Withdrawn NIST Technical Series Publication

Warning Notice

The attached publication has been withdrawn (archived), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Withdrawn Publication	
Series/Number	NIST Interagency/Internal Report (NISTIR) 8161
Title	Recommendation: Closed Circuit Television (CCTV) Digital Video Export Profile – Level 0
Publication Date(s)	December 2016
Withdrawal Date	April 8, 2019
Withdrawal Note	NISTIR 8161 is superseded in its entirety by publication of NISTIR 8161, Revision 1 (April 2019)
Superseding Publication(s) *(if applicable)*	
The attached publication has been **superseded by** the following publication(s):	
Series/Number	NIST Interagency/Internal Report (NISTIR) 8161, Revision 1
Title	Recommendation: Closed Circuit Television (CCTV) Digital Video Export Profile – Level 0 (Revision 1)
Author(s)	Lawrence D. Nadel, Mary T. Laamanen, Michael D. Garris, Craig S. Russell
Publication Date(s)	April 8, 2019
URL/DOI	https://doi.org/10.6028/NIST.IR.8161r1
Additional Information *(if applicable)*	
Contact	
Latest revision of the attached publication	
Related Information	
Withdrawal Announcement Link	

Date Updated: May 6, 2019

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

NISTIR 8161

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

Michael Garris
Mary Laamanen
Craig Russell
Lawrence Nadel

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

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

This page intentionally blank

NISTIR 8161

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

Michael Garris[†]
Mary Laamanen[‡]
Craig Russell[‡]
Lawrence Nadel[†]
Information Access Division – Image Group[†]
Software and Systems Division – Software Quality Group[‡]
Information Technology Laboratory

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

December 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Disclaimer

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgements

We would like to acknowledge and thank the Federal Bureau of Investigation(FBI) for supporting the National Institute of Standards and Technology (NIST) in the development of this Recommendation for Closed Circuit Television (CCTV) Digital Video Export Profile.

Abstract

This document is a recommendation prescribing a data interchange format for the syntactic representation of information needed to achieve a base “Level 0” of interoperability when exporting and processing video recordings captured by closed circuit television (CCTV) digital video recording (DVR) systems. In summary, this profile of standards leverages the Moving Picture Experts Group-4 (MPEG-4) Part 14 (MP4) digital multimedia file container, storing one H.264 encoded digital video bitstream containing embedded time codes defined by the Motion Industry Standards Board (MISB), and Extensible Metadata Platform (XMP)-formatted metadata that is used to determine a CCTV DVR System Clock Offset. The video output format described in this document has been developed to support law enforcement investigations.

This specification was prepared by the National Institute of Standards and Technology (NIST), in collaboration with the Federal Bureau of Investigation, and in conjunction with the CCTV / DVR community.

Keywords

codec, digital video, export file, format standards, H.264, interoperability, law enforcement investigations, MISB, MP4, surveillance, time stamp, timestamp

Table of Contents

1 Introduction 1
1.1 Purpose and Scope 1
1.2 Organization of this Document 2
2 Terms, Acronyms, and Organizations 3
3 Profile Specification 5
3.1 MP4 File Container 5
3.2 H.264 Video Bitstream 6
3.3 Date and Time Metadata 6
3.3.1 SEI Messages 6
3.3.2 MISB Precision Time Stamp 7
3.3.3 Embedded Time Mode-Source Codes 7
3.4 System Clock Offset 8
3.4.1 ClockOffset UUID Box 10
3.4.2 ClockOffset XMP Packet 10
4 Future Work and Directions 12
5 References 14
Appendix A – Implementation Resources 15
Appendix B – Time Mode-Source Code Rationale (Reliability of Time Recorded) 16
Appendix C – ClockOffset Data Element Definitions 17
Appendix D – ClockOffset Schemas 19
Appendix E – ClockOffset XMP Packet Example 22

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.

1.1 Purpose and Scope

The purpose of this recommended profile is to define 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. This will increase the evidentiary value and timeliness of CCTV video data and facilitate interoperable data sharing.

This profile 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 be compliant to this specification, a CCTV system shall support the interoperable data format specified herein; however, a compliant system may output video data in additional formats of the manufacturer's choosing. This specification 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 specification are out of scope, and left to future standardization efforts.

The data format solution prescribed in this document represents a base "Level 0" of interoperability chosen to address the following fundamental requirements:

1) Preserve quality – a compliant CCTV system shall provide the option to export video at the same level of quality as onboard the system;
2) Be generally playable – the standard output format shall be generally playable by common video players (e.g., Media Player, QuickTime, and VLC);
3) Annotate time stamps – the video data shall be annotated with "precision time stamps" [MISB] at the atomic (frame) level; and
4) Record System Clock Offset metadata – a compliant CCTV system shall record the time and date from the DVR system clock—the Export System Time, along with the current time and date from a reference clock—the External Reference Clock Time, to determine any time difference between the two clocks.

