**NISTIR 8161**
**Revision 1**

# Recommendation: Closed Circuit Television (CCTV) Digital Video Export Profile – Level 0 (Revision 1)

Lawrence Nadel
Mary Laamanen
Michael Garris
Craig Russell

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8161r1

National Institute of Standards and Technology
U.S. Department of Commerce

This page intentionally blank

**NISTIR 8161**
**Revision 1**

# Recommendation: Closed Circuit Television (CCTV) Digital Video Export Profile – Level 0 (Revision 1)

Lawrence Nadel
Michael Garris
*Information Access Division*
*Information Technology Laboratory*

Mary Laamanen
Craig Russell
*Software and Systems Division*
*Information Technology Laboratory*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8161r1

April 2019


U.S. Department of Commerce
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology
*Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology*

**National Institute of Standards and Technology Interagency or Internal Report 8161r1**
**Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8161r1, 24 pages (April 2019)**

**This publication is available free of charge from:**
**https://doi.org/10.6028/NIST.IR.8161r1**

## Acknowledgements

At the request of the Federal Bureau of Investigation (FBI), NIST performed research and community outreach that led to the development of this revised *Recommendation: Closed Circuit Television (CCTV) Digital Video Export Profile – Level 0*. We would like to acknowledge the FBI for their support of this endeavor. Thank you to Hans Busch, Per Björkdahl, Stefan Andersson, and other members of the Open Network Video Interface Forum (ONVIF) for their collaboration to address the law enforcement video surveillance export requirements presented by NIST.

## Abstract

This document updates and replaces NISTIR 8161. This revised recommendation continues to focus on storing metadata to support video analytics. It reflects NIST's collaboration with relevant standards community members to facilitate an effective approach workable to all involved.

At the request of the FBI, NIST conducted research and developed NISTIR 8161 as a recommendation to address the FBI's minimum interoperability requirements for the exporting and exchange of video recordings captured by closed circuit television (CCTV) digital video recording (DVR) systems. NIST termed these requirements "Level 0" and addressed them as follows:

- **Standard file container** – MP4 digital multimedia file containers
- **High quality commonly used codec** – H.264 (and future variants) encoded digital video bitstreams
- **Electronically processable UTC timestamp associated with each video frame** – standardized timestamp stored at the bitstream level
- **Recording of system clock offset metadata** – record the export system (i.e., DVR) UTC clock time and a reliable external reference time that is determined at the time of video export

NIST shared its findings and recommendations with video industry hardware and software manufacturers, and the relevant standards community. This led to NIST collaborating with the Open Network Video Interface Forum (ONVIF) to enhance their *Export File Format Specification* to support the essential functionality of NISTIR 8161. Working with ONVIF has improved the likelihood of industry's adaptation to law enforcement requirements. Additionally, ONVIF contributed its *Export File Format Specification* to the International Electrotechnical Commission (IEC) for inclusion in its standard *IEC 62676-2-32, Video surveillance systems for use in security applications – Part 2-32: Recording control and replay based on web services,* which has an expected publication date of mid-2019.

As described herein, NIST recommends industry implementation of the ONVIF and IEC standards noted above. These standards provide acceptable alternative implementation approaches to what NIST proposed in NISTIR 8161 for recording and storing time information as follows:

- **Electronically processable UTC timestamp associated with each video frame** – standardized timestamp stored as MP4 metadata
- **Recording of system clock offset metadata** – at the time of video export, determine and record a corrected video start time

Adoption of the above standards provides additional useful capabilities including:

- The recording of additional surveillance export metadata (e.g., recording equipment used, export file creation time, name of export operator)

- Assurance of data integrity and chain of custody - the exported video file can be signed digitally, initially by the individual performing the export operation, and subsequently as the file is shared and analyzed

The recommendations provided in this document are intended to support law enforcement investigations. This document was prepared by the National Institute of Standards and Technology (NIST), in collaboration with the Federal Bureau of Investigation (FBI), and in conjunction with the CCTV / DVR community.



