Media Forensics Analysis In Digital Times

By

Catalin Grigoras

Presented At

The Digital Forensic Research Conference

DFRWS 2014 USA Denver, CO (Aug 3rd - 6th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http://dfrws.org
Media Forensics Analysis in Digital Times

Catalin GRIGORAS, Ph.D.
Assistant Professor, UCD, NCMF
Disclaimer

The products or software presented in these slides are only mentioned and used as tools for forensic analysis and the intention of this presentation is solely educational.
Forensic sciences are concerned with the explanation or reconstruction of events, attempting to determine:

- What happened?
- How it happened?
- Where it happened?
- When it happened?
- Who was involved?
Basic Principles in Media Forensics

The stages of the physical evidence process

- Occurrence of the crime
- Recovery
- Media Analysis
- Interpretation
- Presentation
Basic Principles in Forensic Audio

The stages of the physical evidence process

- Occurrence of acoustic crime
- Recovery
- Audio Analysis
- Interpretation
- Presentation
Basic Principles in Forensic Image & Video

The stages of the physical evidence process

- Occurrence of the crime
- Recovery
- Image Analysis
- Interpretation
- Presentation
Forensic Evidence

Physical (Classical) Evidence

“Physical objects that establish that a crime has been committed, can provide a link between a crime and its victim, perpetrator” (Saferstein, 2004).

Digital Evidence

“Digital data that establish that a crime has been committed, can provide a link between a crime and its victim, or can provide a link between a crime and the perpetrator” (Carrier & Spafford, 2003)
Basic Principles in Forensic Sciences

1. Principles Concerning Evidence Recovery

**Nothing should be added, lost, damaged or obliterated in the Recovery process.** Particular attention should be paid to avoiding contamination. Where there is risk of losing or damaging evidence, great care should be taken and the appropriate experts should be called in. Exhibit items should be safely and securely packaged as soon as possible. Crime scenes and recovered evidence may pose biological or chemical hazards. Appropriate health and safety measures must be taken when collecting and transporting evidence.
Use:
- Hardware/software write blockers (e.g. Tableau 8, ComboDock, etc.)
- Forensic bit-stream copy software (e.g. FTK Imager, WinHex, EnCase, etc.)
- HASH tools (e.g. HASH Tab, jacksum, iSide, digestIT, FTK Imager, etc.)
2. Principles Concerning Analysis

Use scientific methods that undergo developmental validation following the scientific method to ensure:

- the **accuracy & precision** $\Rightarrow$ exactness
- the **repeatability** = same scientist can repeat the analysis and obtain same, similar or compatible results
- the **reproducibility** = other scientists can repeat the same analysis and obtain same, similar or compatible results of the procedure.
Basic Principles in Media Forensics

Basic Principles in Forensic Sciences

3. Principles Concerning Interpretation

**Principle of individuality**: Two evidence (objects or phenomena) may be indistinguishable but no two evidence or phenomena are identical.

**Principle of comparison**: Two evidence are said to match when there are no unexplained, forensically significant differences between them.
4. Principles Concerning Presentation

Working within an ethical framework, a forensic scientist should fully disclose and present impartial evidence which is readily understandable and neither overstated nor understated.

It is important for forensic scientists to have and follow a code of ethics. Most forensic professional associations (ENFSI, IAFPA, etc.) have such codes, which their members must follow.
The International Organization on Computer Evidence (IOCE) principles approved at the International Hi-Tech Crime and Forensics Conference in October 1999:

1. Upon seizing digital evidence, actions taken should **not change that evidence**.
2. When it is necessary for a person to access original digital evidence, that person must be forensically **competent**.
3. All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully **documented**, preserved, and available for review.
4. An individual is **responsible** for all actions taken with respect to digital evidence while the digital evidence is in their possession.
Digital Evidence

Original Digital Evidence

SWGDE & IOCE Digital Evidence Standards and Procedures (1999):

*Original Digital Evidence*: Physical items and the data objects associated with such items at the time of acquisition or seizure.

