NISTIR 8172

Assessment of Closed Circuit Digital Video Recording and Export Technologies

Michael Garris
Mary Laamanen
Craig Russell
Lawrence Nadel

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8172

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

This page intentionally blank

NISTIR 8172

Assessment of Closed Circuit Television Digital Video Recording and Export Technologies

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.8172

March 2017

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

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

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) to perform the work described in this document and in the development of the Recommendation for Closed Circuit Television (CCTV) Digital Video Export Profile.

Abstract

The National Institute of Standards and Technology (NIST) in collaboration with the Federal Bureau of Investigation (FBI) conducted research to define and recommend an interoperable data solution to assist law enforcement in acquiring and analyzing digital video evidence from disparate systems. This document supplements the recommendation developed in NISTIR 8161 – "Recommendation: Closed Circuit Television (CCTV) Digital Video Export Profile – Level 0". This supplement describes the research activities, methods, and results that led to the recommended standards profile. It also provides web links to the sample files used to conduct the research and validate implementation of the recommendation.

NIST welcomes and seeks continued industry and other stakeholder comments concerning the initial (Level 0) recommendation and potential future enhancements. NIST looks forward to identifying and working with the pertinent standards community to move the recommendation into a formal standard that becomes adopted widely by industry.

Keywords

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

Table of Contents

1 Introduction 1
1.1 Purpose and Scope 1
1.2 Technical Approach 2
1.3 Organization of this Document 3
2 Terms and Definitions 4
3 Industry Outreach 7
3.1 Introduction 7
3.2 Trade Show Attendance 7
3.2.1 ISC East – November 18-19, 2015 7
3.2.2 ISC West – April 6-8, 2016 7
3.2.3 ISC East – November 16-17, 2016 9
3.3 Summary and Next Steps 10
4 DVR Manufacturer Published Capabilities 11
4.1 Technical Approach 11
4.2 Summary of Results 11
4.3 Observations and Findings 12
5 CCTV DVR Technology Investigation Laboratory 13
5.1 Laboratory Purpose 13
5.2 CCTV DVR Selection Strategy 13
5.3 Playback Station 14
5.4 Observations and Findings 14
6 Underpinnings Study – Demonstrated DVR Capabilities 15
6.1 Technical Approach 15
6.2 Summary of Results 16
6.2.1 GUI Inspection 16
6.2.2 Onboard Inspection 16
6.2.3 Export File Inspection 17
6.3 Observations and Findings 17
6.3.1 GUI Inspection 17
6.3.2 Onboard Inspection 18

6.3.3 Export File Inspection 18
7 Video Player Software Study 19
7.1 Technical Approach 19
7.2 Summary of Results 20
7.3 Observations and Findings 21
8 Conclusions Supporting NIST Video Export Recommendations in NISTIR 8161 22
8.1 MP4 Video File Container 22
8.2 H.264 Advanced Video Coding 22
8.3 MISB Precision Time Stamp 23
8.4 DVR System Clock Offset Metadata 24
9 References 26
Appendix A - Table of DVR Manufacturers' Published Capabilities 27
Appendix B - Tables of Demonstrated DVR Capabilities by Device 28
Appendix C - Investigation of H.265 Readiness for Recommendation 33
C.1 H.265 Profiles 33
C.2 H.265 Bitstream 34
C.3 Standard Adoption 35
C.4 SEI Message Support 35

1 Introduction

Video evidence from Closed Circuit Television (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 for subsequent review [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 interchange data format will expedite the collecting of evidence from multiple systems and improve the processing of the information.

The National Institute of Standards and Technology (NIST) in collaboration with the Federal Bureau of Investigation (FBI) conducted research to define and recommend an interoperable data solution to assist law enforcement in acquiring digital video evidence, improving forensic processes and techniques, and bridging the gap between CCTV systems and downstream investigators. The overall aim was increase the evidentiary value and timeliness of CCTV video data, and facilitate interoperable data sharing.

1.1 Purpose and Scope

This document is intended as a supplement[1] to the interoperability data solution in [NISTIR-8161] to describe and document the applied research that led to the recommendations put forth, which may be summarized as the use of:

- MP4 video file container [MP4]
- H.264 advanced video compression [H264-ISO & H264-ITU]
- Motion Imagery Standards Board (MISB) precision time stamps [MISB][2]

[1] Additional information and resources, including the example video files referenced in Section 7 of this document, can be obtained at https://www.nist.gov/programs-projects/digital-video-exchange-standards

[2] NISTIR 8161 also recommends a time mode-source code to be recorded with each MISB precision time stamp.

- DVR system clock offset metadata[3]

This activity was focused on defining a standards-based, interoperable, syntactic data solution to assist law enforcement in acquiring surveillance video evidence 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. How the video is captured and stored inside the CCTV system as well as standard operating procedures and best practices are not directly in scope. Semantic properties (e.g., parameters governing data quality and fitness for use) relating to the data collected are also out of the current scope and are deferred to future standardization efforts.

1.2 Technical Approach

Four primary elements comprise the technical approach of this digital video export profile project:

- Hands-on technology investigation and discovery
- Identify existing standards
- Build community (Law Enforcement, Industry, & Standards Development Organizations)
- Promote adoption

Figure 1-1 provides a more detailed visualization of this approach. NIST defined the video data export problem and minimum requirements to achieve data exchange interoperability. NIST then conducted a representative technical market survey of the range of CCTV Digital Video Recorders (DVR) product offerings and did not find any products that met the minimum requirements. NIST also surveyed existing CCTV video recording standards and could not identify any one standard that addressed each of the minimum requirements identified; however, it appeared that several standards implemented together in the form of a "standards profile" could likely meet many of the requirements. Simultaneously, NIST began building a community of law enforcement, industry, and standards development organization stakeholders to discuss the fundamental problem identified and the feasibility of potential solutions; the thought was that this same community could be contacted in the future to help promote adoption of a recommended solution. To gain hands-on experience with CCTV DVR interfaces and technical capabilities, and to verify vendor technical specifications, NIST acquired four sample DVRs; they were operated and analyzed in the lab in conjunction with both commonly available video player software and proprietary CCTV DVR vendor-provided software. A standards profile was then configured that addressed the minimum requirements. A reference video file was created to demonstrate implementation of the profile. The video portion of this file was demonstrated to be playable by the commonly available software players. (Note that player software enhancements would be needed to make use of the metadata components added.) NIST began discussing the proposed solution with members of the stakeholder community to gauge feasibility and support.

[3] The recommendation for DVR system clock offset metadata is based on the Extensible Metadata Platform standard [XMP1 & XMP3].

