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

DFRWS Denver, CO, Aug 4th, 2014

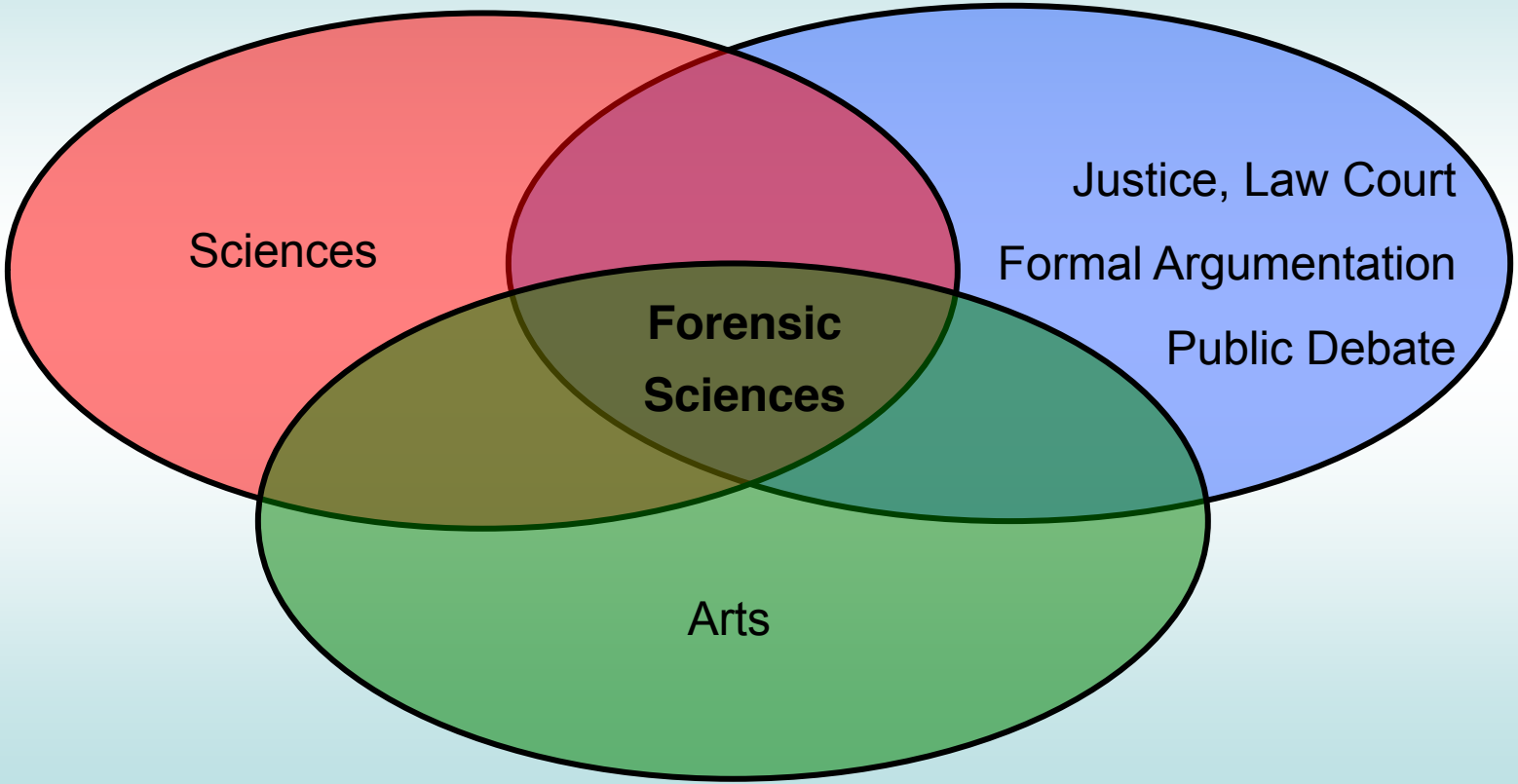
Media Forensics Analysis in Digital Times

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

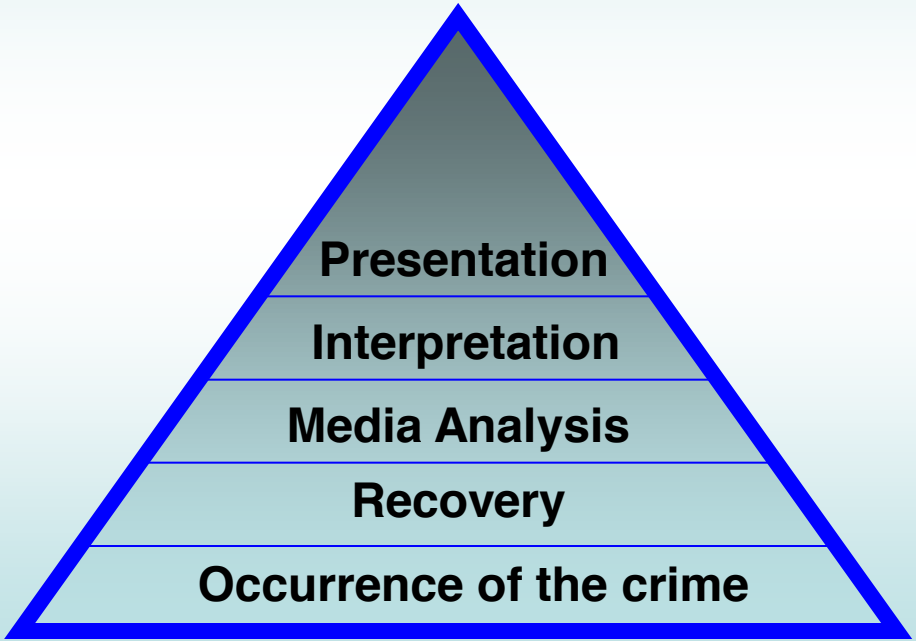


Forensic sciences are concerned with the explanation or reconstruction of events, attempting to determine:

- What happened ?
- How it happened ?
- Where it happened ?
- When it happened ?
- Who was involved ?

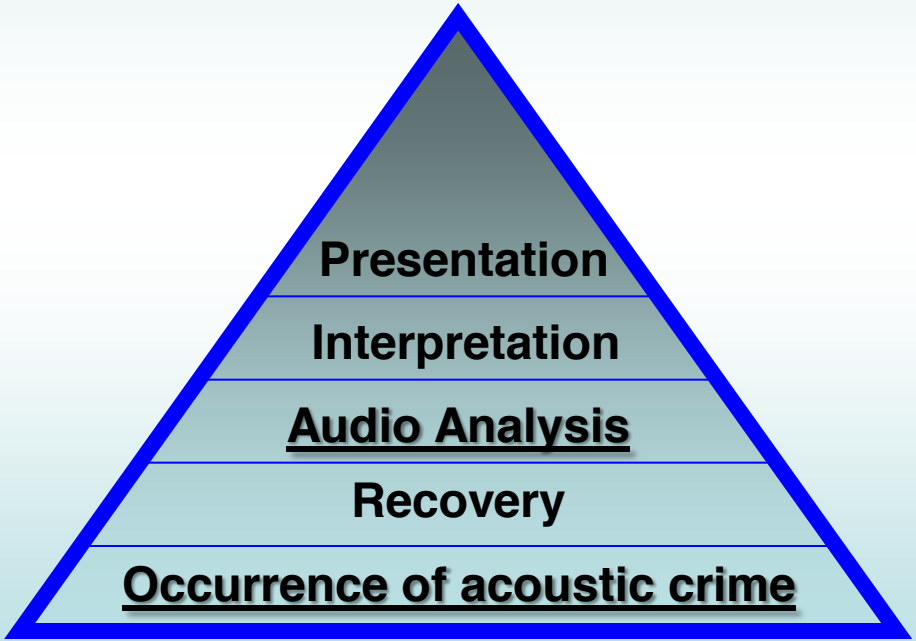
Basic Principles in Media Forensics

The stages of the physical evidence process



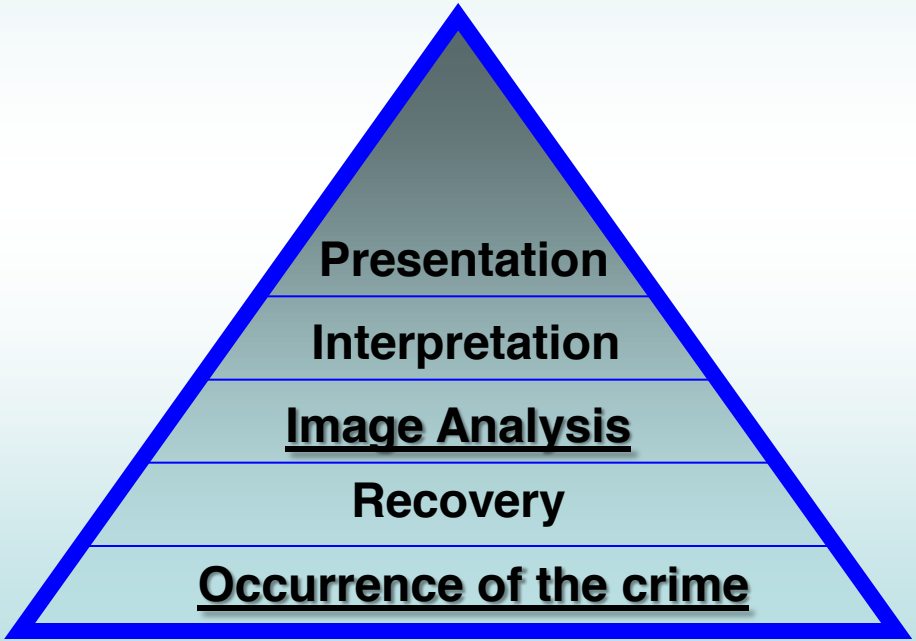
Basic Principles in Forensic Audio

The stages of the physical evidence process



Basic Principles in Forensic Image & Video

The stages of the physical evidence process



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 Media Forensics

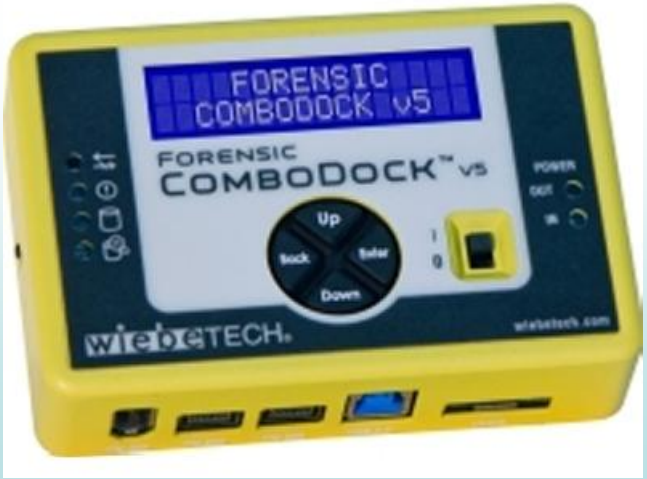
Basic Principles in Forensic Sciences

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.)



Basic Principles in Media Forensics

Basic Principles in Forensic Sciences

2. Principles Concerning Analysis

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

- the **accuracy & precision** ⇨ 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.

Basic Principles in Media Forensics

Basic Principles in Forensic Sciences

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.

Basic Principles in Media Forensics

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

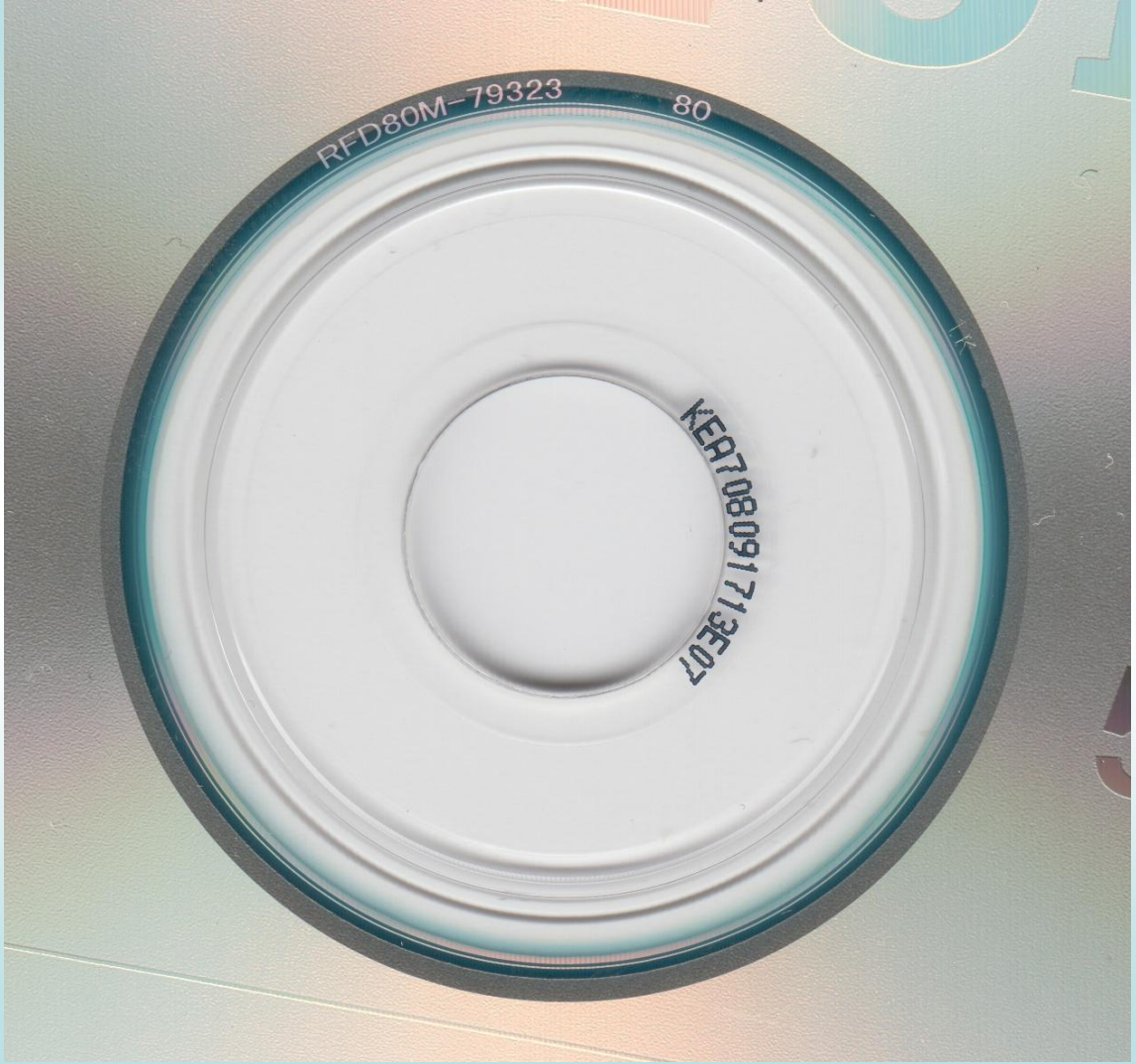
An analogue evidence (audio recording, photo or video recording) always has an original to which it relates in either negative or positive form (i.e. the negatives from which photographic prints are made, transparencies or the magnetic recording on a video or audio tape). Copies can be made from the 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.

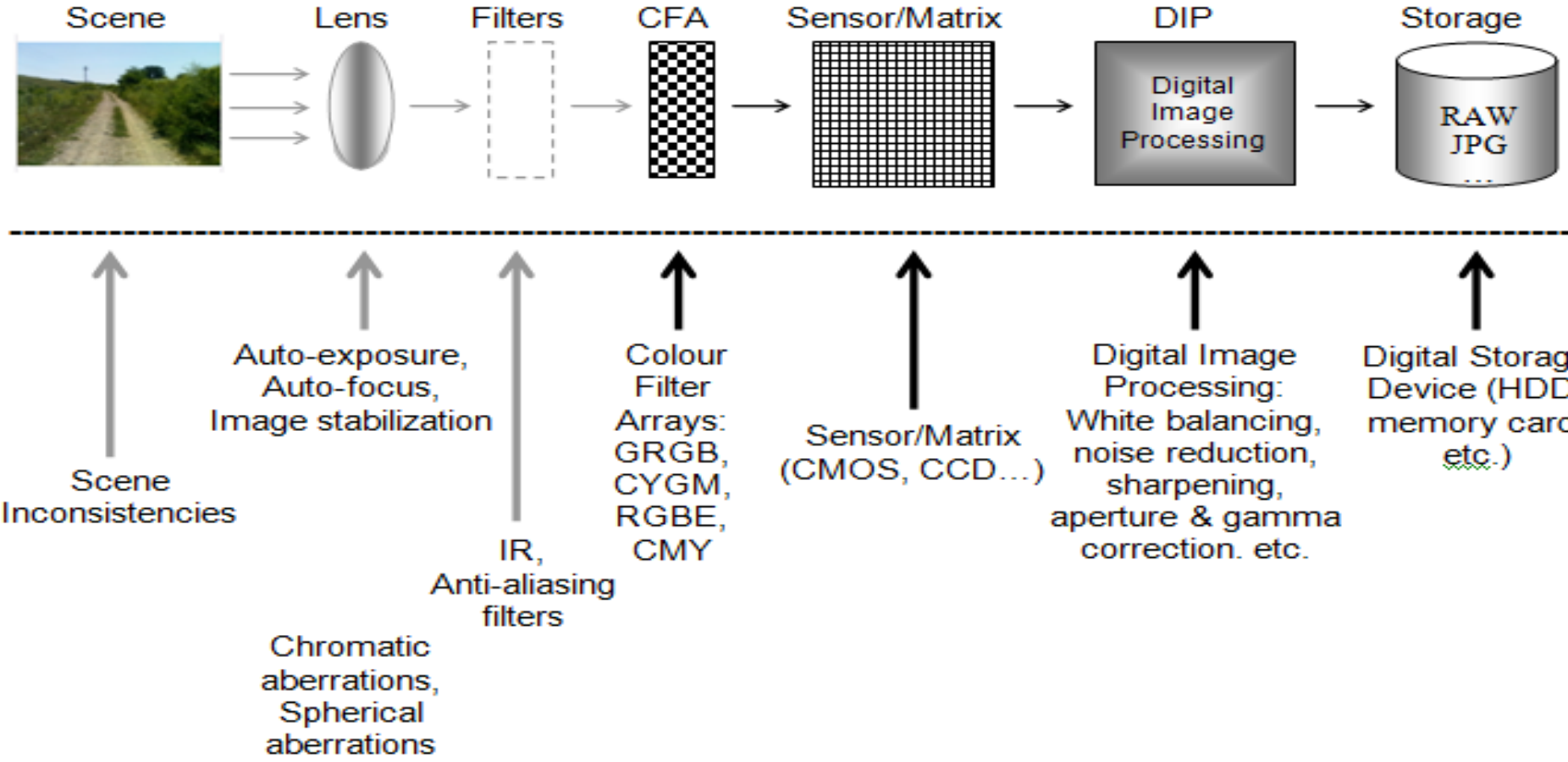
Forensic Authentication of Digital Media Evidence

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*

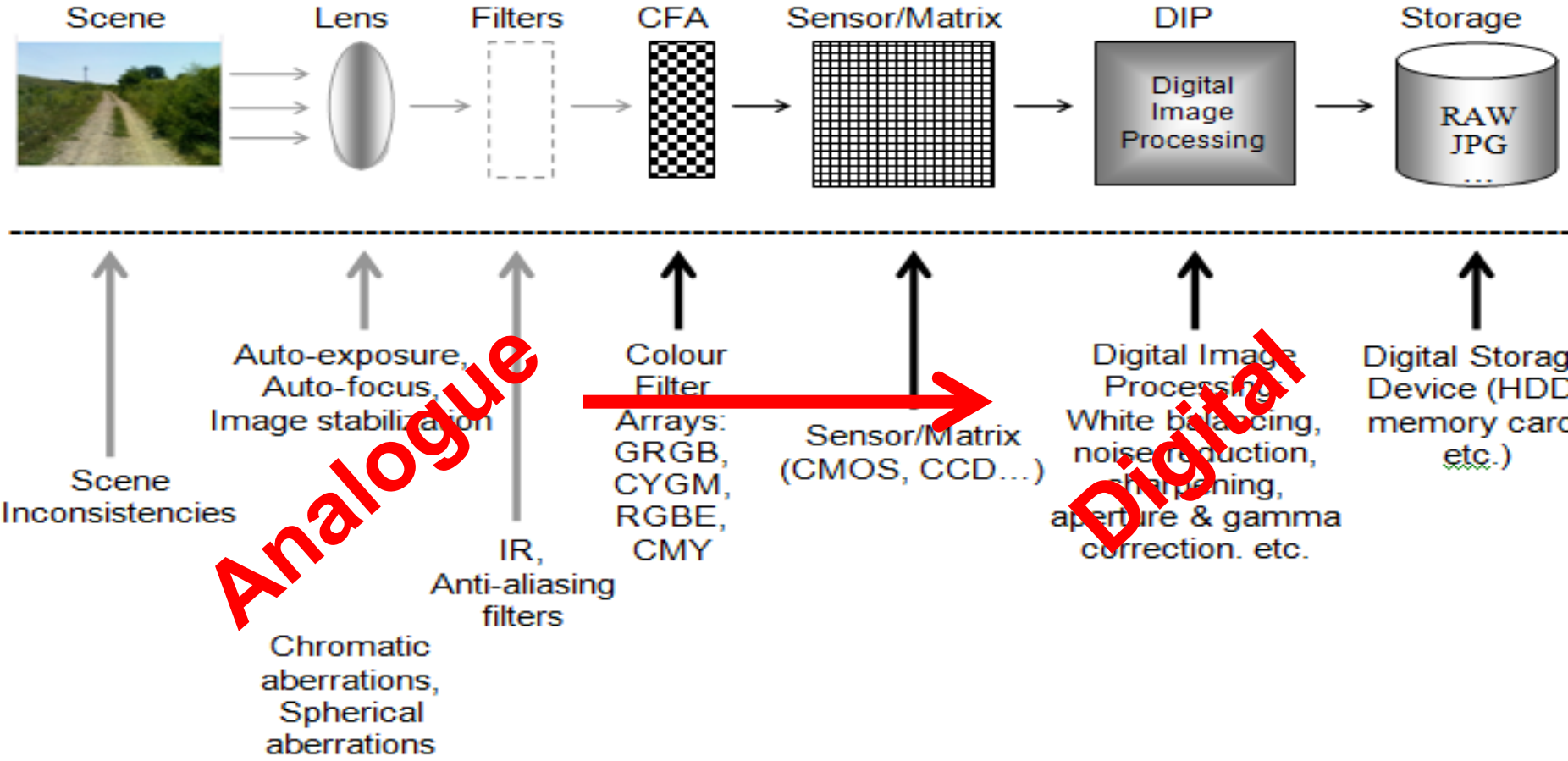

Office DEPOT
1-800-GO-DEPOT
1-800-463-3768
www.officedepot.com
CD-R
52X 700MB
ABFO No. 2
5 4 3 2 1 mm
mm 1 2 3 4 5