Media manipulation

Media manipulation is the application of different editing techniques to audios/photos/videos/IT data/information/evidence in order to create an illusion or deception, through analogue or digital means.
Forensic media concepts

An analogue evidence (audio recording, photo or video recording) always has an original to which it relates in either negative or positive form (i.e. the negatives from which photographic prints are made, transparencies or the magnetic recording on a video or audio tape). Copies can be made from the original and normally there will be little difference between them, but as further copies are made from these copies then the quality is likely to deteriorate.

For a digital evidence the 'original' consists of the data first recorded in memory, from which the digital audio signal or image can be generated. Because the recorded information is represented as a finite set of numbers, exact copies may be made. Each stage of copying is precise and there is no loss of information quality between generations. Thus it becomes impossible to say which is a first generation: the implication is that any digital data can be thought of as being 'the original' even if it is produced from a copied set of data, unless it is tagged in some way to identify it as the first generation made.
Forensic Authentication of Digital Media Evidence

1. **Hardware**: write-blockers, PC, digital audio recorders, mics, etc.
2. **Software**: write-blockers, digital imaging, HASH, hex viewers, structure/logic analysis, image/viewers editors, analysis, etc.
3. **Databases**: file samples, user manuals*, software, etc.
4. **Analysis Methods**:  
   4.1. Photos, forensic bit-streams, HASH, create working copy  
   4.2. MAC, metadata, structure/logic  
   4.3. Pixel level analysis  
   + visual inspection/analysis
Digital Photography: JPEG, RAW

Scene → Lens → Filters → CFA → Sensor/Matrix → DIP → Storage

Scene Inconsistencies
- Auto-exposure,
- Auto-focus,
- Image stabilization

Auto-exposure, Auto-focus, Image stabilization
- Scene Inconsistencies
- IR, Anti-aliasing filters
- Chromatic aberrations, Spherical aberrations

Colour Filter Arrays: GRGB, CYGM, RGBE, CMY
- Colour Filter Arrays: GRGB, CYGM, RGBE, CMY
- Sensor/Matrix (CMOS, CCD…)

Sensor/Matrix (CMOS, CCD…)
- Sensor/Matrix (CMOS, CCD…)
- Digital Image Processing: White balancing, noise reduction, sharpening, aperture & gamma correction, etc.

Digital Image Processing: White balancing, noise reduction, sharpening, aperture & gamma correction, etc.
- Digital Image Processing: White balancing, noise reduction, sharpening, aperture & gamma correction, etc.
- Digital Storage Device (HDD, memory card, etc.)

Digital Storage Device (HDD, memory card, etc.)
Digital Photography: JPEG, RAW

Scene → Lens → Filters → CFA → Sensor/Matrix → Digital Image Processing → Storage

Analogue → Digital

Scene Inconsistencies → Auto-exposure, Auto-focus, Image stabilization

Auto-exposure, Auto-focus, Image stabilization → Colour Filter Arrays: GRGB, CYGM, RGBE, CMY

Chromatic aberrations, Spherical aberrations → IR, Anti-aliasing filters

Digital Image Processing: White balancing, noise reduction, sharpening, aperture & gamma correction, etc.

Digital Storage Device (HDD, memory card, etc.)
Digital Photography: JPEG, RAW

Analogue

Digital
Color Filter Array (CFA)

Bayer filter

Matrix / Sensor

Color Filter Array Sensor

Light

R  2xG  B
Matrix (pixel sensor) = an optic to electric energy transducer.

Its Photo-Response Non-Uniformity (PRNU) can be used in forensic image analysis to:

- verify / identify the suspect camera
- check for copy / paste traces between images generated by different cameras
Digital Photography: JPEG, RAW

Scene -> Lens -> Filters -> CFA -> Sensor/Matrix -> DIP (Digital Image Processing) -> Storage (RAW JPG...)