## Keywords

CCTV, codec, digital video, export file, H.264, interoperability, law enforcement investigation, metadata, MP4, ONVIF, timestamp, video analytics, video recording, video standards, video surveillance

# Table of Contents

## List of Tables



## List of Figures

# 1 Introduction

Video evidence from CCTV recording systems is a powerful resource for forensic investigations. With the proliferation of these systems from banks, to stores, parking lots, and homes; illegal and violent activities are seldom out of view. However, when an event occurs, investigators can quickly be overwhelmed by the variety of formats and the volume of data they have to analyze. Take the bombing at the Boston Marathon in 2013 for example. The FBI received over 13 000 videos and assigned 120+ analysts working around the clock before the video clip that broke open the case was discovered [PELLEY]. To help manage this crushing wave of digital evidence, forensic tools must be able to ingest CCTV video data quickly and seamlessly. Today, exporting video from CCTV systems and importing the video into investigative environments and applications often involves data conversion resulting in degraded image quality, loss of metadata, and costly delays.

Many steps must be taken to properly obtain and secure the video from a crime scene. This is compounded when dealing with large scale public incidents where video from many different CCTV systems must be collected, correlated, and analyzed. During the acquisition process, law enforcement officials need to collect the relevant video footage to retrieve and view [SWGIT]. Due to the differences in equipment and export formats, the process is costly and time consuming. Current CCTV systems often output video in proprietary formats along with propriety software needed for viewing. This (along with often degraded image quality) adds an extra burden to the evidence collecting process [SWGDE]. Using a common data interchange format will expedite the collecting of evidence from multiple systems and improve the processing of the information.

To address the issues described above, the FBI requested that NIST conduct research and relevant community outreach to facilitate the development of a digital file export standard that, at a minimum, would address the following fundamental interoperability needs. NIST has termed these needs “Level 0” requirements.

- **Standard file container** - the standard output format shall be generally playable by common video players (e.g., Windows[1] Media Player, QuickTime[2], and VLC[3])
- **High quality commonly used codec** - a suitable CCTV system shall provide the option to export video at the same level of quality as onboard the system
- **Electronically processable timestamp associated with each video frame** – each video frame shall be associated with a standardized, unique timestamp (i.e., date and time)
- **Recording of system clock offset metadata** – record the export system (i.e., DVR) clock time and a reliable external reference time that is determined at the time of video export

[1] Windows is a registered trademark of Microsoft Corp.
[2] QuickTime is a registered trademark of Apple Inc.
[3] VLC is a registered trademark of the VideoLAN organization.

NIST applied the following guiding principles in addressing the requirements above:

1) Do no harm – with export, preserving the native video quality captured by the CCTV system thus avoiding transcoding and recompressing
2) Promote key metadata – starting with date and time (with future provisions for location and camera metadata)
3) Leverage existing standards to the extent feasible
4) Use a flexible container – selecting a format that supports general playability and multiple data streams
5) Minimize cost – aligning the standards solution as closely as possible to Industry's common export features and codecs, leading to increased acceptance and adoption, while minimizing cost to the end user

The content of this recommendation document is based largely on a series of independent studies conducted by NIST that were published as NISTIR 8172 [NIST-8172] and subsequent socialization of NISTIR 8161 [NIST-8161] with industry and the relevant standards community. NIST collaborated with the Open Network Video Interface Forum (ONVIF[4]) to enhance their *Export File Format Specification (Version 18.12)* [ONVIF] to support the essential functionality of [NIST-8161], which was based on law enforcement requirements conveyed to NIST by the FBI. It should be noted that [ONVIF] has been adopted by the International Electrotechnical Commission (IEC) in its standard *IEC 62676-2-32, Video surveillance systems for use in security applications – Part 2-32: Recording control and replay based on web services* [62676-2-32-IEC].

NIST believes that this revised recommendation provides the most practical and expeditious approach at this time to achieve commercial adoption of a video file export format based on an international standard that meets law enforcement's most fundamental interoperability requirements and is expandable to meet higher level needs.

### 1.1 Purpose and Scope

This document updates and replaces NISTIR 8161. The purpose of this recommendation remains the same, focusing on storing metadata to support video analytics, but the specific standardized implementation approach is different. This document describes and promotes an interoperable data solution to assist law enforcement in acquiring evidence, improving forensic processes and techniques, and bridging the gap between CCTV systems and downstream investigators. Such interoperability increases the value and timeliness of CCTV video data to law enforcement investigations and facilitates interoperable data sharing. This document also serves to profile some aspects of [ONVIF] and [62676-2-32-IEC] and suggest updates for consideration beyond "Level 0" requirements.

