deboli e lontane dal luogo di ripresa.

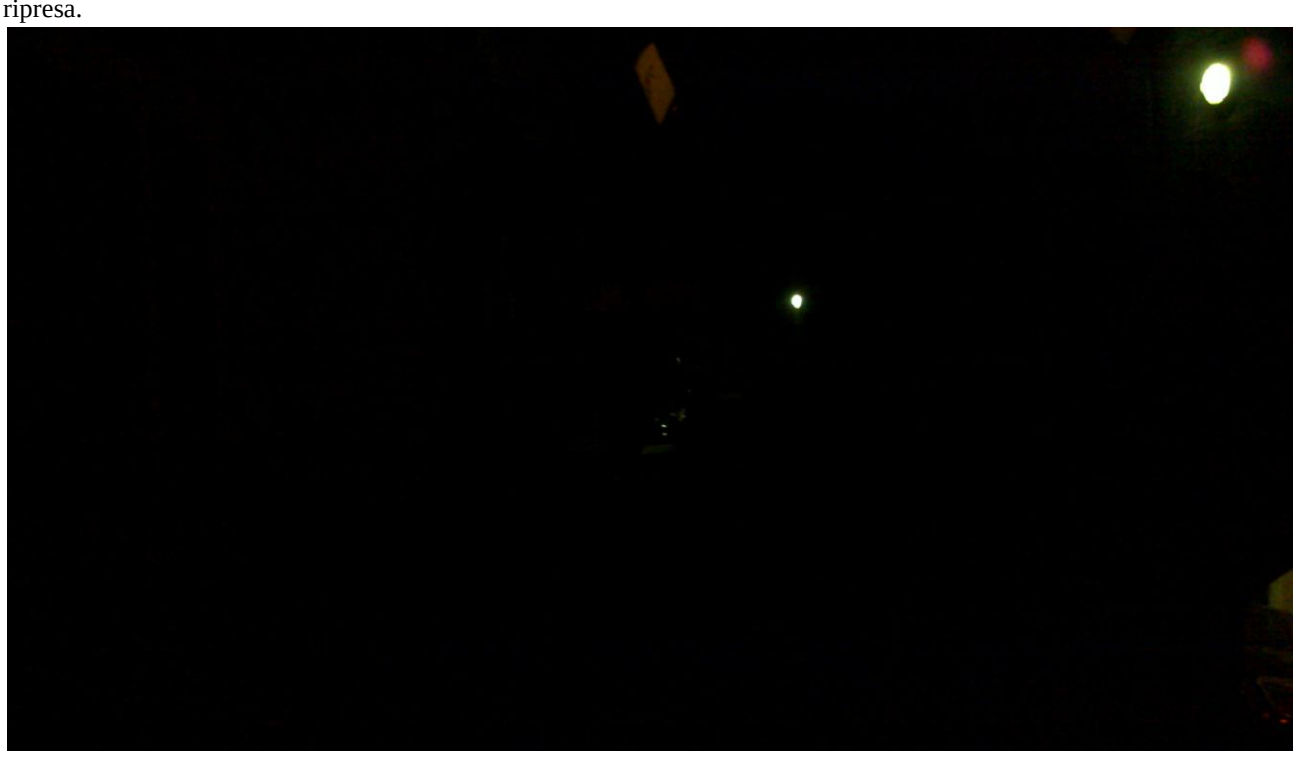

Fig 1. *20110522_033 - copia.jpg (Originale)*

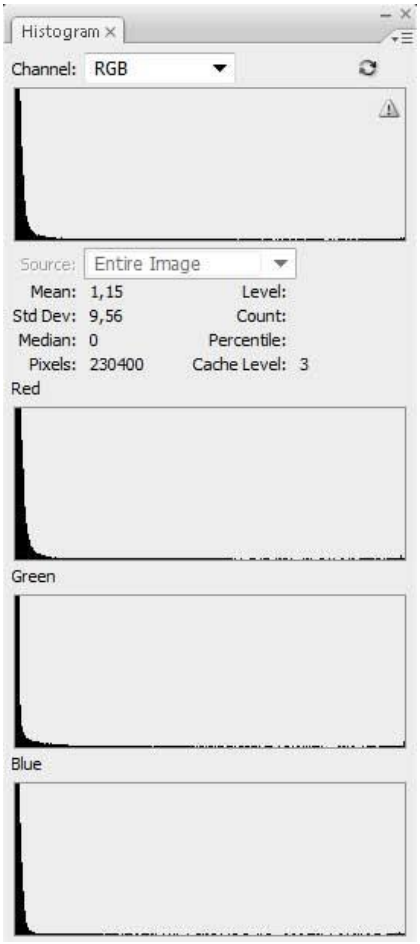

Fig 2: Istogramma *20110522_033 - copia.jpg (Originale)*

Ad una prima disamina l'istogramma (fig. 1) dell'immagine presentava valori presenti solamente relativamente alle frequenze più basse, e quindi per i toni più scuri. Tutte le informazioni sulle frequenze medie o alte non risultano minimamente presenti.

Enfatizzando le tonalità di ombre e luci utilizzando il filtro Curve di Amped Five, si riesce a scorgere apparentemente una parete sulla sinistra con un ingresso. Si tratta possibilmente di un ambiente chiuso e abbastanza ampio come un garage o un sotterraneo. Al centro dell'immagine sono presenti altri riflessi su sfondo nero che sembrano come fari e targhe di automobili (fig 2).

Tuttavia l'applicazione di una curva di livelli che enfatizzi i toni più chiari, comporta il risalto del rumore introdotto dal sensore fotografico rendendo l'immagine complessiva parecchio sporca e sgranata. Nonostante l'applicazione di filtri che attenuano il rumore e di un filtro convolutivo di media, non risultano visibili particolari apprezzabili.

Resta quindi molto aleatorio potere descrivere la scena con un margine di dettaglio apprezzabile.

Cfr. immagine processata, filtri applicati e bibliografia allegati:

- immagine *20110522_033-postprocess.bmp*,
- report filtri e bibliografia *20110522_033-AmpedReport.htm*

Fig 3. 20110522_033-postprocess.bmp (Processata)

Foto denominata 20110522_034 - copia.jpg

Il luogo ripreso appare essere verosimilmente un garage dove sono parcheggiati veicoli, alcuni dei quali ripresi attraverso un riflesso su uno specchietto retrovisore di un'autovettura.