Analogue vs Digital

Scene Inconsistencies
Auto-exposure, Auto-focus, Image stabilization
IR, Anti-aliasing filters
Chromatic aberrations, Spherical aberrations

Colour Filter Arrays: GRGB, CYGM, RGBE, CMY
Sensor/Matrix (CMOS, CCD...)
Digital Image Processing: White balancing, noise reduction, sharpening, aperture & gamma correction, etc.
Digital Storage Device (HDD, memory card, etc.)
The native spectral RBG or MYC is converted into a standard R’G’B’ (sRGB) color space by a 3x3 color correction matrix. sRGB is the standard color format for most digital imaging input and output devices.

\[
\begin{bmatrix}
  a_{11} & a_{12} & b_{13} \\
  a_{21} & a_{22} & a_{23} \\
  a_{31} & a_{32} & a_{33}
\end{bmatrix}
\begin{bmatrix}
  M \\
  Y \\
  C
\end{bmatrix}
= 
\begin{bmatrix}
  R' \\
  G' \\
  B'
\end{bmatrix}
\]

\[
\begin{bmatrix}
  b_{11} & b_{12} & b_{13} \\
  b_{21} & b_{22} & b_{23} \\
  b_{31} & b_{32} & b_{33}
\end{bmatrix}
\begin{bmatrix}
  R \\
  G \\
  B
\end{bmatrix}
= 
\begin{bmatrix}
  R' \\
  G' \\
  B'
\end{bmatrix}
\]

(from Kodak (2003) Color Correction for Image Sensors, Application Note)
JPEG (Joint Photographic Experts Group) is a common lossy compression method in digital photography, and JPEG compressed images are usually stored in the JFIF (JPEG File Interchange Format) file format.

Nearly every digital camera can save images in the JPEG/JFIF format, which supports 8 bits per color (red, green, blue) for a 24-bit total, producing relatively small files. When not too great, the compression does not noticeably detract from the image's quality, but JPEG files suffer generational degradation when repeatedly edited and saved. The JPEG/JFIF format also is used as the image compression algorithm in many Adobe PDF files.
The **JPEG** Compression Algorithm

$sRGB \rightarrow YCrCb$

- DCT
- Quantization
- Entropy Encoder
- EXIF & Thumbnail
- JPG File
The JPEG Compression Algorithm

1. **sRGB** → **YCrCb**
2. **DCT**
3. **Quantization**
4. **Entropy Encoder**
5. **EXIF & Thumbnail**
6. **JPG File**
JPEG Color Space Conversion

The color conversion matrix from the standard sRGB color space to the YCrCb color space for JPEG compression:

\[
\begin{bmatrix}
+0.289 & +0.587 & +0.114 \\
-0.169 & -0.441 & +0.500 \\
+0.500 & -0.418 & -0.081
\end{bmatrix}
\begin{bmatrix}
R' \\
G' \\
B'
\end{bmatrix} =
\begin{bmatrix}
Y \\
Cb \\
Cr
\end{bmatrix}
\]

(from Kodak (2003) Color Correction for Image Sensors, Application Note)
The JPEG Compression Algorithm

sRGB → YCrCb

DCT → Quantization → Entropy Encoder → EXIF & Thumbnail → JPG File
\[ X_{k_1,k_2} = \sum_{n_1=0}^{N_1-1} \left( \sum_{n_2=0}^{N_2-1} x_{n_1,n_2} \cos \left[ \frac{\pi}{N_2} \left( n_2 + \frac{1}{2} \right) k_2 \right] \right) \cos \left[ \frac{\pi}{N_1} \left( n_1 + \frac{1}{2} \right) k_1 \right] \]

\[ = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} x_{n_1,n_2} \cos \left[ \frac{\pi}{N_1} \left( n_1 + \frac{1}{2} \right) k_1 \right] \cos \left[ \frac{\pi}{N_2} \left( n_2 + \frac{1}{2} \right) k_2 \right]. \]

\[ G_{u,v} = \sum_{x=0}^{7} \sum_{y=0}^{7} \alpha(u)\alpha(v) g_{x,y} \cos \left[ \frac{\pi}{8} \left( x + \frac{1}{2} \right) u \right] \cos \left[ \frac{\pi}{8} \left( y + \frac{1}{2} \right) v \right] \]