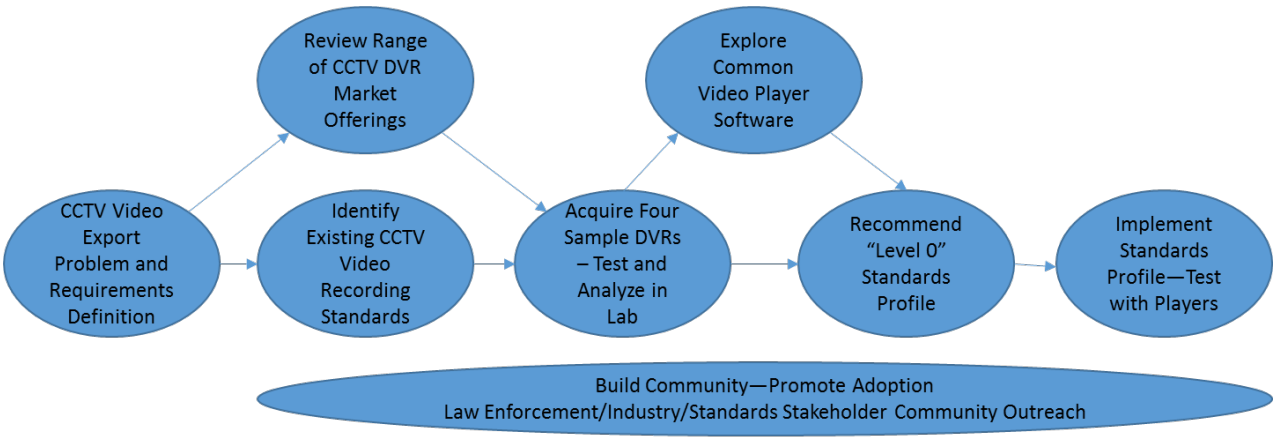

Figure 1-1. Visualization of Technical Approach

1.3 Organization of this Document

The main sections of this document summarize the primary research performed and most important findings. Appendices provide additional detail and background information.

Section 2 lists key acronyms and terms, as well as relevant file type and video resolution definitions. Section 3 describes the industry outreach conducted by NIST to gain suggestions and feedback and ensure that any recommendations proven in the laboratory were, in fact, feasible for product implementation and would be beneficial to industry. Section 4 provides the manufacturers' published capabilities of various CCTV DVR models, as well as the four laboratory models purchased by NIST to investigate the capabilities and operational configuration of commercially available products. Section 5 describes the NIST laboratory configured and outfitted to investigate and demonstrate current CCTV DVR technologies and data export approaches. Section 6 describes the capabilities of these products as exercised by NIST researchers. Section 7 provides the results of a video player software study conducted to demonstrate that a reference implementation of NIST's recommended video export profile could be played as intended by popular player software. Section 8 describes how the findings of the research conducted led to each of the video export profile recommendations put forth in NISTIR 8161. Section 9 cites references that were used in this work. Appendices provide tables of manufacturer-provided DVR capabilities, NIST-demonstrated DVR capabilities, and background information on the H.265 video compression standard.

2 Terms and Definitions

Table 2-1. Acronyms and Terms

CCTV	Closed Circuit Television – a CCTV system typically includes a DVR and one or more video cameras
codec	Compression/Decompression - a means for encoding or decoding a digital data stream.
DVR	Digital Video Recorder
FAT32	File Allocation Table
FBI	Federal Bureau of Investigation
GB	Gigabyte
GUI	Graphical User Interface
IDR	Instantaneous Decoder Refresh
IP	Internet Protocol
ISC	International Security Conference
ISO	International Organization for Standardization
ITU	International Telecommunication Union
JTC-VC	Joint Collaborative Team on Video Coding
MISB	Motion Imagery Standards Board
MJPEG	Motion 'Joint Photographic Experts Group' (compression standard)
MPEG	Moving Picture Experts Group
MPEG-LA	Moving Picture Experts Group – License Agreement
NAL	Network Abstraction Layer
NGA	National Geospatial-Intelligence Agency
NIST	National Institute of Standards and Technology
NTSC	National Television System Committee – video standard used in North America and most of South America.
ONVIF	Open Network Video Interface Forum
PAL	Phase Alternating Line – color encoding system for analog television used in broadcast systems in most countries
PCP	Primary Coded Picture
PPS	Picture Parameter Set
QVGA	Quarter Video Graphics Array
SEI	Supplemental Enhancement Information
SIA	Security Industry Association
SPS	Sequence Parameter Set
TB	Terabyte
USB	Universal Serial Bus
UUID	Universally Unique Identifier
VGA	Video Graphics Array
XML	Extensible Markup Language
XMP	Extensible Metadata Platform
720P	HD resolution with progressive scan – 1280 x 720
1080P	Full HD resolution with progressive scan – 1920 x 1080

Table 2-2. File Type Definitions

File Name	Description
ASF	The Advanced Systems Format is a Microsoft proprietary digital audio and digital video container format used for streaming media. It does not specify how the video should be compressed but specifies the structure of the video and audio steam. Metadata such as title, author, and copyright bibliographic data may be included.
AVI	The Audio Video Interleaved file format was introduced in the early 1990s by Microsoft as part of its Video for Windows technology. It is an older file container format supporting both audio and video and the playback of both streams.
AVI Subtitles	The AVI file and the *ums decoder filter* file are exported to the same directory location. The *ums decoder filter* file is needed for playback.
DAV	This is an encrypted file format created by a DVR365 digital video recorder and used to capture video from CCTV cameras. The video captured by the cameras is saved to the recorder in a modified MPEG file format and encrypted. Playback requires the DVR365 player software.
H.264 (MPEG-4 Part 10, MPEG-4 AVC)	The Advanced Video Coding (AVC) format is currently one of the most commonly used formats for the recording, compression, and distribution of video content. Uses include streaming broadcast and optical media.
H.265 (MPEG-H Part 2)	High Efficiency Video Coding (HEVC) - one of several possible successors to H.264.
MP4 (MPEG-4 Part 14)	This is a digital multimedia container format most commonly used to store video and audio, but can also be used to store other data such as subtitles and still images. MP4 is an open standard that was based on the QuickTime format specification. This open format is supported by a variety of players and tools across different operating systems.
NSF	Proprietary format. This is an exclusive video format. Playback requires an HD player exported along with this video stream or the DVR player.
TS (MPEG-TS, MTS)	This transport stream is a standard digital container format for transmission and storage of audio, video, along with programming and system information. A TS file specifies a container format encapsulating packetized elementary streams, with error correction and synchronization features.

Table 2-3. Resolution Definitions

Format	Definitions	NTSC (pixels)	PAL (pixels)
QCIF	Quarter Common Intermediate Format -1/4 of the CIF Resolution	176 × 120	176 × 144
CIF	Common Intermediate Format – Also known as Full CIF	352 x 240	352 x 288
2CIF	2 times Common Intermediate Format	704 x 240	704 x 288
4CIF	4 times Common Intermediate Format	704 x 480	704 x 576
HD1	Half of D1 resolution	352 x 480	352 x 576
D1	Same Resolution as 4CIF	704 x 480	704 x 576
960H	Format requiring support from both the DVR and cameras	960 x 480	960 x 576
WD1	Wide D1	960 x 480	960 x 576

3 Industry Outreach

3.1 Introduction

While working to develop a technically sound, standards-based solution for video export interoperability, NIST researchers engaged industry stakeholders to obtain their suggested approaches and also ensure that any NIST recommendations proven in the laboratory were, in fact, feasible for product implementation. The aim was to align with current industry practice to the extent possible to minimize implementation cost and encourage manufacturer adoption. To this end, NIST attended three industry trade shows that are well-attended by the video surveillance security industry – the Security Industry Association (SIA) (http://www.securityindustry.org/) International Security Conference (ISC) East 2015, ISC West 2016, and ISC East 2016. Historically, ISC East has drawn around 200 security industry exhibitor vendors, whereas ISC West has been approximately five times larger, attracting about 1000 such exhibitors.