In meeting these requirements, the following guiding principles were applied:

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 – inventing as little new as possible;
4) Use a flexible container – selecting a format that supports general playability and multiple data streams; and
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 resulting recommendation herein is based largely on a series of independent studies conducted by NIST to be published.

1.2 Organization of this Document

Section 2 lists terms and acronyms referenced throughout this document, Section 3 presents the technical specification of this recommendation, and Section 4 discusses future work and directions. Section 5 provides pertinent references, including the standards profiled in this document. Appendix A identifies and provides web links to resources developed by NIST to support implementation of the recommendations contained in this document. Appendix B describes the rationale for associating a Time Mode-Source Code with each time stamp. Appendix C, Appendix D, and Appendix E contain XML element definitions, XML schemas, and a sample XML data packet implementation, respectively.

2 Terms, Acronyms, and Organizations

Table 1 – Terms

Schema	W3C standard for defining vocabularies and structures used to describe the content and semantics of XML documents.
User Data (Unregistered)	User defined data carried in an SEI message that is not part of the H.264 standard. This data does not have an assigned ITU-T registered code.
UTC Precision Time	Standard representation of time based on Coordinated Universal Time (UTC)

Table 2 – Acronyms

AVC	Advanced Video Coding
CCTV	Closed Circuit Television
codec	Encoder and Decoder
DVR	Digital Video Recorder
H.264	Advanced Video Coding Standard
KLV	Key-Length-Value
MP4	Digital Multimedia Container Format
NAL	Network Abstraction Layer
SDO	Standards Developing Organization
SEI	Supplemental Enhancement Information
UTC	Coordinated Universal Time
UUID	Universal Unique Identifier
XML	Extensible Markup Language
XMP	Extensible Metadata Platform (Adobe)

Table 3 – Organizations

BCOE	Biometric Center of Excellence
FBI	Federal Bureau of Investigation
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
ITU	International Telecommunication Union
MISB	Motion Imagery Standards Board
MPEG	Moving Picture Experts Group
MXU	Multimedia Exploitation Unit
NIST	National Institute of Standards and Technology
SMPTE	Society of Motion Picture & Television Engineers
SWGDE	Scientific Working Group on Digital Evidence
SWGIT	Scientific Working Group Image Technology
W3C	World Wide Web Consortium

3 Profile Specification

This section details the various standards selected as part of this recommended profile. 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 specification 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 shall have the ability to export the data in an MPEG-4 Part 14 (MP4) digital multimedia file container. Each exported MP4 file container shall store one video stream and optionally corresponding audio and metadata streams, followed at the end by a data packet containing System Clock Offset metadata as illustrated in Figure 1. The complete definition of the MP4 file format can be found in [MP4].

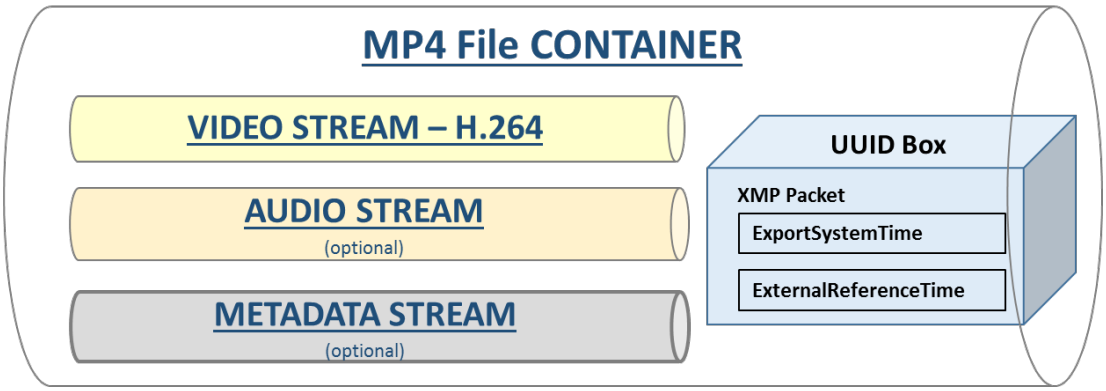

Figure 1 – Example export MP4 file container with one video data stream, optional audio and metadata streams, and one UUID Box containing System Clock Offset metadata

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 benefit to this is that the 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) has 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 shall have the ability to export one video stream per MP4 container with video data compressed and formatted according to the H.264 Advanced Video Coding standard. The complete definition of H.264 formatted video bitstream is found in [H264-ITU, H264-ISO].