Source:

http://en.wikipedia.org/wiki/JPEG

The **JPEG** Compression Algorithm

- **sRGB** → **YCrCb**
- **DCT**
- **Quantization**
- **Entropy Encoder**
- **EXIF & Thumbnail**
- **JPG File**
Original JPEG file: IMG-1773.jpg

<table>
<thead>
<tr>
<th>Luminance Quantization Table:</th>
<th>Chrominance Quantization Table:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 1 1 2 3 6 8 10</td>
<td>4 4 5 9 15 26 26 26</td>
</tr>
<tr>
<td>1 1 2 3 4 8 9 8</td>
<td>4 4 5 10 19 26 26 26</td>
</tr>
<tr>
<td>2 2 2 3 6 8 10 8</td>
<td>5 5 8 9 26 26 26 26</td>
</tr>
<tr>
<td>2 2 3 4 7 12 11 9</td>
<td>9 10 9 13 26 26 26 26</td>
</tr>
<tr>
<td>3 3 8 11 10 16 15 11</td>
<td>15 19 26 26 26 26 26 26</td>
</tr>
<tr>
<td>3 5 8 10 12 15 16 13</td>
<td>26 26 26 26 26 26 26 26</td>
</tr>
<tr>
<td>7 10 11 12 15 17 17 14</td>
<td>26 26 26 26 26 26 26 26</td>
</tr>
<tr>
<td>14 13 13 15 14 14 14 14</td>
<td>26 26 26 26 26 26 26 26</td>
</tr>
</tbody>
</table>
The JPEG Compression Algorithm

\[ sRGB \rightarrow YCrCb \]

- DCT
- Quantization
- Entropy Encoder
- EXIF & Thumbnail
- JPG File
Entropy encoding, zigzag ordering, quantized DCT coefficients

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>5</th>
<th>6</th>
<th>14</th>
<th>15</th>
<th>27</th>
<th>28</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>7</td>
<td>13</td>
<td>16</td>
<td>26</td>
<td>29</td>
<td>42</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>12</td>
<td>17</td>
<td>25</td>
<td>30</td>
<td>41</td>
<td>43</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>11</td>
<td>18</td>
<td>24</td>
<td>31</td>
<td>40</td>
<td>44</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>19</td>
<td>23</td>
<td>32</td>
<td>39</td>
<td>45</td>
<td>52</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>22</td>
<td>33</td>
<td>38</td>
<td>46</td>
<td>51</td>
<td>55</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>34</td>
<td>37</td>
<td>47</td>
<td>50</td>
<td>56</td>
<td>59</td>
<td>61</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>36</td>
<td>48</td>
<td>49</td>
<td>57</td>
<td>58</td>
<td>62</td>
<td>63</td>
<td></td>
</tr>
</tbody>
</table>
Entropy encoding, zigzag ordering, quantized DCT coefficients
The JPEG Compression Algorithm

sRGB → YCrCb

DCT → Quantization → Entropy Encoder → EXIF & Thumbnail → JPG File
Original EXIF

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make</td>
<td>&quot;Canon&quot;</td>
</tr>
<tr>
<td>Model</td>
<td>&quot;Canon PowerShot G2&quot;</td>
</tr>
<tr>
<td>Orientation</td>
<td>Row 0: top, Col 0: left</td>
</tr>
<tr>
<td>XResolution</td>
<td>180/1</td>
</tr>
<tr>
<td>YResolution</td>
<td>180/1</td>
</tr>
<tr>
<td>ResolutionUnit</td>
<td>Inch</td>
</tr>
<tr>
<td>DateTime</td>
<td>&quot;2010:10:31 11:24:46&quot;</td>
</tr>
<tr>
<td>YCbCrPositioning</td>
<td>Centered</td>
</tr>
<tr>
<td>ExifOffset</td>
<td>@ 0x00C4</td>
</tr>
<tr>
<td>etc.</td>
<td></td>
</tr>
</tbody>
</table>
Edited JPG EXIF:

- PaintShop Photo Pro 13.00

Filename: 'DSC01830_2.jpg'
FileModDate: '21-Jun-2011 11:41:41'
FileSize: 833611
Format: 'jpg'
FormatVersion: '
Width: 2816
Height: 2112
BitDepth: 24
ColorType: 'truecolor'
FormatSignature: '
NumberOfSamples: 3
CodingMethod: ' Huffman'
CodingProcess: ' Sequential'
Comment: {}
ImageDescription: '
Make: ' SONY '
Model: ' DSC-S600 '
Orientation: 1
XResolution: 72
YResolution: 72
ResolutionUnit: ' Inch'
Software: 'PaintShop Photo Pro 13.00 '
DateTime: '2011:06:21 11:41:40 '
YCbCrPositioning: ' Co-sited'
DigitalCamera: [1x1 struct]
Edited JPG EXIF:

-No brand
-No model
-No settings
-Adobe Photoshop
-Etc.
Edited JPG
EXIF:

- No brand
- No model
- No settings
- Etc.

Filename: 'soldat1.jpg'
FileModDate: '24-Feb-2010 14:49:06'
FileSize: 17673
Format: 'jpg'
FormatVersion: ''
Width: 400
Height: 266
BitDepth: 24
ColorType: 'truecolor'
FormatSignature: ''
NumberOfSamples: 3
CodingMethod: 'Huffman'
CodingProcess: 'Sequential'
Comment: {}
The **JPEG** Compression Algorithm

\[s_{RGB} \rightarrow Y_{CrCb}\]

1. **DCT** → **Quantization** → **Entropy Encoder** → **EXIF & Thumbnail** → **JPG File**
Examples

lena.bmp  lena.jpg
Examples

lena.bmp - lena.jpg (eye details)
Digital Image Authentication Framework

General steps:

1. Check the file’s name, HASH, format and MAC stamps
2. Check for scene inconsistencies (e.g. shadows, light reflections, etc.)
3. Check for traces of (re)compression
4. Check for rescaling traces
5. Check for CFA inconsistencies
6. Check for color, luminance inconsistencies
7. Check for source camera (PRNU)
8. Check for traces of copy/paste, etc.
Digital Image Analysis: PRNU
Matrix (pixel sensor) = an optic to electric energy transducer.

Its Photo-Response Non-Uniformity (PRNU) can be used in forensic image analysis to:

- verify / identify the suspect camera
- check for copy / paste traces between images generated by different cameras
Erroneous PRNU models

Recommended PRNU models
Evidence

Refernce database

Suspect camera
Authentic digital photo

Bit-stream the memory

Copy/Paste the file

Rescale / Crop, etc.

Adjust brightness, contrast, colours, etc.

Counterfeited / tampered / doctored photo
sRGB \rightarrow \text{YCrCb}

\begin{align*}
\text{CFA} & \rightarrow \text{Sensor/Matrix} \\
\text{DIP} & \rightarrow \text{Storage} \\
\text{Digital Image Processing} & \\
\text{EXIF & Thumbnail} & \\
\text{JPG File} & \\
\end{align*}
Original JPEG file: IMG-1773.jpg

Camera:
Canon Power Shot G2

Settings:
2272x1704
Low JPEG compression (high JPEG quality)
Original JPEG file: IMG-1773.jpg

Compression Analysis
Recompressed JPEG file: IMG_1773-resize50

Compression Analysis
Colour Filter Array (CFA) Analysis
Colour Filter Array (CFA) Analysis

Recompressed JPEG file: IMG_1773-resize50
DCT Coefficients Analysis
Recompressed JPEG file: IMG_1773-resize50.jpg

DCT Coefficients Analysis
Internet examples

Hand on Shoulder
http://3.bp.blogspot.com/_EHZsoUS6SIA/R8ylHlSSjoI/AAAAAAAAAAo/VDR9yhn0Xgk/s1600-h/Kbh7nxKMcMJP.jpg