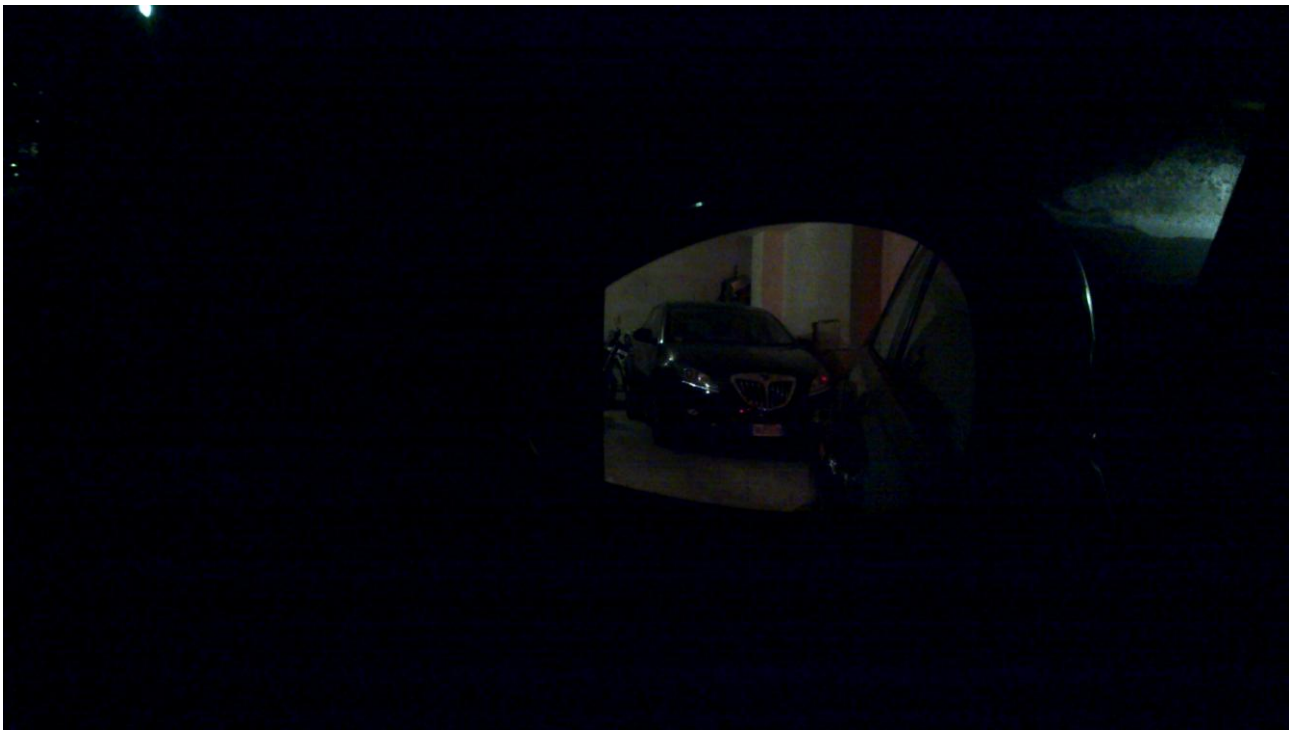

Fig 4. *20110522_034 - copia.jpg (Originale)*

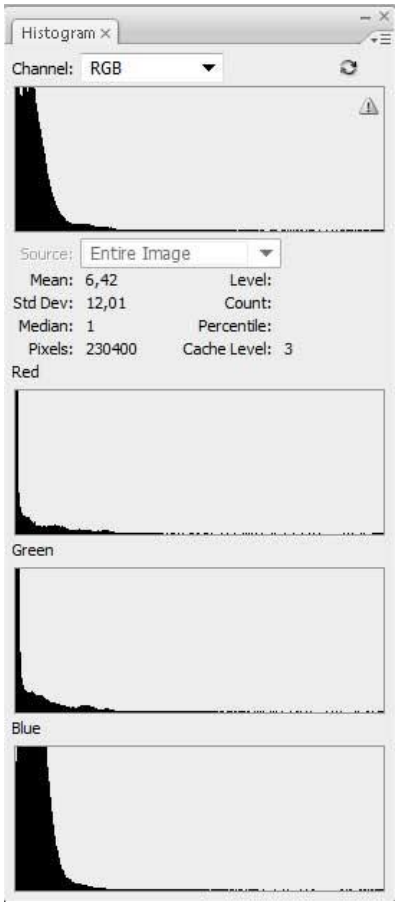

Fig 5: Istogramma *20110522_034 - copia.jpg (Originale)*

Anche per questa immagine valgono le stesse considerazioni fatte per la precedente riguardo alla luminosità della scena. Come si evince dall'istogramma dell'immagine, sono presenti per lo più frequenze basse che indicano la presenza di toni molto scuri. Quei pochi campioni sulle alte frequenze riguardano la scena ripresa nel riflesso dello specchietto.

Si è quindi scelto di esaminare accuratamente tale scena avvalendosi dei filtri di Amped Five.

Si è inizialmente specchiata l'immagine, poiché la scena appunto riprendeva un soggetto riflesso su uno specchietto di un'autovettura.

Quindi si è proceduto enfatizzando le tonalità più chiare agendo con il filtro curve, e applicando una maschera di contrasto alla regione identificata come targa di un **autovettura Lancia Yspilon** in maniera da migliorarne la lettura senza introdurre artefatti rilevanti.