3.3 Date and Time Metadata

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 shall be in a standard interoperable format, called time stamps, and embedded within and throughout the video data stream itself. If a video file is ever damaged where only part of the video data is recovered, the fragment will still be time-referenced. The time stamp shall be a data record within the video stream, and shall not be "burned" into the pixel data of the video itself—this preserves the original integrity of the digital video evidence.

3.3.1 SEI Messages

To meet this requirement, a compliant CCTV system shall store timing metadata within standard H.264 Supplemental Enhancement Information (SEI) messages as illustrated in Figure 2. An SEI message is transmitted in an SEI Raw Byte Sequence Payload within the H.264 bitstream [RICHARDSON]. These messages are sent in separate payload units (i.e., within each video frame) that can be parsed by investigative tools. This standard profile specifies two different SEI message types to be embedded within the H.264 bitstream: 1) a standard precision time stamp described in Section 3.3.2, and 2) a time mode-source code described in Section 3.3.3.

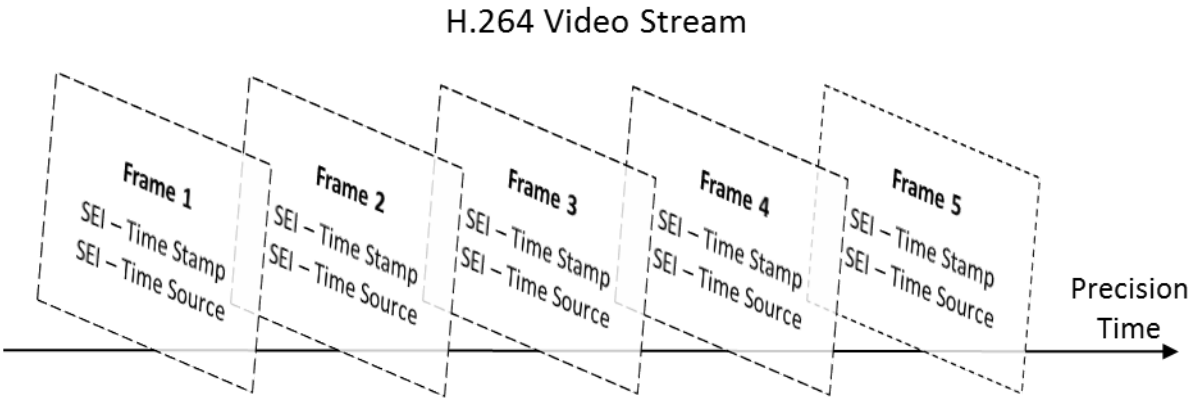

Figure 2 – Conceptual illustration of precision time stamp and time source embedded in each video frame

3.3.2 MISB Precision Time Stamp

To meet the requirement of embedded interoperable absolute time, a compliant CCTV system shall utilize precision time stamps according to the MISB 0604.3 standard. These time stamps are an encoding of the common Coordinated Universal Time (UTC), and each time stamp shall be inserted into the H.264 bitstream as an SEI message of type User Data (Unregistered). The complete definition for the MISB Precision Time Stamp can be found in [MISB].

3.3.3 Embedded Time Mode-Source Codes

The source of the time (i.e., the clock) referenced by a CCTV system will vary depending on the capabilities of the specific system. As a best practice, CCTV systems should utilize globally synchronized and highly accurate time sources such as time servers and network time protocols. Depending on the connectivity of the CCTV system, time may be only available from a less-reliable local system clock. To identify the source of time used in the recording of video data, a compliant CCTV system shall insert a time mode-source code along with each embedded MISB precision time stamp. Each time mode-source code shall be inserted into the H.264 bitstream as an SEI message of type User Data (Unregistered).

A time mode-source SEI message shall be an 11-byte record composed of a 10-byte ASCII header string, “timesource”, followed by a 1-byte time mode-source code that represents the pairwise combination of System Clock Set Mode and System Clock Set Source. Table 4 provides the mapping of the header string from ASCII to its hexadecimal byte equivalent. Table 5 lists the 1-byte values assigned to possible time sources. A knowledge of how and from what source a CCTV system clock was set can provide a sense for time value reliability, and thus offer significant evidentiary value. This rationale is explained further Appendix B.

