UNIVERSITÀ DEGLI STUDI FIRENZE

Scuola di Ingegneria

Corso di Laurea Magistrale in Ingegneria Informatica

Forensic Analysis of Video File Containers

Saverio Meucci

Anno Accademico 2015/2016

Introduction

In an increasingly digital world, the analysis of the multimedia objects is rapidly assuming importance in the context of digital investigation.

Multimedia Forensics has developed many techniques with the goal of providing aid in making decisions about a digital content authenticity, integrity and origin.

Introduction

We have focused our attention on Source Identification and Integrity Verification of digital videos acquired by smartphones and tablets.

Forensic Analysis is based on the research of the so called *fingerprints*, left both by the acquisition device and by the post-processing steps.

In this regard, techniques mainly use two different tools:

1. **Audio-video signal**: the research of inconsistencies and artefacts in the digital content.
2. **Metadata**: the determination of their compatibility, completeness, and consistency.

Video File Container - What's inside?

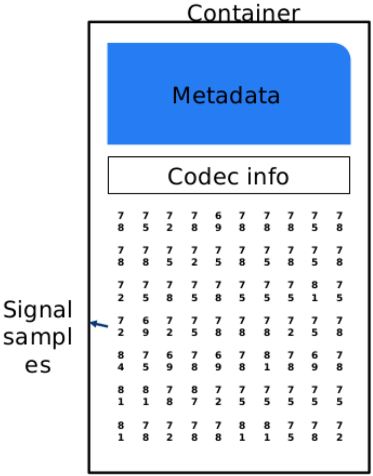
Contained data, structured information about the content, like:

- Content-related metadata (acquisition time, place, settings, etc.)
- Number of tracks/signals (e.g. a video container may include several video tracks.)

Codec data, necessary information to decode and present the signal, like:

- Quantization tables.
- Information for entropy decoding

Encoded signal(s)



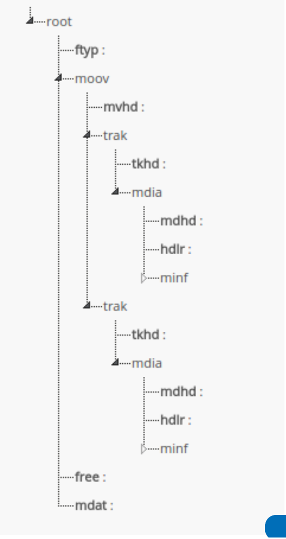
78	75	72	78	69	78	78	78	75	78
78	78	75	72	75	78	75	78	75	78
72	75	78	75	78	75	75	75	81	75
72	69	72	75	78	78	78	72	75	78
84	75	69	78	69	78	81	78	69	78
81	81	78	87	72	75	75	75	75	75
81	78	72	78	78	81	81	75	78	72

Video File Container - Structure

As defined by the *ISO Base Media File Format Standard* [1], file containers have a object-oriented type structure.

Each object, called *box* or *atom*, includes specifics information about the media and are identified by 4-byte characters (e.g. *ftyp*, *mdat*, *moov*, etc.).

Boxes can have fields and can contain other boxes.



Video File Container - Why?

As noticed by *Gloe et al.* [2], the video format standards (e.g. *ISO Base Media* [1], *MP4* [3], *MOV*[4]) for the file container prescribe only a limited number of features.

Video File Container - Why?

As noticed by *Gloe et al.* [2], the video format standards (e.g. *ISO Base Media* [1], *MP4* [3], *MOV*[4]) for the file container prescribe only a limited number of features.

⇓

Freedom of interpretation for the device manufacturers in terms of design decisions (order of the boxes, attributes values, etc.).

Video File Container - Why?

As noticed by *Gloe et al.* [2], the video format standards (e.g. *ISO Base Media* [1], *MP4* [3], *MOV*[4]) for the file container prescribe only a limited number of features.

$$\Downarrow$$

Freedom of interpretation for the device manufacturers in terms of design decisions (order of the boxes, attributes values, etc.).

$$\Downarrow$$

Low-level information to be exploited by the Forensic Analyst.

Source Identification

Given a video, we want to assess its origin based on its file container.

We split the problem in binary questions.

Ex. Does the video belongs to Samsung?
... to Samsung Galaxy S3?
... to Huawei G6?
... to Apple?
... to Apple iPhone 5?

Given a question, the dataset is queried to obtain two classes (videos for which the answer is true, and the complementary).

For each question, we want to define a compatibility score.

Source Identification - Training

Determine whether a video belongs to a class C (e.g. Samsung).

We split the ground-truth in two sets:

$$\Omega = X_C \cup X_{\overline{C}} = x_1, \ldots, x_{N_C} \in C \cup x_1, \ldots, x_{N_{\overline{C}}} \in \overline{C}$$

Ω contains all the attributes ω of the boxes contained in each of the ground-truth media.

We determine the discrimination power of each of the attributes ω for the class C and $\overline{C}$.

$$W_C(\omega) = \frac{\sum_{i=1}^{N_C} \mid X_i \cap \omega \mid}{N_C} \qquad W_{\overline{C}}(\omega) = \frac{\sum_{i=1}^{N_{\overline{C}}} \mid X_i \cap \omega \mid}{N_{\overline{C}}}$$

Source Identification - Test

Given a media query $X = \omega_1, ...\omega_t$, we solve the two hypothesis test problem:

$$H_0 : X \in \overline{C}$$

$$H_1 : X \in C$$

Then we determine the likelihood ratio of observing $\omega_j, j = 1 \dots t$.

$$P(\omega_j | H_0) = \Omega_{\overline{C}}(\omega_j)$$

$$P(\omega_j | H_1) = \Omega_C(\omega_j)$$

$$L(X) = \prod_{\omega_j} \frac{\Omega_C(\omega_j)}{\Omega_{\overline{C}}(\omega_j)}$$

Then, using $l(X) = lnL(X)$ can be used to determine whether X belongs to class C.

Source Identification - Correlated Features

We have supposed that the values of the attributes of a certain box are independently distributed. However, some features might be correlated.

When considering a box, given a vector of likelihood ratios $\overline{x} = (x_1, \ldots, x_n)$, we compute the likelihood as:

$$L(\overline{x}) = \prod_{i=1}^{n} x_i^{\alpha_i}$$

with

$$\alpha_i = \frac{(n-1)\gamma_i + 1}{n}$$

$$\gamma_i = -\frac{n}{logn} P(x_i) logP(x_i)$$

and where $P(x_i)$ represents the probability of finding that value of ratio in the vector.

Source Identification - Experiments

Source Identification - Results

Integrity Verification

Integrity Verification - Experiments

Integrity Verification - Results

Web Application

Conclusions

References