This recommendation document applies to the data format output (the file export) of video recordings from CCTV systems. How the video is captured and stored inside the CCTV system is not directly in scope. To meet the "Level 0" requirements noted, a CCTV system must support

[4] ONVIF is a registered trademark of the Open Network Video Interface Forum.

the interoperable data format described herein; however, a compliant system may output video data in additional formats of the manufacturer's choosing. This recommendation addresses the syntactic representation of the video data. Semantic properties (e.g., parameters governing data quality and fitness for use) relating to the population of data within this recommendation are out of scope and left to future standardization efforts.

The primary audiences for this document are CCTV/DVR system manufacturers, the relevant standards community, and law enforcement video analytics software developers and practitioners.

### 1.2 Organization of this Document

Section 2 lists terms and acronyms referenced throughout this document, Section 3 presents the technical elements of this recommendation, Section 4 recommends additional elements beyond those specified in the original version of this document, and Section 5 suggests future work and directions. Section 6 provides a table of pertinent references, including the standards recommended and profiled in this document. Throughout this document, items in this table are referenced as [reference identifier].

## 2 Terms, Acronyms, and Organizations

**Table 1 - Acronyms**

| | |
|---|---|
| AF | Application Format |
| CCTV | Closed Circuit Television |
| codec | Encoder and Decoder |
| CSTB | CorrectStartTime Box |
| DVR | Digital Video Recorder |
| H.264 | MPEG-4 Part 10 - Advanced Video Coding Standard |
| MAC | Media Access Control (address) |
| MP4 | Digital Multimedia Container Format |
| SDO | Standards Developing Organization |
| SUEP | Surveillance Export |
| SUMI | Surveillance Media Information |
| TFDT | Track Fragment Decode Time |
| URL | Uniform Resource Locator |
| UTC | Coordinated Universal Time |
| VLC | A free and open-source, portable, cross-platform media player and streaming media server developed by the VideoLAN[5] Project |

**Table 2 - Organizations**

| | |
|---|---|
| FBI | Federal Bureau of Investigation |
| IEC | International Electrotechnical Commission |
| ISO[6] | International Organization for Standardization |
| ITL | Information Technology Laboratory |
| ITU | International Telecommunication Union |
| MPEG | Moving Picture Experts Group |
| NIST | National Institute of Standards and Technology |
| ONVIF | Open Network Video Interface Forum |
| SWGDE | Scientific Working Group on Digital Evidence |
| SWGIT | Scientific Working Group Image Technology |

[5] VideoLAN is a registered trademark of the VideoLAN organization.
[6] ISO is a registered trademark of the International Organization for Standardization.

# 3 Profile Elements

This section details the standards and specific elements pertinent to this recommendation. These standards were chosen after researching the current state of the industry with a focus on file export types and key metadata gaps. Date, time, and camera information are useful in investigations and should be preserved [SWGIT]. One of the challenges facing digital forensic investigators is the ever-increasing volume of collected data from a variety of devices and the lack of standardization from any of the sources [LILLIS]. By standardizing on the export file format with a focus on date and time, data collection will be improved and investigators can effectively triage data acquired from CCTV systems.

This recommendation prescribes: 1) a flexible standard file container, 2) a standard encoded video stream, 3) standard embedded date and time metadata, and 4) a standard encoding for System Clock Offset metadata.

## 3.1 MP4 File Container

After the recorded video is captured, a compliant CCTV system must have the ability to export the data in an MPEG-4 Part 12 [MP4-12] MP4 digital multimedia file container. Each exported MP4 file container must store one video stream (note: storage of multiple video streams in one file container is also possible, and may be desirable, but this capability is not a "Level 0" requirement), optionally a corresponding audio stream, and metadata as illustrated in Figure 1. The complete definition of the MP4 base file format can be found in [MP4-12].