3.2 Trade Show Attendance

3.2.1 ISC East – November 18-19, 2015

Attendance at this conference permitted NIST to engage video surveillance vendors, articulate law enforcement stakeholder needs, and introduce the goals of this project. It was described how industry adoption of open standards for data formats, interfaces, and transport protocols would greatly improve the evidentiary value and timeliness of video data for law enforcement. A written project summary and NIST contact information were distributed. NIST was also able to gain a good appreciation for the video surveillance and DVR products available and their approach to video file export and time stamping. Overall, most of the vendors engaged responded positively to the objectives of the project. They thought there was a viable solution and indicated a willingness to help. A contact list was developed for future reference.

3.2.2 ISC West – April 6-8, 2016

ISC West offered a wider variety and more comprehensive group of vendors to engage ranging from codec electronic circuit manufacturers to DVR manufacturers to full end-to-end video surveillance system manufacturers and integrators. By the time of ISC West, NIST had drafted a preliminary technical solution for standards-based video export and time stamping. Interested vendors were provided with a double-sided half-page handout that illustrated NIST's draft solution, the project's guiding principles, key questions for industry, and NIST contact information. NIST updated and expanded its industry contact list for future reference. Law enforcement stakeholder needs were expressed as shown in Table 3-1.

Table 3-1. Summary of Video Export Interoperability Problems and Proposed Solutions

Problem	Solution
Too many flavors of export file (often proprietary)	Choose consistent standard output data format
Proprietary export files will not play on common video players	Choose standard output data format that is playable across common video players
Video quality in export often worse than onboard video quality	Wrap native-quality onboard bitstream in export file without degrading
Data and time often missing in export	Embed a standard precision timestamp within bitstream frames

At the time of ISC West, NIST's draft solution could be summarized as follows:

- Container file – MPEG-2 Transport Stream (*.ts)
- Video stream – H.264 (MPEG-4 Part 10)
- Supplemental Enhancement Information (SEI) messages used to embed a precision time stamp in each H.264 video frame

This led NIST to ask the following key questions to each of the vendors engaged. The consensus responses to each question is indicated below the question.

- What standardized container file would be best to use?
    - Most vendors suggested AVI. NIST noted that AVI is a Microsoft de-facto industry standard and not one developed and managed by an accredited standards development organization.
    - Concerning MPEG-2 Transport Stream, most vendors indicated that this format was acceptable but not all that commonly used; MPEG-4 was suggested as an alternative.
- Are SEI messages suitable for embedding a precision time stamp in each video frame?
    - Most vendor representatives were not sure about this question and said they would need to check further with their technical experts.
- Is the use of Epoch time to convey precision time acceptable?
    - This approach was deemed acceptable.
- Is the proposed standards profile too complex or too costly to implement?
    - In general, the vendor representatives did not think the draft solution was too complex or too costly to implement; however, each vendor's engineering team would need to analyze further to see if any performance degradation was likely.
- Might the draft solution require a redesign of the codec chipsets used?
    - Most vendor representatives who could address this question said that further engineering analysis would be required. However, they believed that metadata (time stamp) injection could be performed off-chip, after video encoding, using firmware or software, and thus not require chipset redesign. There will be a performance limit that determines how much metadata can be injected. The larger vendors tend to use their own System on Chip chipsets, whereas other

vendors use more commodity designs from specialized integrated circuit manufacturers.

The responses to the above questions and the positive reactions to NIST's overall approach led to keeping all aspects of the draft solution as is except for use of the MPEG-2 Transport Stream container file. Following the trade show, NIST researched use of MP4 container files and determined that this would be a viable solution. MP4 then replaced MPEG-2 Transport Stream in the proposed solution.

3.2.3 ISC East – November 16-17, 2016

Several months before this trade show, the FBI introduced a new requirement to record in the exported video file the Export System Time (i.e., time on the DVR system clock) and an External Reference Time. Following significant research, a standards-based approach was developed to address this requirement. At the time of this conference, NIST's draft solution was summarized as follows:

- Container file – MP4 (MPEG-4 Part 14)
- Video stream – H.264 (MPEG-4 Part 10)
- Supplemental Enhancement Information (SEI) messages used to embed a MISB (Epoch) precision time stamp in each H.264 video frame
- Export System Time and External Reference Time stored in an MP4 container file using a Universally Unique Identifier (UUID) Box containing an Extensible Metadata Platform (XMP) packet

NIST engaged relevant vendors and provided background for the digital video export interoperability project and described NIST's revised proposed solution. A written two-page summary of this information and NIST contact information was distributed. An interesting side note was that when meeting one of the vendor representatives who was engaged at ISC West, he recalled the ISC West conversation and produced from a small portfolio of papers he was carrying the very handout he was given at ISC West.

Given the current stage of the project, two key questions were asked:

- Is the proposed solution feasible? Consider level of complexity and cost to implement.
    - The consensus response was that the proposed solution was feasible and that the solution would likely not be too complex or too costly to implement. Further engineering analysis by each vendor would be required to confirm.
- What do you see as potential barriers to adoption?
    - Generally, no major barriers were cited.

There appeared to be a trend that the large vendors providing end-to-end systems and services were less interested in inter-system interoperability. One large vendor said that they did not accept videos from other vendors' systems. The vendor went on to say that they integrate with all video cameras; but, when it comes to videos captured on other systems, the other vendors do not implement many of the special features, including anti-tampering security mechanisms, that

this vendor does via their own proprietary format. As might be expected, vendors whose main business was providing video analytic services appeared to be the most interested in NIST's proposed standard for video export interoperability.

One additional note was that many of the vendors viewed the Open Network Video Interface Forum (ONVIF) as the key standards developer for the video surveillance industry and suggested that NIST work with ONVIF to move the recommended standards profile to a formal standard. ONVIF describes itself as "a non-profit organization of nearly 500 members driving the development of open global standards for effective interoperability of IP-based physical security products."

3.3 Summary and Next Steps

The industry outreach described above was important in assuring that NIST's initial work was on track towards developing a video export interoperability standard that would be feasible to implement, cost-effective, and amenable to industry. Continued industry engagement helped to shape, in a specific fashion, the final recommendation put forth, namely, the use of an MP4 container file.

NIST welcomes and seeks continued industry and other stakeholder comments concerning the initial (Level 0) recommendation and potential future enhancements. NIST is planning continued industry and stakeholder engagement, and looks forward to identifying and working with the pertinent standards community to move the recommendation into a formal standard that becomes adopted widely by industry.