Table 4 – Byte Assignments for ASCII Header, "timesource"

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9	Byte 10
t	i	m	e	s	o	u	r	c	e
0x74	0x69	0x6D	0x65	0x73	0x6F	0x75	0x72	0x63	0x65

Table 5 – Byte 11 Assignment for Embedded Time Mode-Source Codes

		System Clock Set Source		
		Time Source Network	**Time Source Non-Network**	**Time Source Unknown**
System Clock Set Mode	**Auto**	**00 (0)** Time/date auto-set directly from network or networked device	**01 (1)** Time/date auto-set from non-networked device	**02 (2)** Time/date was not set by system owner; could have been pre-set by factory/vendor
	Manual	**03 (3)** Time/date obtained from networked device (e.g., cell phone) and entered manually	**04 (4)** Time/date obtained from non-networked device (e.g., watch, clock, ...) and entered manually	**05 (5)** Time/date had been entered manually but from an unknown source

Note: Byte values are shown in table as **hex (decimal)**. Shaded boxes represent possible but unlikely occurrences.

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 and source in which the system clock was set as described in Section 3.3.3. 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 investigative analysis later [SWGIT2].

Two different clock observations are needed to calculate the System Clock Offset: 1) the time and date on the DVR system clock (the Export System Time); along with 2) the current time and date from an external reference clock (the External Reference Time). System Clock Offset is calculated as the difference between Export System Time and External Reference Time. Both Export System Time and External Reference Time can be further described by the record mode and time source of their respective clocks (similar to the encoding used in Section 3.3.3).

Two pairs, totaling four data elements shall be recorded: (Export System Time, Export System Time Mode-Source Code) and (External Reference Time, External Reference Time Mode-Source

Code). Export System Time and External Reference Time shall be formatted in UTC offset format. The Export System Time Mode-Source Code shall be defined by the pairwise combination of values listed in Table 6. Similarly, the Export External Reference Time Mode-Source Code shall be defined by the pairwise combination of values listed in Table 7.

Table 6 – Export System Time Mode-Source Codes

Export System Time Record Mode	Export System Time Source: Time Source Network	Time Source Non-Network	Time Source Unknown
Auto	**06 (6)** Time/date auto-recorded from DVR system clock that was set from network or networked device	**07 (7)** Time/date auto-recorded from DVR system clock that was set from non- networked device	**08 (8)** Time/date auto-recorded from DVR system clock that was set from unknown source
Manual	**09 (9)** Time/date manually read/recorded from DVR system clock that was set from network or networked device	**0A (10)** Time/date manually read/recorded from DVR system clock that was set from non- networked device	**0B (11)** Time/date manually read/recorded from DVR system clock that was set from unknown source

Note: Byte values are shown in table as **hex (decimal)**. Shaded boxes represent possible but unlikely occurrences.

Table 7 – Export External Reference Time Mode-Source Codes

External Reference Time Record Mode	External Reference Time Source: Time Source Network	Time Source Non-Network	Time Source Unknown
Auto	**0C (12)** Time/date auto-recorded from external reference clock that was set from network or networked device	**0D (13)** Time/date auto-recorded from external reference clock that was set from non-networked device	**0E (14)** Time/date auto-recorded from external reference clock that was set from unknown source
Manual	**0F (15)** Time/date manually entered from external reference clock that was set from network or networked device	**10 (16)** Time/date manually entered from external reference clock that was not set from network or networked device	**11 (17)** Time/date manually entered from external reference clock that was set from an unknown time source

Note: Byte values are shown in table as **hex (decimal)**. Shaded boxes represent possible but unlikely occurrences.

3.4.1 ClockOffset UUID Box

As illustrated in Figure 1, System Clock Offset (ClockOffset) metadata shall be encapsulated within a standard MP4 UUID box structure and embedded at the end of the MP4 export video file. The UUID box format is specified in Adobe XMP Specification Part 3 [XMP3] and shall be assigned the unique identifier "BE7ACFCB 97A942E8 9C719994 91E3AFAC". Figure 3 depicts ClockOffset metadata formatted as an XMP packet (described in the next section) and encapsulated in an MP4 UUID box.