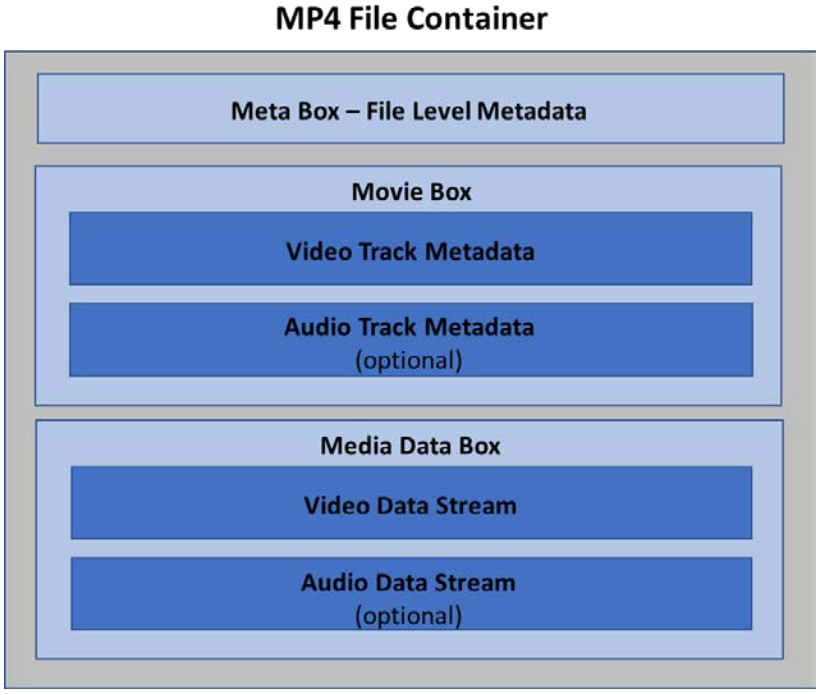


**Figure 1 – Example export MP4 file container with one video data stream, optionally a corresponding audio stream, and metadata [MP4-12]**

## 3.2 H.264 Video Bitstream

CCTV systems commonly rely on lossy compression to store, handle, and export the vast amounts of data recorded. This is a type of compression that removes unnecessary components of the video to reduce the file size. Lossy compression is often used in multimedia recordings because the video and audio hold a significant amount of redundant information [PONLATHA]. The operational benefit is that the video files are greatly reduced in size thus saving time and resources when transferring and/or storing.

NIST research (both through manufacturer documentation and laboratory hands-on inspection of CCTV systems) revealed that the H.264 lossy compression video standard is a widely utilized codec within CCTV systems and commonly used for distributing video content. It is jointly published by the International Telecommunication Union (ITU) and International Organization for Standardization (ISO).

A compliant CCTV system must have the ability to export one video stream (note: storage of multiple video streams in one file container is also possible, and may be desirable, but this capability is not a "Level 0" requirement) per MP4 container with video data compressed and formatted according to the H.264 Advanced Video Coding standard. The complete definition of an H.264 formatted video bitstream is found in [H264-ITU, H264-ISO]. H.265 [H265-ITU] will be equally acceptable as popularity and adoption of H.265 grows.

## 3.3 Date and Time Metadata

### 3.3.1 *startTime*

Perhaps the most critical metadata associated with video recordings needed to support investigations is an accurate reference to the date and time of capture. Timing data must be in a standard interoperable format, called timestamps. Timestamps for exported video files intended for law enforcement applications must conform to the specifications in [MP4-12], [23000-10-ISO], and [ONVIF]. The unique timestamp of each video frame can be determined from a knowledge of the video frame number and frame rate, and by referencing the absolute time recorded at the start of video capture (*startTime*[7], see *Surveillance Media Information* box (*sumi*) in Figure 2). Timestamps must not be "burned" into the pixel data of the video itself—this preserves the original integrity of the digital video evidence.

The (Application Format) *AF Identification* box, which extends the *Surveillance Media Information* box (*sumi*), contains the *startTime* element. [ONVIF] defines the *startTime* element as "the UTC based time of the first media sample in the fragment". An exported video file may be structured either as a single stream of data (i.e., a single fragment) or as multiple fragments. The *AF Identification* box is identified as a box of type *sumi* [23000-10-ISO].

[7] In this document, italics are used to denote value names specified in the profiled ISO, IEC, and ONVIF standards.