RFD80M-79323 80
KEA7080917137E07

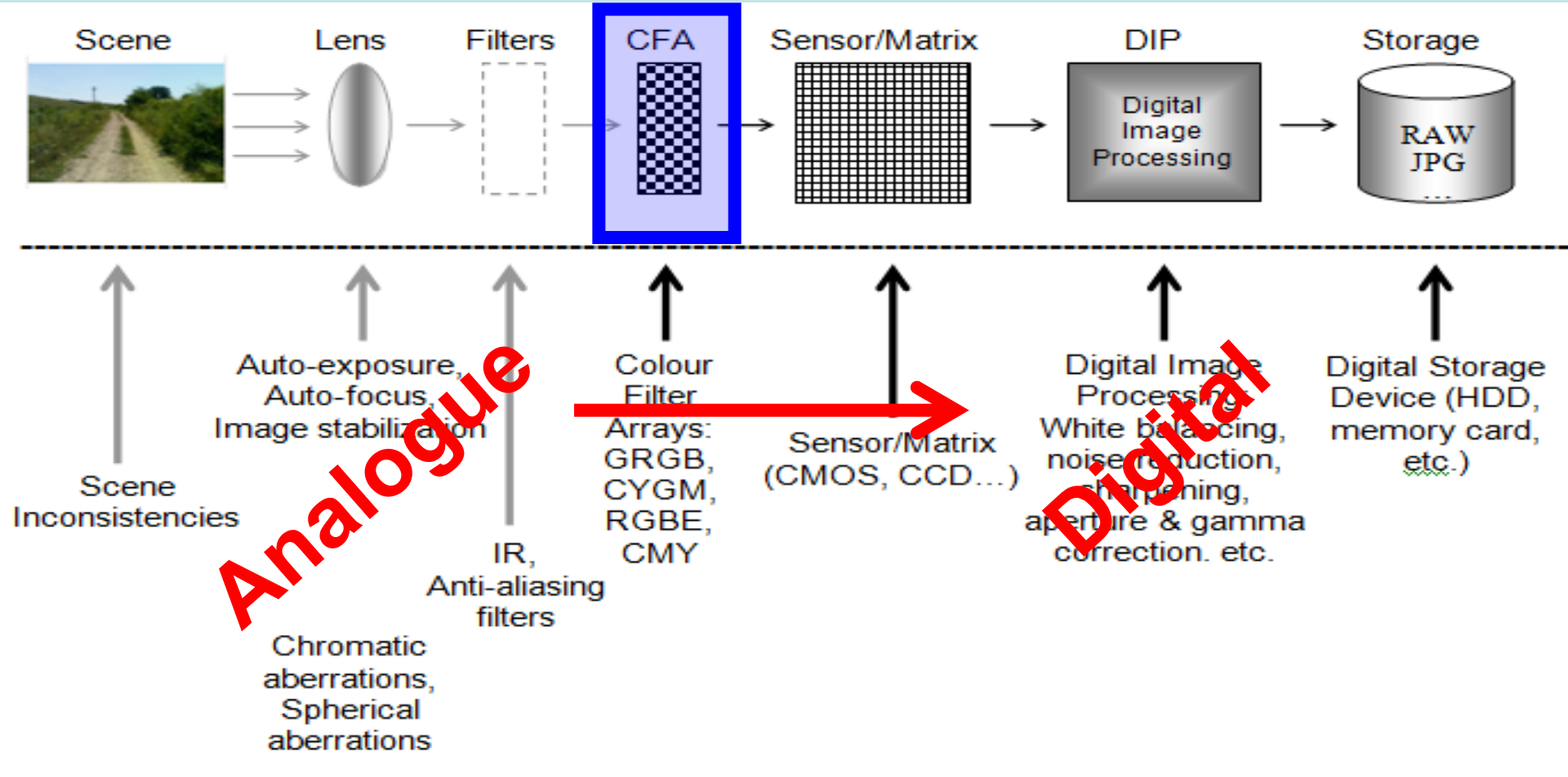
Digital Photography: JPEG, RAW



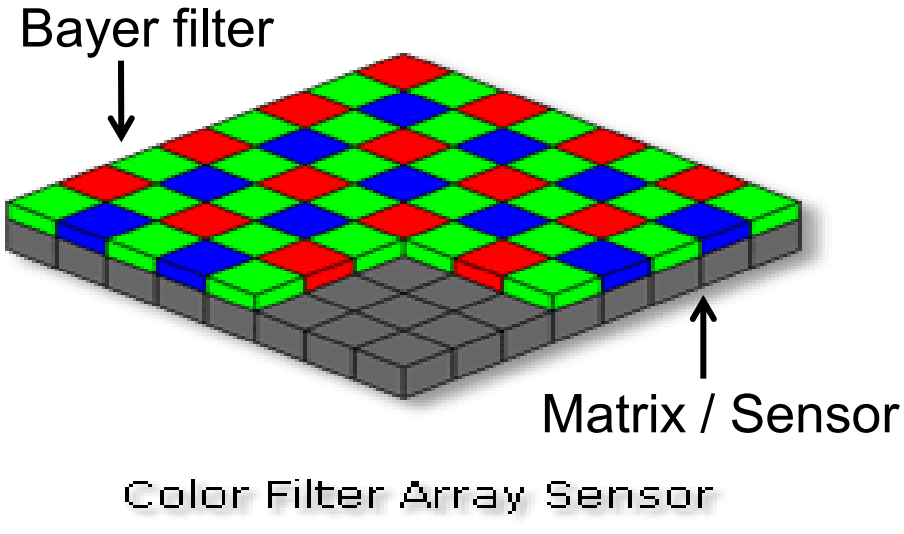
Digital Photography: JPEG, RAW

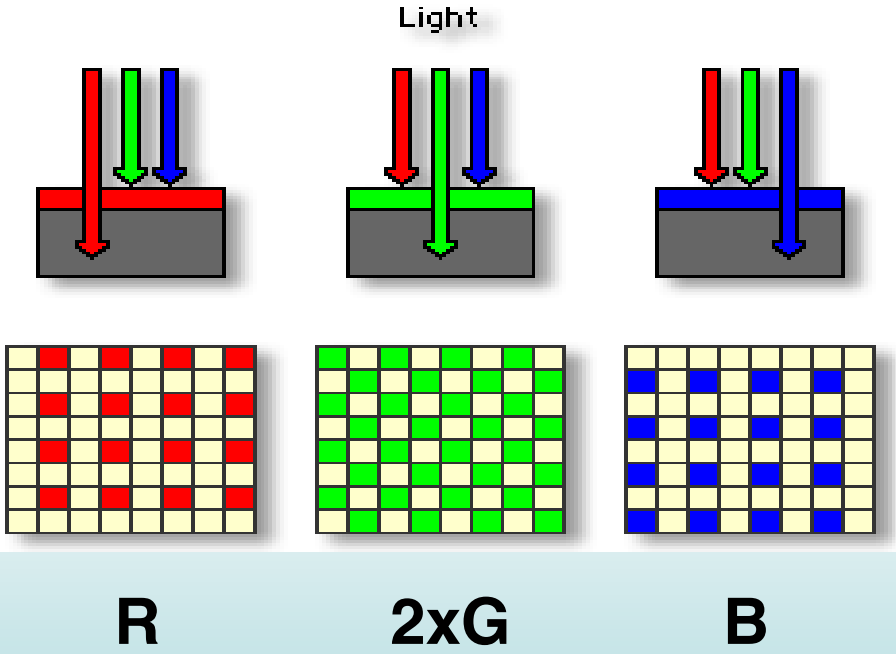


Digital Photography: JPEG, RAW

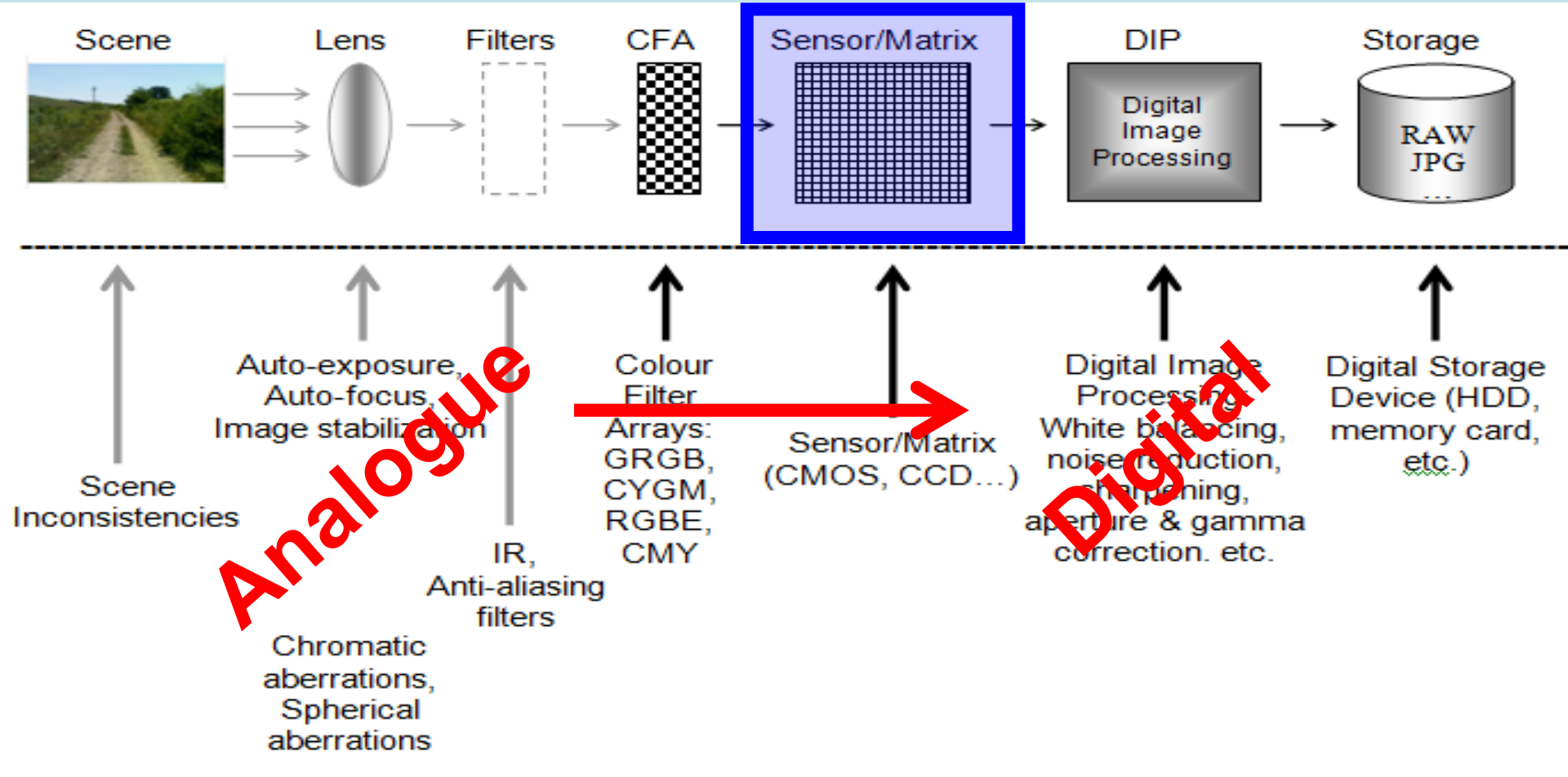


Color Filter Array (CFA)





Digital Photography: JPEG, RAW



Matrix (pixel sensor)

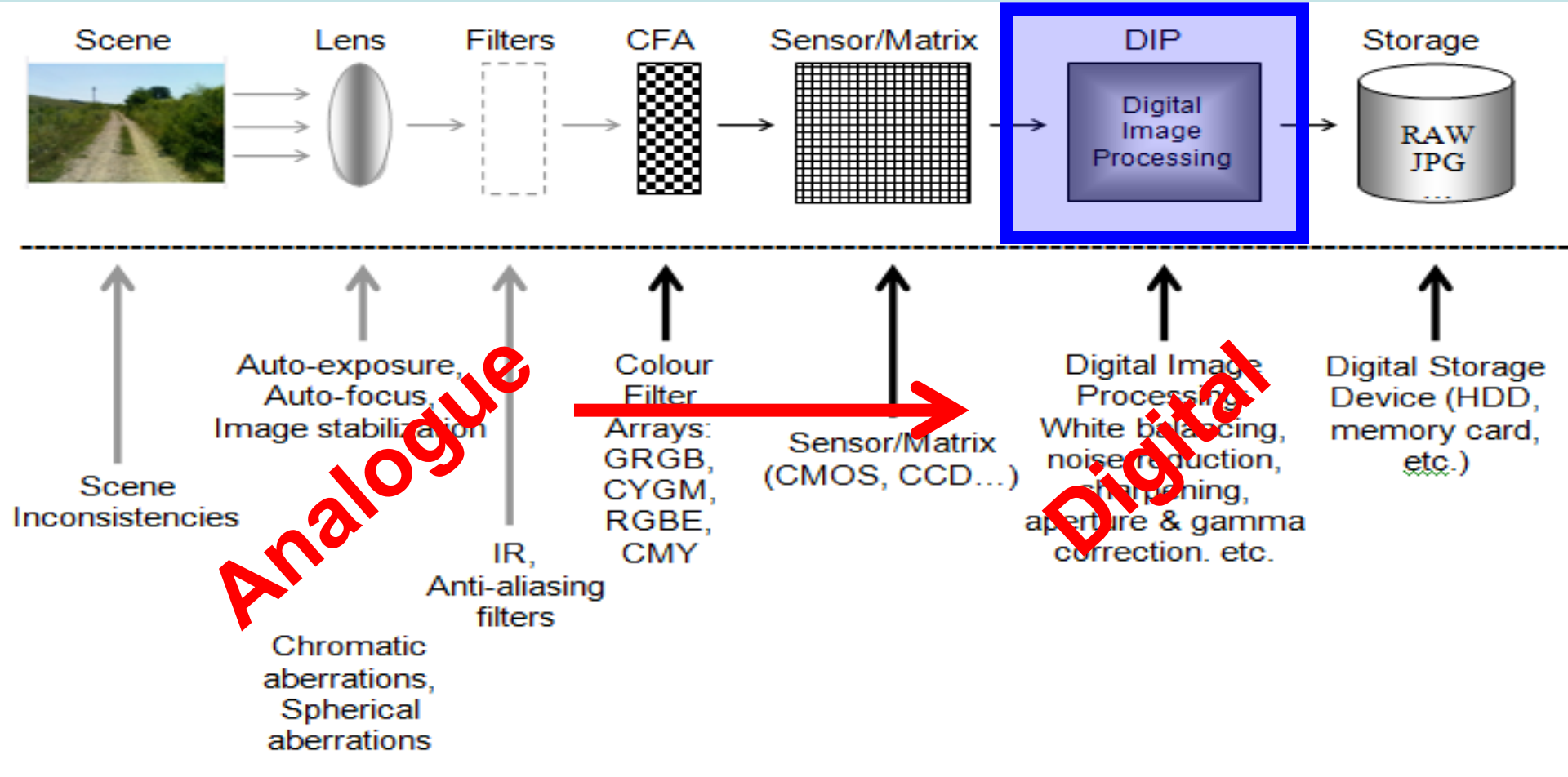
Matrix (pixel sensor) = an optic to electric energy transducer.

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



Digital Image Processing

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.

color correction matrix *sRGB*

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

MYC

color correction matrix *sRGB*

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

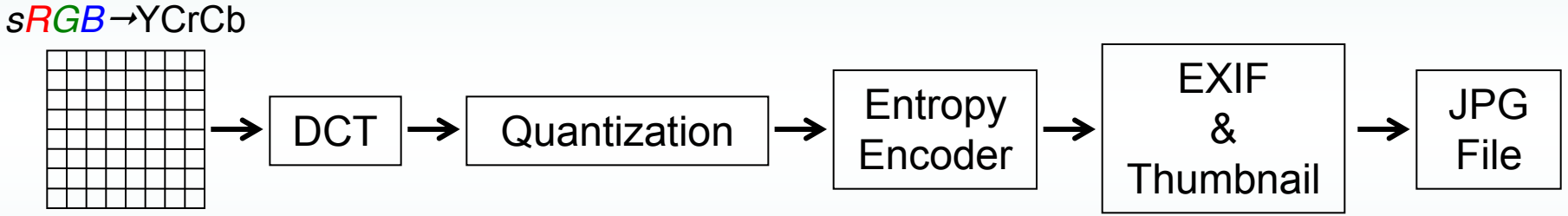
RGB

(from Kodak (2003) *Color Correction for Image Sensors, Application Note*)

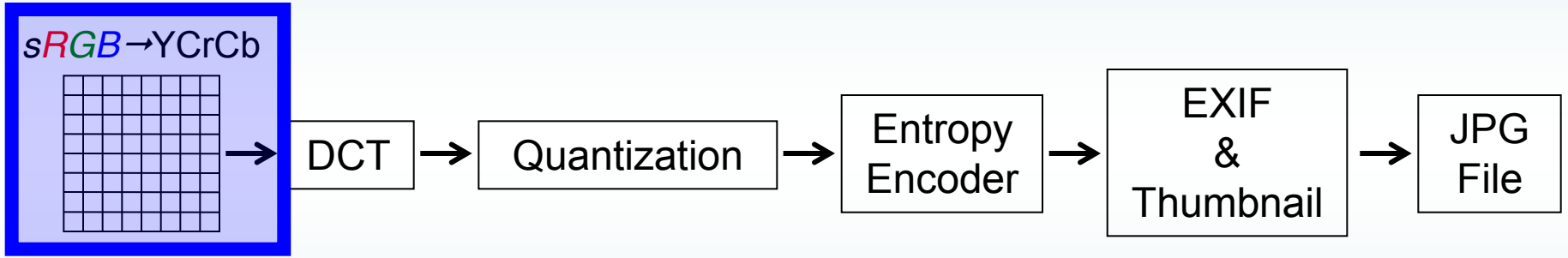
JPEG (Joint Photographic Experts Group) is common lossy compression method in digital photography, and JPEG compressed images are usually stored in the **JFIF** (JPEG File Interchange Format) file format.

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



The **JPEG** Compression Algorithm



JPEG Color Space Conversion

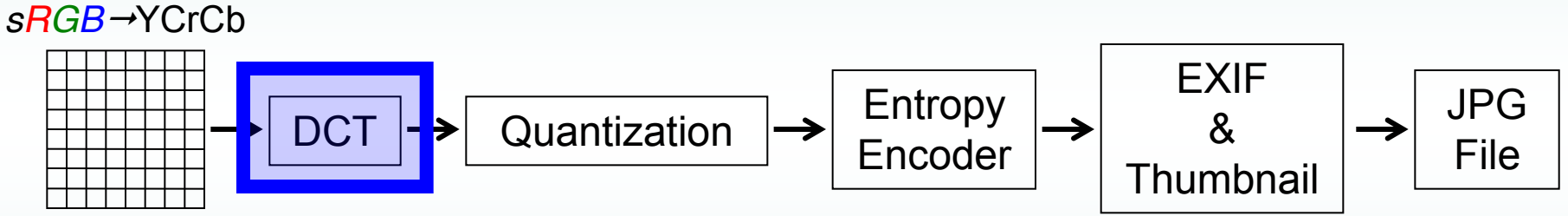
The color conversion matrix from the standard sRGB color space to the YCrCb color space for JPEG compression:

JPEG color conversion matrix *sRGB* *YCrCb*

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

(from Kodak (2003) Color Correction for Image Sensors, Application Note)

The **JPEG** Compression Algorithm



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

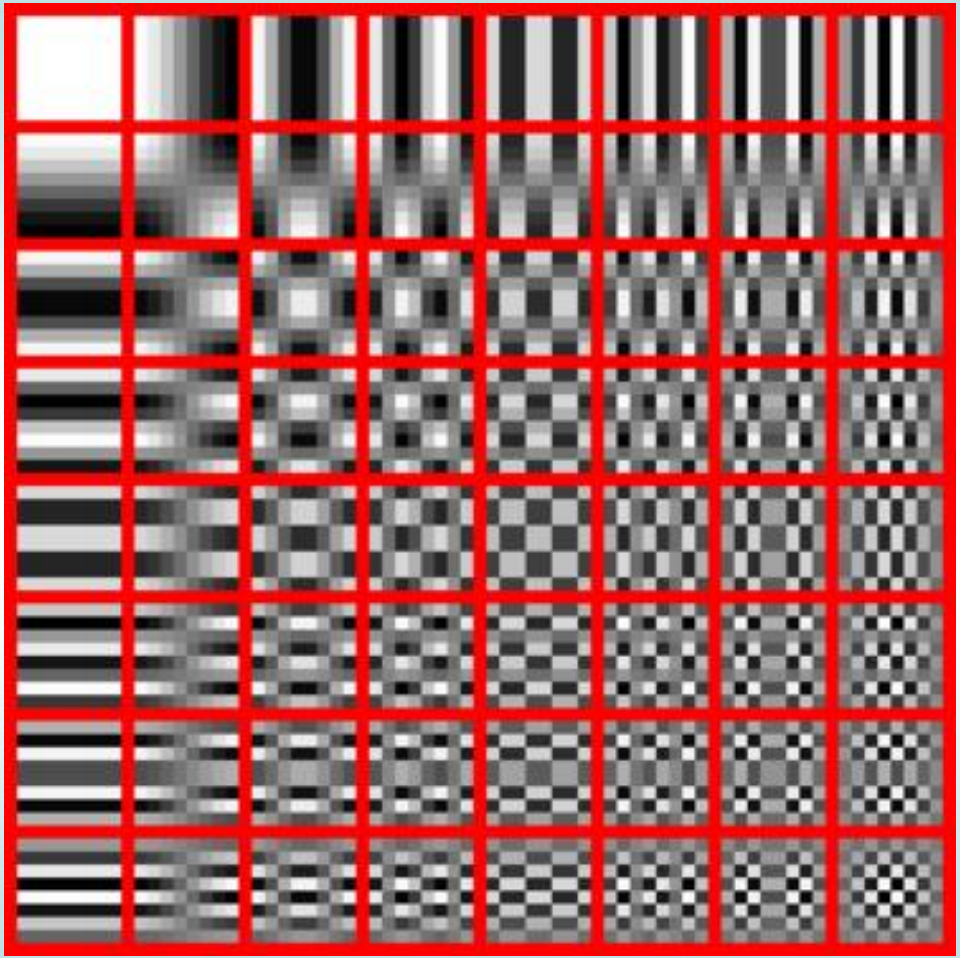
$$= \sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1} x_{n_1,n_2}\cos\left[\frac{\pi}{N_1}\left(n_1+\frac{1}{2}\right)k_1\right]\cos\left[\frac{\pi}{N_2}\left(n_2+\frac{1}{2}\right)k_2\right].$$

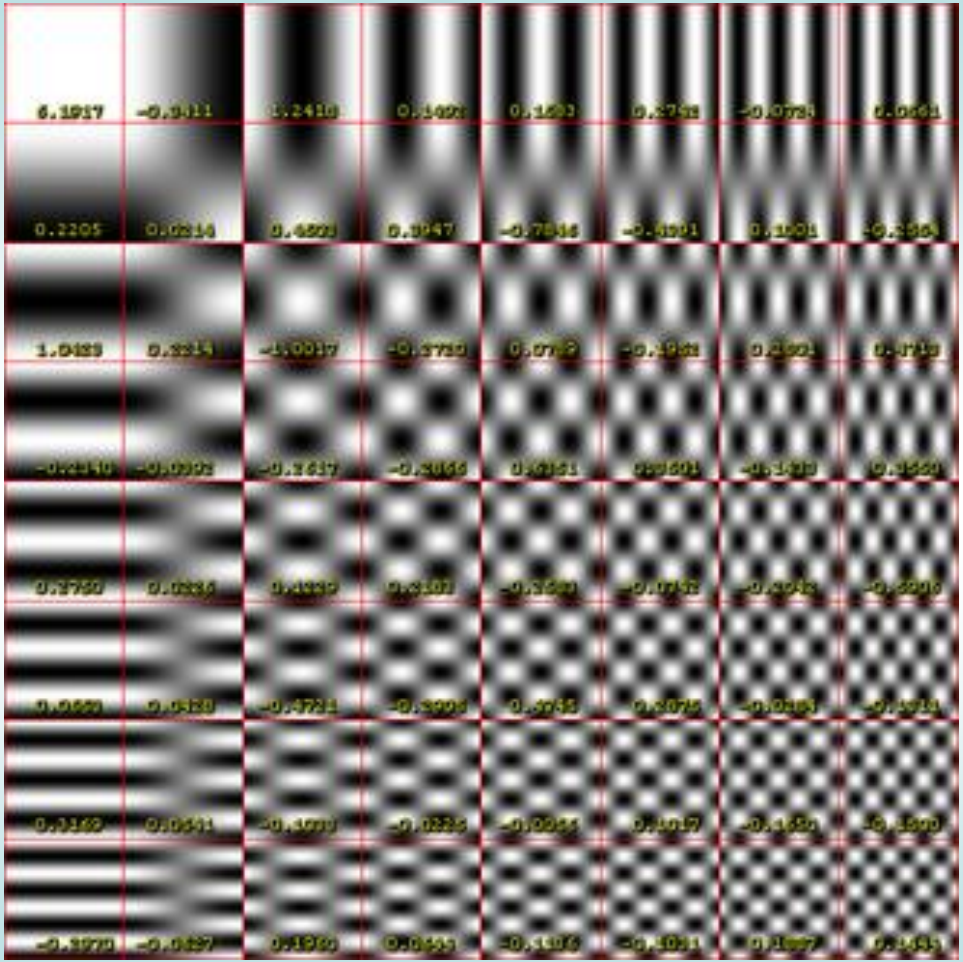
$$G_{u,v} = \sum_{x=0}^{7}\sum_{y=0}^{7}\alpha(u)\alpha(v)g_{x,y}\cos\left[\frac{\pi}{8}\left(x+\frac{1}{2}\right)u\right]\cos\left[\frac{\pi}{8}\left(y+\frac{1}{2}\right)v\right]$$

Source:

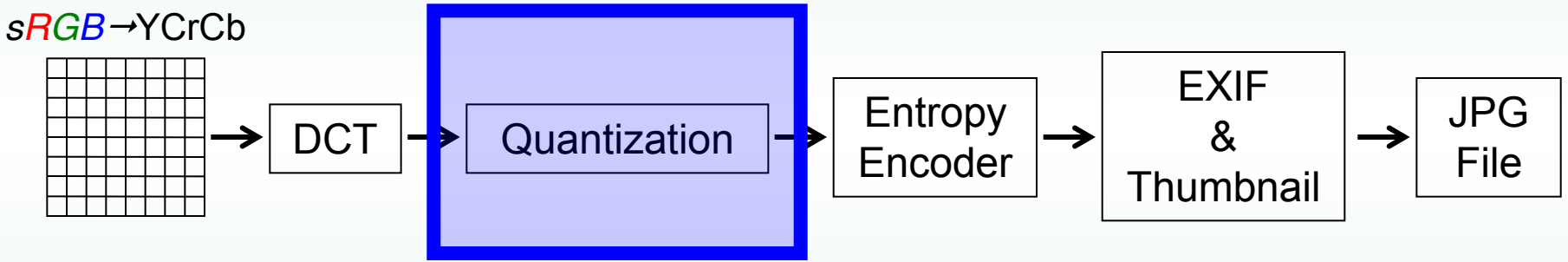
http://en.wikipedia.org/wiki/JPEG

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





The **JPEG** Compression Algorithm



Original JPEG file: IMG-1773.jpg

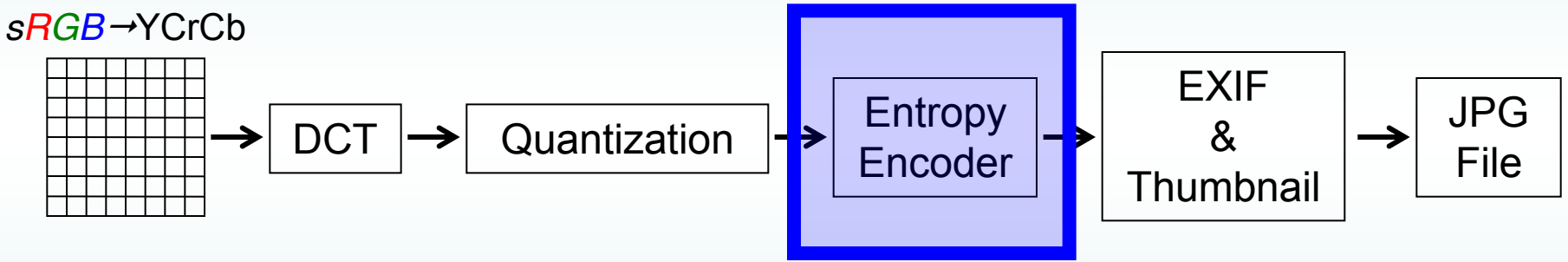
Luminance Quantization Table:

1	1	1	2	3	6	8	10
1	1	2	3	4	8	9	8
2	2	2	3	6	8	10	8
2	2	3	4	7	12	11	9
3	3	8	11	10	16	15	11
3	5	8	10	12	15	16	13
7	10	11	12	15	17	17	14
14	13	13	15	15	14	14	14

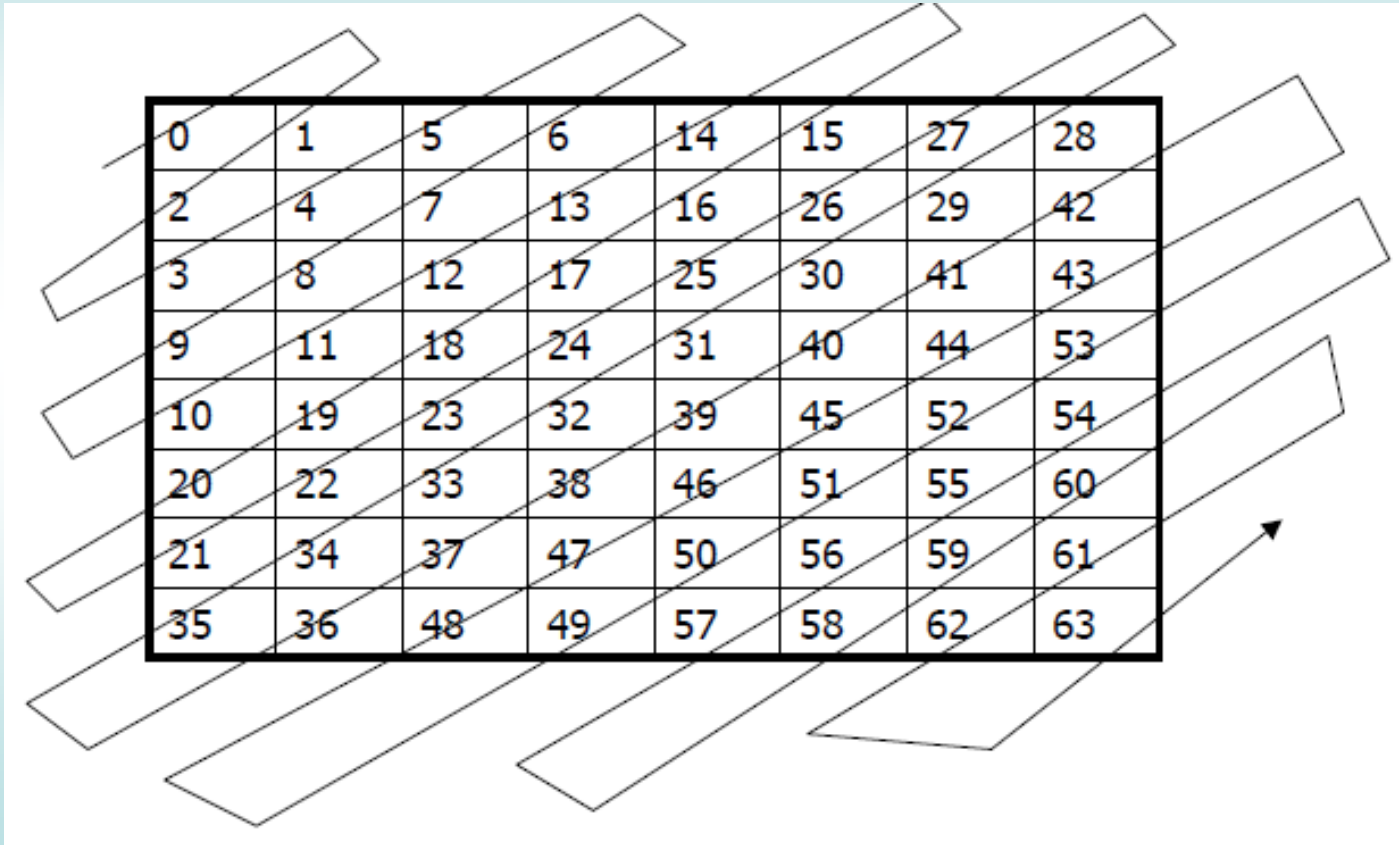
Chrominance Quantization Table:

4	4	5	9	15	26	26	26
4	4	5	10	19	26	26	26
5	5	8	9	26	26	26	26
9	10	9	13	26	26	26	26
15	19	26	26	26	26	26	26
26	26	26	26	26	26	26	26
26	26	26	26	26	26	26	26
26	26	26	26	26	26	26	26

The **JPEG** Compression Algorithm

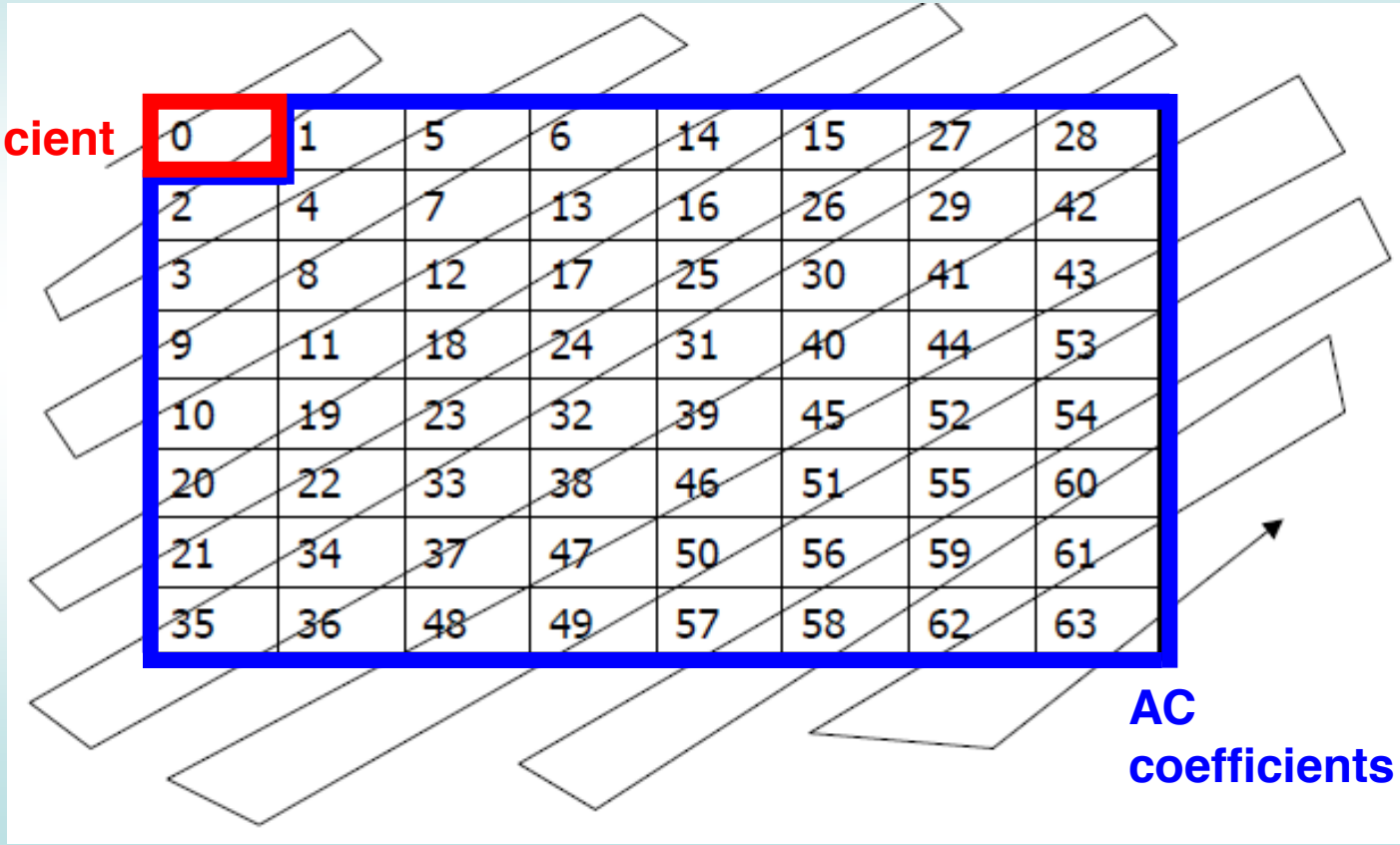


Entropy encoding, zigzag ordering, quantized DCT coefficients

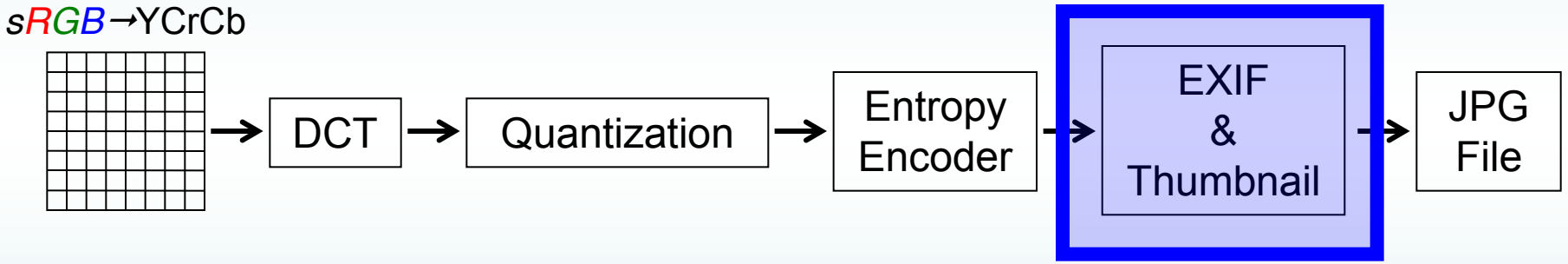


0	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

Entropy encoding, zigzag ordering, quantized DCT coefficients



The **JPEG** Compression Algorithm



Original EXIF

[Make] = "Canon"
[Model] = "Canon PowerShot G2"
[Orientation] = Row 0: top, Col 0: left
[XResolution] = 180/1
[YResolution] = 180/1
[ResolutionUnit] = Inch
[DateTime] = "2010:10:31 11:24:46"
[YCbCrPositioning] = Centered
[ExifOffset] = @ 0x00C4
etc.

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.

```
                Filename: 'WAR%202X2.JPG'
             FileModDate: '21-Jun-2011 11:35:42'
                FileSize: 54181
                  Format: 'jpg'
           FormatVersion: ''
                   Width: 640
                  Height: 480
                BitDepth: 24
               ColorType: 'truecolor'
         FormatSignature: ''
         NumberOfSamples: 3
            CodingMethod: 'Huffman'
          CodingProcess: 'Sequential'
                 Comment: {}
              ImageWidth: 640
             ImageLength: 480
          BitsPerSample: [8 8 8]
PhotometricInterpretation: 'RGB'
             Orientation: 1
         SamplesPerPixel: 3
             XResolution: 96
             YResolution: 96
          ResolutionUnit: 'Inch'
                Software: 'Adobe Photoshop CS5 Windows '
                DateTime: '2011:06:21 11:35:36 '
           DigitalCamera: [1x1 struct]
```

Edited JPG

EXIF:

-No brand

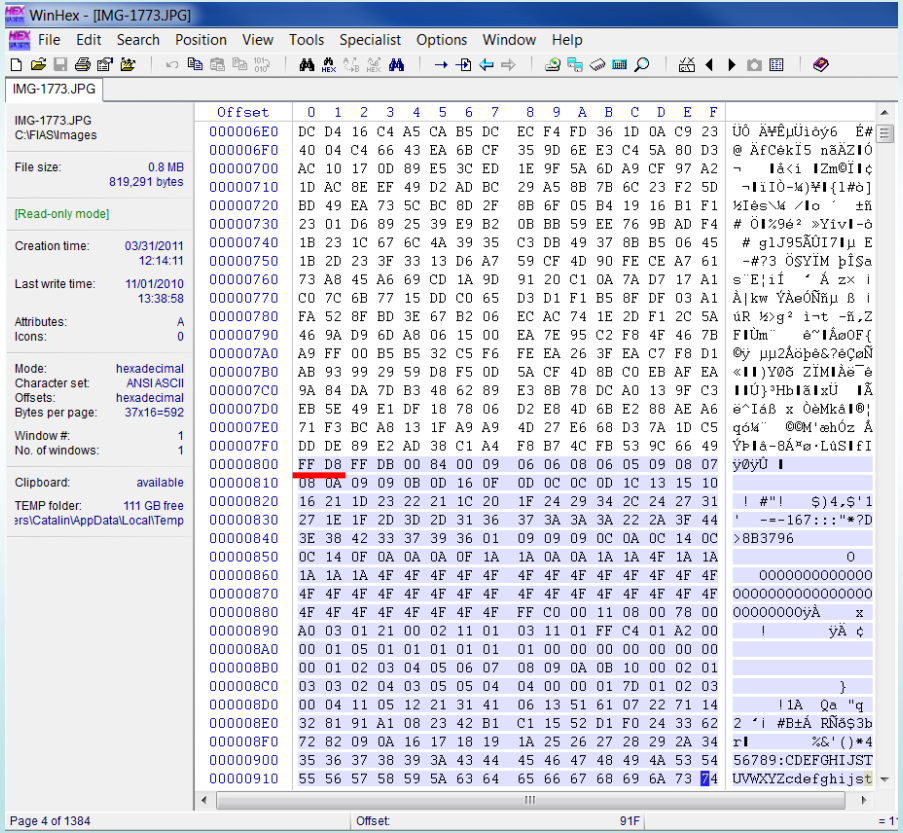
-No model

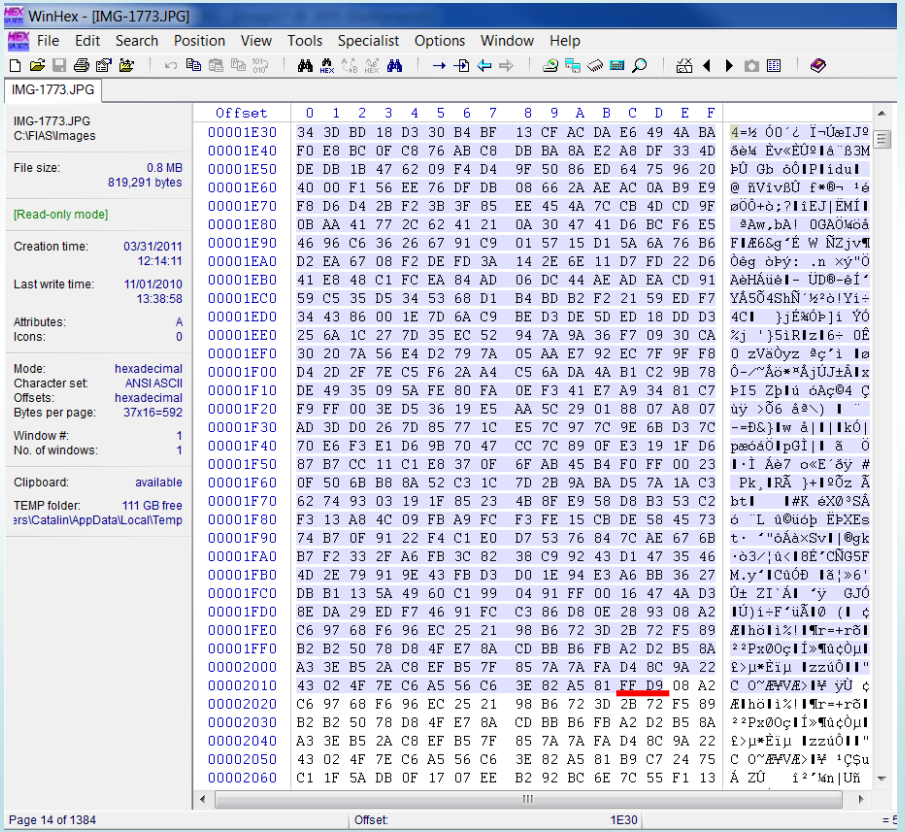
-No settings

-Etc.