Sarkozy
http://www.lemondedelaphoto.com/4-Retouche-et-presse-generaliste,2937.html

Victoria Secret
http://www2.victoriassecret.com/commerce/onlineProductDisplay.vs?namespace=pro ductDisplay&origin=onlineProductDisplay.jsp&event=display&prnbr=EF-227524&cgname=OSCLODRSDAY

Wolf
http://socialtech.ca/ade/misc/wolf_full_size.jpg
WTC Tourist
http://urbanlegends.about.com/library/blphoto-wtc.htm
http://urbanlegends.about.com/library/n_tourist_guy.htm

NASA+Moon+Plane
http://apod.nasa.gov/apod/ap100929.html
http://apod.nasa.gov/apod/image/1009/moonplane_thomas_big.jpg

Tahiti-Haiti
http://www.trombon.ro/international/romania-a-trimis-ajutoare-in-tahiti
http://www.adrants.com/images/bikini_girls.jpg
http://www.duatravel.com/site_images/destinations/locations/tahiti_nui.jpg
68

Après leurs discours officiels en présence de personnalités des mondes politique et religieux, le Pape et le président de la République quittent la salle des Fêtes de l’Elf. 

1. The mini belt. 
Brown (27). 
$172 - 500. 

2. A poet ease. 
La cami. 
Stripes XS - XL. 
SALE $19. 

3. Wide and stone
pendant.
Piedras semi preciosas combinadas con plata, imán, coral y hasta con hilos. Este es el producto de Paula y Cristina cuando ocasionan a la moda con un toque de estilo.

Este es la propuesta de Teresa Almenara y de sus diseñadores tan sugerentes como irrepetibles.
Compression Level Analysis: new-V275298-35Q

CLA, RGB

normalized f

CL=116.7958  116.5515  117.4368  116.9281

CLA, RGB, log scale

normalized f

Compression Cepstrum: new-V275298-35Q

Cepstrum

index
Internet examples
Analysis & Discussions

Case: WTC Tourist
http://urbanlegends.about.com/library/blphoto-wtc.htm

Evidence:
- One Internet JPG file
- JPG EXIF without photo camera, no suspect photo camera

Methods & Tools:
- Visual inspection, scene inconsistencies
- EXIF, DCT, PRNU…tools
EXIF:
- Not typical for original digital photos
- Typical for JPG files generated/saved with an image editor and "Save EXIF" disabled

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>'missing_lg2.jpg'</td>
</tr>
<tr>
<td>FileModDate</td>
<td>'28-Mar-2011 18:56:42'</td>
</tr>
<tr>
<td>FileSize</td>
<td>32223</td>
</tr>
<tr>
<td>Format</td>
<td>'jpg'</td>
</tr>
<tr>
<td>FormatVersion</td>
<td>''</td>
</tr>
<tr>
<td>Width</td>
<td>550</td>
</tr>
<tr>
<td>Height</td>
<td>380</td>
</tr>
<tr>
<td>BitDepth</td>
<td>24</td>
</tr>
<tr>
<td>ColorType</td>
<td>'truecolor'</td>
</tr>
<tr>
<td>FormatSignature</td>
<td>''</td>
</tr>
<tr>
<td>NumberOfSamples</td>
<td>3</td>
</tr>
<tr>
<td>CodingMethod</td>
<td>'Huffman'</td>
</tr>
<tr>
<td>CodingProcess</td>
<td>'Sequential'</td>
</tr>
<tr>
<td>Comment</td>
<td>{}</td>
</tr>
</tbody>
</table>
Results interpretation & Discussions

- Visual and photogrammetric inspection revealed (possible) scene inconsistencies
- Digital analysis revealed:
  - the EXIF is not typical for original digital photos
  - possible traces of JPG recompression (CLA)(DCT)
  - Correlation Map, DCT Map, ELA, PRNU inconsistencies
- Not authentic photo
Doctored Image, copy/paste small green grass areas over the mid lady

File: Ladies_doct.bmp
Clone detection results for

Block size = 4 pixels
Authentic analogue recording(s)

Non-authentic analogue recordings

Copy/copies
Copy fragment(s)
Deletions
Counterfeiting

Tampered/doctored recordings
Digital Audio

- Authentic digital files containing authentic recording(s)
  - built-in memory
  - removable memory

Bit stream data image

File copy

No manipulation:
- Audio Enhancement
- Deletions, etc.