Successivamente attraverso un'operazione di convoluzione si è cercato di attenuare il cosiddetto rumore (cfr voce di glossario), maggiormente visibile dopo l'introduzione dei processa menti precedenti, applicando un filtro di media ai bit che compongono l'immagine.

Infine si sono eliminate le informazioni sul colore convertendo l'immagine in scala di grigi, per eliminare disturbi visivi e aberrazioni cromatiche introdotte dal tipo sensore fotografico usato dal telefonino cellulare, poco sensibile alla ripresa di scene buie. (fig. 6)

Fig 6. *20110522_034 - postprocess.bmp (Processata)*

Nonostante l'applicazione di tale catena di filtri volta al miglioramento della qualità dell'immagine, non è possibile identificare con ragionevole certezza la targa dell'autovettura, tutt'al più si ha come l'impressione di scorge qualche numero che compone la **targa: ** 275 *F** dove gli asterischi fanno da segnaposto per i caratteri completamente illeggibili. (fig. 7)

Fig 7. 20110522_034-Ingrandimento.bmp (Processata)

Cfr. immagine processata, filtri applicati e bibliografia allegati:

- immagine *20110522_034-postprocess.bmp*, immagine *ingrandimento 34.bmp*
- report filtri e bibliografia *20110522_033-AmpedReport.htm*

Foto denominata 20110522_036 - copia.jpg

Tale immagine ad una prima disamina risulta completamente nera e priva di qualsiasi soggetto ripreso (fig 8). Lo stesso istogramma (fig 9) mostra unicamente la presenza di campioni unicamente per le frequenze più basse