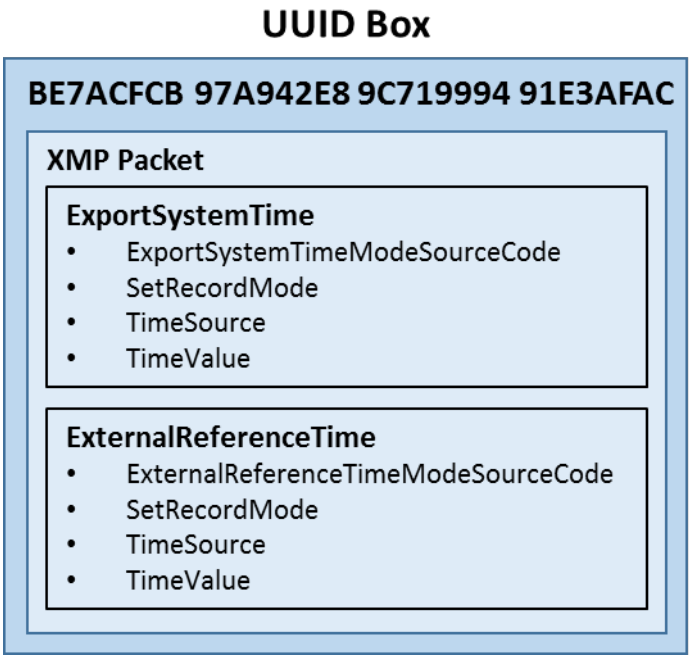

Figure 3 – Encapsulated ClockOffset Metadata within UUID Box

3.4.2 ClockOffset XMP Packet

ClockOffset metadata shall be collected and stored in an XMP packet in accordance with the XMP data model and core namespaces as defined in the open standard "Adobe XMP Specification Part 1", which has also been adopted as ISO 16684-1:2011 [XMP1]. XMP is based on XML. This section provides an overview of how the ClockOffset metadata shall be stored in the standard export video file. Appendix C, Appendix D, and Appendix E provide XMP and XML implementation details.

Figure 4 illustrates the data model supporting both Export System Time and External Reference Time. There are four data objects associated with each type of recorded time. The data objects listed on the left side of the figure are associated with ExportSystemTime and working from top to bottom include a hex code from Table 6; followed correspondingly by two string values SetRecordMode (taking on values "Auto" or "Manual") and TimeSource (taking on values "Network", "NonNetwork", or "Unknown"); and the last data object is TimeValue containing a

UTC formatted date and time string. The data objects listed on the right side of the Figure 4 are associated with ExternalReferenceTime and are the same as those listed for ExportSystemTime, with the exception that the first three data objects derive their values according to Table 7.

Data element definitions for these data objects are defined in Appendix C. Supporting XML schemas are listed in Appendix D, and an XML instance is provided as an example in Appendix E.

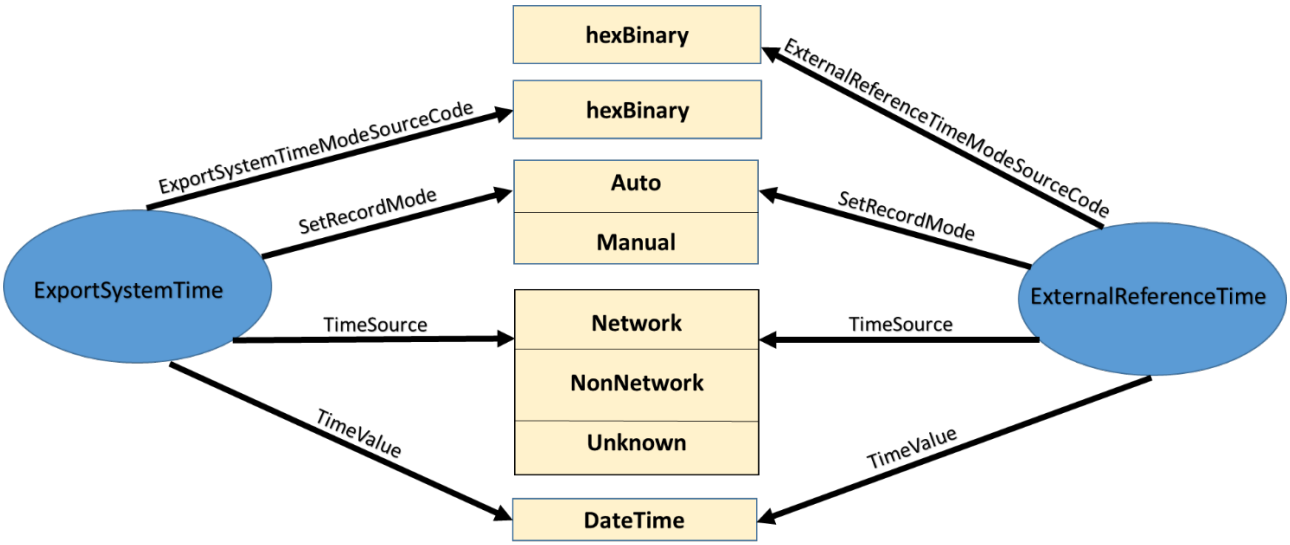

Figure 4 – ClockOffset Data Model

4 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 evidentiary value and utility of digital video evidence. Successful adoption of this standards profile will provide an interoperable foundation and starting point on which future capabilities can be built. This section suggests a number of future areas for CCTV system standards research and development.