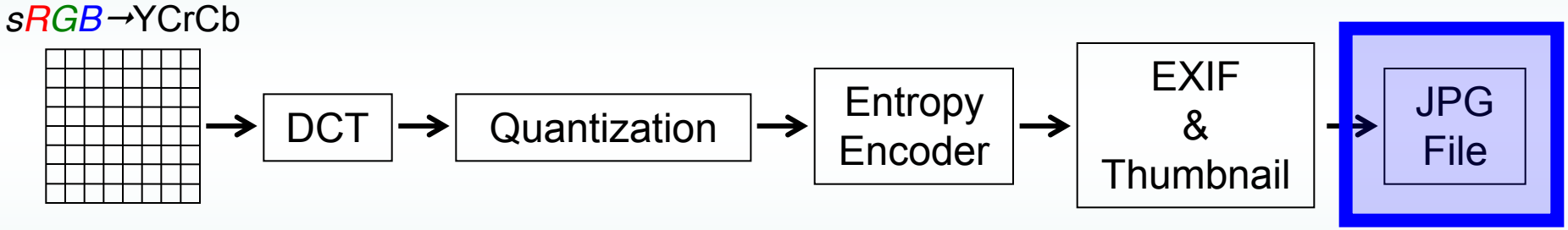
```
        Filename: 'soldat1.jpg'
     FileModDate: '24-Feb-2010 14:49:06'
        FileSize: 17673
          Format: 'jpg'
   FormatVersion: ''
           Width: 400
          Height: 266
        BitDepth: 24
       ColorType: 'truecolor'
FormatSignature: ''
NumberOfSamples: 3
    CodingMethod: 'Huffman'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

Thumbnail


WinHex - [IMG-1773.JPG]
File Edit Search Position View Tools Specialist Options Window Help
IMG-1773.JPG
IMG-1773.JPG
C:\FIAS\Images
File size: 0.8 MB
819,291 bytes
[Read-only mode]
Creation time: 03/31/2011 12:14:11
Last write time: 11/01/2010 13:38:58
Attributes: A
Icons: 0
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 37x16=592
Window #: 1
No. of windows: 1
Clipboard: available
TEMP folder: 111 GB free
ers\Catalin\AppData\Local\Temp
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
000006E0 DC D4 16 C4 A5 CA B5 DC EC F4 FD 36 1D 0A C9 23
000006F0 40 04 C4 66 43 EA 6B CF 35 9D 6E E3 C4 5A 80 D3
00000700 AC 10 17 0D 89 E5 3C ED 1E 9F 5A 6D A9 CF 97 A2
00000710 1D AC 8E EF 49 D2 AD BC 29 A5 8B 7B 6C 23 F2 5D
00000720 BD 49 EA 73 5C BC 8D 2F 8B 6F 05 B4 19 16 B1 F1
00000730 23 01 D6 89 25 39 E9 B2 0B BB 59 EE 76 9B AD F4
00000740 1B 23 1C 67 6C 4A 39 35 C3 DB 49 37 8B B5 06 45
00000750 1B 2D 23 3F 33 13 D6 A7 59 CF 4D 90 FE CE A7 61
00000760 73 A8 45 A6 69 CD 1A 9D 91 20 C1 0A 7A D7 17 A1
00000770 C0 7C 6B 77 15 DD C0 65 D3 D1 F1 B5 8F DF 03 A1
00000780 FA 52 8F BD 3E 67 B2 06 EC AC 74 1E 2D F1 2C 5A
00000790 46 9A D9 6D A8 06 15 00 EA 7E 95 C2 F8 4F 46 7B
000007A0 A9 FF 00 B5 B5 32 C5 F6 FE EA 26 3F EA C7 F8 D1
000007B0 AB 93 99 29 59 D8 F5 0D 5A CF 4D 8B C0 EB AF EA
000007C0 9A 84 DA 7D B3 48 62 89 E3 8B 78 DC A0 13 9F C3
000007D0 EB 5E 49 E1 DF 18 78 06 D2 E8 4D 6B E2 88 AE A6
000007E0 71 F3 BC A8 13 1F A9 A9 4D 27 E6 68 D3 7A 1D C5
000007F0 DD DE 89 E2 AD 38 C1 A4 F8 B7 4C FB 53 9C 66 49
00000800 FF D8 FF DB 00 84 00 09 06 06 08 06 05 09 08 07
00000810 08 0A 09 09 0B 0D 16 0F 0D 0C 0C 0D 1C 13 15 10
00000820 16 21 1D 23 22 21 1C 20 1F 24 29 34 2C 24 27 31
00000830 27 1E 1F 2D 3D 2D 31 36 37 3A 3A 3A 22 2A 3F 44
00000840 3E 38 42 33 37 39 36 01 09 09 09 0C 0A 0C 14 0C
00000850 0C 14 0F 0A 0A 0A 0F 1A 1A 0A 0A 1A 1A 4F 1A 1A
00000860 1A 1A 1A 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F
00000870 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F
00000880 4F 4F 4F 4F 4F 4F 4F 4F FF C0 00 11 08 00 78 00
00000890 A0 03 01 21 00 02 11 01 03 11 01 FF C4 01 A2 00
000008A0 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00
000008B0 00 01 02 03 04 05 06 07 08 09 0A 0B 10 00 02 01
000008C0 03 03 02 04 03 05 05 04 04 00 00 01 7D 01 02 03
000008D0 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14
000008E0 32 81 91 A1 08 23 42 B1 C1 15 52 D1 F0 24 33 62
000008F0 72 82 09 0A 16 17 18 19 1A 25 26 27 28 29 2A 34
00000900 35 36 37 38 39 3A 43 44 45 46 47 48 49 4A 53 54
00000910 55 56 57 58 59 5A 63 64 65 66 67 68 69 6A 73 74
Page 4 of 1384
Offset: 91F


WinHex - [IMG-1773.JPG]
File Edit Search Position View Tools Specialist Options Window Help
IMG-1773.JPG
IMG-1773.JPG
C:\FIAS\Images
File size: 0.8 MB
819,291 bytes
[Read-only mode]
Creation time: 03/31/2011 12:14:11
Last write time: 11/01/2010 13:38:58
Attributes: A
Icons: 0
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 37x16=592
Window #: 1
No. of windows: 1
Clipboard: available
TEMP folder: 111 GB free
ers\Catalin\AppData\Local\Temp
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00001E30 34 3D BD 18 D3 30 B4 BF 13 CF AC DA E6 49 4A BA
00001E40 F0 E8 BC 0F C8 76 AB C8 DB BA 8A E2 A8 DF 33 4D
00001E50 DE DB 1B 47 62 09 F4 D4 9F 50 86 ED 64 75 96 20
00001E60 40 00 F1 56 EE 76 DF DB 08 66 2A AE AC 0A B9 E9
00001E70 F8 D6 D4 2B F2 3B 3F 85 EE 45 4A 7C CB 4D CD 9F
00001E80 0B AA 41 77 2C 62 41 21 0A 30 47 41 D6 BC F6 E5
00001E90 46 96 C6 36 26 67 91 C9 01 57 15 D1 5A 6A 76 B6
00001EA0 D2 EA 67 08 F2 DE FD 3A 14 2E 6E 11 D7 FD 22 D6
00001EB0 41 E8 48 C1 FC EA 84 AD 06 DC 44 AE AD EA CD 91
00001EC0 59 C5 35 D5 34 53 68 D1 B4 BD B2 F2 21 59 ED F7
00001ED0 34 43 86 00 1E 7D 6A C9 BE D3 DE 5D ED 18 DD D3
00001EE0 25 6A 1C 27 7D 35 EC 52 94 7A 9A 36 F7 09 30 CA
00001EF0 30 20 7A 56 E4 D2 79 7A 05 AA E7 92 EC 7F 9F F8
00001F00 D4 2D 2F 7E C5 F6 2A A4 C5 6A DA 4A B1 C2 9B 78
00001F10 DE 49 35 09 5A FE 80 FA 0E F3 41 E7 A9 34 81 C7
00001F20 F9 FF 00 3E D5 36 19 E5 AA 5C 29 01 88 07 A8 07
00001F30 AD 3D D0 26 7D 85 77 1C E5 7C 97 7C 9E 6B D3 7C
00001F40 70 E6 F3 E1 D6 9B 70 47 CC 7C 89 0F E3 19 1F D6
00001F50 87 B7 CC 11 C1 E8 37 0F 6F AB 45 B4 F0 FF 00 23
00001F60 0F 50 6B B8 8A 52 C3 1C 7D 2B 9A BA D5 7A 1A C3
00001F70 62 74 93 03 19 1F 85 23 4B 8F E9 58 D8 B3 53 C2
00001F80 F3 13 A8 4C 09 FB A9 FC F3 FE 15 CB DE 58 45 73
00001F90 74 B7 0F 91 22 F4 C1 E0 D7 53 76 84 7C AE 67 6B
00001FA0 B7 F2 33 2F A6 FB 3C 82 38 C9 92 43 D1 47 35 46
00001FB0 4D 2E 79 91 9E 43 FB D3 D0 1E 94 E3 A6 BB 36 27
00001FC0 DB B1 13 5A 49 60 C1 99 04 91 FF 00 16 47 4A D3
00001FD0 8E DA 29 ED F7 46 91 FC C3 86 D8 0E 28 93 08 A2
00001FE0 C6 97 68 F6 96 EC 25 21 98 B6 72 3D 2B 72 F5 89
00001FF0 B2 B2 50 78 D8 4F E7 8A CD BB B6 FB A2 D2 B5 8A
00002000 A3 3E B5 2A C8 EF B5 7F 85 7A 7A FA D4 8C 9A 22
00002010 43 02 4F 7E C6 A5 56 C6 3E 82 A5 81 FF D9 08 A2
00002020 C6 97 68 F6 96 EC 25 21 98 B6 72 3D 2B 72 F5 89
00002030 B2 B2 50 78 D8 4F E7 8A CD BB B6 FB A2 D2 B5 8A
00002040 A3 3E B5 2A C8 EF B5 7F 85 7A 7A FA D4 8C 9A 22
00002050 43 02 4F 7E C6 A5 56 C6 3E 82 A5 81 B9 C7 24 75
00002060 C1 1F 5A DB 0F 17 07 EE B2 92 BC 6E 7C 55 F1 13
Page 14 of 1384
Offset: 1E30

The **JPEG** Compression Algorithm



Examples

lena.bmp

lena.jpg

Examples

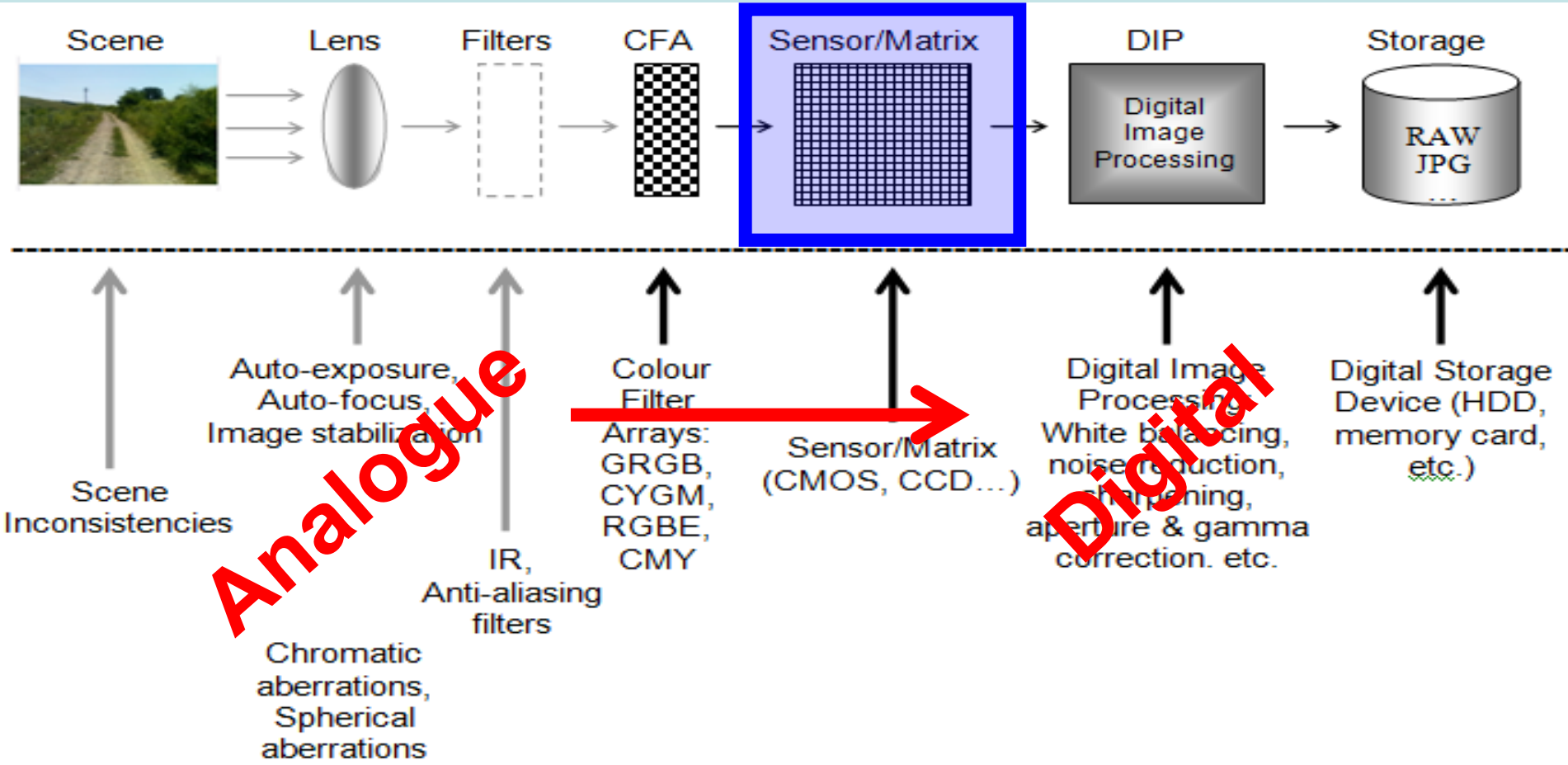
lena.bmp - lena.jpg (eye details)

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)

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

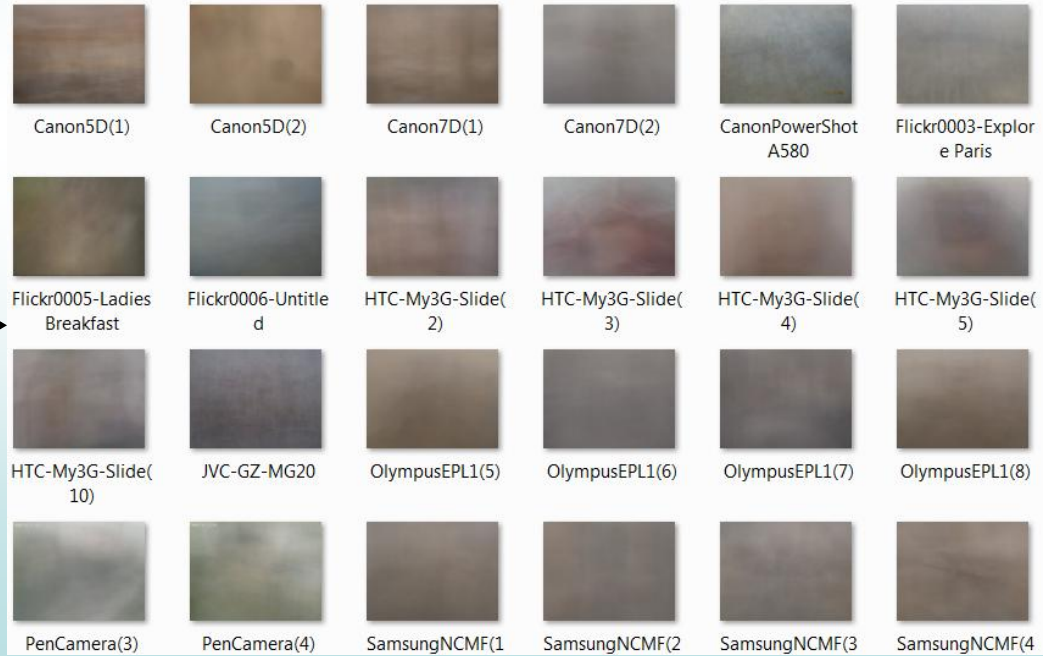
Erroneous PRNU models

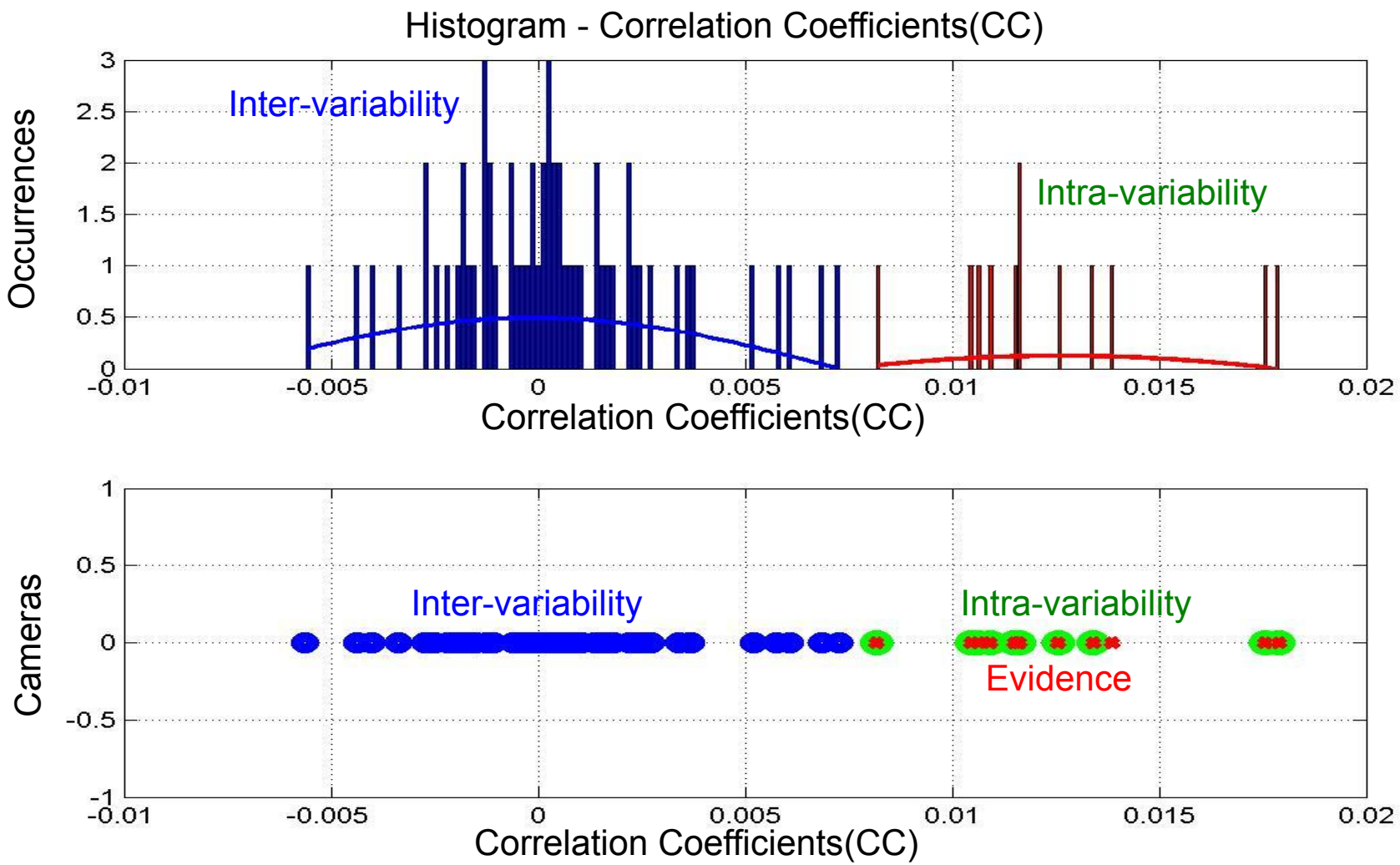
Recommended PRNU models

Evidence

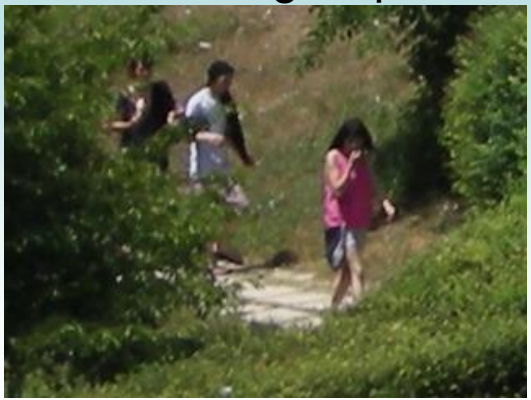
Suspect camera

Reference database



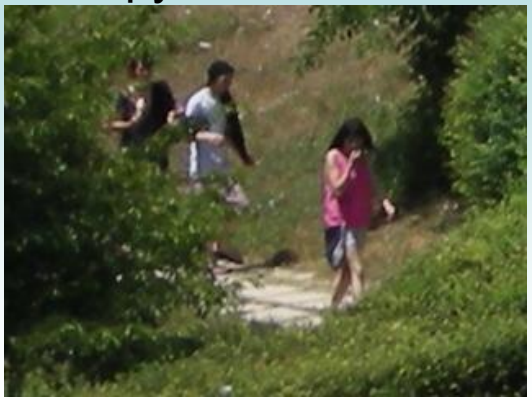

Histogram - Correlation Coefficients(CC)
Occurrences
Inter-variability
Intra-variability
3
2.5
2
1.5
1
0.5
0
-0.01
-0.005
0
0.005
0.01
0.015
0.02
Correlation Coefficients(CC)
Cameras
Inter-variability