4 DVR Manufacturer Published Capabilities

4.1 Technical Approach

Before purchasing DVR systems for hands-on investigation, the NIST research team conducted a documentation study to better understand the features and capabilities of common CCTV DVR products. A list of manufacturer products was compiled based on sponsor recommendations. Using this list as a reference, a spreadsheet of product specifications was compiled from information obtained from each vendor's website. The resulting spreadsheet was not intended to be an exhaustive list of DVRs found on the open market, but rather a sufficient representation from which to base the purchase of the laboratory systems used in this research.

4.2 Summary of Results

Table 4-1 provides a subset of the DVR features listed in Appendix A. To maintain manufacturer and product model anonymity, each manufacturer's name has been coded as D1, D2, …, Dn and product model number as M1, M2, …, Mn.

Table 4-1. Summary of Key DVR Features by Manufacturer (D#) and Model (M#)
(Highlighted rows indicate laboratory DVR models acquired for hands-on investigation)

COMPANY	MODEL	DRIVE SIZE	CHANNELS	COMPRESSION	Recording Resolution	USB
D1	M1	**1TB**	**4**	**H.264**	**D1; CIF; 960H**	USB 2.0
D1	M2	1-4TB	4	H.264	D1; 4CIF; CIF; QCIF	USB 2.0
D2	M1	**500GB**	**4**	**H.264**	**D1; HD1; CIF**	USB 2.0
D2	M2	1-3TB	8	H.264	720P	USB 2.0
D3	M1	**1TB**	**4**	**H.264**	**1080p; 720p; 960H; D1; HD1; 2CIF; CIF**	USB 2.0
D3	M2	2-8TB	4	H.264	720P; 1080P	USB 2.0
D4	M1	**1TB**	**16**	**H.264**	**D1; CIF; 960H**	USB 2.0
D5	M1	1-4TB	4	H.264	Main stream: 1080P; 720P; VGA; WD1; 4CIF; CIF Sub-stream: WD1; 4CIF; CIF; QCIF; QVGA	USB 2.0
D6	M1	NA	16	H.264/M-JPEG	480NTSC/400 PAL(2CIF) 480NTSC/400PAL(CIF)	USB 2.0
D7	M1	NA	8	H.264	NTSC: 960H; 720 x 480 PAL: 960H; 720 x 576	USB 2.0
D8	M1	1-4TB	16	H.264	1080P; 720P; 960H; D1; 4CIF; CIF; QCIF	USB 2.0
D8	M1	500GB	8	MPEG-4, MJPEG	NA	NA
D10	M1	1-4TB	4	H.264 High profile	1080P; 1080P; 720P	USB 2.0
D11	M1	NA	16	H.264	CIF; 2CIF; D1	N/A
D12	M1	up to 8TB	8	H.264	1080P; 720P; 960H; D1; 4CIF; CIF; QCIF	USB 2.0
D13	M1	NA	24	H.264 High profile	960H; D1; CIF	USB 2.0
D14	M1	1TB	8 -16	H.264	CIF; 2CIF; 4CIF	USB 2.0
D15	M1	NA	8	H.264	1080P / 60 Hz 1280 × 1024 / 60 Hz 720P / 60 Hz 1024 × 768 / 60 Hz	N/A
D16	M1	up to 32TB	16	H.264	D1; HD1; 2CIF; CIF; QCIF	USB 2.0
D17	M1	500GB-2TB	8	H.264/MJPEG	1080P	N/A

4.3 Observations and Findings

After completing this review of DVR features, it was clear that many of the CCTV systems offered the same capabilities, for example, support for similar interoperable camera qualities. Each of the systems supported H.264 compression, and USB 2.0 for video export to external drives. Each system studied had an internal hard drive with storage capacity as much as eight terabytes. This data collection and analysis provided insight into the current state of CCTV surveillance technologies. The knowledge gained guided purchase decisions of four laboratory devices highlighted in the table above.

5 CCTV DVR Technology Investigation Laboratory

This section describes the Technology Investigation Laboratory configured and outfitted to demonstrate and study current CCTV DVR technologies and data export approaches.

5.1 Laboratory Purpose

The investigation laboratory was built to enable applied research in which each DVR device was examined according to its constituent components in a controlled manner. Each device's GUI, hard drive, and data export process was studied.

The initial challenge was to purchase the DVRs within budgetary constraints. A broad range of design factors were observed to impact system cost:

- Number of cameras
- Quality of cameras
- Number of channels supported
- Size of onboard or external storage
- User interface
- Remote network access

Prices for CCTV systems ranged anywhere from $350 to millions of dollars.

5.2 CCTV DVR Selection Strategy

NIST desired to investigate CCTV technologies that are typically encountered in law enforcement investigations. The selection of CCTV systems for the research investigations was shaped by guidance provided by NIST's project sponsor. Following this guidance, various DVR model vendor specifications were assembled into a spreadsheet (see Table 4-1) and commonalities and differences across devices were analyzed. It became clear that all of the devices regardless of cost had similar external and internal design features, so it was determined that purchasing low- and mid-range priced systems was suitable for this research.

Four CCTV DVR systems were acquired for investigation. They are highlighted in Table 4-1 with the designation D1M1, D2M1, D3M1, and D4M1. Each system purchased was priced below $3000.

5.3 Playback Station

The NIST CCTV DVR Technology Investigation Lab was created to facilitate video captures and playback tests that were consistent and repeatable across the systems examined. Central to the laboratory was the video playback station shown in Figure 5-1. The station was configured with multiple cameras (seen on the left) to enable laboratory DVR devices (seen on the right) to capture the same calibrated video segment simultaneously from a high resolution computer monitor. Each video capture playback segment was timed to ensure consistency.

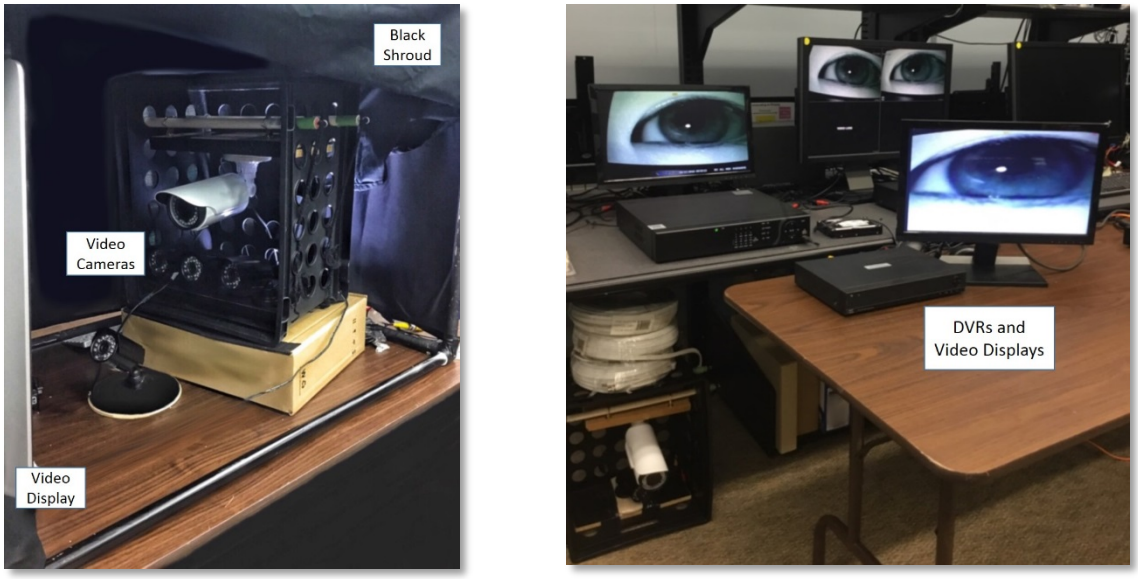

Figure 5-1. DVR Technology Investigation Lab Setup

5.4 Observations and Findings

The methodology deployed in the lab proved successful. The lab configuration allowed for repeatable and measurable test results. Data was collected on each DVR device simultaneously by using the same capture input process. The video data captured by each DVR was then exported and examined for consistency and playability.