The current requirement of H.264 is consistent with common industry practice at this time. Research and development is ongoing in the pursuit of more advanced codecs in support of higher resolution, higher quality, and more compact / compressed video bitstreams. Over time this profile should consider adoption of more advanced standard video codecs - H.265 for example [H265-ITU].

This specification 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.

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.

This profile 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 model and 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 streams to be included within the MP4 container will be strategically important. This will involve looking at both Key Length Value (KLV) standard formats [SMPTE] as well as XML-based data models.

Community adoption of this profile will significantly enhance the investigative utility of CCTV recordings. While the details of this specification 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 specification, and should cover actions such as user installation and setup of CCTV systems, and procedures for capture and use of System Clock Offset metadata.

In order to enhance the evidentiary value of digital video evidence, security enhancing methods should be developed and integrated into an enhanced interoperable capability. This may include digital signing, hashing, and encrypting.

This specification in its current form is a NIST recommendation developed with FBI and CCTV community input. The community may be served if this specification were to be adopted as a "Level 0" interoperability standard by an established Standards Developing Organization (SDO). Research should be done to identify relevant and potential SDOs.

5 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
LILLIS	Lillis, David, et al. "Current Challenges and Future Research Areas for Digital Forensic Investigation." CDFSL Proceedings 2016.
MISB	MISB ST 0604.3. "Time Stamping Compressed Motion Imagery." 27 February 2014. http://www.gwg.nga.mil/misb/docs/standards/ST0604.3.pdf
MP4	ISO/IEC 14496-14:2003. "Information technology – Coding of audio-visual objects – Part 14: MP4 file format." http://www.iso.org/iso/catalogue_detail.htm?csnumber=38538
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.
RCHARDSON	Richardson, I. E. "The H.264 Advanced Compression Standard." 2nd ed. John Wiley and Sons, Ltd., 2010.
SMPTE	SMPTE ST 336:2007. "Data Encoding Protocol Using Key-Length-Value." August 22, 2007.
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 2012.06.08. 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 2013.09.27. https://www.swgit.org/pdf/Section%2024%20Best%20Practices%20for%20the%20Retrieval%20of%20Digital%20Video?docID=141
XMP1	XMP Specification Part 1 - Data Model, Serialization, and Core Properties, April, 2012; also ISO 16684-1:2012 - Graphic technology -- Extensible metadata platform (XMP) specification -- Part 1: Data model, serialization and core properties. http://wwwimages.adobe.com/content/dam/Adobe/en/devnet/xmp/pdfs/XMP%20SDK%20Release%20cc-2016-08/XMPSpecificationPart1.pdf
XMP3	XMP Specification Part 3 – Storage in Files, August 2016 http://wwwimages.adobe.com/content/dam/Adobe/en/devnet/xmp/pdfs/XMP%20SDK%20Release%20cc-2016-08/XMPSpecificationPart3.pdf

Appendix A – Implementation Resources

The resources listed below have been developed and provided by NIST to support implementation of this recommendation. They may be downloaded from https://www.nist.gov/programs-projects/digital-video-exchange-standards.

- Video file that illustrates implementation of the recommendations provided in this document
- ClockOffset XML Schemas (listed in – ClockOffset Schemas)
  - ClockOffset.xsd
  - TimeValueset.xsd
- ClockOffset XMP packet example (listed in – ClockOffset XMP Packet Example)

Appendix B – Time Mode-Source Code Rationale (Reliability of Time Recorded)

This appendix describes the rationale for implementing the Time Mode-Source Codes presented in Table 5, Table 6, and Table 7 for setting of the CCTV System clock, and for recording the Export System Time and External Reference Time, respectively. The general concept is that the time provided by a networked time source (e.g., NIST Time Server) will be more reliable than the time obtained from a non-networked time source (e.g., a conventional, personal wristwatch that has been set manually), and which may be more accurate than a time source of unknown origin. Likewise, a time value that is recorded automatically (i.e., electronically) is less subject to error or imprecision than a time value that is recorded manually (e.g., keyed into a computer). Given how critical the time of a recorded event is when analyzing video evidence, capturing the time source and recording mode will be useful in conveying the reliability of the recorded time values. Table 8 provides relative reliability rankings of the Time Source and Time Set/Record Mode pairs.

This specification provides the ability to store metadata that can provide a sense for the reliability of recorded time values. However, further research and development will be required to determine how to implement this capability and use this information in an effective and consistent a fashion.