Intra-variability
Evidence
1
0.5
0
-0.5
-1
-0.01
-0.005
0
0.005
0.01
0.015
0.02
Correlation Coefficients(CC)

Authentic digital photo



Bit-stream the memory

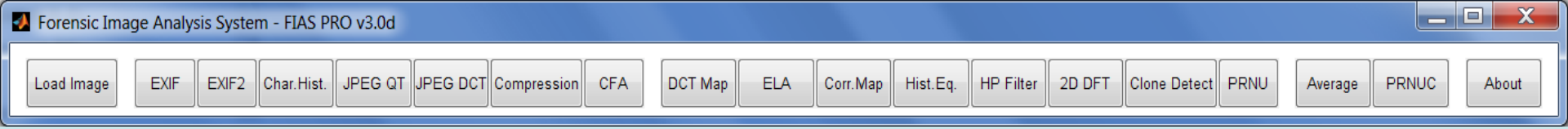
Copy/Paste the file

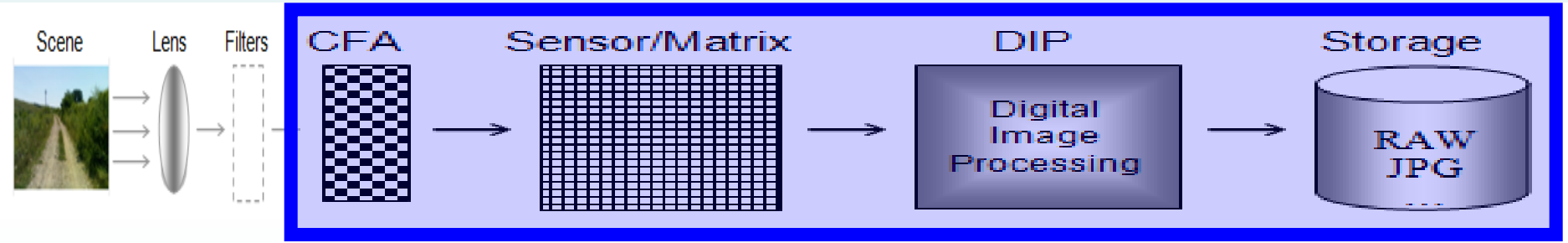


Rescale / Crop, etc.

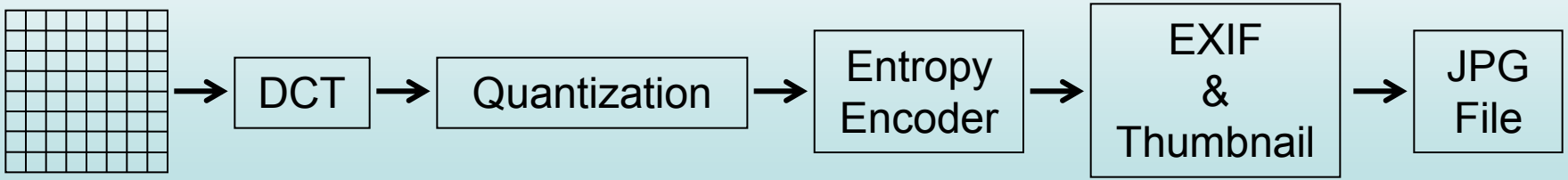
Adjust brightness, contrast, colours, etc.

Counterfeited / tampered / doctored photo


Forensic Image Analysis System - FIAS PRO v3.0d
Load Image
EXIF
EXIF2
Char.Hist.
JPEG QT
JPEG DCT
Compression
CFA
DCT Map
ELA
Corr.Map
Hist.Eq.
HP Filter
2D DFT
Clone Detect
PRNU
Average
PRNUC
About


Scene
Lens
Filters
CFA
Sensor/Matrix
DIP
Digital Image Processing
Storage
RAW
JPG

sRGB→YCrCb


DCT
Quantization
Entropy Encoder
EXIF & Thumbnail
JPG File

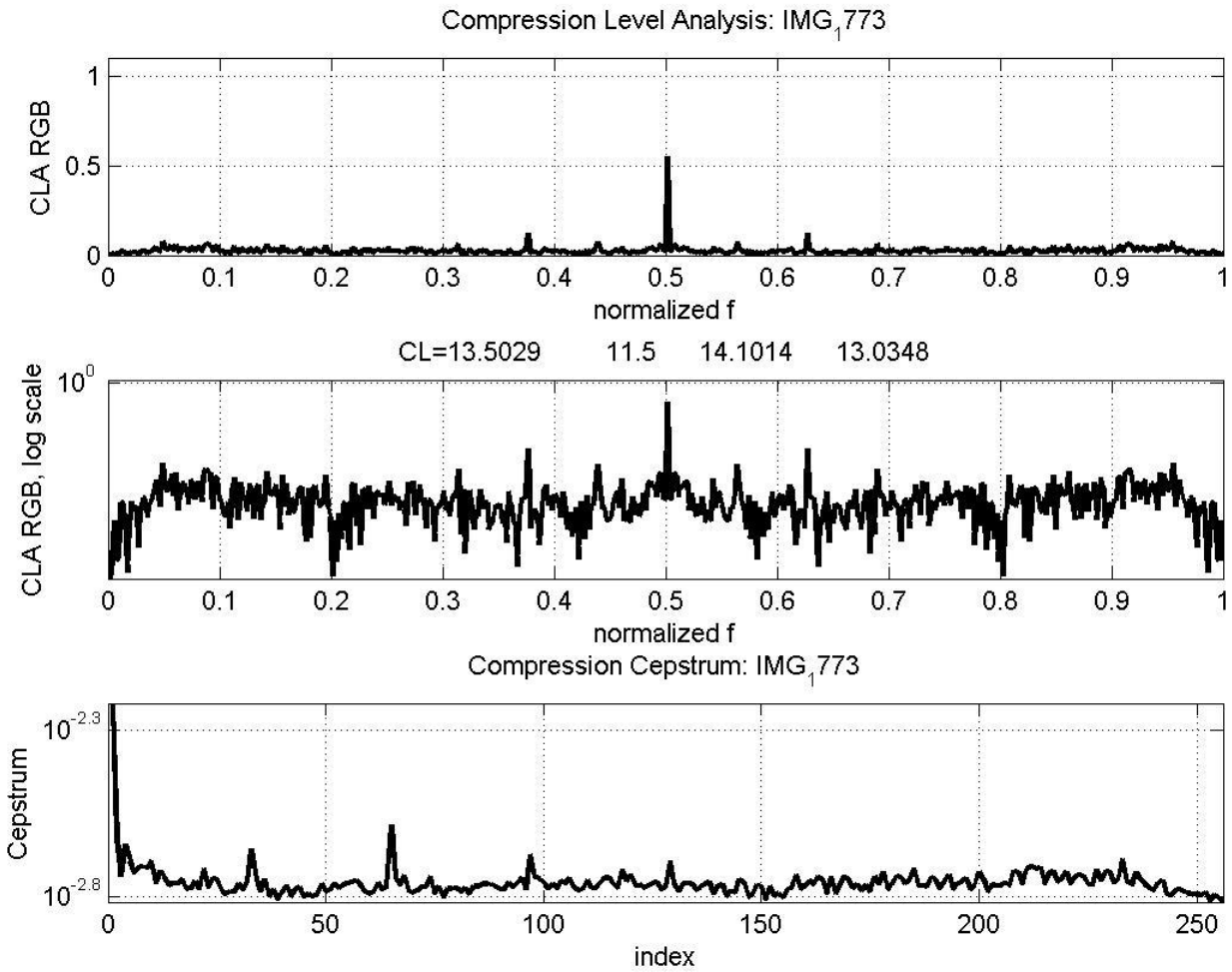
Original JPEG file:
IMG-1773.jpg

Camera:
Canon Power Shot G2

Settings:
2272x1704
Low JPEG compression (high JPEG quality)

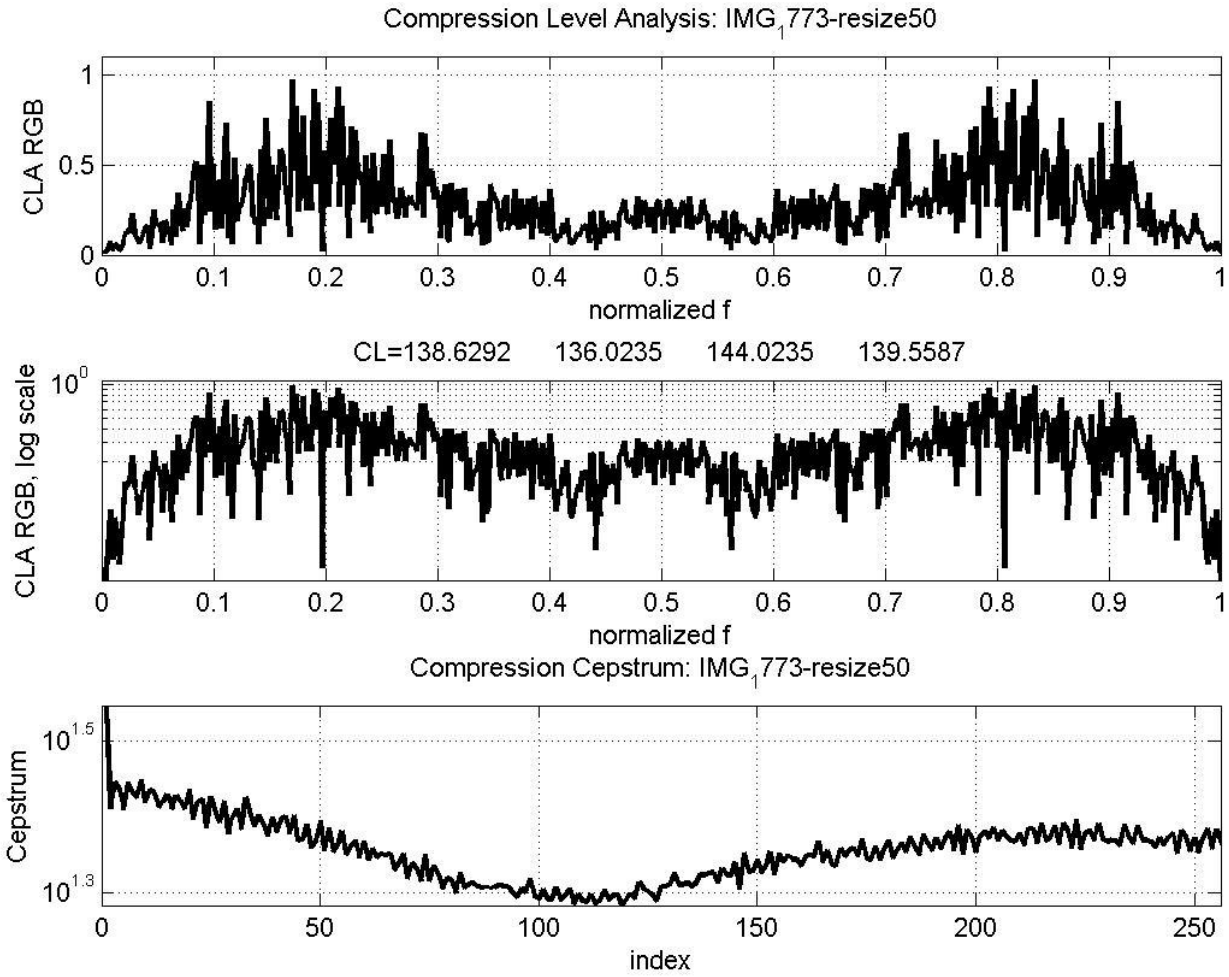
Original JPEG file: IMG-1773.jpg

Compression Analysis



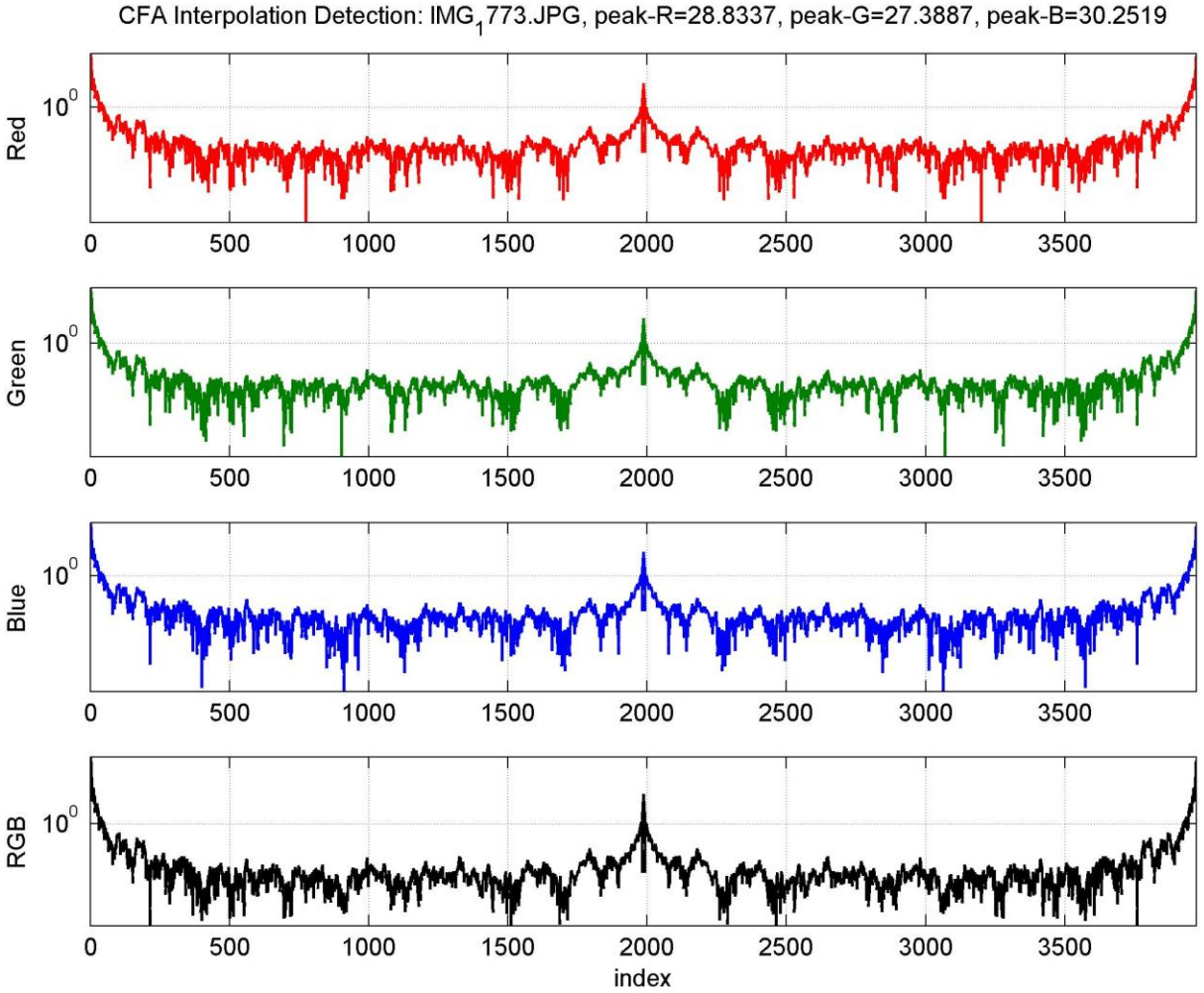
Recompressed JPEG file:
IMG_1773-resize50

Compression Analysis



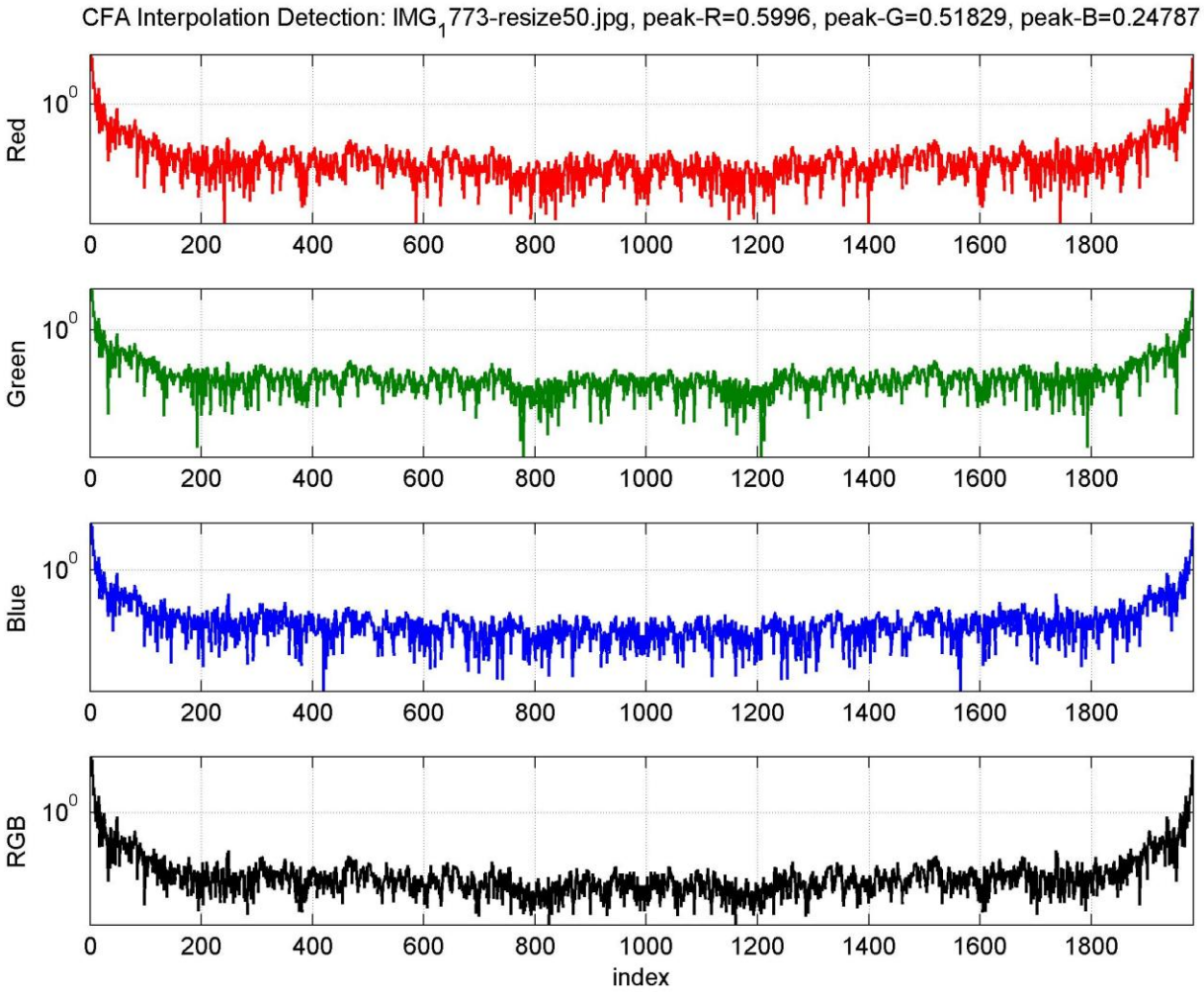
Original JPEG file: IMG-1773.jpg

Colour Filter Array (CFA) Analysis



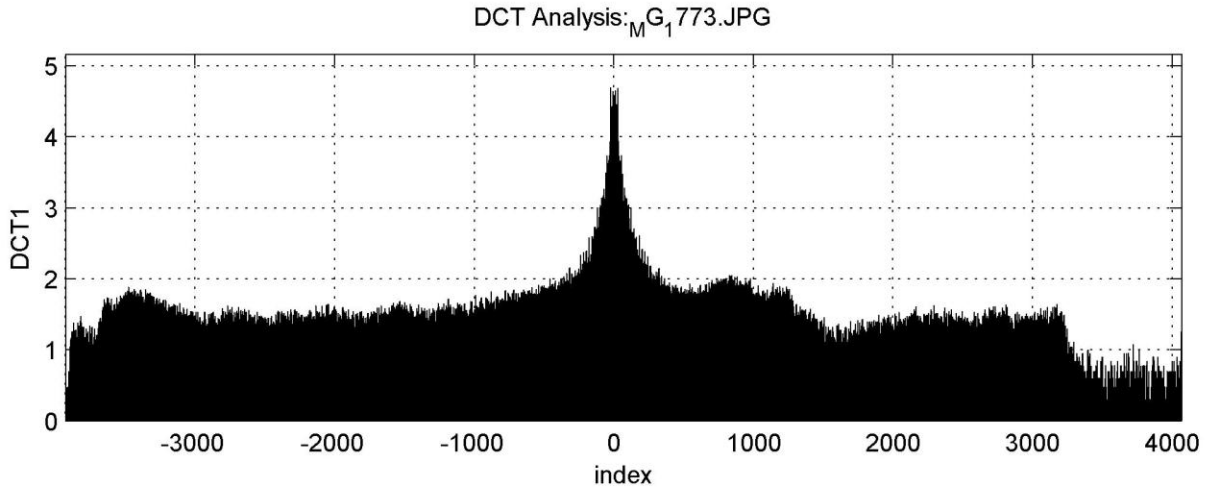
Recompressed JPEG file: IMG_1773-resize50

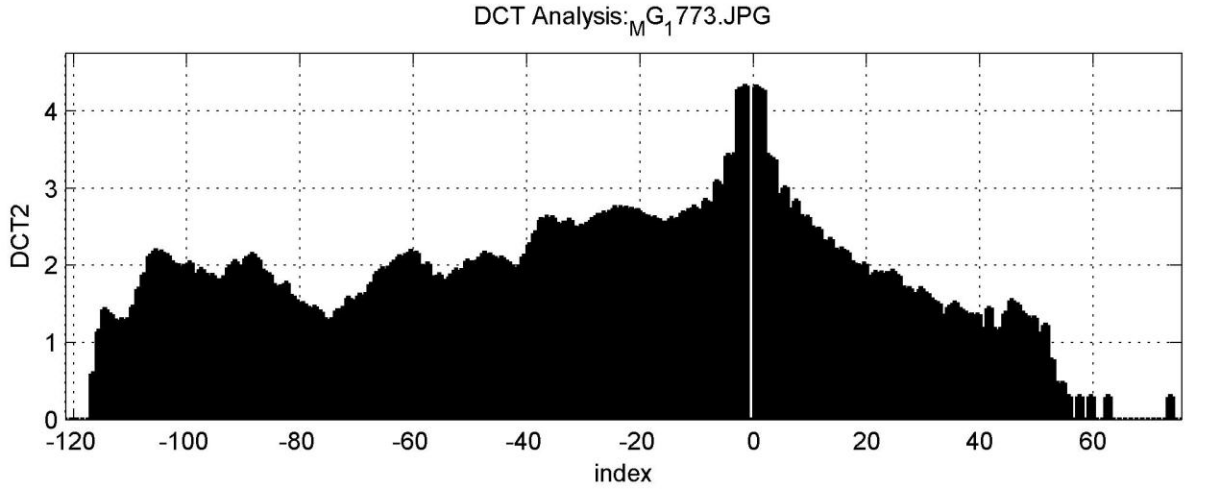
Colour Filter Array (CFA) Analysis



Original JPEG file: IMG-1773.jpg

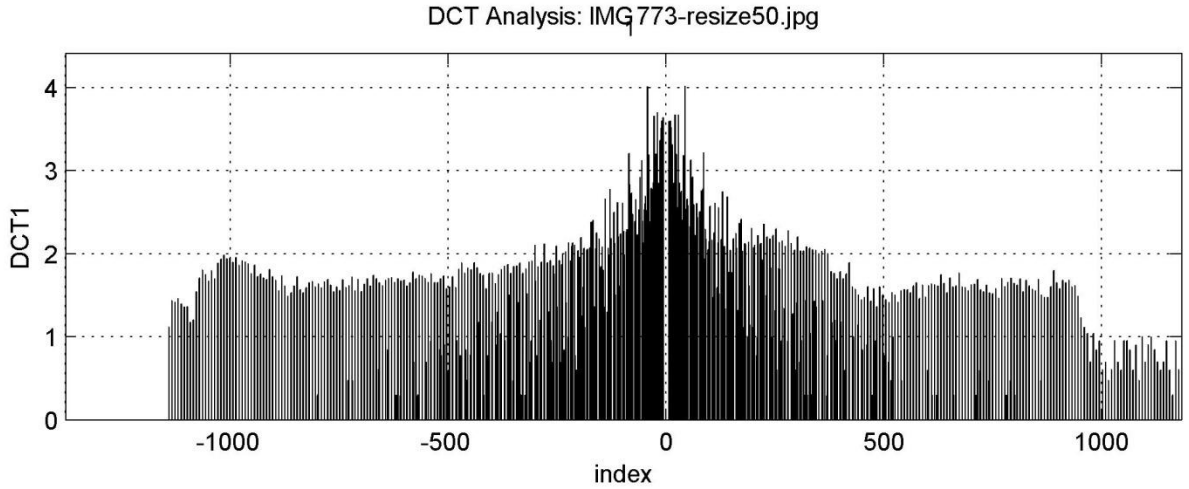
DCT Coefficients Analysis

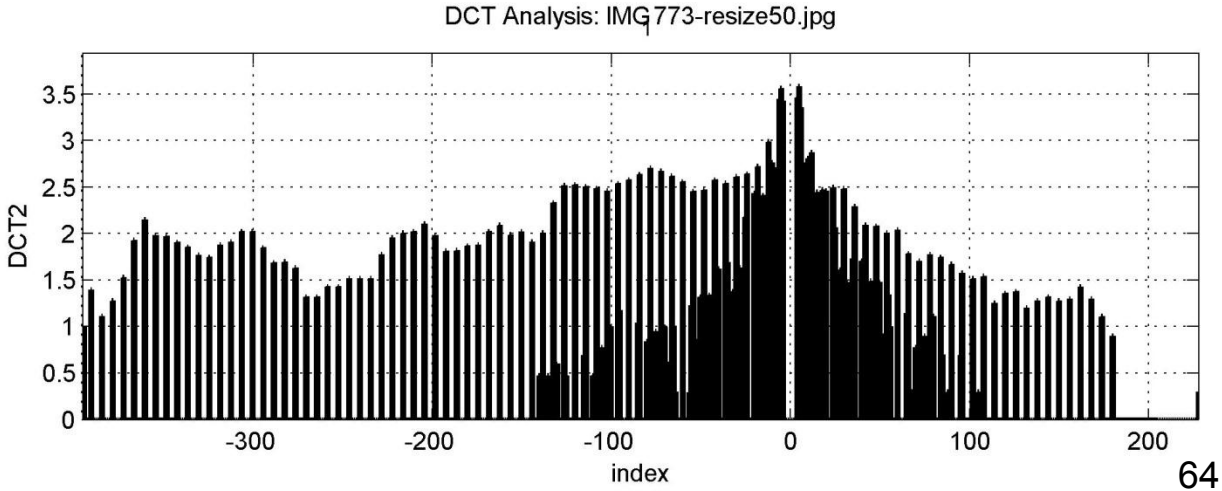




Recompressed JPEG file:
IMG_1773-resize50.jpg

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://www.hackerfactor.com/blog/index.php?/archives/322-Body-By-Victoria.html
http://www2.victoriassecret.com/commerce/onlineProductDisplay.vs?namespace=productDisplay&origin=onlineProductDisplay.jsp&event=display&prnbr=EF-227524&cgname=OSCLODRSDAY

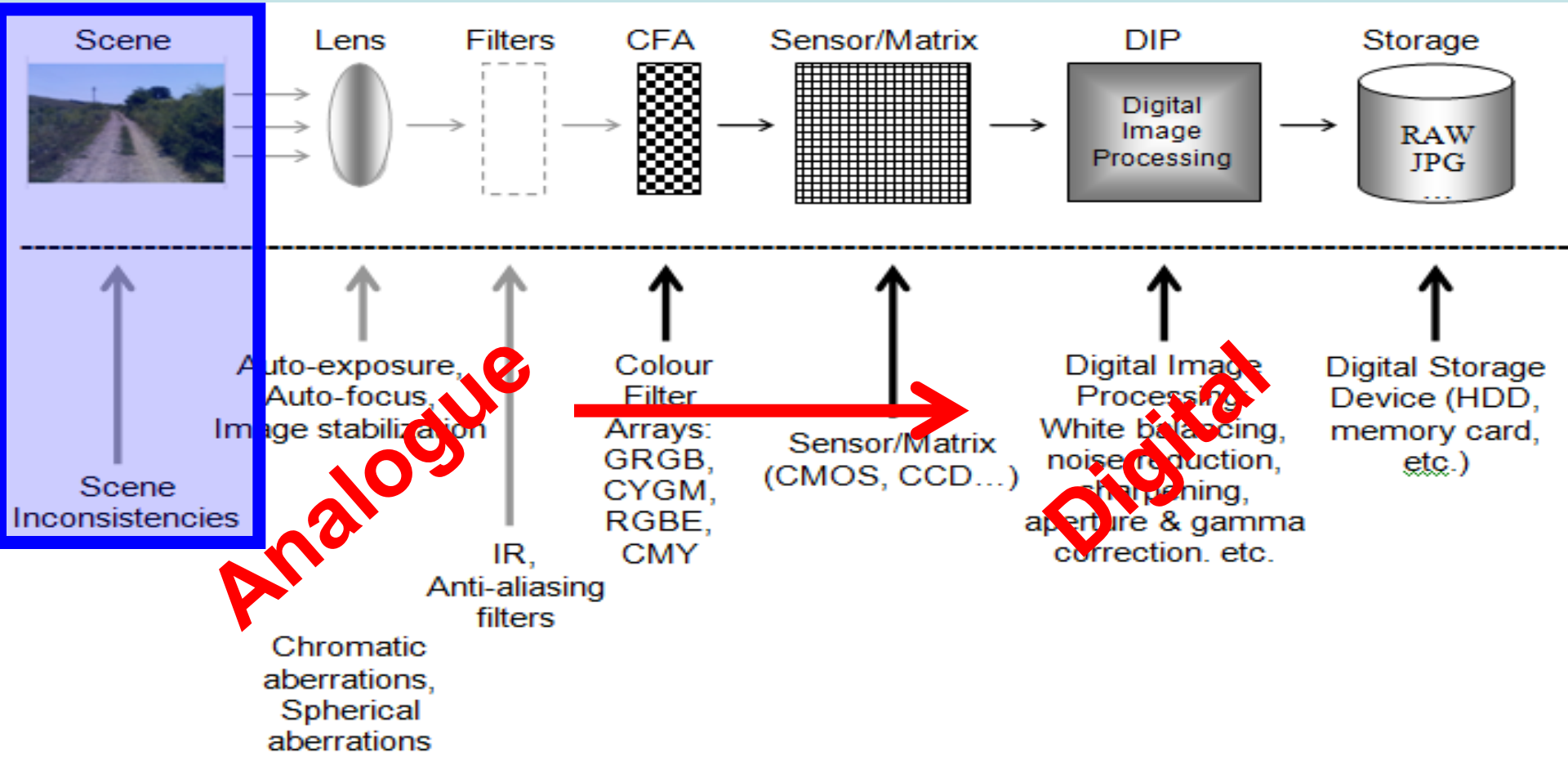
Wolf
http://socialtech.ca/ade/misc/wolf_full_size.jpg

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

Digital Photography Analysis



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'Elysée.

l with tie
awaiian
Back zip.
tton poplin.
-173-483
0.

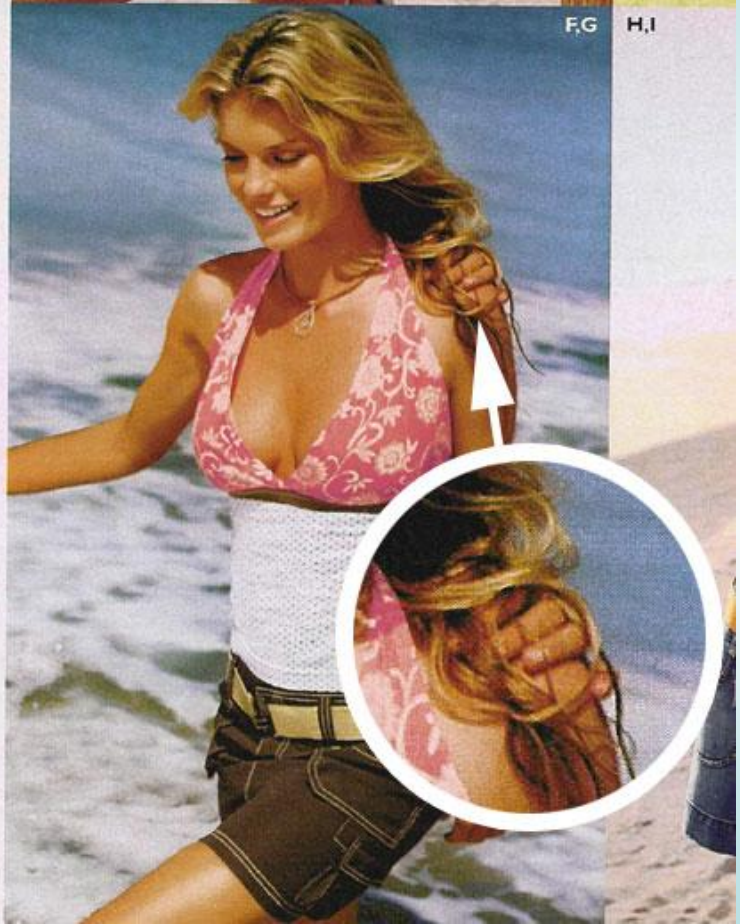
in floral and
, surfer
st seaming
nported
2-656

l. The mini
belt.
Brown (27).
fiber.
-172-500
0.

ler ease.
r a cami.
Stripe
zes XS-XL.
SALE $19.

n. Wide
d stone
andex.

9.50.

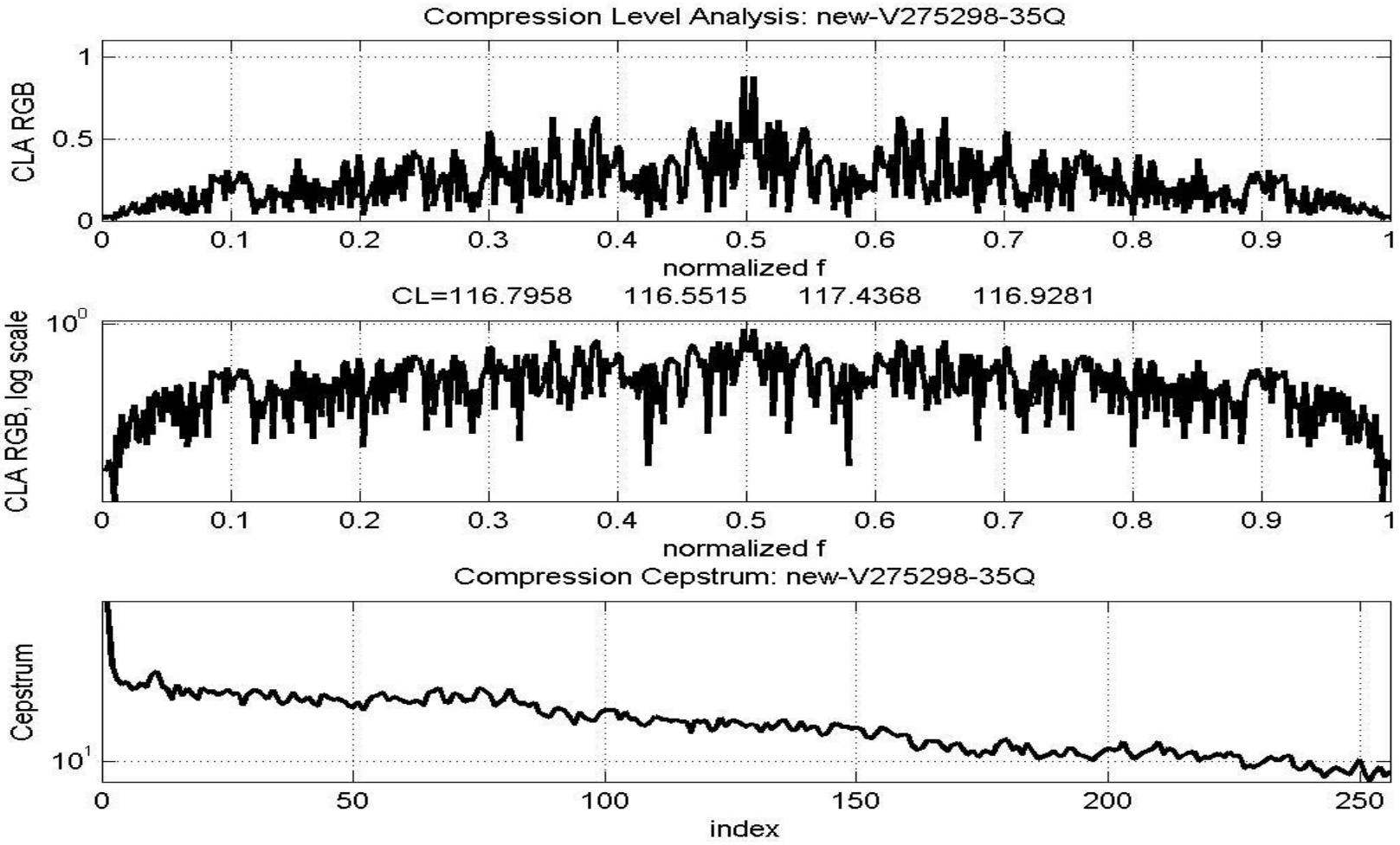


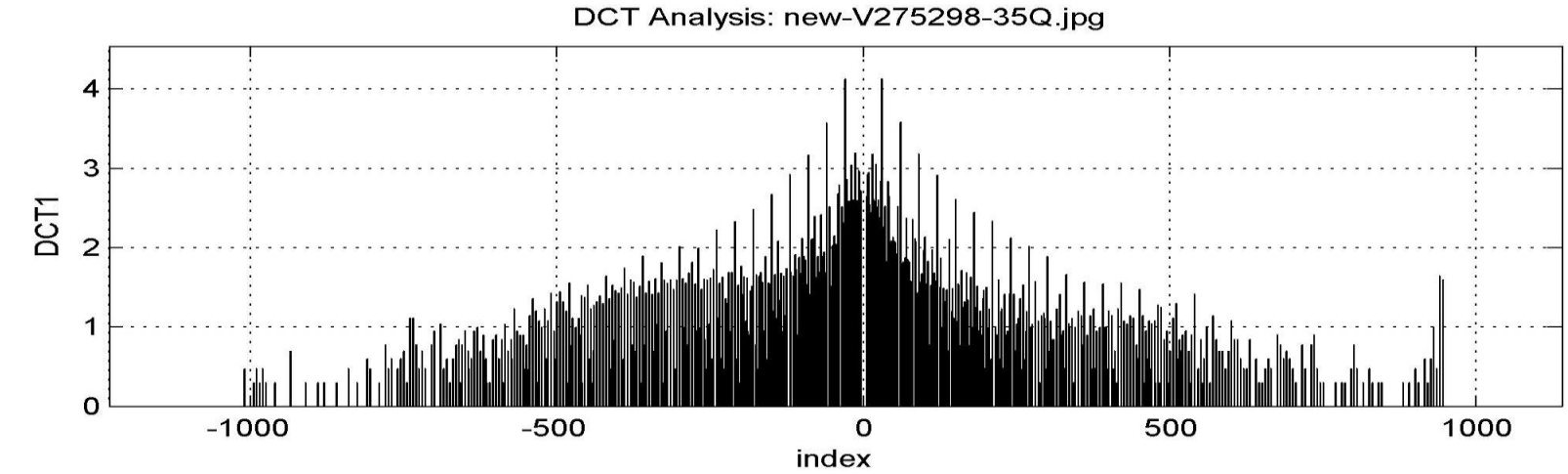
?

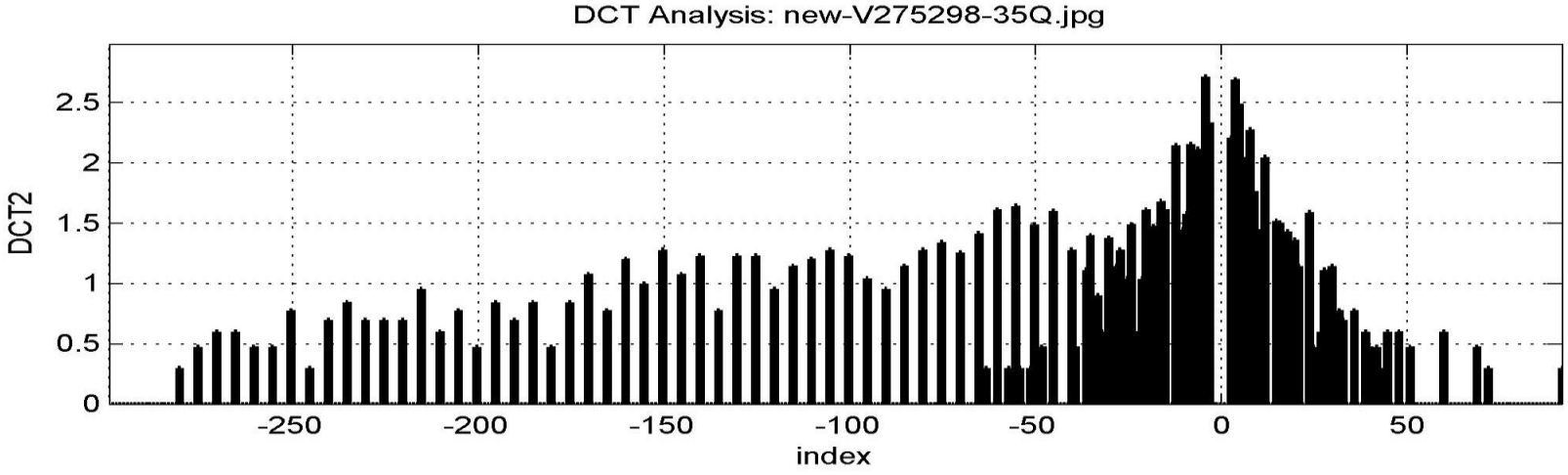

Piedras
semipreciosas
combinadas con
plata, jaspe, corales
y hasta con hilos.
Esta es la propuesta
de Teresa Aldama y
de sus diseños tan
sugestivos como
irrepetibles

?


Piedras
semipreciosas
combinadas con
plata, jaspe, corales
y hasta con hules.
Esta es la propuesta
de Teresa Aldama y
de sus diseños tan
sugestivos como
irrepetibles


Compression Level Analysis: new-V275298-35Q
CLA RGB
1
0.5
0
0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1
normalized f
CL=116.7958 116.5515 117.4368 116.9281
CLA RGB, log scale
10^0
0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1
normalized f
Compression Cepstrum: new-V275298-35Q
Cepstrum
10^1
0 50 100 150 200 250
index


DCT Analysis: new-V275298-35Q.jpg
DCT1
4
3
2
1
0
-1000
-500
0
500
1000
index


DCT Analysis: new-V275298-35Q.jpg
DCT2
2.5
2
1.5
1
0.5
0
-250
-200
-150
-100
-50
0
50
index

?


Original
Doctored


Original


Doctored

Internet examples
Analysis & Discussions

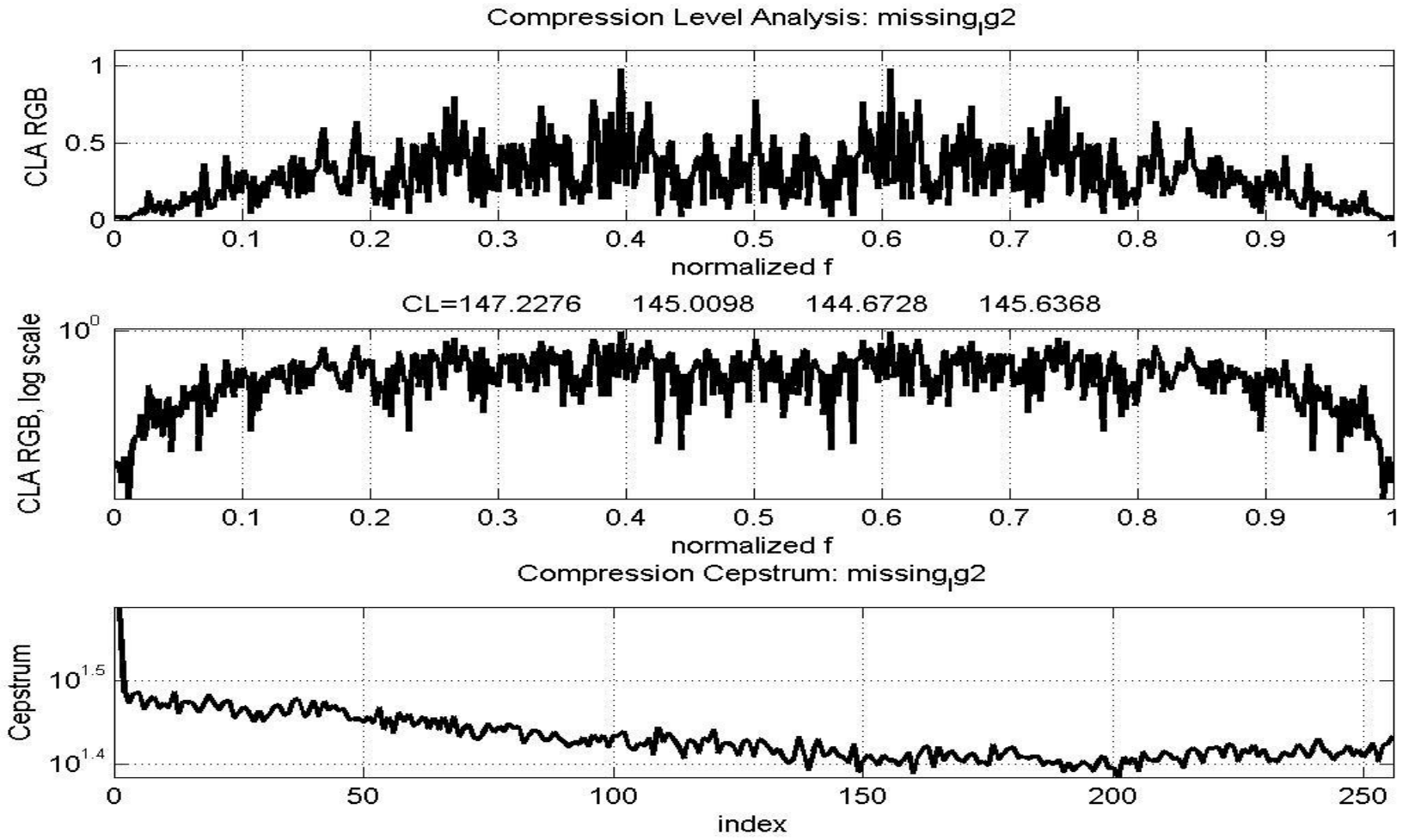
Case: WTC Tourist
http://urbanlegends.about.com/library/blphoto-wtc.htm

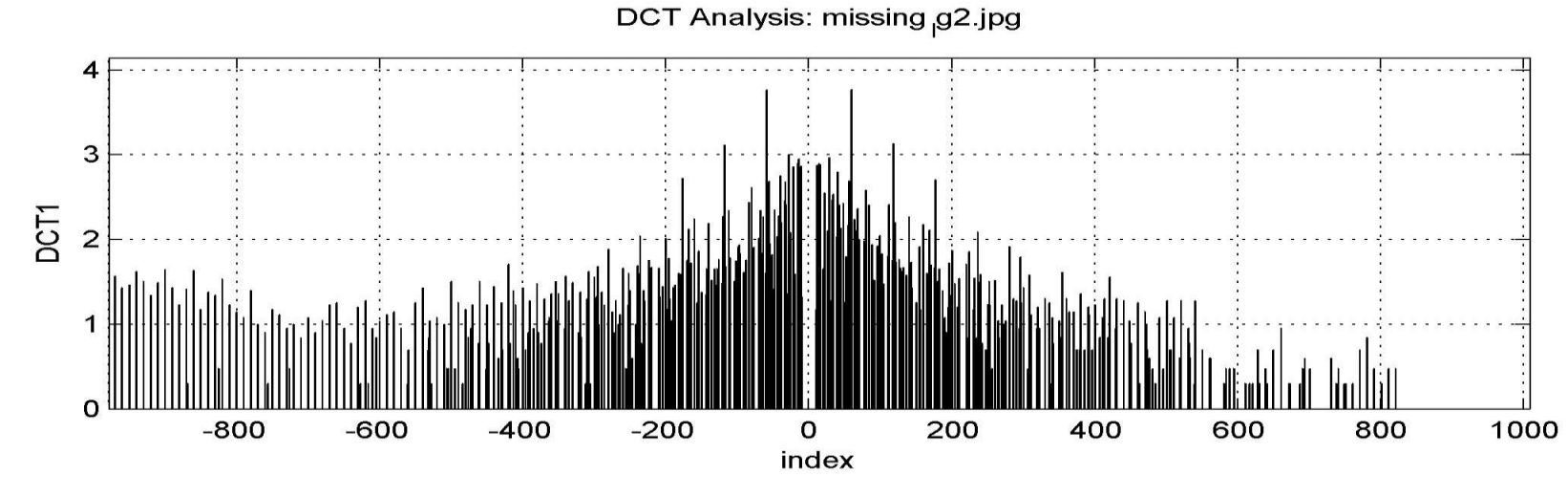
Evidence:
-One Internet JPG file
-JPG EXIF without photo camera, no suspect photo camera

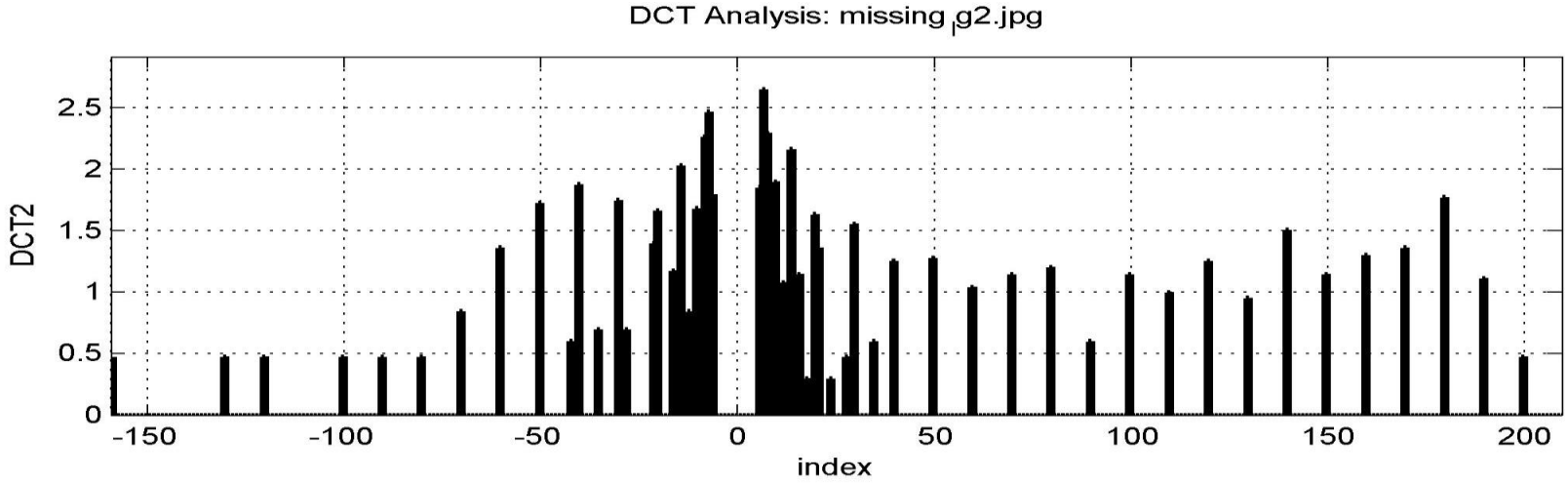
Methods & Tools:
-Visual inspection, scene inconsistencies
-EXIF, DCT, PRNU…tools

EXIF:
-Not typical for original digital photos
-Typical for JPG files generated/saved with an image editor and “Save EXIF” disabled

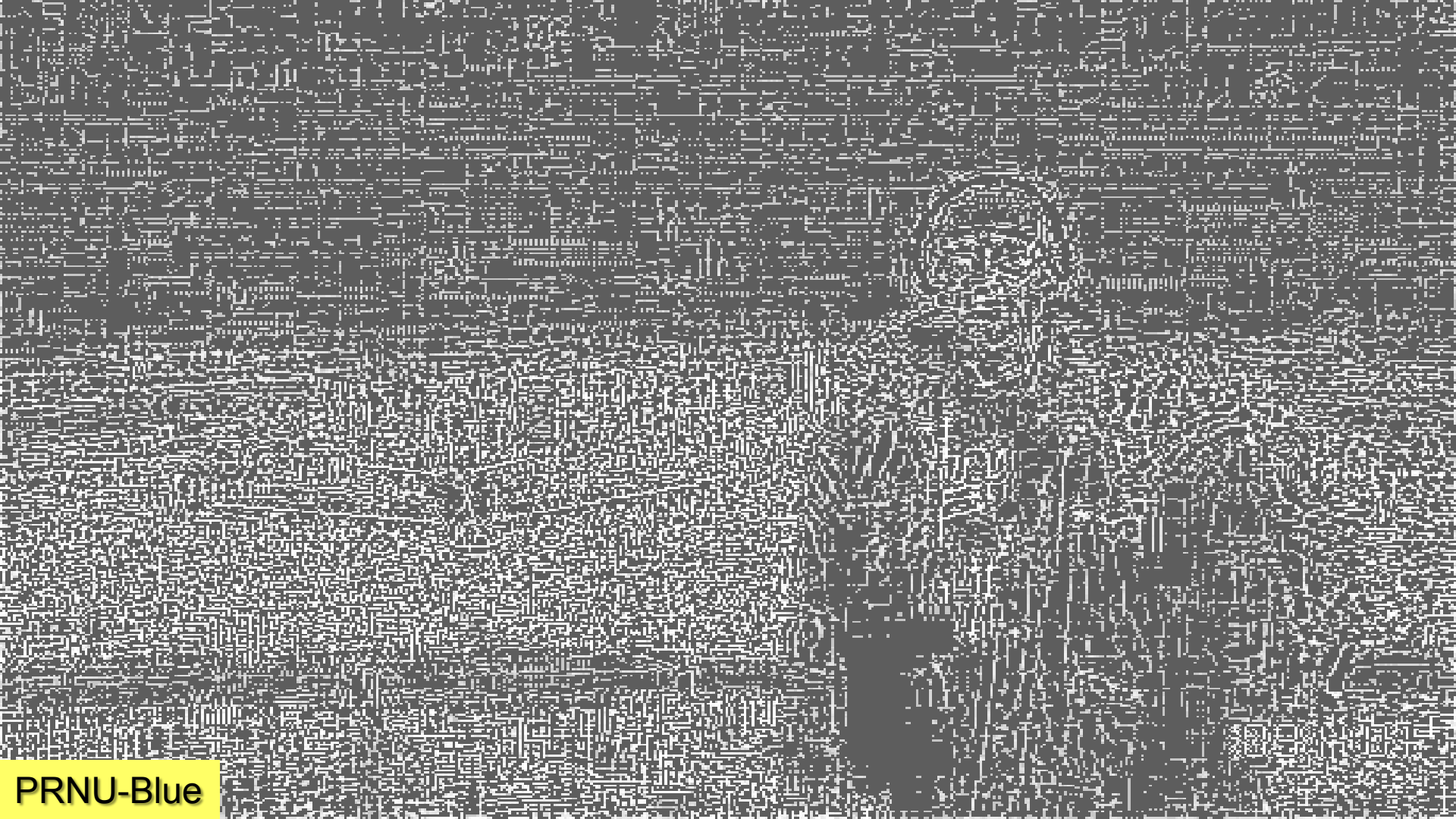
```
        Filename: 'missing_lg2.jpg'
    FileModDate: '28-Mar-2011 18:56:42'
        FileSize: 32223
          Format: 'jpg'
  FormatVersion: ''
           Width: 550
          Height: 380
        BitDepth: 24
       ColorType: 'truecolor'
FormatSignature: ''
NumberOfSamples: 3
   CodingMethod: 'Huffman'
  CodingProcess: 'Sequential'
         Comment: {}
```


Compression Level Analysis: missing_g2
CLA RGB
normalized f
CL=147.2276 145.0098 144.6728 145.6368
CLA RGB, log scale
normalized f
Compression Cepstrum: missing_g2
Cepstrum
index


DCT Analysis: missing_g2.jpg
DCT1
index
4
3
2
1
0
-800
-600
-400
-200
0
200
400
600
800
1000

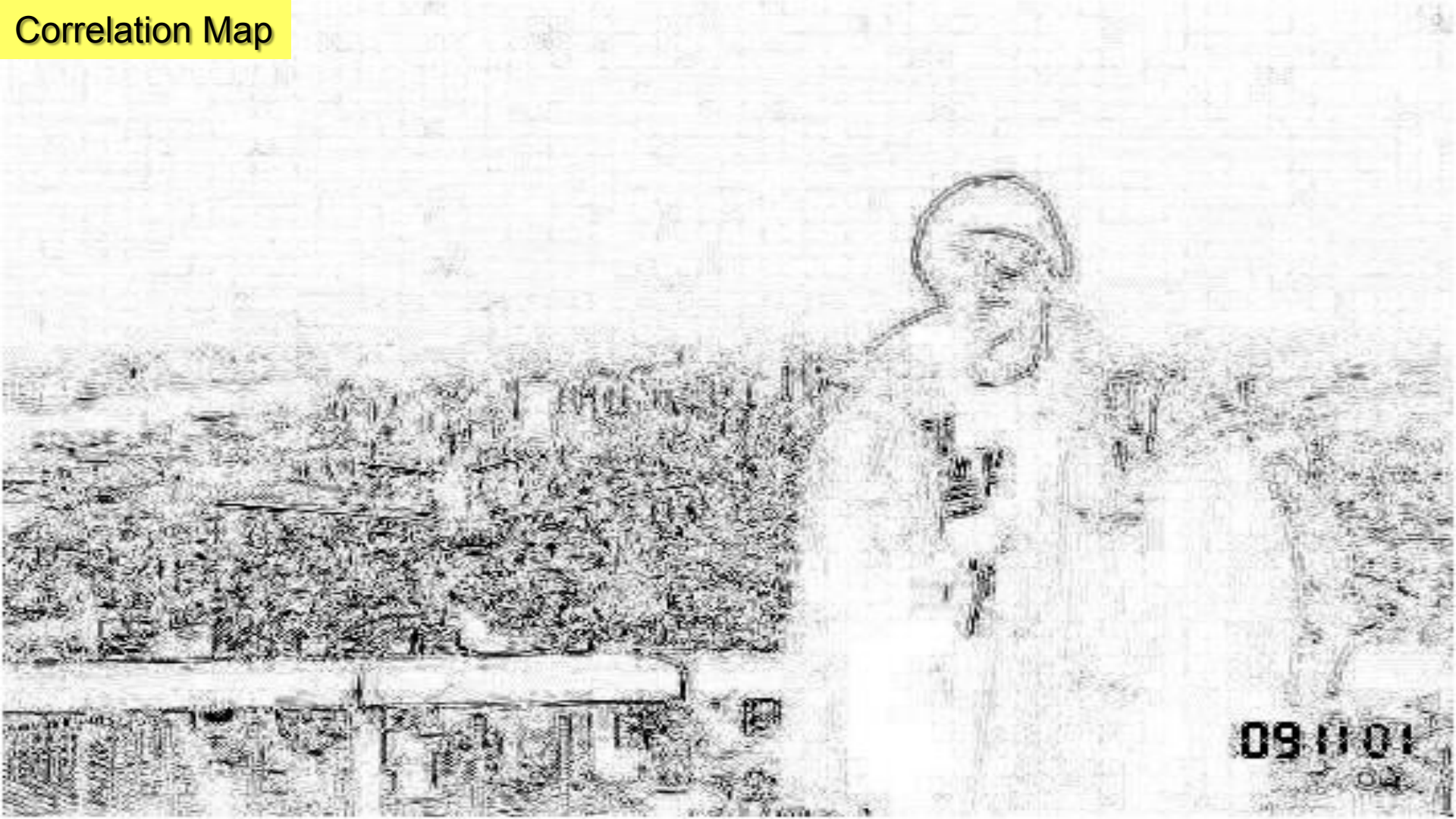

DCT Analysis: missing_g2.jpg
DCT2
index
2.5
2
1.5
1
0.5
0
-150
-100
-50
0
50
100
150
200

Evidence


PRNU-Blue


DCT AC

Correlation Map



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

Original Image

File:
Ladies-before.bmp

Doctored Image, copy/paste small green grass areas over the mid lady

File: Ladies_doct.bmp

Clone detection results for

Block size=
4 pixels

Analogue Audio

Authentic analogue recording(s)

Copy/ copies

Copy fragment(s)

Deletions

Counterfeiting

Tampered/doctored recordings

Non-authentic analogue recordings

Digital Audio

Authentic digital files containing authentic recording(s)

- built-in memory

- removable memory

Bit stream data image

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

File copy

File copies containing authentic recording(s)

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

No manipulation:
-Audio Enhancement
-Deletions, etc.

Edited recordings

(forensic results)

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

Tampered/doctored recordings

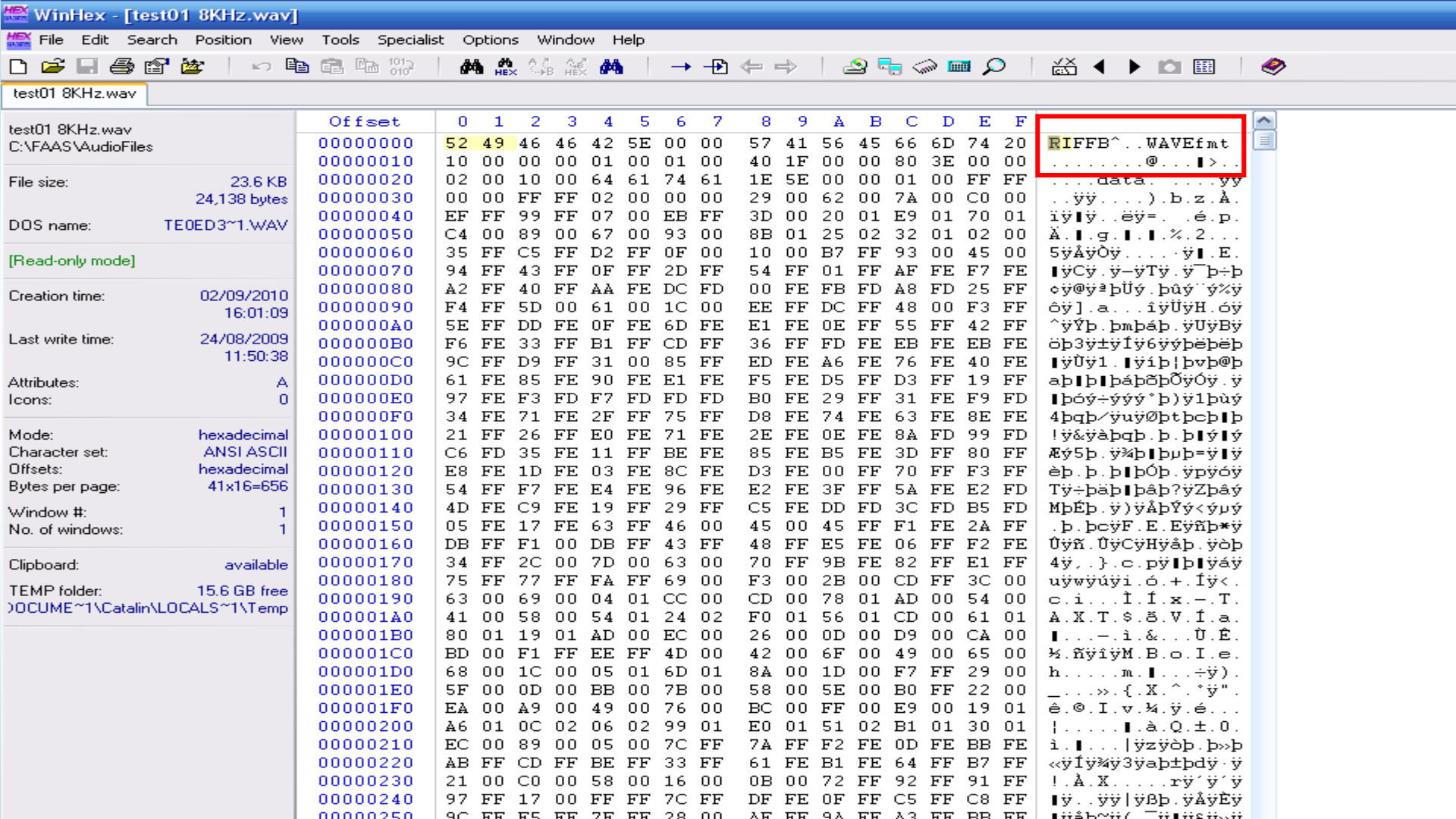
(conterfeiting results)

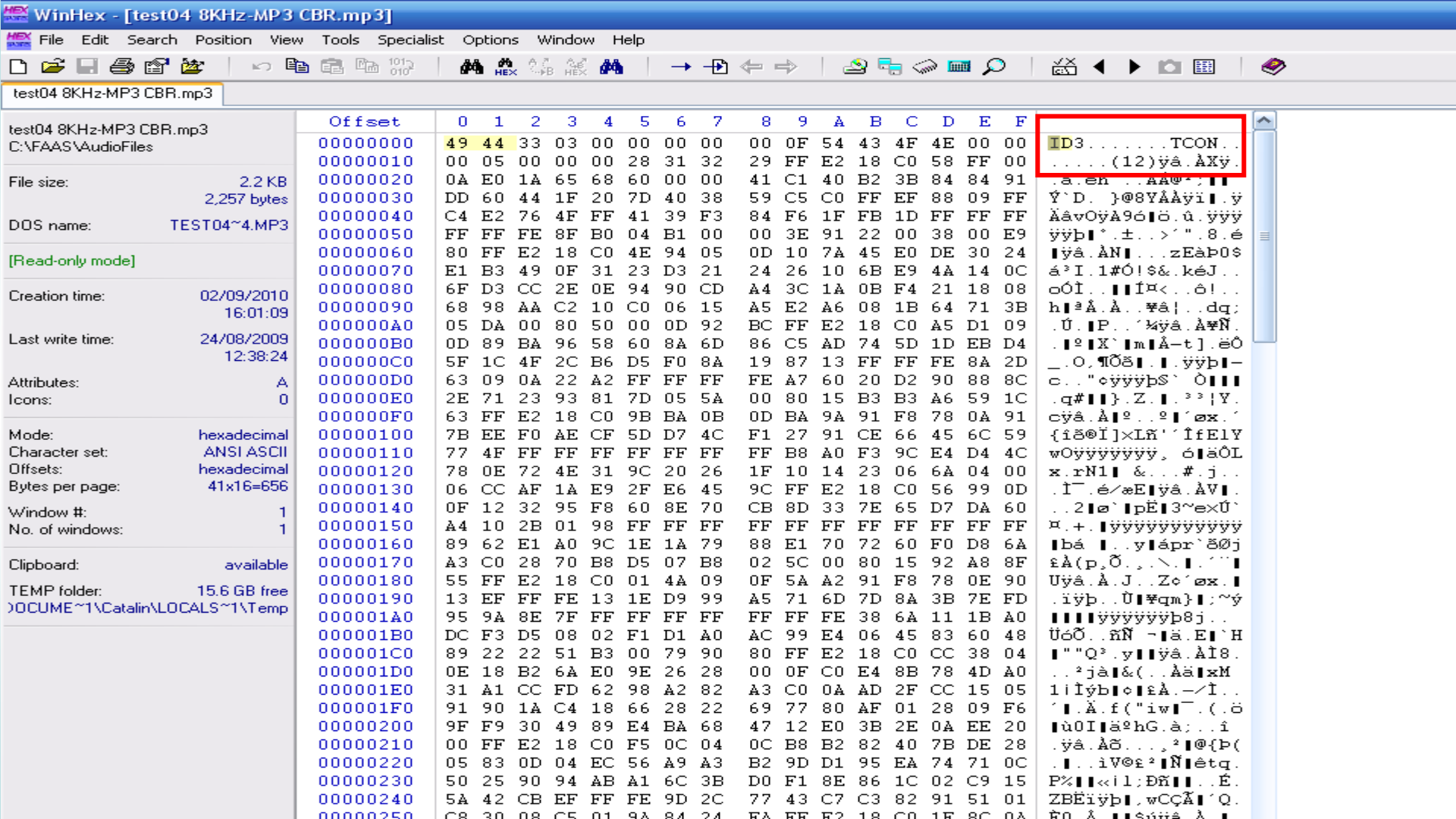
Non-authentic files/recordings

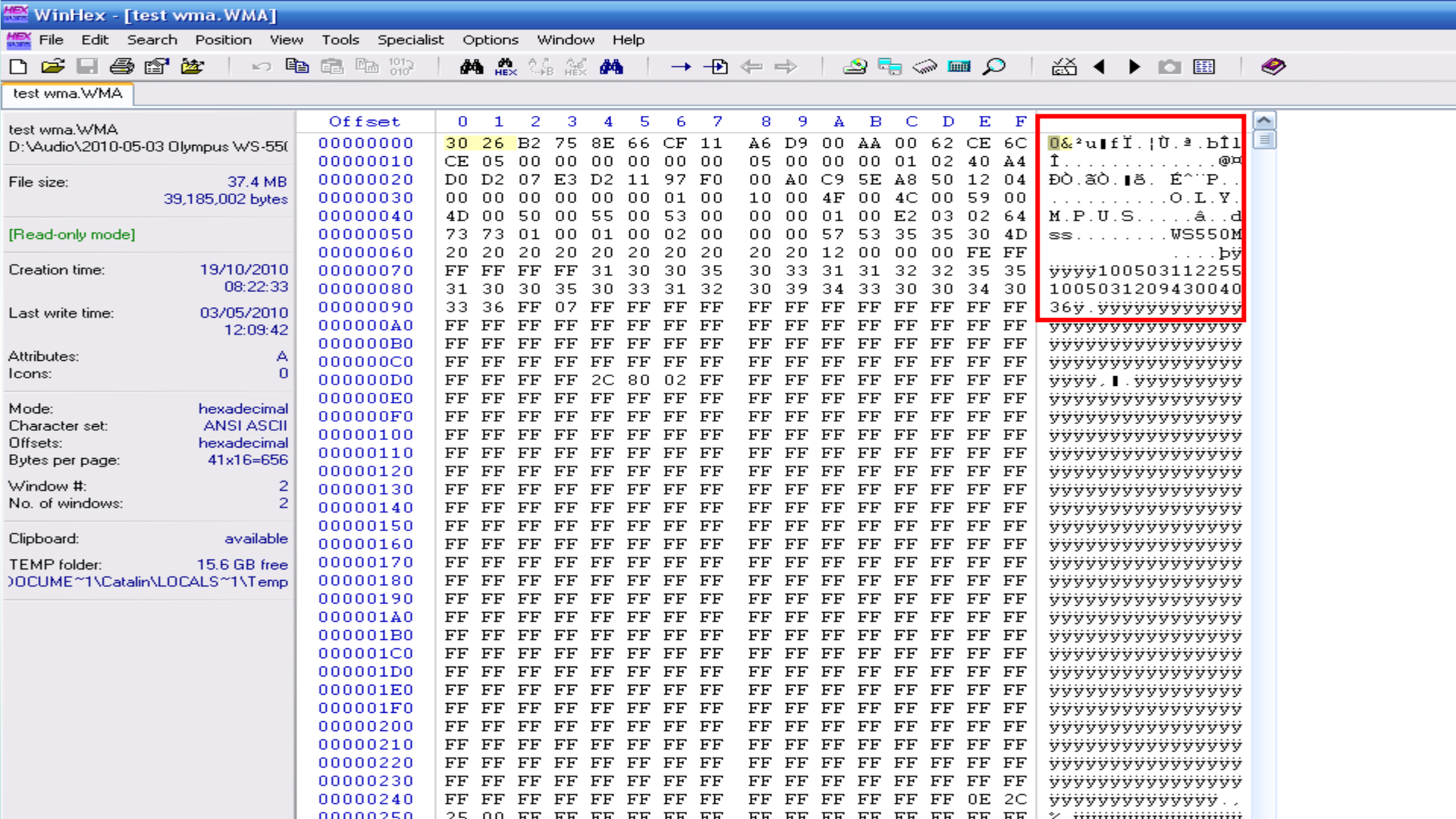
Forensic Authentication of Digital Audio - Framework

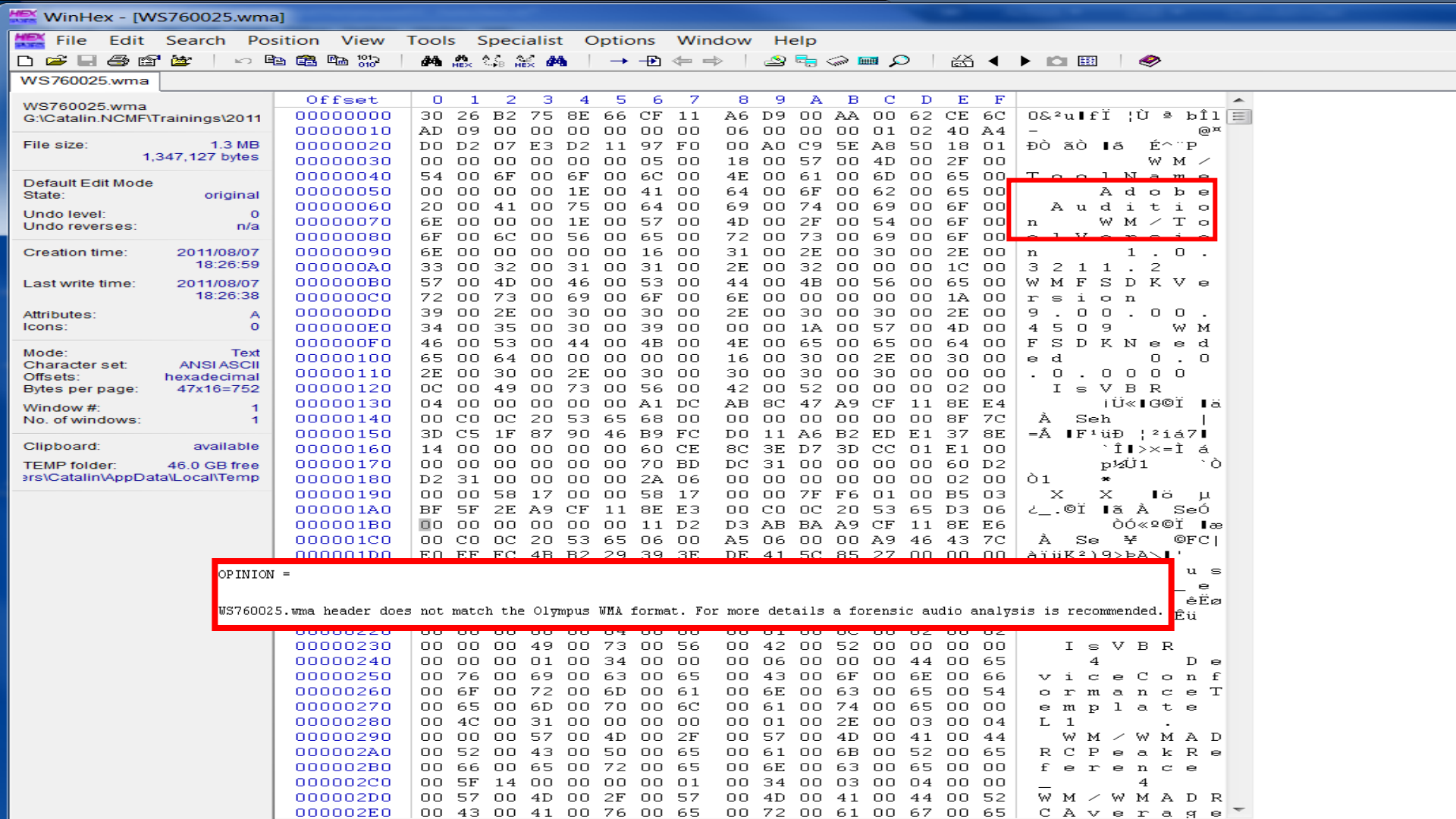
1. **Hardware**: write-blockers, PC, digital audio recorders, mics, etc.
2. **Software**: write-blockers, digital imaging, HASH, hex viewers, structure/logic analysis, audio editors, audio analysis, etc.
3. **Databases**: file samples, user manuals*, software, LTAS, ENF, etc.
4. **Analysis Methods**:
    - 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 - [test01 8KHz.wav]
File Edit Search Position View Tools Specialist Options Window Help
test01 8KHz.wav
test01 8KHz.wav
C:\FAAS\AudioFiles
File size: 23.6 KB
24,138 bytes
DOS name: TE0ED3~1.WAV
[Read-only mode]
Creation time: 02/09/2010
16:01:09
Last write time: 24/08/2009
11:50:38
Attributes: A
Icons: 0
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 41x16=656
Window #: 1
No. of windows: 1
Clipboard: available
TEMP folder: 15.6 GB free
)OCUME~1\Catalin\LOCALS~1\Temp
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 52 49 46 46 42 5E 00 00 57 41 56 45 66 6D 74 20 RIFFB^..WAVEfmt
00000010 10 00 00 00 01 00 01 00 40 1F 00 00 80 3E 00 00 ....@....>..
00000020 02 00 10 00 64 61 74 61 1E 5E 00 00 01 00 FF FF ....data.^....ÿÿ
00000030 00 00 FF FF 02 00 00 00 29 00 62 00 7A 00 C0 00 ..ÿÿ....).b.z.À.
00000040 EF FF 99 FF 07 00 EB FF 3D 00 20 01 E9 01 70 01 ïÿ™ÿ..ëÿ=. .é.p.
00000050 C4 00 89 00 67 00 93 00 8B 01 25 02 32 01 02 00 Ä.‰.g.“.‹.%.2...
00000060 35 FF C5 FF D2 FF 0F 00 10 00 B7 FF 93 00 45 00 5ÿÅÿÒÿ.....ÿ“.E.
00000070 94 FF 43 FF 0F FF 2D FF 54 FF 01 FF AF FE F7 FE ”ÿCÿ.ÿ-ÿTÿ.ÿ¯þ÷þ
00000080 A2 FF 40 FF AA FE DC FD 00 FE FB FD A8 FD 25 FF ¢ÿ@ÿªþÜý.þûý¨ý%ÿ
00000090 F4 FF 5D 00 61 00 1C 00 EE FF DC FF 48 00 F3 FF ôÿ].a...îÿÜÿH.óÿ
000000A0 5E FF DD FE 0F FE 6D FE E1 FE 0E FF 55 FF 42 FF ^ÿÝþ.þmþáþ.ÿUÿBÿ
000000B0 F6 FE 33 FF B1 FF CD FF 36 FF FD FE EB FE EB FE öþ3ÿ±ÿÍÿ6ÿýþëþëþ
000000C0 9C FF D9 FF 31 00 85 FF ED FE A6 FE 76 FE 40 FE œÿÙÿ1.…ÿíþ¦þvþ@þ
000000D0 61 FE 85 FE 90 FE E1 FE F5 FE D5 FF D3 FF 19 FF aþ…þ‘þáþõþÕÿÓÿ.ÿ
000000E0 97 FE F3 FD F7 FD FD FD B0 FE 29 FF 31 FE F9 FD —þóý÷ýýý°þ)ÿ1þùý
000000F0 34 FE 71 FE 2F FF 75 FF D8 FE 74 FE 63 FE 8E FE 4þqþ/ÿuÿØþtþcþŽþ
00000100 21 FF 26 FF E0 FE 71 FE 2E FE 0E FE 8A FD 99 FD !ÿ&ÿàþqþ.þ.þŠý™ý
00000110 C6 FD 35 FE 11 FF BE FE 85 FE B5 FE 3D FF 80 FF Æý5þ.ÿ¾þ…þµþ=ÿ€ÿ
00000120 E8 FE 1D FE 03 FE 8C FE D3 FE 00 FF 70 FF F3 FF èþ.þ.þŒþÓþ.ÿpÿóÿ
00000130 54 FF F7 FE E4 FE 96 FE E2 FE 3F FF 5A FE E2 FD Tÿ÷þäþ–þâþ?ÿZþâý
00000140 4D FE C9 FE 19 FF 29 FF C5 FE DD FD 3C FD B5 FD MþÉþ.ÿ)ÿÅþÝý<ýµý
00000150 05 FE 17 FE 63 FF 46 00 45 00 45 FF F1 FE 2A FF .þ.þcÿF.E.Eÿñþ*ÿ
00000160 DB FF F1 00 DB FF 43 FF 48 FF E5 FE 06 FF F2 FE Ûÿñ.ÛÿCÿHÿåþ.ÿòþ
00000170 34 FF 2C 00 7D 00 63 00 70 FF 9B FE 82 FF E1 FF 4ÿ,.}.c.pÿ›þ‚ÿáÿ
00000180 75 FF 77 FF FA FF 69 00 F3 00 2B 00 CD FF 3C 00 uÿwÿúÿi.ó.+.Íÿ<.
00000190 63 00 69 00 04 01 CC 00 CD 00 78 01 AD 00 54 00 c.i...Ì.Í.x..T.
000001A0 41 00 58 00 54 01 24 02 F0 01 56 01 CD 00 61 01 A.X.T.$.ð.V.Í.a.
000001B0 80 01 19 01 AD 00 EC 00 26 00 0D 00 D9 00 CA 00 €....ì.&...Ù.Ê.
000001C0 BD 00 F1 FF EE FF 4D 00 42 00 6F 00 49 00 65 00 ½.ñÿîÿM.B.o.I.e.
000001D0 68 00 1C 00 05 01 6D 01 8A 00 1D 00 F7 FF 29 00 h.....m.Š...÷ÿ).
000001E0 5F 00 0D 00 BB 00 7B 00 58 00 5E 00 B0 FF 22 00 _...».{.X.^.°ÿ".
000001F0 EA 00 A9 00 49 00 76 00 BC 00 FF 00 E9 00 19 01 ê.©.I.v.¼.ÿ.é...
00000200 A6 01 0C 02 06 02 99 01 E0 01 51 02 B1 01 30 01 ¦.....™.à.Q.±.0.
00000210 EC 00 89 00 05 00 7C FF 7A FF F2 FE 0D FE BB FE ì.‰...|ÿzÿòþ.þ»þ
00000220 AB FF CD FF BE FF 33 FF 61 FE B1 FE 64 FF B7 FF «ÿÍÿ¾ÿ3ÿaþ±þdÿ·ÿ
00000230 21 00 C0 00 58 00 16 00 0B 00 72 FF 92 FF 91 FF !.À.X.....rÿ’ÿ‘ÿ
00000240 97 FF 17 00 FF FF 7C FF DF FE 0F FF C5 FF C8 FF —ÿ..ÿÿ|ÿßþ.ÿÅÿÈÿ


WinHex - [test04 8KHz-MP3 CBR.mp3]
File Edit Search Position View Tools Specialist Options Window Help
test04 8KHz-MP3 CBR.mp3
test04 8KHz-MP3 CBR.mp3
C:\FAAS\AudioFiles
File size: 2.2 KB
2,257 bytes
DOS name: TEST04~4.MP3
[Read-only mode]
Creation time: 02/09/2010
16:01:09
Last write time: 24/08/2009
12:38:24
Attributes: A
Icons: 0
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 41x16=656
Window #: 1
No. of windows: 1
Clipboard: available
TEMP folder: 15.6 GB free
)OCUME~1\Catalin\LOCALS~1\Temp
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 49 44 33 03 00 00 00 00 00 0F 54 43 4F 4E 00 00 ID3.....TCON..
00000010 00 05 00 00 00 28 31 32 29 FF E2 18 C0 58 FF 00 .....(12)ÿâ.ÀXÿ.
00000020 0A E0 1A 65 68 60 00 00 41 C1 40 B2 3B 84 84 91 .à.eh`..AÁ@²;„„
00000030 DD 60 44 1F 20 7D 40 38 59 C5 C0 FF EF 88 09 FF Ý`D. }@8YÅÀÿï.ˆ.ÿ
00000040 C4 E2 76 4F FF 41 39 F3 84 F6 1F FB 1D FF FF FF Äâv0ÿA9ó„ö.û.ÿÿÿ
00000050 FF FF FE 8F B0 04 B1 00 00 3E 91 22 00 38 00 E9 ÿÿþ.°.±..>'".8.é
00000060 80 FF E2 18 C0 4E 94 05 0D 10 7A 45 E0 DE 30 24 €ÿâ.ÀN”...zEàÞ0$
00000070 E1 B3 49 0F 31 23 D3 21 24 26 10 6B E9 4A 14 0C á³I.1#Ó!$&.kéJ..
00000080 6F D3 CC 2E 0E 94 90 CD A4 3C 1A 0B F4 21 18 08 oÓÌ..”.Í¤<..ô!..
00000090 68 98 AA C2 10 C0 06 15 A5 E2 A6 08 1B 64 71 3B h˜ªÂ.À..¥â¦..dq;
000000A0 05 DA 00 80 50 00 0D 92 BC FF E2 18 C0 A5 D1 09 .Ú.€P..'¼ÿâ.À¥Ñ.
000000B0 0D 89 BA 96 58 60 8A 6D 86 C5 AD 74 5D 1D EB D4 .‰º–X`Šm†Å-t].ëÔ
000000C0 5F 1C 4F 2C B6 D5 F0 8A 19 87 13 FF FF FE 8A 2D _.O,¶ÕðŠ.‡.ÿÿþŠ-
000000D0 63 09 0A 22 A2 FF FF FF FE A7 60 20 D2 90 88 8C c..¢ÿÿÿþ§` Ò.ˆŒ
000000E0 2E 71 23 93 81 7D 05 5A 00 80 15 B3 B3 A6 59 1C .q#“.}.Z.€.³³¦Y.
000000F0 63 FF E2 18 C0 9B BA 0B 0D BA 9A 91 F8 78 0A 91 cÿâ.À›º..º.‘øx.‘
00000100 7B EE F0 AE CF 5D D7 4C F1 27 91 CE 66 45 6C 59 {îð®Ï]×Lñ'‘ÎfElY
00000110 77 4F FF FF FF FF FF FF FF B8 A0 F3 9C E4 D4 4C wOÿÿÿÿÿÿÿ¸ ó.äÔL
00000120 78 0E 72 4E 31 9C 20 26 1F 10 14 23 06 6A 04 00 x.rN1.œ &...#.j..
00000130 06 CC AF 1A E9 2F E6 45 9C FF E2 18 C0 56 99 0D .Ì¯.é/æEœÿâ.ÀV™.
00000140 0F 12 32 95 F8 60 8E 70 CB 8D 33 7E 65 D7 DA 60 ..2•ø`ŽpË.3~e×Ú`
00000150 A4 10 2B 01 98 FF FF FF FF FF FF FF FF FF FF FF ¤.+.˜ÿÿÿÿÿÿÿÿÿÿ
00000160 89 62 E1 A0 9C 1E 1A 79 88 E1 70 72 60 F0 D8 6A ‰bá .œ..yˆápr`ðØj
00000170 A3 C0 28 70 B8 D5 07 B8 02 5C 00 80 15 92 A8 8F £À(p¸Õ.¸.\.€.’¨.
00000180 55 FF E2 18 C0 01 4A 09 0F 5A A2 91 F8 78 0E 90 Uÿâ.À.J..Z¢‘øx.
00000190 13 EF FF FE 13 1E D9 99 A5 71 6D 7D 8A 3B 7E FD .ïÿþ..Ù™¥qm}Š;~ý
000001A0 95 9A 8E 7F FF FF FF FF FF FF FE 38 6A 11 1B A0 •šŽ.ÿÿÿÿÿÿþ8j..
000001B0 DC F3 D5 08 02 F1 D1 A0 AC 99 E4 06 45 83 60 48 ÜóÕ..ñÑ ¬™ä.Eƒ`H
000001C0 89 22 22 51 B3 00 79 90 80 FF E2 18 C0 CC 38 04 ‰""Q³.y.€ÿâ.ÀÌ8.
000001D0 0E 18 B2 6A E0 9E 26 28 00 0F C0 E4 8B 78 4D A0 ..²jàž&(..Àä‹xM
000001E0 31 A1 CC FD 62 98 A2 82 A3 C0 0A AD 2F CC 15 05 1¡Ìýb˜¢‚£À.-/Ì..
000001F0 91 90 1A C4 18 66 28 22 69 77 80 AF 01 28 09 F6 ‘.Ä.f("iw€¯.(.ö
00000200 9F F9 30 49 89 E4 BA 68 47 12 E0 3B 2E 0A EE 20 ŸùOI‰ähG.à;..î
00000210 00 FF E2 18 C0 F5 0C 04 0C B8 B2 82 40 7B DE 28 .ÿâ.Àõ...¸²‚@{Þ(