The implementation of the playback station aided in verifying one major aspect of each device, namely that all the DVRs tested produced H.264 compressed video. This finding was a catalyst in moving the work forward in the direction of an interoperable solution. With all the devices supporting H.264, a standard solution at a fundamental level was determined achievable.

6 Underpinnings Study – Demonstrated DVR Capabilities

An underpinnings study was conducted to determine if and how specific data is stored on and exported from each of the four laboratory systems. Each system was studied using the *vendor-provided GUI* to determine recording control settings that impacted the data at the byte level when stored to the internal hard drive. It was important to understand these settings when analyzing the captured video and exported video.

Following the GUI study, an *onboard inspection* was conducted that focused on how data from video captures was written to each system's hard drive. Each hard drive was examined at the byte level to verify that H.264 with Supplemental Enhancement Information (SEI) messages existed in the video streams. In addition to the H.264, the video bitstream was analyzed for additional identifiable metadata (time stamp, camera type, location settings) that is of value in an event investigation.

The final focus of this study was to determine how video captures are represented when they are exported off the systems. An examination of the *exported video files* (of various container types) was done to look for any indication of H.264 along with the metadata of interest.

6.1 Technical Approach

The results of this study were based on a review of video captures from the systems as influenced by their recording settings. A visual inspection of the recording settings for each device determined the amount of control a user had in selecting and storing information about each video capture. The video was captured for a set time interval using the playback station and similar settings were chosen across the systems for consistency and comparison.

Once a video was recorded, byte level verification was performed to examine the DVR hard drives for H.264 encoding and metadata. Each hard drive was removed from its DVR and attached to a computer using a forensic hardware write blocker. The hard drive was mounted as an external drive to the host computer allowing access to the stored data. Using a hex editing tool, NIST researchers were able to manually carve out identifiable H.264 video segments from the hard drive. The segment of data containing video was identified by a starting hex value of 00 00 00 01 and by an ending value of FF FF FF FF. The H.264 stream was analyzed using a bitstream analyzing tool to determine if the carved video was well formed. This analysis also was used to determine if SEI messages were included as part of the stream.

The final stage of this study documented information about the video captures once they were transferred off the DVRs to external media. Each system provided support for moving a video capture off the system to a backup device. The backup function settings were controlled through the GUI allowing a user to select from a list of possible export file container types. All of the CCTV DVR systems supported the capability to attach a USB 2.0 external hard drive for backup purposes.

For each laboratory DVR, an external backup hard drive was attached and formatted according to the file system supported by the DVR. In all cases examined, the file system was FAT32. Once a backup hard drive was formatted and mounted, the video was exported from the onboard DVR hard drive using the backup choices available for each system. Each USB backup drive was then mounted on a computer and the exported files were analyzed for H.264 with SEI messages and metadata. Each of the video export files were examined using the tool *MediaInfo* (http://mediaarea.net/en/MediaInfo) to identify the video compression codec. Following the metadata analysis, the files were demultiplexed to separate the encapsulated data streams. The separated video streams were studied using a H.264 bitstream analyzer tool (https://github.com/aizvorski/h264bitstream) to locate and identify any SEI messages and metadata.

6.2 Summary of Results

Appendix B provides details of the capabilities observed and tabulated for each of the DVRs examined in this study. The sub-sections below summarize the observations.

6.2.1 GUI Inspection

Analysis was conducted using each DVR system's GUI to see if there was any indication of the H.264 capture and other relevant metadata. Each system GUI identified a video capture using a system-specific time stamp format. One of the DVRs provided a user-controlled selection drop-down list of potential camera models. Table 6-1 summarizes information and other metadata displayed through the GUI.

Table 6-1. DVR System Information Displayed via GUI

DVR_ID	Model_ID	H.264	SEI Messages	Time Stamp	Time Source	Camera ID
D1	M1	No	No	Yes	No	No
D2	M1	No	No	Yes	No	No
D3	M1	Yes	No	Yes	No	No
D4	M1	No	No	Yes	No	Yes

6.2.2 Onboard Inspection

Table 6-2 shows the results from the investigation of the video captures as they were stored onboard each DVR's hard drive. Each system supported H.264 and all but one had SEI message types embedded in the video stream. Time stamp, time source, and camera ID metadata were not observed within the onboard video stream. These types of metadata, if recorded, must have been stored elsewhere within the DVR system.

Table 6-2. Onboard Inspection of Recorded Video by DVR

DVR_ID	Model_ID	H.264	SEI Messages	Time Stamp	Time Source	Camera ID
D1	M1	Yes	Yes	No	No	No
D2	M1	Yes	Yes	No	No	No
D3	M1	Yes	Yes	No	No	No
D4	M1	Yes	No	No	No	No

6.2.3 Export File Inspection

As shown in Table 6-3, all four DVR systems exported at least one type of video file containing an H.264 video stream. Three of the four systems also exported video files containing SEI messages. Time stamp, time source, and camera ID metadata were not present in any of the exported files. The DAV file type listed in the table is a proprietary format, so its content was not readily verifiable and the resulting observations listed as "Unknown".

Table 6-3. Exported File Characteristics by DVR

DVR_ID	Model_ID	File Type	H.264	SEI Messages	Time Stamp	Time Source	Camera ID
D1	M1	NSF	Yes	Yes	No	No	No
D1	M1	AVI-subtitle	Yes	Yes	No	No	No
D1	M1	AVI	Yes	Yes	No	No	No
D2	M1	AVI	Yes	Yes	No	No	No
D3	M1	ASF	Yes	No	No	No	No
D3	M1	DAV	Unknown	Unknown	Unknown	Unknown	Unknown
D4	M1	NSF	Yes	Yes	No	No	No
D4	M1	AVI	Yes	Yes	No	No	No

6.3 Observations and Findings

6.3.1 GUI Inspection

Examination of each laboratory DVR showed all contain similar user interface features with consistent recording settings, export options, and video captures that were divided into onboard segments using a built-in calendar-based layout design. The intuitive construction of these interfaces made for ease of selection and export of video data.

Specific findings were as follows:

- The D3M1 GUI identified H.264 as the lossy compression algorithm.
- The D4M1 GUI presented the user with a drop down list of '*camera types.*'
- Date and time were used to identify the duration of a video capture.

6.3.2 Onboard Inspection

Following video capture, each hard drive was removed from its system and separately analyzed by carving, collecting, and analyzing the format and content of the video data. Upon analysis, all the hard drives had evidence of H.264 encoded video.