### 3.3.2 *ExportUnitTime*

The *Surveillance Export* box (*suep* box) includes the *ExportUnitTime* element. [ONVIF] defines the *ExportUnitTime* element as "an integer that gives the date and time designation as defined in ISO/IEC 14496-12 [MP4-12] of when the export operation has been started".
**Note: The *ExportUnitTime* is equivalent to the Export System Time defined in [NISTIR-8161] when the Export System Time is determined concurrently with the start of an export operation.**

### 3.3.3 Video Stream Fragmentation

Relative time values are also applicable when the MP4 file is fragmented. Fragmentation permits playback of one portion of a file while another portion is being recorded. For fragmented MP4 files, [ONVIF] mandates the use of the Track Fragment Decode Time (*tfdt*) box. [ONVIF] requires that "each track fragment shall contain the Track Fragment Decode Time box "tfdt" as defined in ISO/IEC 14496-12 to ease seeking during playback". The absolute starting time of each video fragment (when fragmentation is used) can be calculated by adding the *tfdt* value (time on the media timeline since initial recording began relative to time zero) to the *startTime* stored within the *sumi AF Identification* box.

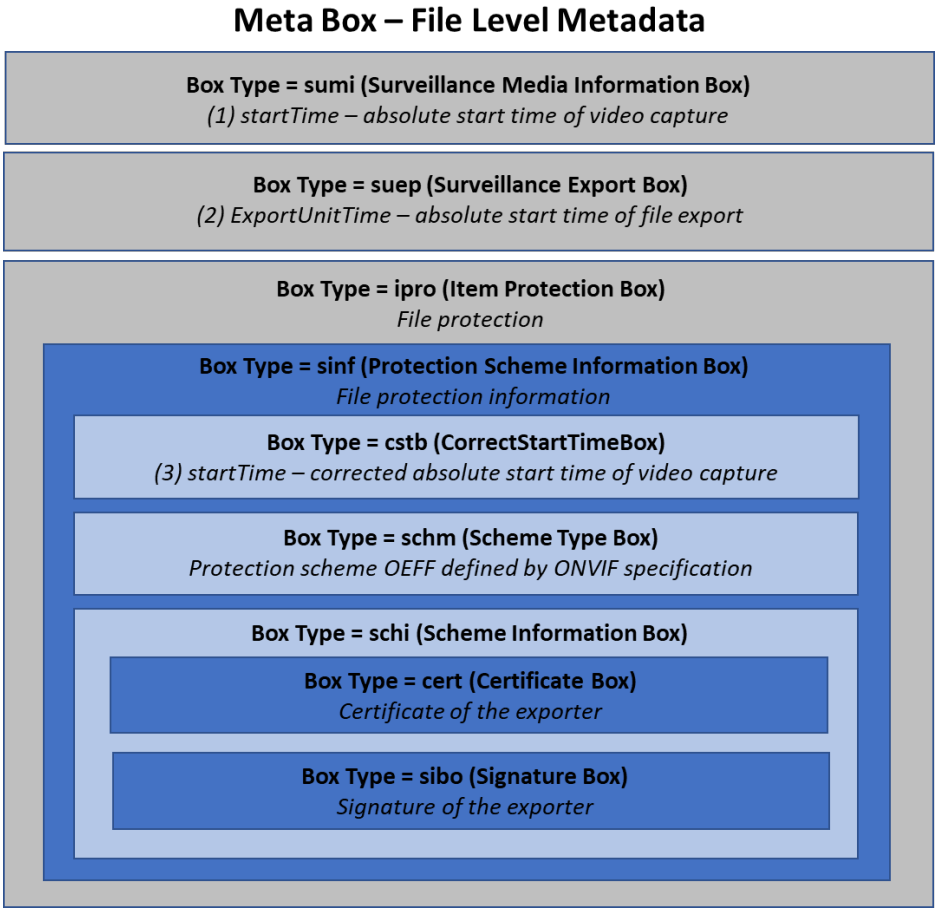


**Figure 2 – Box structure of [ONVIF] illustrating placement of absolute timestamps for (1) start time of video capture, (2) start time of file export, & (3) corrected start time of video capture**

### 3.4 System Clock Offset

Establishing the time of a video recording is critical for analyzing video evidence, which may involve synchronizing video recordings from multiple DVRs or other video recording devices. A CCTV system clock may be more or less synchronized to absolute time depending on the mode (i.e., manual or automatic time entry) and source (e.g., network time server, cell phone display, wristwatch) by which the system clock was set. As a best practice, discrepancy with the CCTV system clock (System Clock Offset) can be observed at the time the video data is exported and used to support subsequent investigative analysis [SWGIT2].