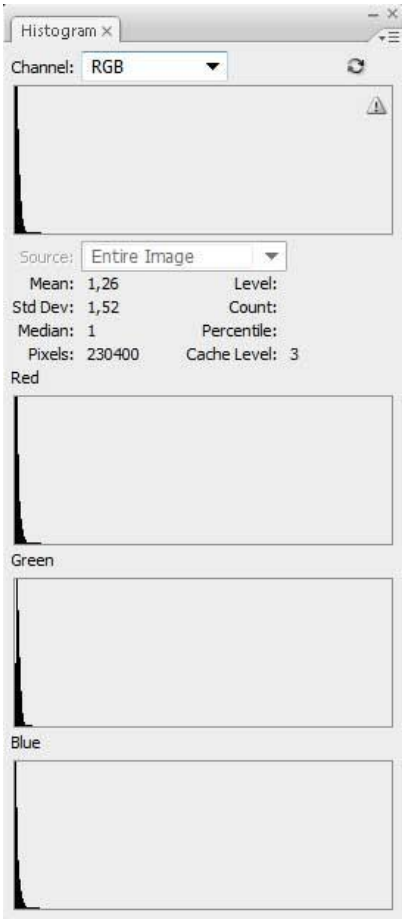

Fig 9: Istogramma *20110522_036 - copia.jpg (Originale)*

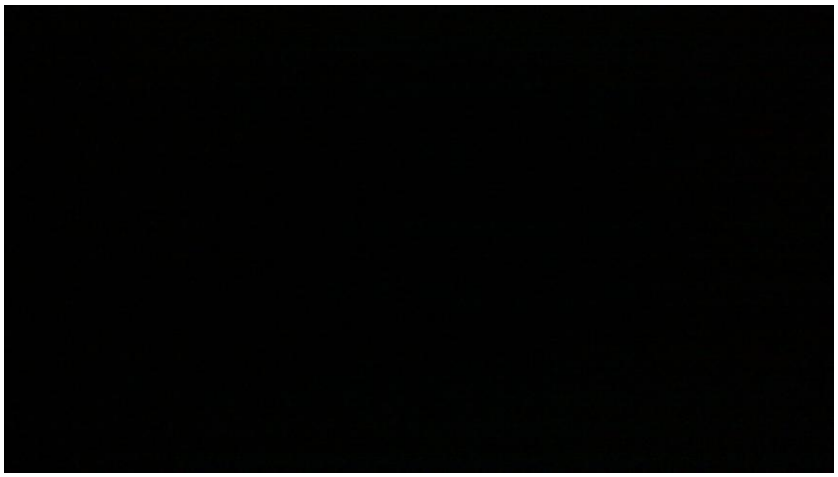

Fig 8. *20110522_036 - copia.jpg (Originale)*

Enfatizzando le tonalità più chiare non si riesce comunque a notare alcuna variazione nel pattern. Si amplifica invece unicamente il rumore del sensore della fotocamera e risultano visibili unicamente pixel rossi, verdi e blu, colori primari che vengono determinati in fase di acquisizione dell'immagine dal sensore della fotocamera (fig 10).

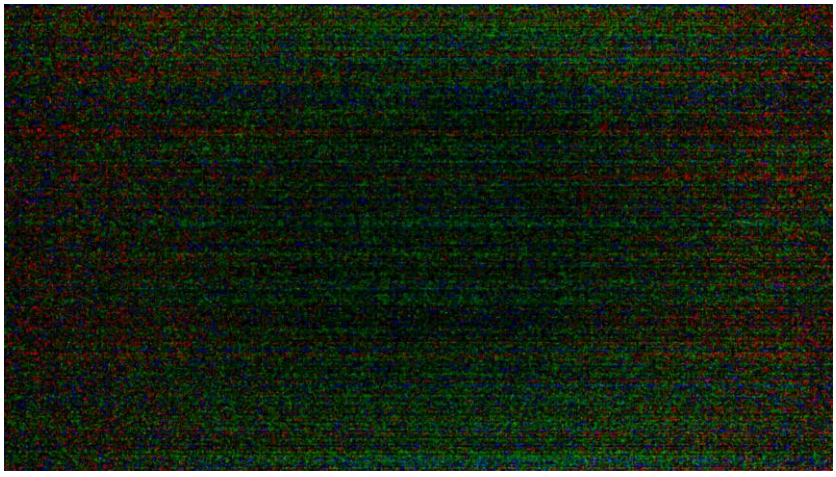

Fig 10. *20110522_036 - postprocess.bmp (Processata)*

Analizzando lo spettro del rumore utilizzando l'algoritmo di http://errorlevelanalysis.com (fig 11), non si è evinta alcuna informazione ulteriore che avrebbe potuto dare luogo a ipotesi di contraffazione, pertanto l'immagine appare essere l'originale acquisito con la fotocamera. Probabilmente il soggetto ha scattato la foto per sbaglio otturando completamente l'obiettivo, in quanto non è presente alcuna fonte di luce, diffusa o locale.

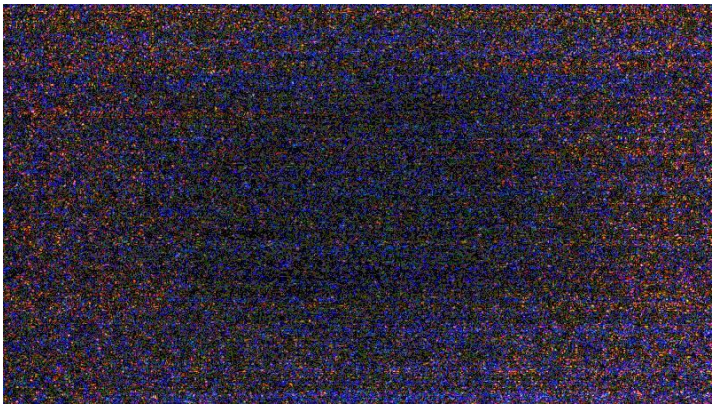

Fig 11: ELA-*20110522_036 - copia.jpg (Analisi livello rumore)*

Conclusioni

Premesso che:

- In data 30/05/2011 venivano consegnate al sottoscritto 3 immagini in formato JPG raffiguranti tre fotografie.
- Nella stessa data il sottoscritto procedeva a esaminare copie conformi dei reperti;

alla luce di quanto esposto è possibile affermare con ragionevole certezza quanto segue:

a) Le tre fotografie venivano scattate utilizzando una fotocamera digitale incorporata su un telefono cellulare Nokia N900 in data 22 Maggio 2011 fra le ore 21.11 e 21.13.

b) Il luogo dove venivano scattate le foto appare verosimilmente lo stesso per le prime due immagini, ossia un garage o un sotterraneo ove sono parcheggiate autovetture.

c) Nonostante l'elevata risoluzione delle tre immagini, queste si presentano di pessima qualità e molto scure in quanto la scena della ripresa non era sufficientemente illuminata e le impostazioni della fotocamera, per sopperire alla mancanza di luce, hanno richiesto una sensibilità ISO (simulata) di tipo ISO-800 che ha introdotto molti artefatti e aberrazioni cromatiche. Ciò ha limitato parecchio le operazioni di analisi che si potevano effettuare sulle immagini

d) la fotografia denominata *20110522_034.jpg* inquadra attraverso uno specchietto retrovisore una autovettura di tipo Lancia Ypsilon, probabilmente di colore scuro metallizzato come nero o blu, verosimilmente con targa europea e con ogni probabilità Italiana.

e) Non è stato possibile riconoscerne la targa a meno di qualche cifra ipotizzata con un elevato margine di errore causato dall'introduzione degli artefatti da parte del sensore in fase di acquisizione. Le cifre della targa ipotizzate sono le seguenti, dove gli asterischi assolvono a segnaposto per le cifre sconosciute: **: ** 275 *F**

In Fede,

Catania 02/06/2011 Marco Zerbo

Glossario

Hash

Algoritmo unidirezionale che riassume tramite una funzione matematica non iniettiva una sequenza di dati in una stringa di pochi bit. 128 bit sono assegnati a un hash md5, 160 bit ad un hash sha1.

Metadati EXIF

Acronimo per Exchangeable Image File Format. E' una specifica per le immagini JPG e TIFF ed utilizzata dalle fotocamere digitali per includere informazioni aggiuntive alle immagini. Tali informazioni (metadati) riguardano:

- Informazioni di date ed ora.
- Impostazioni della fotocamera come il modello ed il produttore della fotocamera, orientamento dell'immagine, apertura, velocità otturatore, lunghezza focale, bilanciamento del bianco, informazioni di sensibilità ISO,c oordinate geografiche del luogo della ripresa
- Una miniatura per visualizzare un'anteprima sul display LCD della fotocamera
- Descrizioni ed informazioni di copyright.

Rumore Digitale

Le fotocamere digitali utilizzano un sensore elettronico che assolve ai compiti della pellicola tradizionale. Questo acquisisce le immagini sottoforma di segnale elettrico. Tale segnale viene amplificato in modo da riuscire a prendere una gamma più ampia di frequenze. In questo modo si introducono delle variazioni sul segnale che mutano le forme d'onda delle frequenze originali partecipando così a creare il cosiddetto rumore digitale.

Oltre al rumore dovuto all'amplificazione del segnale, vi è inoltre un rumore intrinseco al sensore dovuto sia alle dimensioni dei pixel del sensore (maggiore sono i megapixel, maggiore è la quantità di rumore introdotta), sia all'elettronica dei componenti del sensore e quindi alla dispersione termica che può indurre ulteriori quantità di rumore nelle immagini.

In generale le cause del rumore si possono riassumere in:

- Dimensioni del sensore. Un sensore grande è generalmente meno rumoroso di uno piccolo
- Dimensioni dei singoli pixel. A parità di dimensioni del sensore, più megapixel introducono più dettaglio ma anche più rumore
- Sensibilità ISO impiegata. Poca luce = alto valore ISO = maggiore amplificazione del segnale = più rumore
- Temperatura del sensore
- Processi produttivi e materiali impiegati

Il rumore digitale è visibile nelle fotografie digitali come una grana multicolore diffusa in maniera causale.