Table 8 – Relative Reliability of Recorded Time

Time Source	Time Set/Record Mode	Relative Reliability Ranking (1 = least reliable)
Network	Auto	4
Network	Manual	3
Non-Network or Unknown	Auto	2
Non-Network or Unknown	Manual	1

Appendix C – ClockOffset Data Element Definitions

The definitions in Table 9 and Table 10 define the XML data elements used in the ClockOffset XMP packet.

Table 9 defines the primary data elements ExportSystemTime and ExternalReferenceTime needed to calculate ClockOffset.

Table 9 – ClockOffset Elements

The namespace URI is http://biometrics.nist.gov/cs_links/DVR_Standards/ClockOffset.
The preferred namespace is *cloSet*.

Name	Type	Definition
cloSet:ExportSystemTime	referenceTimeType	Defines the time setting on the DVR system at the time video is exported off the system.
cloSet:ExternalReferenceTime	referenceTimeType	Defines the time setting of an external clock at the time video is exported off the system.

Table 10 defines the data elements and possible values that comprise the complex elements ExportSystemTime and ExternalReferenceType.

Table 10 – TimeValueset Elements

The namespace URI is http://biometrics.nist.gov/cs_links/DVR_Standards/TimeValueSet.
The preferred namespace is *timeval*.

Name	Type	Definition
timeval:Export SystemTimeModeSouceCode	Choice	The hexcode value for the Export System Time Record Mode Source Code. This code value shall be recorded at one of the following six values: 06, 07, 08, 09, 0A, 0B.
timeval:ExternalReferenceTimeModeSourceCode	Choice	The hexcode value for the External Reference Time Mode Source Code. This code value shall be recorded at one of the following six values: 0C, 0D, 0E, 0F, 10, 11.
timeval:SetRecordMode	Choice	The clock mode when time is set or recorded. The choices are Auto or Manual. Auto – The time is automatically set or recorded. Manual – The time is manually set or recorded.
timeval:TimeSource	Choice	The time source used when setting or recording the time. The choices are Network, NonNetwork or Unknown. Network – The time source is a networked device. NonNetwork – The time source is a non-network device. Unknown – The time source is unknown.
timeval:TimeValue	dateTime	The recorded export time value for the Export System Time and the External Reference Time. The time shall use the UTC offset format. YYYY-MM-DDThh:mm:ss-00:00 or YYYY-MM-DDThh:mm:ss+00:00

Appendix D – ClockOffset Schemas

ClockOffset.xsd – This schema defines the complex element types Export System Time and External Reference Time.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns=”http://biometrics.nist.gov/cs_links/DVR_Standards/ClockOffset”
xmlns:timeval=”http://biometrics.nist.gov/cs_links/DVR_Standards/TimeValueset”
targetNamespace=”http://biometrics.nist.gov/cs_links/DVR_Standards/ClockOffset”
elementFormDefault="qualified">
<xs:import namespace=”http://biometrics.nist.gov/cs_links/DVR_Standards/TimeValueset”
schemaLocation="http://biometrics.nist.gov/cs_links/DVR_Standards/TimeValueset.xsd"/>

  <xs:element name="ExportSystemTime" type="ExportSystemTimeSetType"/>
  <xs:element name="ExternalReferenceTime" type="ReferenceTimeSetType"/>

  <xs:complexType name="ExportSystemTimeSetType">
    <xs:annotation>
      <xs:documentation>Defines the metadata values needed for recording the system
export time.</xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element ref="timeval:ExportSystemTimeModeSourceCode"/>
      <xs:element ref="timeval:SetRecordMode"/>
      <xs:element ref="timeval:TimeSource"/>
      <xs:element ref="timeval:TimeValue"/>
    </xs:sequence>
  </xs:complexType>

   <xs:complexType name="ReferenceTimeSetType">
    <xs:annotation>
      <xs:documentation>Defines the metadata values needed for recording time from the
external reference clock.</xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element ref="timeval:ExternalReferenceTimeModeSourceCode"/>
      <xs:element ref="timeval:SetRecordMode"/>
      <xs:element ref="timeval:TimeSource"/>
      <xs:element ref="timeval:TimeValue"/>
    </xs:sequence>
  </xs:complexType>


  <xs:element name="ClockOffset">
    <xs:annotation>
      <xs:documentation>Clock Offset relies on the collected setting from the system
clock at the time of export and the external reference clock settings at the time of
export. </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="ExportSystemTime"/>
        <xs:element ref="ExternalReferenceTime"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