00000220 05 83 0D 04 EC 56 A9 A3 B2 9D D1 95 EA 74 71 0C .ƒ..ìV©£²Ñ•êtq.
00000230 50 25 90 94 AB A1 6C 3B D0 F1 8E 86 1C 02 C9 15 P%”«¡l;Ðñ†..É.
00000240 5A 42 CB EF FF FE 9D 2C 77 43 C7 C3 82 91 51 01 ZBËïÿþ.,wCÇÃ‚‘Q.


WinHex - [test wma.WMA]
File Edit Search Position View Tools Specialist Options Window Help
test wma.WMA
test wma.WMA
D:\Audio\2010-05-03 Olympus WS-55(
File size: 37.4 MB
39,185,002 bytes
[Read-only mode]
Creation time: 19/10/2010
08:22:33
Last write time: 03/05/2010
12:09:42
Attributes: A
Icons: 0
Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 41x16=656
Window #: 2
No. of windows: 2
Clipboard: available
TEMP folder: 15.6 GB free
)OCUME~1\Catalin\LOCALS~1\Temp
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 30 26 B2 75 8E 66 CF 11 A6 D9 00 AA 00 62 CE 6C
00000010 CE 05 00 00 00 00 00 00 05 00 00 00 01 02 40 A4
00000020 D0 D2 07 E3 D2 11 97 F0 00 A0 C9 5E A8 50 12 04
00000030 00 00 00 00 00 00 01 00 10 00 4F 00 4C 00 59 00
00000040 4D 00 50 00 55 00 53 00 00 00 01 00 E2 03 02 64
00000050 73 73 01 00 01 00 02 00 00 00 57 53 35 35 30 4D
00000060 20 20 20 20 20 20 20 20 20 20 12 00 00 00 FE FF
00000070 FF FF FF FF 31 30 30 35 30 33 31 31 32 32 35 35
00000080 31 30 30 35 30 33 31 32 30 39 34 33 30 30 34 30
00000090 33 36 FF 07 FF FF FF FF FF FF FF FF FF FF FF FF
000000A0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000B0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000C0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000D0 FF FF FF FF 2C 80 02 FF FF FF FF FF FF FF FF FF
000000E0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000000F0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000100 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000110 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000120 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000130 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000140 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000150 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000160 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000170 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000180 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000190 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001A0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001B0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001C0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001D0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001E0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
000001F0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000200 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000210 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000220 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000230 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00000240 FF FF FF FF FF FF FF FF FF FF FF FF FF FF 0E 2C

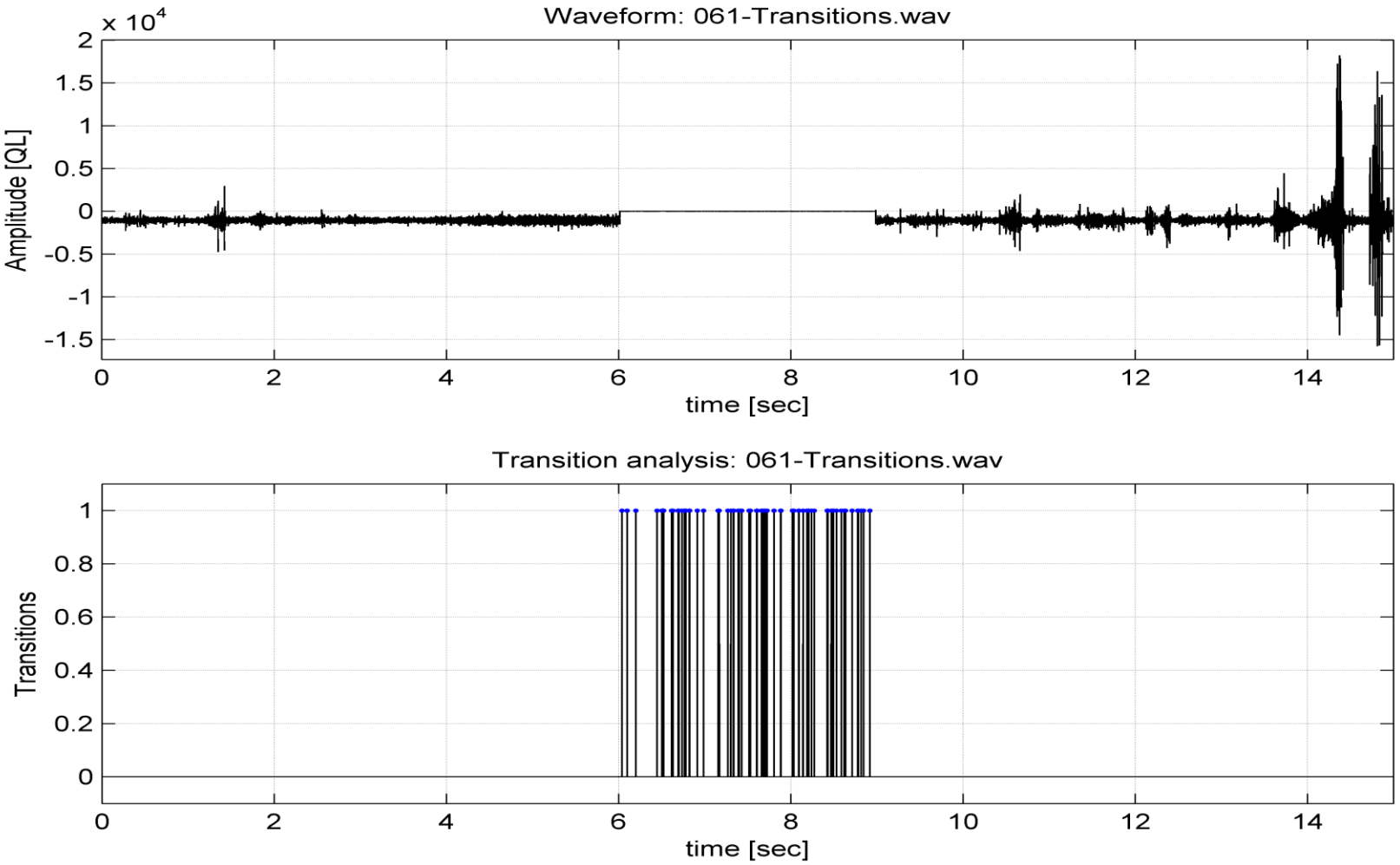

WinHex - [WS760025.wma]
File Edit Search Position View Tools Specialist Options Window Help
WS760025.wma
WS760025.wma
G:\Catalin.NCMF\Trainings\2011
File size: 1.3 MB
1,347,127 bytes
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 2011/08/07 18:26:59
Last write time: 2011/08/07 18:26:38
Attributes: A
Icons: 0
Mode: Text
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 47x16=752
Window #: 1
No. of windows: 1
Clipboard: available
TEMP folder: 46.0 GB free
ers\Catalin\AppData\Local\Temp
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 30 26 B2 75 8E 66 CF 11 A6 D9 00 AA 00 62 CE 6C
00000010 AD 09 00 00 00 00 00 00 06 00 00 00 00 01 02 40 A4
00000020 D0 D2 07 E3 D2 11 97 F0 00 A0 C9 5E A8 50 18 01
00000030 00 00 00 00 00 00 05 00 18 00 57 00 4D 00 2F 00
00000040 54 00 6F 00 6F 00 6C 00 4E 00 61 00 6D 00 65 00
00000050 00 00 00 00 1E 00 41 00 64 00 6F 00 62 00 65 00
00000060 20 00 41 00 75 00 64 00 69 00 74 00 69 00 6F 00
00000070 6E 00 00 00 1E 00 57 00 4D 00 2F 00 54 00 6F 00
00000080 6F 00 6C 00 56 00 65 00 72 00 73 00 69 00 6F 00
00000090 6E 00 00 00 00 00 16 00 31 00 2E 00 30 00 2E 00
000000A0 33 00 32 00 31 00 31 00 2E 00 32 00 00 00 1C 00
000000B0 57 00 4D 00 46 00 53 00 44 00 4B 00 56 00 65 00
000000C0 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 1A 00
000000D0 39 00 2E 00 30 00 30 00 2E 00 30 00 30 00 2E 00
000000E0 34 00 35 00 30 00 39 00 00 00 1A 00 57 00 4D 00
000000F0 46 00 53 00 44 00 4B 00 4E 00 65 00 65 00 64 00
00000100 65 00 64 00 00 00 00 00 16 00 30 00 2E 00 30 00
00000110 2E 00 30 00 2E 00 30 00 30 00 30 00 30 00 00 00
00000120 0C 00 49 00 73 00 56 00 42 00 52 00 00 00 02 00
00000130 04 00 00 00 00 00 A1 DC AB 8C 47 A9 CF 11 8E E4
00000140 00 C0 0C 20 53 65 68 00 00 00 00 00 00 00 8F 7C
00000150 3D C5 1F 87 90 46 B9 FC D0 11 A6 B2 ED E1 37 8E
00000160 14 00 00 00 00 00 60 CE 8C 3E D7 3D CC 01 E1 00
00000170 00 00 00 00 00 00 70 BD DC 31 00 00 00 00 60 D2
00000180 D2 31 00 00 00 00 2A 06 00 00 00 00 00 00 02 00
00000190 00 00 58 17 00 00 58 17 00 00 7F F6 01 00 B5 03
000001A0 BF 5F 2E A9 CF 11 8E E3 00 C0 0C 20 53 65 D3 06
000001B0 00 00 00 00 00 00 11 D2 D3 AB BA A9 CF 11 8E E6
000001C0 00 C0 0C 20 53 65 06 00 A5 06 00 00 A9 46 43 7C
000001D0 E0 FF FC 4B B2 29 39 3F DF 41 5C 85 27 00 00 00
OPINION =
WS760025.wma header does not match the Olympus WMA format. For more details a forensic audio analysis is recommended.
00000230 00 00 00 49 00 73 00 56 00 42 00 52 00 00 00 00
00000240 00 00 00 01 00 34 00 00 00 06 00 00 00 44 00 65
00000250 00 76 00 69 00 63 00 65 00 43 00 6F 00 6E 00 66
00000260 00 6F 00 72 00 6D 00 61 00 6E 00 63 00 65 00 54
00000270 00 65 00 6D 00 70 00 6C 00 61 00 74 00 65 00 00
00000280 00 4C 00 31 00 00 00 00 00 01 00 2E 00 03 00 04
00000290 00 00 00 57 00 4D 00 2F 00 57 00 4D 00 41 00 44
000002A0 00 52 00 43 00 50 00 65 00 61 00 6B 00 52 00 65
000002B0 00 66 00 65 00 72 00 65 00 6E 00 63 00 65 00 00
000002C0 00 5F 14 00 00 00 00 01 00 34 00 03 00 04 00 00
000002D0 00 57 00 4D 00 2F 00 57 00 4D 00 41 00 44 00 52
000002E0 00 43 00 41 00 76 00 65 00 72 00 61 00 67 00 65

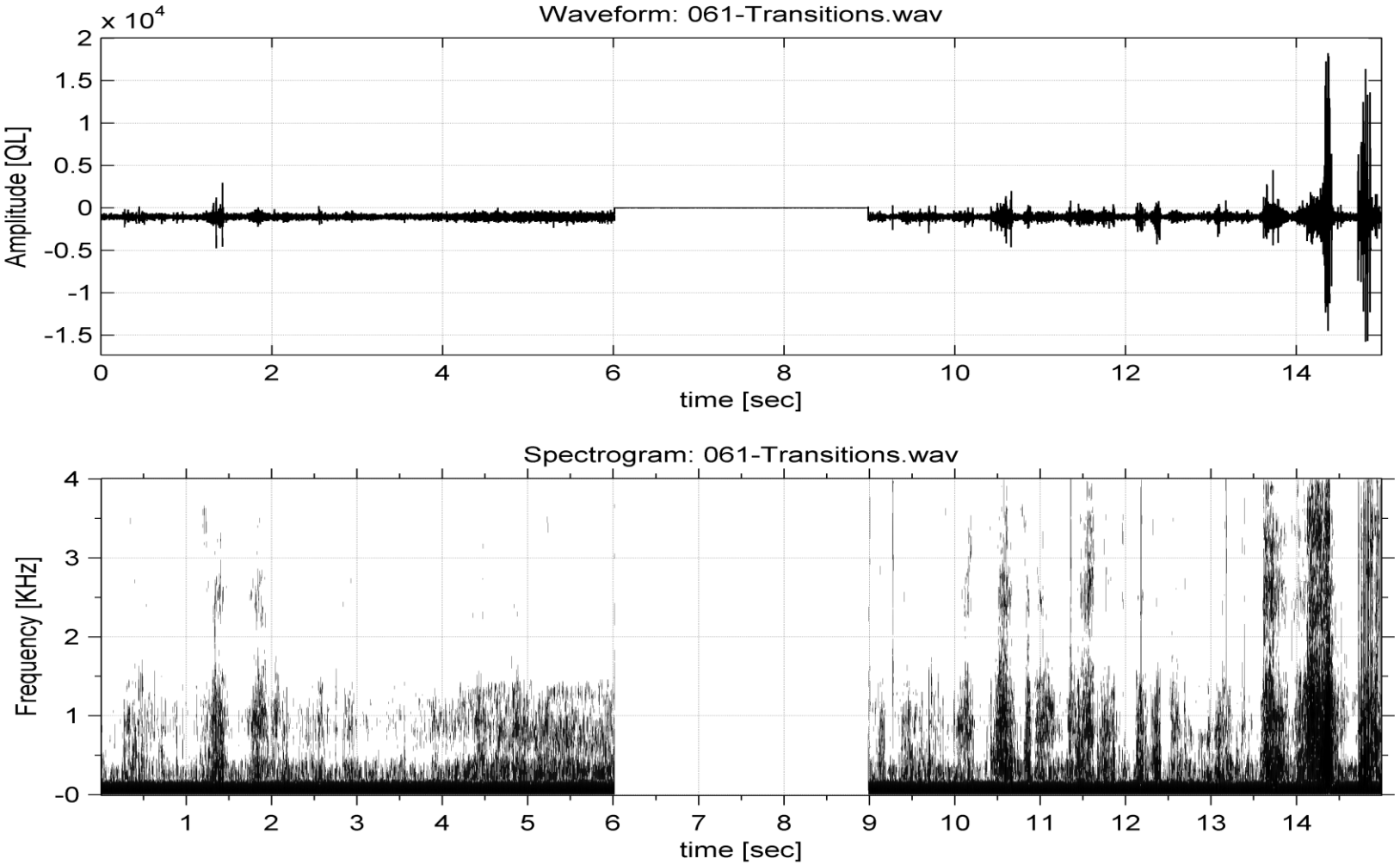
Wav File Format

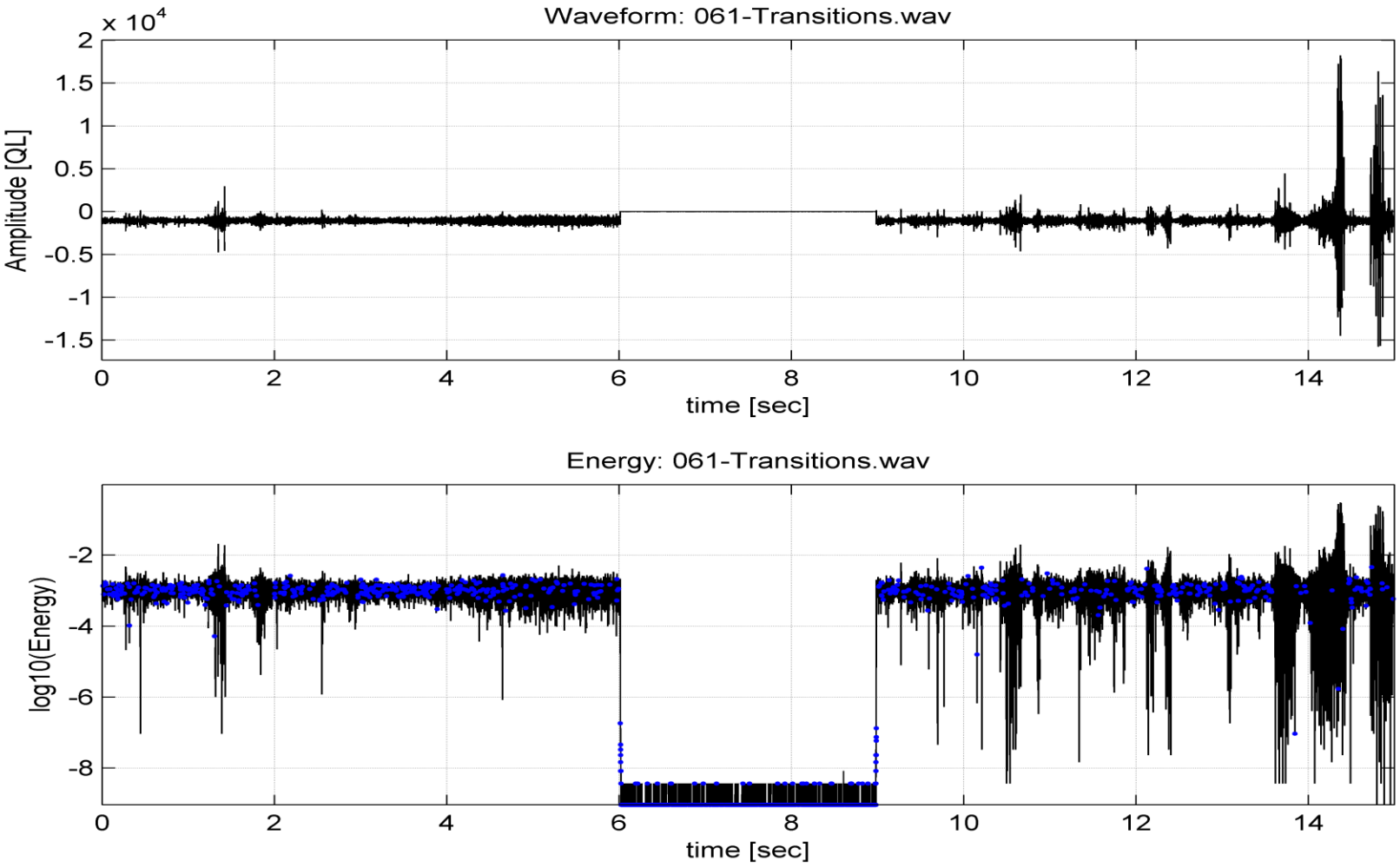
Wave File Header

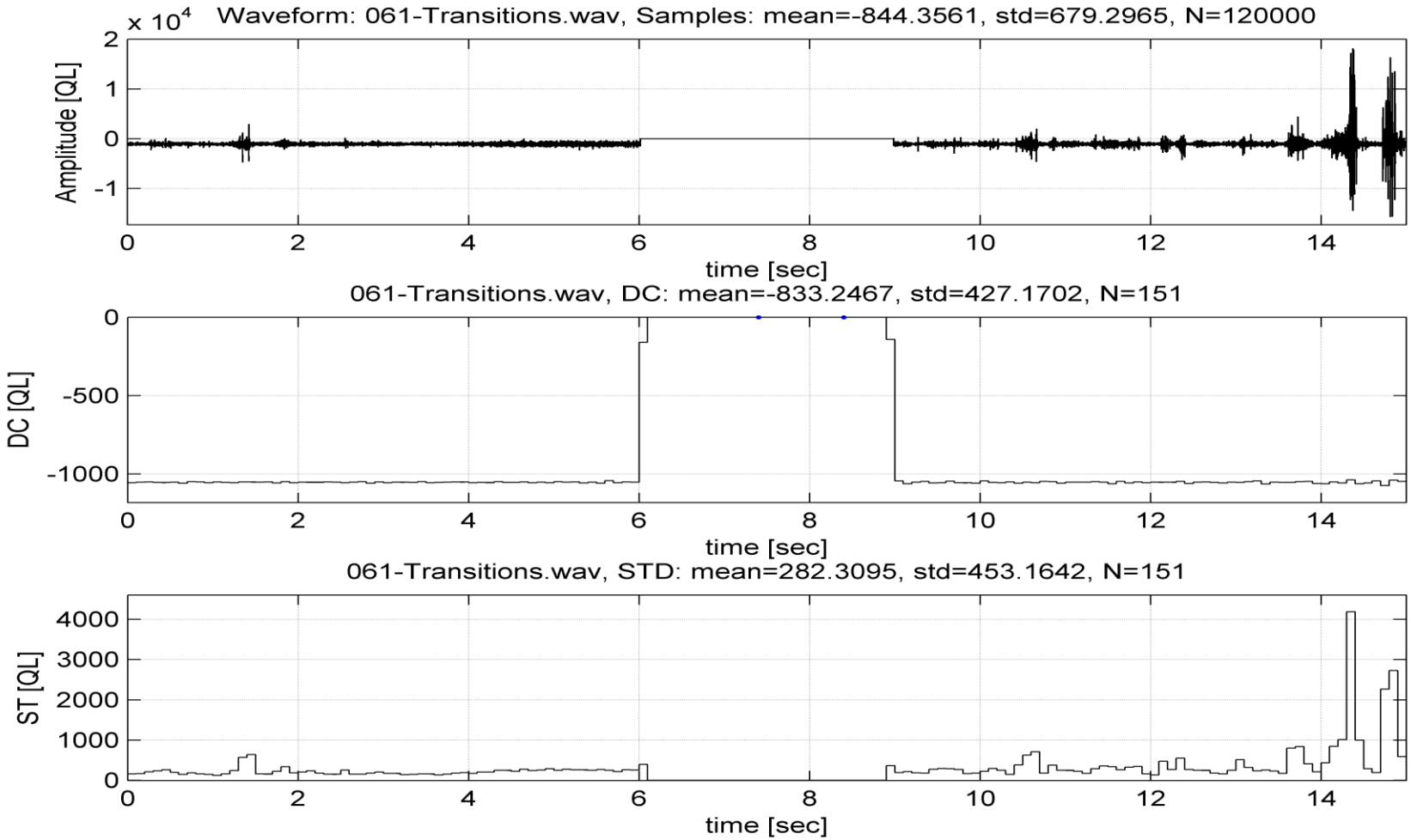
Offset	Size	Description	Value
0x14	**2**	**Compression**	**1 (PCM)**
0x16	2	nChannels	
0x18	4	Fs	
0x22	2	Bit Depth	