Specific findings were as follows:

- All the onboard disk drives contained H.264 video data.
- For three of the four DVR systems, video segments were successfully carved and demonstrated playable using *ffmpeg* (http://ffmpeg.org/).
- The bitstream analyzer tool used indicated that embedded SEI messages were present in the H.264 stream on three of the four systems.

6.3.3 Export File Inspection

All the DVR systems allowed for backup to external media over USB 2.0. Before exporting the video data, the external media needed formatting applied by the specific system. All the exports were identified by a file name that included date and time. The choice of file export was driven by the user interface selection unique to each device.

Specific findings were as follows:

- Three of the four DVR systems provided multiple export file formats.
- All exported files were named using recorded date and time.
- Three of the four DVR systems supported a proprietary file format that required a proprietary player. (In this case, an export included both a video clip in the proprietary format along with an executable player application.)
- All of the export file containers supported H.264, with the exception of the proprietary DAV file container which could not be verified.

7 Video Player Software Study

A critical requirement for video interoperability is for the exported video files from CCTV surveillance systems to be readably viewable by law enforcement investigators and judicial officials. To this end, a video player study was conducted to test the playability of a variety of digital video file formats on common video players across popular operating systems.

7.1 Technical Approach

NIST researchers collected sample video files from the laboratory DVR systems as well as from external open sources representing a variety of file types of particular interest listed in Table 7-1.

A selection of common video players, natively installed on several different operating systems were used to determine support for the sample collection of video container files. The video players used in testing were VLC (VideoLAN Organization), Windows Media Player (Microsoft) and QuickTime (Apple Computer) running on various versions of Microsoft Windows and Mac OS X. An attempt was made to open and play each of the video files with each of the players and results were tabulated (shown in Table 7-2) as to whether playback was successful.

Table 7-1. Digital Video File Formats Studied

File ID	Source	Extension	Video Compression	SEI Embedded
F1	**D3M1**	.dav	Unknown	No
F2	**D1M1**	.h264	H.264	Yes
F3	**D3M1**	.asf	H.264	No
F4	**D1M1**	.avi	H.264	Yes
F5	**MISB**	.mpg	H.264	Yes
F6	**MISB**	.ts	H.264	Yes
F7	**WEB1**[4]	.mp4	H.264	Yes
F8	**WEB2**[5]	.mp4	H.265	No
F9	**WEB3**[6]	.mp4	H.264	Yes

Files F1 through F4 in Table 7-1 were exported by two of the laboratory DVR systems. (The H.264 file F2 was simply a raw video bitstream exported as part of a proprietary bundle from device D1M1.) File F5 is a sample file provided to NIST from the National Geospatial-Intelligence Agency (NGA), formatted as MPEG-TS, and containing embedded MISB compliant precision time stamps. The only difference between F5 and F6 is with the assigned file extension (".mpg" versus ".ts").

[4] H.264 Flower and Insect video (http://biometrics.nist.gov/cs_links/DVR_Standards/*web1.mp4*); original source at http://orangehd.com/blog/flower-and-insect/

[5] H.265 Clip0005 video (http://biometrics.nist.gov/cs_links/DVR_Standards/*web2.mpeg*); original source at http://www.cinemartin.com/cinec/samples/

[6] H.264 NIST Reference Implementation video (http://biometrics.nist.gov/cs_links/DVR_Standards/*web3.mp4*)

The remaining three video files are formatted as MP4, each containing a different video clip downloaded from an open internet source. File F7 contains an H.264 Advanced Video Coding (AVC) encoded bitstream [H264-ISO, H264-ITU]. File F8 contains an H.265 High Efficiency Video Coding (HEVC) encoded bitstream [H265-ITU].

Perhaps the most important file in this list is F9, as it is a prototype video file serving as a NIST reference implementation of all the interoperability recommendations made in NISTIR 8161. The contents of file F9 incorporates: a) an MP4 video file container, b) an H.264 encoded video stream, c) embedded MISB precision time stamps, and d) DVR system clock offset metadata.

7.2 Summary of Results

Table 7-2 summarizes the results observed when attempting to play each test video file on various versions of common video players. 'Yes' indicates the video file successfully played using the player indicated, while 'No' indicates the test file was not playable with the player indicated. The columns of the table are organized in three groupings (VLC, Media Player, and QuickTime) and ordered within each group left-to-right with new players and operating systems listed first progressing to older versions.

Table 7-2. Video Player Results

File ID	**VLC 2.2.1** on Windows 7 Enterprise	**Media Player 12** on Windows 10 Pro	**Media Player 12** on Windows 8 - 64 bit	**Media Player 12** on Windows 7 Enterprise	**Media Player 11.06** on Windows Vista Home Premium	**QuickTime 10.4** on Mac OS X 10.11.2	**QuickTime 10.3** on Mac OS X 10.95	**QuickTime 7.9** on Windows 7 Enterprise
F1	No	No	No	No	No	No	No	No
F2	Yes	No	No	No	No	No	No	No
F3	Yes	Yes	Yes	Yes	Yes	No	No	No
F4	Yes	Yes	Yes	Yes	Yes	No	No	Yes
F5	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
F6	Yes	Yes	Yes	Yes	No	Yes	Yes	No
F7	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
F8	Yes*	No	**	No	**	No	No	**
F9	Yes*	Yes	**	Yes	**	Yes	**	**

* VLC 2.2.2 Windows 7 Enterprise had replaced VLC 2.2.1 at the time the testing was conducted.
** Players no longer available at the time the testing was conducted.

7.3 Observations and Findings

The following observations are drawn from Table 7-2:

- File F9 (NIST's reference implementation video file) was supported by all the latest versions of players tested including VLC, Media Player, and QuickTime. This finding supports all the interoperability recommendations in NISTIR 8161.
- No non-proprietary video player supported file F1 – the DAV format. Only VLC supported file F2 – the NSF (raw H.264) video segment. The lack of player support for these files points to the need for industry adoption of an interoperable standards-based file format.
- In general, VLC was the most supportive of the test files, and Media Player was able to play more video file types than QuickTime.
- In general, newer versions of players and operating systems were supportive of more types of video files than older ones.
- The standard container formats (MPEG-TS and MP4) in conjunction with H.264 video encoding were supported by all the latest players, and the majority of players overall. This finding supports NIST's recommendation of the MP4 video file container.
- Only VLC supported file F8, the file with the H.265 encoded video stream. This finding helped guide NIST to recommend only H.264 encoding for export video interoperability, leaving consideration for including H.265 to the future, giving more time for wide-spread market adoption.

8 Conclusions Supporting NIST Video Export Recommendations in NISTIR 8161

NISTIR 8161 makes four key recommendations towards achieving interoperable CCTV digital video recordings. This report documents the research and decisions made in support of these recommendations, which is summarized below.

8.1 MP4 Video File Container

Section 4 describes the research that was carried out to compile and analyze published capabilities across a sampling of CCTV DVR systems produced by various manufacturers. As seen in Table A-1, there is widespread support for H.264 video encoding, and upon discussion with manufacturers[7], this H.264 support is most commonly realized through the use of AVI files. The prevalent use of AVI files is also observed by three out of the four laboratory DVR systems studied by NIST (see Appendix B). However popular, the AVI file format has not been formally standardized.