Edited recordings

Manipulation:
- Audio Enhancement
- Delete/Add
- (Re)compression, etc.

Tampered/doctored recordings

Non-authentic files/recordings

Bit stream (bit-to-bit copy) containing clones of the authentic files with authentic recording(s)

File copies containing authentic recording(s)

- Non-authentic / copied files
- Recordings consistent with authentic digital audio recordings

(forensic results)

(counterfeiting results)
Forensic Authentication of Digital Audio - Framework

1. **Hardware**: write-blockers, PC, digital audio recorders, mics, etc.
2. **Software**: write-blockers, digital imaging, HASH, hex viewers, structure/logic analysis, audio editors, audio analysis, etc.
3. **Databases**: file samples, user manuals*, software, LTAS, ENF, etc.
4. **Analysis Methods**:
   4.1. Photos, forensic bit-streams, HASH, create working copy
   4.2. MAC, metadata, structure/logic, conversions
   4.3. Time domain: waveform, energy, power, DC, transitions, butt splice, statistics
   4.4. Frequency domain: spectrum/FFT, spectrogram, compression
   4.5. Other: ADC → DAC, Phase, ENF

+ critical listening
WinHex - [WS760025.wma]

WS760025.wma
G:\Catalin.NCMF\Trainings\2011

File size: 1.3 MB
3.147.127 bytes

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 2011/07/07 19:20:59
Last write time: 2011/07/07 19:26:36

Attributes: A
Icons: .

Mode: Text
Character set: ANSI ASCII
Offsets: hexadecimal
47x16:752

Window #
No. of windows: 1

Clipboard: available
TEMP folder: 40.0 GB free
%\Catalin\AppData\Local\Temp

Opinion =

WS760025.wma file header does not match the Olympus WMA format. For more details a forensic audio analysis is recommended.
## Wav File Format

### Wave File Header

<table>
<thead>
<tr>
<th>Offset</th>
<th>Size</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x14</td>
<td>2</td>
<td>Compression</td>
<td>1 (PCM)</td>
</tr>
<tr>
<td>0x16</td>
<td>2</td>
<td>nChannels</td>
<td></td>
</tr>
<tr>
<td>0x18</td>
<td>4</td>
<td>Fs</td>
<td></td>
</tr>
<tr>
<td>0x22</td>
<td>2</td>
<td>Bit Depth</td>
<td></td>
</tr>
</tbody>
</table>

```
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 52 49 46 46 00 00 38 00 57 41 56 66 6D 74 20 RIFF..8.WAVEfmt
00000010 10 00 00 00 01 00 02 00 44 AC 00 00 10 B1 02 00 ...........D-...±..
00000020 04 00 10 00 64 61 74 61 D4 FF 37 00 00 00 00 00 00 00 00 00 00 00 00 ....dataÔï7.....
00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```
Waveform: 061-Transitions.wav, Samples: mean=-844.3561, std=679.2965, N=120000

DC: mean=-833.2467, std=427.1702, N=151

STD: mean=282.3095, std=453.1642, N=151
Some transition samples (see 061-Transitions-06-Transitions.txt):

48312
48313
48314
48780
48781
49599
51573
51574
52016
52095
52116
...

Waveform: 060-DM620013

Waveform: 060-DM620013-gen2-mp3pro

LTAS comparison: MQD=2.659, CC=0.98077, NFFT=44100
(2min) CC inter-variability: $\max = 0.93785$; CC intra-variability: $\min = 0.33163$

(2min) MQD intra-variability: $\max = -2.0227$; MQD inter-variability: $\min = -2.4801$