Two different clock observations are required to calculate the System Clock Offset: 1) the time and date on the DVR system clock (the *ExportUnitTime*) and 2) the concurrent time and date from an external reference clock (the External Reference Time). System Clock Offset is calculated as the difference between *ExportUnitTime* and External Reference Time. System Clock Offset can be used to determine a corrected video starting time (i.e., *startTime* element in *CorrectStartTimeBox*).

The *CorrectStartTimeBox* (*cstb*) contains the *startTime* element as illustrated in Figure 2. [ONVIF] defines the *startTime* element as "the UTC-based time represented by the number of 100 nanosecond intervals since January 1, 1601 of the first media sample in the first fragment". The *startTime* value in the *CorrectStartTimeBox* is intended to correct (i.e., use as a replacement when applicable) the *startTime* value in the *sumi* box referenced in Section 3.3.1 of this document. Although ONVIF does not mandate use of the *CorrectStartTimeBox*, for law enforcement applications to be consistent with law enforcement best practice [SWGIT2], NIST recommends that this box be mandatory to ensure that the DVR system time was verified for accuracy at the time of file export. NIST recommends that the *ExportUnitTime* and the External Reference Time be captured "as simultaneously as possible".

Currently, [ONVIF] does not provide a data structure for recording the External Reference Time, but simply uses this value to determine a Corrected Start Time, if needed. The Corrected Start Time (i.e., value of *startTime* in the *CorrectStartTimeBox*) equals the value of *startTime* in the *sumi* box plus the External Reference Time minus the *ExportUnitTime* when the External Reference Time and *ExportUnitTime* are determined at the same moment in time. As noted in Section 5, for law enforcement documentary recordkeeping and ease of reference, NIST recommends that future consideration be given for explicit storage of the External Reference Time value, even though such storage could be viewed as redundant.

# 4 New Elements Recommended

As a first step to support law enforcement applications, [NISTIR-8161] focused on specifying a standardized timestamp in video stream captures from surveillance systems and requiring the MP4 file container as a file export format. Other information of value to law enforcement investigations was noted for future consideration but not directly addressed in the intentionally fundamental "Level 0" profile. Since [ONVIF] has already moved forward via its *SurveillanceExportBox* (*suep)* to provide the ability to store ordered information about the source and exporting of video captures, and a digital signature of the export operator, NIST recommends that these capabilities, described in Sections 4.1.1-4.1.3 below, be implemented to support law enforcement applications [SWGIT].

## 4.1 Additional Surveillance Export Metadata

### 4.1.1 Recording Equipment

[ONVIF] mandates storing information related to the camera, microphone, and exporting system in the *SurveillanceExportBox*. This data includes a set of fields that describe the source of recorded video, the source of recorded audio, and the system device (i.e., DVR) used to export the video surveillance data file. For each of these elements, the name, unique physical address (MAC), and access address (URL) shall be recorded when applicable. The camera source provides a field for recording camera information for multi-channel devices. The Export File Creation Time and Export Operator are fields associated with the export system device.

### 4.1.2 Export File Creation Time

ONVIF provides a standard means to capture the starting time of export file creation (*ExportUnitTime*). This was not an explicit requirement addressed in [NISTIR-8161] but is needed for calculating the system clock offset value in the context that the *ExportUnitTime* is equivalent to the Export System Time defined in [NISTIR-8161] when the Export System Time is determined concurrently with when an export operation has been started (see Section 3.3.2).

### 4.1.3 Export Operator

This field gives the name or identification of the operator that performs the export from the surveillance system. This source information included in the file strengthens the chain of custody by linking the handlers with the evidence. [ONVIF] does not mandate the use of this field. However, NIST recommends the use of this field as a requirement for law enforcement applications.

### 4.2 Digital Signature

For future consideration [NISTIR-8161] identified the need for securing acquired evidence but did not explicitly provide a structured approach. The document listed additional important metadata and features for future consideration such as security enhancing methods. These methods included digital signing, hashing, and encrypting. [ONVIF] addresses this need for verifying the contents of an exported file by providing the capability to store digital signatures. The signature identifies the individual responsible for performing the file export as well as any subsequent operations on the exported file, and provides some assurance, including an audit trail, against tampering. NIST recommends that the usage of digital signatures, hashing, and encryption be considered as a best practice, if not a requirement, for law enforcement applications.