A search for viable standard video file formats led NIST researchers to the large family of MPEG standards. Initially the NIST team investigated the merits of the mature MPEG2 Transport Stream (MPEG-TS) format used heavily within broadcast media and military surveillance applications. The use of this format proved promising, though further consideration was given to the newer and more familiar MP4 format defined in MPEG-4 Part 14 [MP4]. MP4 is a digital multimedia format most commonly used to store video and audio, and can also store captions and metadata about the file. A file that adheres to the MPEG-4 Part 14 standard is typically identified with the file extension "mp4". The MP4 test files used in the video player software study described in Section 7 were well-supported across the suite of video players, and in the end MP4 was selected as the recommended video file container format.

8.2 H.264 Advanced Video Coding

For digital video interoperability it is important to not only specify the file container but also the format of the encoded video and supporting metadata therein. The family of MPEG-4 standards includes H.264, defined in MPEG-4 Part 10. H.264 is used to encode video streams in a compressed form reducing the overall size of the container file.

All the studies in this report show widespread CCTV DVR industry support for H.264 video encoding. The DVR manufacturer published capabilities listed in Section 4 revealed that all products researched supported H.264 compression. The results from the investigations in Section 5 showed all four laboratory DVR systems produced onboard H.264 compressed video. The underpinnings study in Section 6 demonstrated that all four laboratory systems had the option and capability of exporting at least one file type containing H.264 compressed video.

[7] Over the course of this research NIST held a series of one-on-one informative discussions with leading CCTV DVR manufacturers at the following security events: International Security Conference (ISC) East 2015, ISC West 2016, and ISC East 2016. (http://www.isceast.com and http://www.iscwest.com).

Finally, the video player software study in Section 7 demonstrated that H.264 compression in conjunction with the MP4 container was supported by all the latest video players (VLC, Media Player, and QuickTime).

Discovering broad product support for H.264 was critical to finding a recommended standards solution that represents lower cost for adoption by the CCTV DVR industry. This is why H.264 was a major focus of this research.

8.3 MISB Precision Time Stamp

This research identified fundamental gaps in metadata that are useful to law enforcement investigations. A critical data element that is currently lacking in video captured by surveillance systems is a standard format for date and time linking captured video to an event, referred to as the time stamp. This gap is seen in the underpinnings study in Section 6, where NIST researchers found no embedded time stamps in exported video files from the four laboratory DVR systems. (Note that time stamps were observed in operating the DVR systems via the manufacturer's GUI, and time stamps were embedded in the names of exported video files; yet, no time stamps were detected within the exported video streams themselves.)

Searching for a standards solution for embedded time stamps, NIST researchers held discussions with government video experts (e.g., National Geospatial-Intelligence Agency), standards developing organizations (e.g., Motion Imagery Standards Board), and CCTV DVR developers. This led to consideration of MISB 604.3, "Time Stamping Compressed Motion Imagery," which prescribes a bit-packed embedding of precision data and time within every frame of a video stream as illustrated in Figure 8-1. As shown in the figure, NISTIR 8161 recommends two types of messages. The first is the MISB precision "Time Stamp", and the second is a "Time Source" message defined by NIST that records the timing source (e.g., network) and the mode in which the time was recorded (e.g., auto). By embedding timing metadata within each video frame, if a video file is ever damaged where only part of the video stream is recovered, the fragment will still be time-referenced.

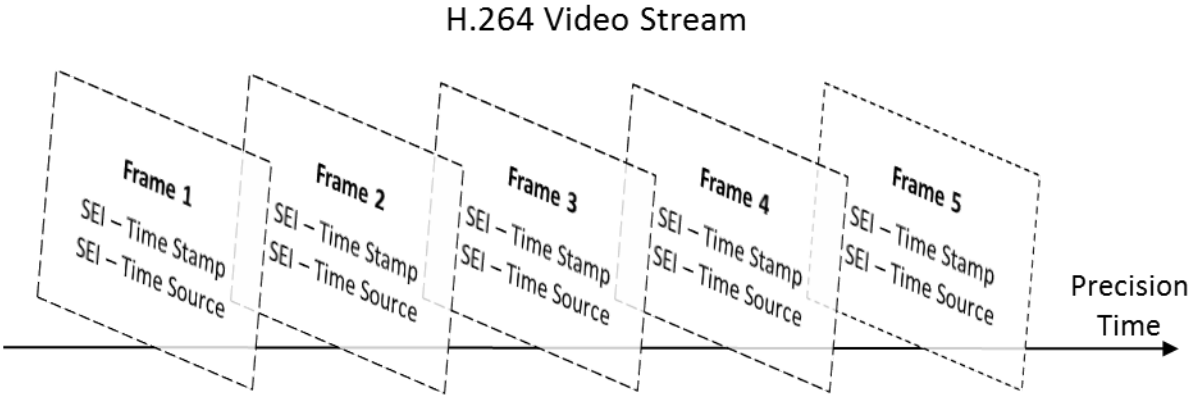

Figure 8-1. Example H.264 Bitstream with Time Stamp Metadata

The MISB time stamp standard embeds date and time information into an H.264 video stream using standard payload units called Supplemental Enhancement Information (SEI) messages. The underpinnings study in Section 6 revealed all four laboratory DVR devices leveraged SEI messages in some fashion within onboard video streams and/or in exported video files. (Note that none of the observed SEI messages were MISB time stamps, but rather messages used for internal device purposes and not deciphered by NIST.) This indicates common general use of SEI messages among DVR developers. All the latest video players studied in Section 7 played MP4/H.264 video files containing SEI messages without any errors or warnings. More importantly, all the latest players successfully played the NIST reference implementation file (file F9 in Table 6-2) embedded with SEI messages containing MISB precision time stamps and Time Source metatdata.

Discovering common use of SEI messages by industry, and observing universal playability of MP4/H.264 video files containing SEI messages was essential to the NIST recommendations for time stamp metadata.

8.4 DVR System Clock Offset Metadata

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 a best practice, discrepancy with the CCTV system clock should be observed at the time the video data is exported and used to support investigative analysis later [SWGIT2].

As the NIST team researched a potential solution, attention was initially focused on the MPEG-7 multimedia content description standard (ISO/IEC 15938) which was created in 2002 and continued to be developed and expanded up to 2011. Further investigation determined that while a comprehensive standard, MPEG-7 has limited adoption and use.

Continuing research led to an alternative video metadata standard, XMP, originally created by Adobe and defined in ISO 16684. According to this standard, an XMP packet can be defined to encode metadata using an XML data model and core namespaces [XMP1]. An XMP packet can be embedded within an MP4 export video by encapsulating the packet within a standard MP4 UUID box structure and adding it to the end of the file [XMP3].

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). The clock offset is calculated as the difference between these two time observations. NISTIR 8161 recommends both of these observed times be recorded in an XMP packet, each with a corresponding time mode-source code, and the packet be embedded in a UUID box at the end of the MP4 video export file.