```
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 45 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  ....dataÔÿ7.....
00000030  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  ................
```


Waveform: 061-Transitions.wav
x 10^4
Amplitude [QL]
time [sec]
Transition analysis: 061-Transitions.wav
Transitions
time [sec]


Waveform: 061-Transitions.wav
x 10^4
Amplitude [QL]
time [sec]
Spectrogram: 061-Transitions.wav
Frequency [KHz]
time [sec]

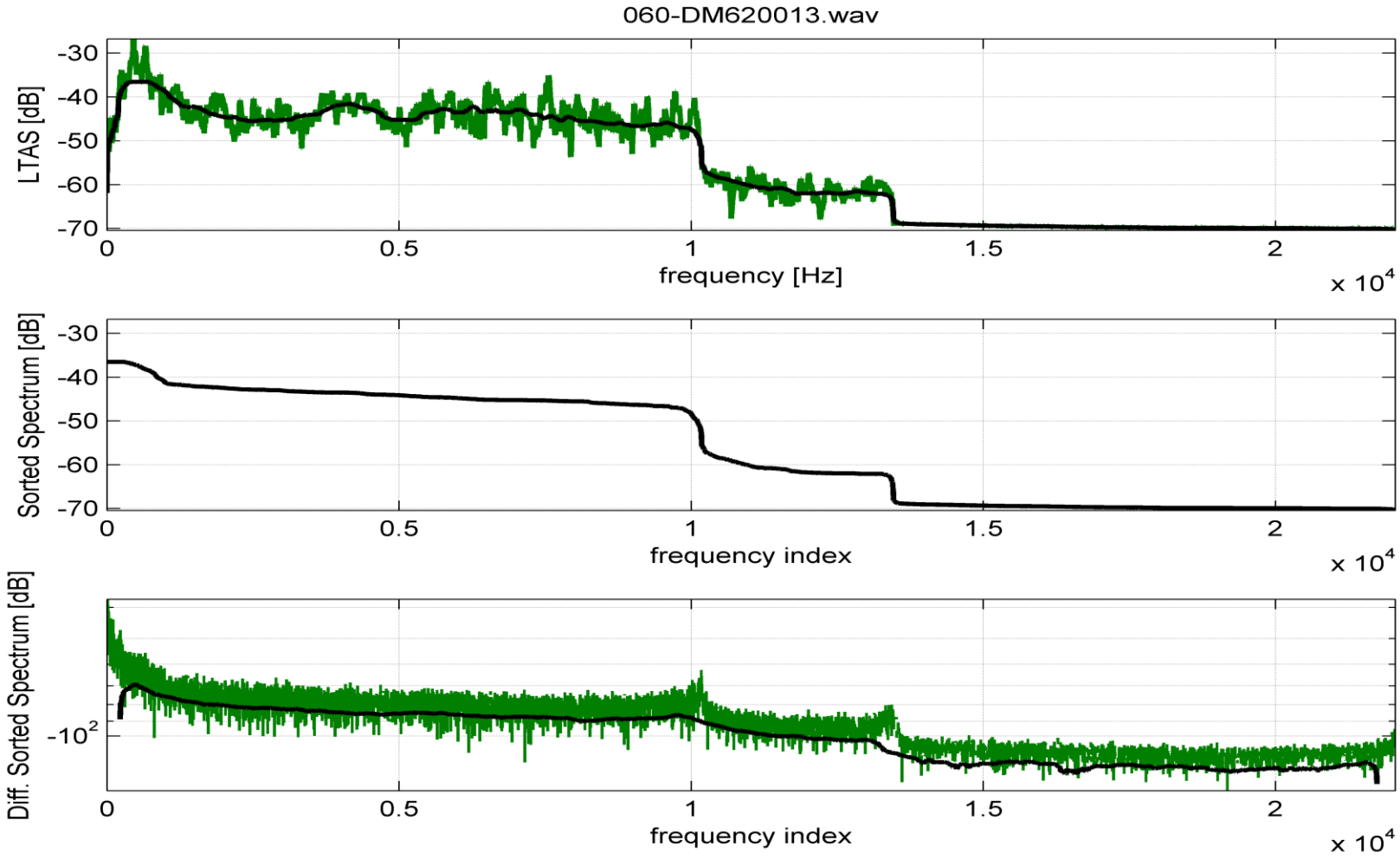

Waveform: 061-Transitions.wav
x 10^4
Amplitude [QL]
time [sec]
Energy: 061-Transitions.wav
log10(Energy)
time [sec]

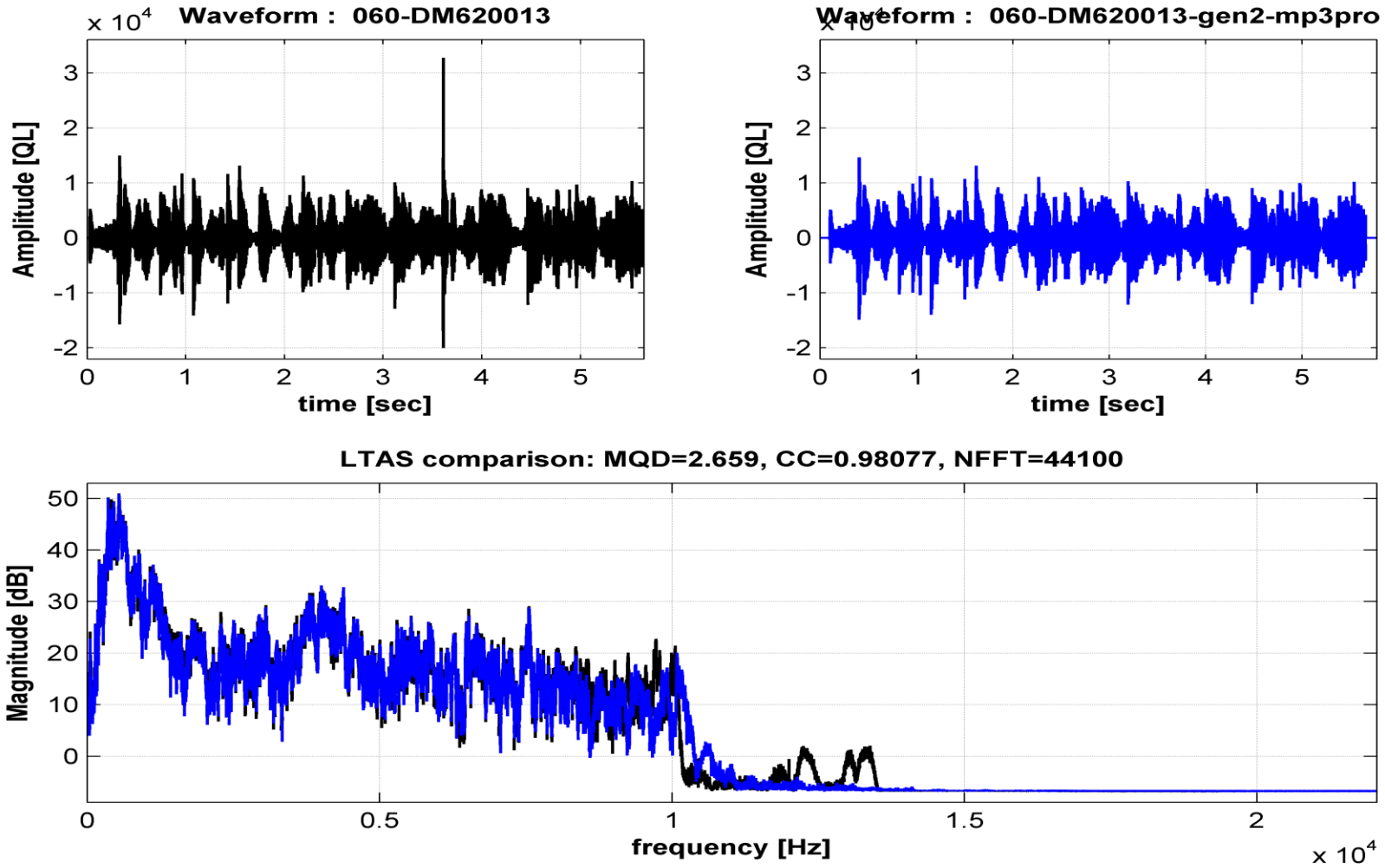

x 10^4
Waveform: 061-Transitions.wav, Samples: mean=-844.3561, std=679.2965, N=120000
Amplitude [QL]
time [sec]
061-Transitions.wav, DC: mean=-833.2467, std=427.1702, N=151
DC [QL]
time [sec]
061-Transitions.wav, STD: mean=282.3095, std=453.1642, N=151
ST [QL]
time [sec]

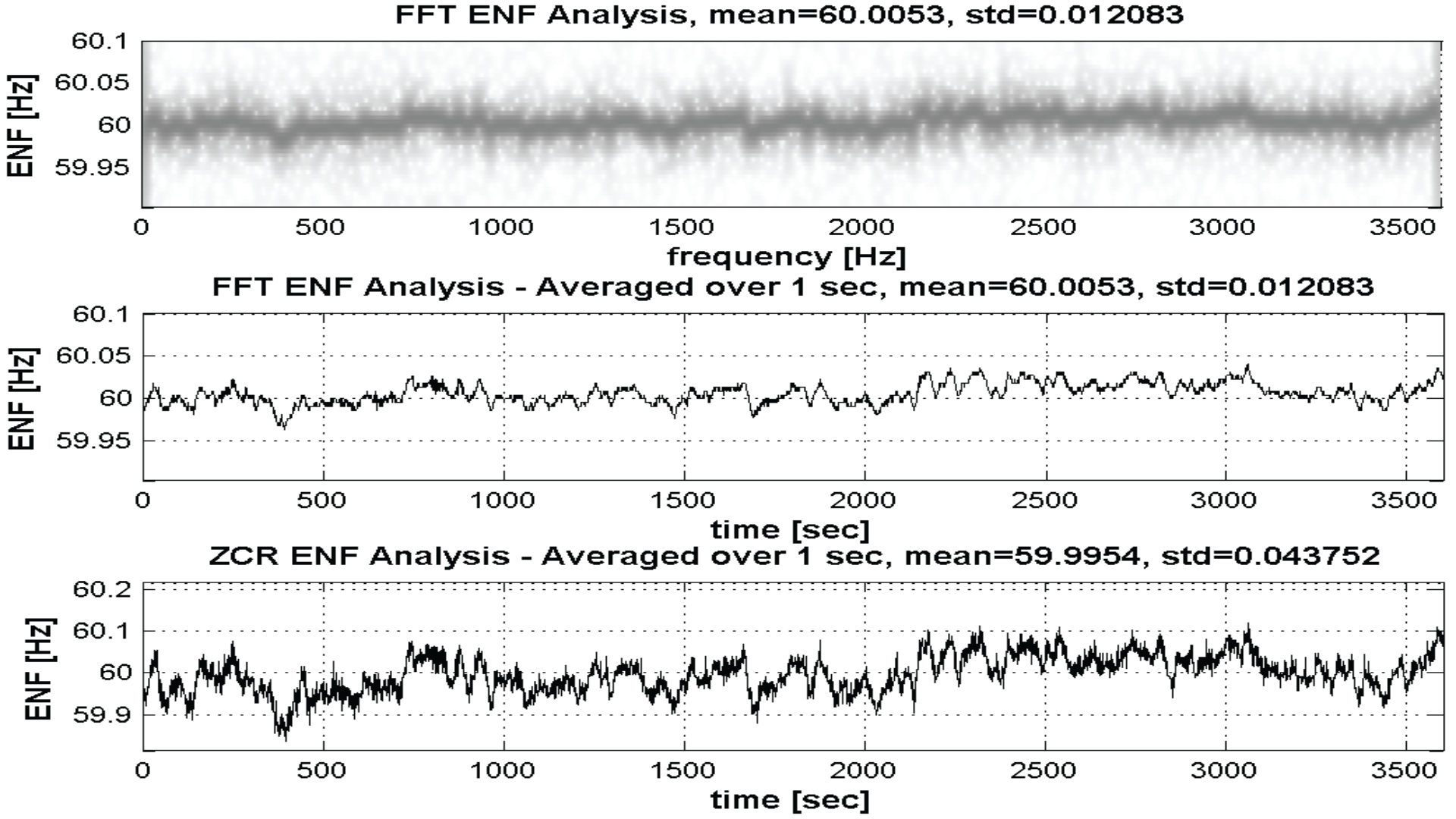
Some transition samples (see **061-Transitions-06-Transitions.txt**):

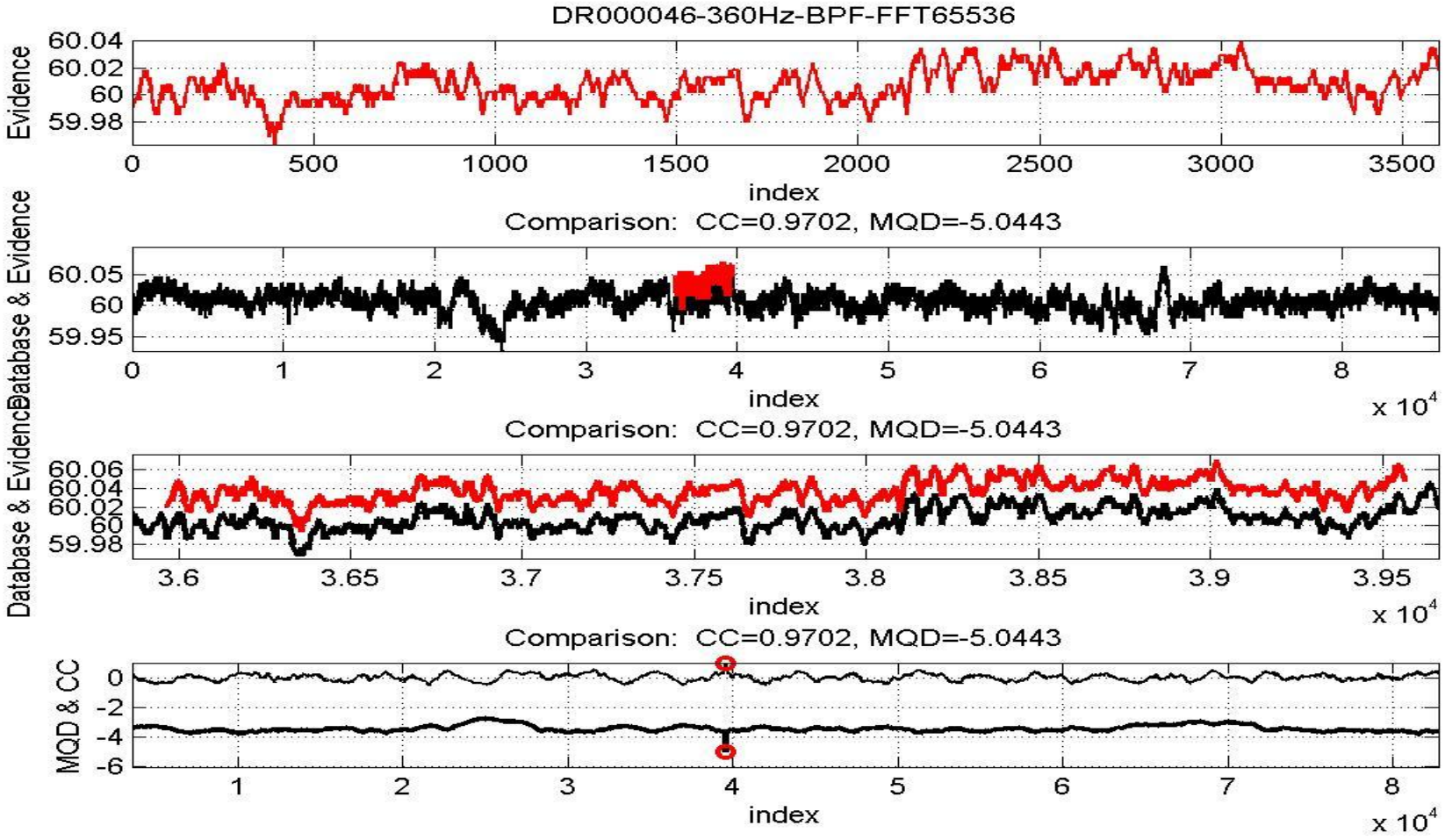
48312
48313
48314
48780
48781
49599
51573
51574
52016
52095
52116

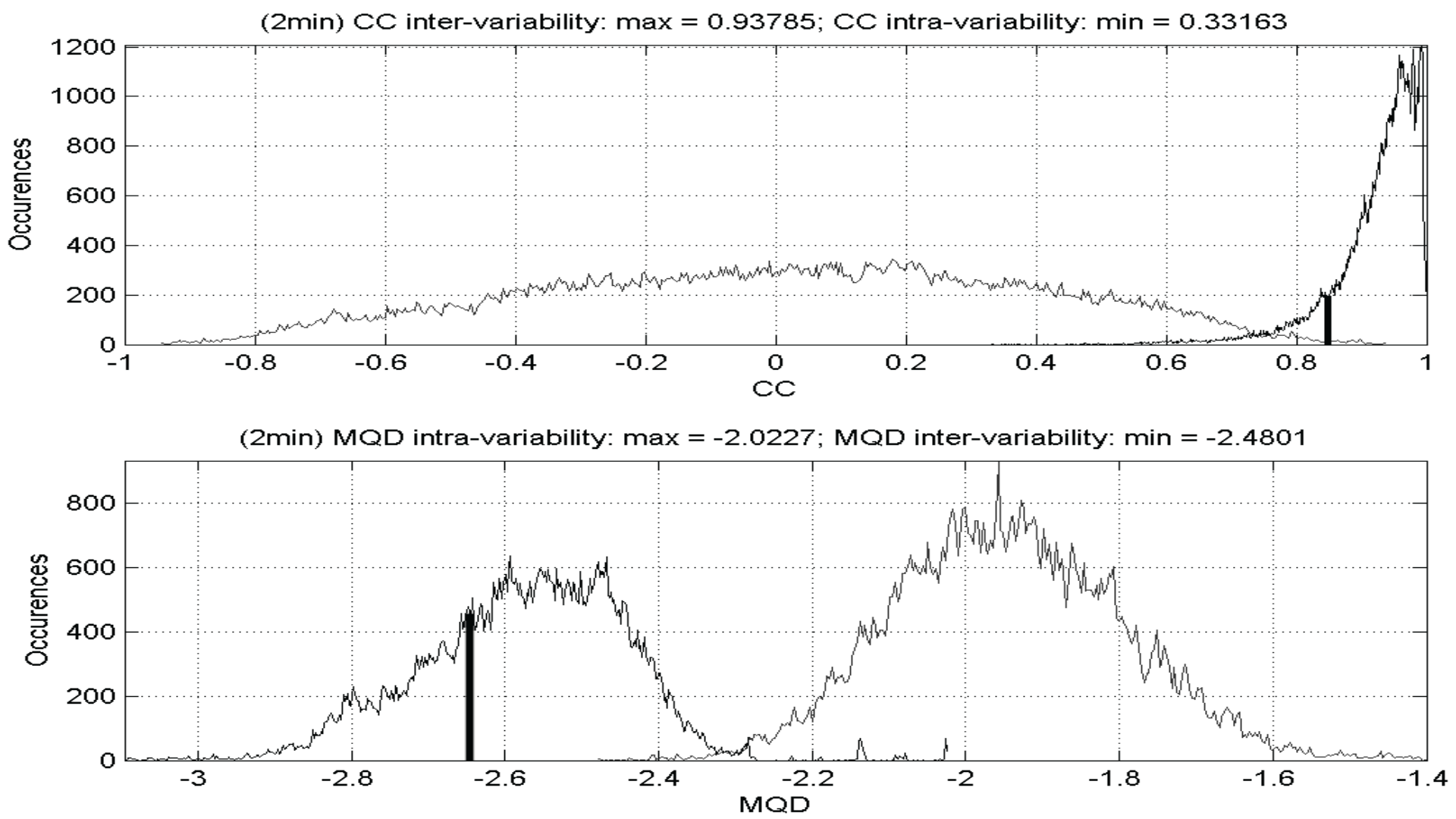
…


060-DM620013.wav
LTAS [dB]
-30
-40
-50
-60
-70
0
0.5
1
1.5
2
frequency [Hz]
x 10^4
Sorted Spectrum [dB]
-30
-40
-50
-60
-70
0
0.5
1
1.5
2
frequency index
x 10^4
Diff. Sorted Spectrum [dB]
-10^2
0
0.5
1
1.5
2
frequency index
x 10^4


Waveform : 060-DM620013
x 10^4
Amplitude [QL]
time [sec]
Waveform : 060-DM620013-gen2-mp3pro
x 10^4
Amplitude [QL]
time [sec]
LTAS comparison: MQD=2.659, CC=0.98077, NFFT=44100
Magnitude [dB]
frequency [Hz]
x 10^4


FFT ENF Analysis, mean=60.0053, std=0.012083
ENF [Hz]
60.1
60.05
60
59.95
0
500
1000
1500
2000
2500
3000
3500
frequency [Hz]
FFT ENF Analysis - Averaged over 1 sec, mean=60.0053, std=0.012083
ENF [Hz]
60.1
60.05
60
59.95
0
500
1000
1500
2000
2500
3000
3500
time [sec]
ZCR ENF Analysis - Averaged over 1 sec, mean=59.9954, std=0.043752
ENF [Hz]
60.2
60.1
60
59.9
0
500
1000
1500
2000
2500
3000
3500
time [sec]


DR000046-360Hz-BPF-FFT65536
Evidence
60.04
60.02
60
59.98
0
500
1000
1500
2000
2500
3000
3500
index
Comparison: CC=0.9702, MQD=-5.0443
Database & Evidence
60.05
60
59.95
0
1
2
3
4
5
6
7
8
index
x 10^4
Comparison: CC=0.9702, MQD=-5.0443
Database & Evidence
60.06
60.04
60.02
60
59.98
3.6
3.65
3.7
3.75
3.8
3.85
3.9
3.95
index
x 10^4
Comparison: CC=0.9702, MQD=-5.0443
MQD & CC
0
-2
-4
-6
1
2
3
4
5
6
7
8
index
x 10^4


(2min) CC inter-variability: max = 0.93785; CC intra-variability: min = 0.33163
Occurences
CC
(2min) MQD intra-variability: max = -2.0227; MQD inter-variability: min = -2.4801
Occurences
MQD

National Center for Media Forensics

A Center of the UC Denver College of Arts & Media

University of Colorado Denver College of Arts & Media
Campus Box 162 • P.O Box 173364
Denver, CO 80217-3364
303.556.2279 • 303.556.2335 (fax)
start@ucdenver.edu

National Center for Media Forensics
Campus Box 154
P.O. Box 173364
Denver, CO 80203
303-315-5850 • 303-832-0483 (fax)
ncmf@ucdenver.edu
http://www.ucdenver.edu/academics/colleges/CAM/Centers/ncmf/Pages/ncmf.aspx