TimeValueset.xsd - This schema is imported into the ClockOffset.xsd and defines the data fields used to record an instance of Export System Time and External Reference Time.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://biometrics.nist.gov/cs_links/DVR_Standards/TimeValueset"
targetNamespace="http://biometrics.nist.gov/cs_links/DVR_Standards/TimeValueset"
elementFormDefault="qualified">

  <xs:element name="SetRecordMode" type="RecordModeType"/>
  <xs:element name="TimeSource" type="TimeSourceType"/>
  <xs:element name="TimeValue" type="xs:dateTime"/>
  <xs:element name="ExportSystemTimeModeSourceCode"
type="ExportSystemTimeHexcodeType"/>
  <xs:element name="ExternalReferenceTimeModeSourceCode"
type="ExternalReferenceTimeHexcodeType"/>


 <xs:simpleType name="ExportSystemTimeHexcodeType">
    <xs:annotation>
      <xs:documentation>Defines the hexCode value for the Time Source and Clock Set
Mode for the Export SystemTime.</xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:hexBinary">
      <xs:enumeration value="06"/>
      <xs:enumeration value="07"/>
      <xs:enumeration value="08"/>
      <xs:enumeration value="09"/>
      <xs:enumeration value="0A"/>
      <xs:enumeration value="0B"/>
      </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="ExternalReferenceTimeHexcodeType">
    <xs:annotation>
      <xs:documentation>Defines the hexCode value for how the Time Source and Clock
Set Mode for the ExternalReferenceTimeSource.</xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:hexBinary">
     <xs:enumeration value="0C"/>
      <xs:enumeration value="0D"/>
      <xs:enumeration value="0E"/>
      <xs:enumeration value="0F"/>
      <xs:enumeration value="10"/>
      <xs:enumeration value="11"/>
    </xs:restriction>
  </xs:simpleType>

 <xs:simpleType name="RecordModeType">
    <xs:annotation>
      <xs:documentation>Defines how the video export time was recorded. This applies
to both ExportSystemTime and the ExternalReferenceTimeSource.</xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
      <xs:enumeration value="Auto"/>
      <xs:enumeration value="Manual"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="TimeSourceType">
    <xs:annotation>
```

```
      <xs:documentation>Defines the source of  time source for the ExportSystemTime
and the ExternalClockReferenceTime.</xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
      <xs:enumeration value="Network"/>
      <xs:enumeration value="NonNetwork"/>
      <xs:enumeration value="Unknown"/>
    </xs:restriction>
  </xs:simpleType>

</xs:schema>
```

Appendix E – ClockOffset XMP Packet Example

```
<?xpacket begin='ï»¿' id='W5M0MpCehiHzreSzNTczkc9d'?>
<x:xmpmeta xmlns:x='adobe:ns:meta/' x:xmptk='Image::ExifTool 10.26'>
<rdf:RDF xmlns:rdf='http://www.w3.org/1999/02/22-rdf-syntax-ns#'>
 <rdf:Description rdf:about=""
     xmlns:dc="http://purl.org/dc/elements/1.1/">
     <dc:title>ClockOffset</dc:title>
 </rdf:Description>
 <rdf:Description rdf:about=""
     xmlns:closet="http://biometrics.nist.gov/cs_links/DVR_Standards/ClockOffset"
     xmlns:timeval="http://biometrics.nist.gov/cs_links/DVR_Standards/TimeValueset">
    <closet:ExportSystemTime>

<timesetval:ExportSystemTimeModeSourceCode>06</timeval:ExportSystemTimeModeSourceCode>
      <timeval:SetRecordMode>Auto</timeval:SetRecordMode>
      <timeval:TimeSource>Network</timeval:TimeSource>
      <timeval:TimeValue>2016-05-12T09:00:00</timeval:TimeValue>
  </closet:ExportSystemTime>
</rdf:Description>

 <rdf:Description rdf:about=""
     xmlns:cloSet="http://biometrics.nist.gov/cs_links/DVR_Standards/ClockOffSet"
     xmlns:timeval="http://biometrics.nist.gov/cs_links/DVR_Standards/TimeValueset">
     <cloSet:ExternalReferenceTime>

<timeval:ExternalReferenceTimeModeSourceCode>10</timeval:ExternalReferenceTimeModeSour
ceCode>
       <timeval:SetRecordMode>Manual</timeval:SetRecordMode>
       <timeval:TimeSource>NonNetwork</timeval:TimeSource>
       <timeval:TimeValue>2016-05-12T09:00:00</timeval:TimeValue>
     </cloSet:ExternalReferenceTime>
</rdf:Description>
</rdf:RDF>
</x:xmpmeta>

<?xpacket end='w'?>
```