# 5 Future Work and Directions

This recommended standards profile represents a base "Level 0" of digital video data interoperability critical to law enforcement applications and investigations. While compliance to this digital video export profile preserves the native quality of the recorded video on output, provides the output video data in a flexible and generally playable container, and specifies an interoperable method for embedding critical date and time metadata; much more may be done to enhance the value and utility of digital video evidence. Successful adoption of this profile will provide an interoperable foundation and starting point on which future capabilities can be built. This section suggests future areas for CCTV system standards research and development.

## 5.1 New Codecs

The current requirement of H.264 is consistent with common industry practice at this time. Research and development are ongoing in the pursuit of more advanced codecs in support of higher resolution, higher quality, and more compact / compressed video bitstreams. Over time the adoption of more advanced standard video codecs beyond H.264 and H.265 should be considered.

## 5.2 Semantic Considerations

This recommendation is limited to the syntactic representation of CCTV video data and important associated metadata. This standard specifies the structural format of interoperable digital video but does not address the semantic quality requirements of the data file contents. Different use cases for processing digital video evidence will require different quality parameters and requirements such as composition, resolution, and illumination. Profiles of quality levels tailored to specific use cases and analytics are anticipated and is an area currently lacking standards.

## 5.3 Codec Profiles and Levels

Additionally, the H.264 standard specifies a range of implementation profiles (i.e., "profiles" and "levels") that correspond to varying degrees of video image resolution and coding/decoding efficiency. When considering encoding schemes, one must also take into account the tradeoff between computational power required and data processing time. Further research is required to categorize the range of video surveillance implementation scenarios and determine which profile(s) would be optimal for each category. For applications where computational power and bandwidth are not significantly limited, the "High" profile is recommended. The "High" profile corresponds to the variety of high definition television formats.

## 5.4 Multiple Data Capture Streams

This recommendation focuses on the digital video stream as encapsulated in a MP4 container. Future developments should study the inclusion of multiple video streams, audio streams, and metadata within a single MP4 container. A CCTV system typically supports multiple cameras each collecting and storing its own separate channel of video data. Having the ability to export multiple video streams in one output file reduces the chance of data loss or mismatch and enables the bundling of different stream types. On the other hand, exporting multiple video streams in a single container file will add complexity, increase payload size, and may not work with common video players.

In addition to timing, other key metadata should be considered for future enhanced capabilities. Such metadata would include geolocation as well as camera metadata including configuration parameters at time of video capture. There also continues to be large investments in developing more effective forensic and analysis tools. As technologies mature, there is an opportunity to standardize metadata extracted from video content that drive these algorithms. Developing standard metadata to be included within the MP4 container will be strategically important.

## 5.5 Fragmented File Format

The MP4 file standard originally did not support file streaming, which lead to adopting the fragmented MP4 for delivery of network content. The fragmented MP4 addressed the issue of content delivery for multi-platform consumption without compromising security or network efficiency. Surveillance systems rely on this format to expand access to streams for consumer convenience. These systems allow for real time streaming, viewable on smartphones, tablets or through web interfaces. One benefit of a fragmented MP4 file is that metadata can be stored independent from the media content. Fragments contain short audio or video portions of an elementary stream that can be delivered as network packets. Consideration should be made to extend this flexible placement of metadata for including additional timestamps in the stored fragments. Each fragment could contain a meta box with the *sumi* elements holding the absolute time when the fragment was created. This data would be in addition to the *tfdt* value as specified by [ONVIF].

## 5.6 Additional Support for System Clock Offset

As stated in Section 3.4, for law enforcement applications, NIST recommends the mandatory recording of system clock offset (i.e., related to corrected start time) data as part of the video export process to ensure that the DVR system time was verified for accuracy at the time of file export. NIST also recommends that the *ExportUnitTime* and the External Reference Time be captured “as simultaneously as possible”, and both values be stored in the MP4 file for both documentary recordkeeping and ease of reference. Currently, [ONVIF] does not provide a data structure for recording the External Reference Time. This time value could be stored as text in a non-mandatory *AdditionalUserInformationBox* (*auib*). This box is provided by [ONVIF] to record

annotated user information. Unfortunately, such annotated data is not clearly defined and would be subject to interpretation. Consideration should be made for a more standard approach to extend the *CorrectStartTimeBox* data structure by adding standard time definitions for both the *ExportUnitTime* and External Reference Time elements.

### 5.7 Standard Operating Procedures and Best Practices

Community adoption of the elements described in this document will significantly enhance the investigative utility of CCTV recordings. While the details of this recommendation support reliable and interoperable data syntax, further consideration should be given by system and application developers to implement the requirements in a usable and operationally effective fashion. Additional standard operating procedures and best practices are needed to promote the consistent and most effective use of the capabilities provided by this recommendation and associated standards. Actions such as user installation and setup of CCTV systems, and procedures for capture and use of System Clock Offset metadata should be addressed.

Work should continue in the international consensus standards community through the collaboration of video technology experts and law enforcement video analytics practitioners to develop additional enhancements that will support law enforcement needs and to promote industry adoption.

## 6 References


| | |
|---|---|
| H264-ISO | ISO/IEC 14496-10:2014. "Information technology – Coding of audio visual objects – Part 10: Advanced Video Coding." http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66069 |
| H264-ITU | ITU-T H.264 (V11) (10/2016). "Recommendation – Advanced video coding for generic audiovisual services." http://www.itu.int/itu-t/recommendations/rec.aspx?rec=H.264 |
| H265-ITU | ITU-T H.265 (V3) (04/2015). "Recommendation – High efficiency video coding." http://www.itu.int/itu-t/recommendations/rec.aspx?rec=H.265 |
| 62676-2-32-IEC | IEC 62676-2-32 (committee ratified, expected publication mid-2019). "Video surveillance systems for use in security applications – Part 2-32: Recording control and replay based on web services." https://www.iec.ch/ |
| LILLIS | Lillis, David, et al. "Current Challenges and Future Research Areas for Digital Forensic Investigation." CDFSL Proceedings 2016. |
| MP4-12 | ISO/IEC-14496-12:2015. "Information technology – Coding of audio-visual objects- Part 12: ISO based media file format." https://www.iso.org/standard/68960.html |
| 23000-10-ISO | ISO/IEC 23000-10:2012. "Information technology – Multimedia application format (MPEG-A) – Part 10: Surveillance application format." https://www.iso.org/standard/60330.html |
| NIST-8161 | Garris, Michael, et al. "Recommendation: Closed Circuit Television (CCTV) Digital Video Export Profile – Level 0". https://doi.org/10.6028/NIST.IR.8161 |
| NIST-8172 | Garris, Michael et al. "Assessment of Closed Circuit Digital Video Recording and Export Technologies." https://doi.org/10.6028/NIST.IR.8172 |
| ONVIF | "ONVIF Export File Format Specification." Version 18.12. December 2018. https://www.onvif.org/specs/stream/ONVIF-ExportFileFormat-Spec.pdf |
| QUICKTIME | Apple QuickTime Player Support. https://support.apple.com/quicktime |
| PELLEY | Pelley, Scott. "Inside the Boston Marathon Bombing Investigation." CBS Transcript. March 23, 2014. http://www.cbsnews.com/news/manhunt-inside-the-boston-marathon-bombing-investigation/ |
| PONLATHA | Ponlatha, S., et al. "Comparison of Video Compressed Standards." International Journal of Computer and Electrical Engineering, Vol. 5, No. 6. December 2013. |

| | |
|---|---|
| SWGDE | Scientific Working Group on Digital Evidence. "SWGDE Recommendations and Guidelines for Using Video Security Systems." Version1.0. September 29, 2015. https://www.swgde.org/documents/Current%20Documents/2015-09-29%20SWGDE%20Recommendations%20and%20Guidelines%20for%20Using%20Video%20Security%20Systems |
| SWGIT | Scientific Working Group Imaging Technology. "Section 4 Recommendations and Guidelines for Using Closed-Circuit Television Systems in Commercial Institutions." Version 3.0. June 8, 2012. https://www.swgit.org/documents/Current%20Documents |
| SWGIT2 | Scientific Working Group Imaging Technology. "Section 24 Best Practices for the Retrieval of Digital Video." Version 1.0. September 27, 2013. https://www.swgit.org/pdf/Section%2024%20Best%20Practices%20for%20the%20Retrieval%20of%20Digital%20Video?docID=141 |