The video player software study in Section 7 demonstrated that all the latest video players (VLC, Media Player, and QuickTime) are able to play the NIST reference implementation file (file F9 in Table 7-2) containing an XMP packet with DVR system clock offset metadata.

9 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
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
NISTIR-8161	Garris, Michael, et al. "Recommendation: Closed Circuit Television (CCTV) Digital Video Export Profile – Level 0," National Institute of Standards and Technology, Interagency Report Number 8161, December 2016. https://doi.org/10.6028/NIST.IR.8161
OZER	Ozer, Jan. "The Future of HEVC: It's Coming, but with Plenty of Questions." Streaming Media Magazine. April/May 2013. http://www.streamingmedia.com/Articles/Editorial/Featured-Articles/The-Future-of-HEVC-Its-Coming-but-with-Plenty-of-Questions-89010.aspx
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/
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
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 - Table of DVR Manufacturers' Published Capabilities

Table A-1. Table of DVR Manufacturers' Published Capabilities

COMPANY	MODEL	DESCRIPTION	PROCESSOR	OS	STORAGE	DRIVE SIZE	CHANNELS	COMPRESSION	RECORDING RESOLUTION	USB	#USB PORTS	NETWORK	NETWORK PROTOCOLS	OTHER BACKUP
D1	M1	4 Camera perfessional gold series	NA	Embedded Linux	SATA	1 TB	4	H.264	D1(704 x 576 / 704 x 480); CIF(352 x 288 / 352 x 240); 960H(960 x 576 / 960 x 480)	USB 2	2	RJ-45 port (10/100M)		E-Sata
D2	M1	D1 Realtime H.264	NA	Embedded Linux	SATA	500 GB	4	H.264	D1(704 x 576 / 704 x 480); HD1(352 x576 / 352 x 480); CIF(352 x 288 / 352 x 240)	USB 2	2	RJ-45 port (10/100M)	TCP/IP;HTTP; DHCP; DNS; DDNS; NTP;SMTP; UPNP; IP Filter	E-Sata
D3	M1	CVI 4 Camera DVR	NA	Embedded Linux	SATA	1 TB	4	H.264		USB 2	2	RJ-45 port (10/100M)		No
D4	M1	NA	NA	Embedded Linux	SATA	1 TB	16	H.264	D1(704 x 576 / 704 x 480); CIF(352 x 288 / 352 x 240); 960H(960 x 576 / 960 x 480)	USB 2	3	RJ-45 port (10/100M)		E-Sata
D1	M2		Embedded	Embedded Linux	SATA	1-4 TB	4	H.264/G.711	D1/4CIF(704×576/704×480) / CIF(352×288/352×240) / QCIF(176×144/176×120)	USB 2	2	RJ-45 port (10/100M)	HTTP, IPv4/IPv6, TCP/IP, UPNP, RTSP, UDP, SMTP, NTP, DHCP, DNS, PPPOE, DDNS, FTP, IP Filter	No
D2	M2	720p Digital Recorder	NA	NA	SATA	1-3 TB	8	H.264	720p	USB 2	2	RJ-45 port (10/100M)	NA	No
D3	M2	HD 40 foot Night Vision Kit	Embedded	Embedded Linux	SATA	2-8 TB	4	H.264	720-1080p	USB 2	2	RJ-45 port (10/100M)	NA	flash
D5	M1	Econ HD-TVI DVR	Embedded Dual-core	Embedded Linux	SATA	1-4 TB	4	H.264/G.711	Main stream: 1080P(non-real-time) / 720P / VGA / WD1 / 4CIF / CIF; Sub-stream: WD1(non-real-time) 4CIF(non-real-time) / CIF / QCIF QVGA /:	USB 2	2	RJ-45 port (10/100M)		No
D6	M1	16 Channel Real-Time WD1/960H DVR	NA	Embedded Linux	SATA 1-4 HDDs	NA	16	H.264/M-JPEG	480NTSC/400 PAL(2CIF),480NTSC/400PAL(CIF)	USB 2	2	2Gb	TCP-IP/DHCP/PPPoE/DDNS/H	
D7	M1	8CH, Real-Time @ D1 and above	NA	Embedded Linux	SATA 1-4 HDDs	NA	8	H.264	NTSC : 960 x 480, 720 x 480 / PAL : 960 x 576, 720 x 576	USB	2	IPv4	TCP/IP, DHCP, PPPoE, SMTP, NTP, HTTP, DDNS, RTP, RTSP, SNMP	No
D8	M1	Performance Series HQA DVRs 720P/1080P DVRS	Embedded	Embedded Linux	SATA	1-4 TB	16	H.264/G.711	1080p:(1920 x1080);720p(1280 x 720); 960H (960 x 576 / 960 x 480); D1(704 x 576 / 704 x 480); 4CIF(704 x 576; 704 x 480); CIF(352 x 288; 352 x 240); QCIF(176 x 144; 176 x 120)	USB 2	2	RJ-45 port (10/100/1000 M)	HTTP; TCP/IP; IPv4/IPv6; UpnP; RTSP; UDP; SMTP; NTP; DHCP; DNS; IP filter; PPPoE; DDNS; FTP; IP filter, P2P	No
D9	M1	Intellex LT Desktop 8 channel 500GB Allows for connecting to Windows PC	NA	NA	NA	500 GB	8	MPEG-4, MJPEG	NA	NA	NA	1XGb	NA	CD/DVD
D10	M1	8CH 1080P AHD DVR	NA	Embedded Linux	SATA 1-2 HDD	1-4 TB	4	H.264 High profile	Analog: 8* 1080p; 4* 1080p; 8* 720p	USB 2	2	RJ-45 port (10/100M)	TCP/IP, PPPOE, DDNS, FTP, NTP, UPNP, SMTP, RTSP, HTTP	No
D11	M1	16-Channel H.264 Stand Alone DVR 480 FPS PM Series, DVD Burner	NA	Linux	Up to 4 HDD's (SATA) + 1 ODD, Support External Storage(Option)	NA	16	H.264 Codec (DSP Based)	By each camera for different resolution setting(CIF/2CIF/D1)	NA	3	Gigabit Ethernet	Dual Stream/Static IP/LAN/DHCP/DDNS	CD/DVD/USB Flash device File Format AVI for Backup
D12	M1	8 Channel Tribrid DVR 720P	Embeedded	Embedded Linux	SATA 1-2HDD	up to 8TB	8	H.264 / G.711	1080p (1920×1080) / 720p (1280×720) / 960H (960×576 / 960×480) / D1 / 4CIF (704×576 / 704×480) / CIF(352×288/352×240) / QCIF(176×144/176×120)	USB 2 Backup	2	RJ-45 Port (10/100/1000M) Backup	HTTP, IPv4/IPv6, TCP/IP, UPNP, RTSP, UDP, SMTP, NTP, DHCP, DNS, PPPOE, DDNS, FTP, IP Filter, SNMP, P2P	No
D13	M1	24CH h.264 DVR w / HDMI/VGA/BNC iPhone/Android App	NA	Embedded Linux	SATA 1-8/ eSATA 1	NA	24	H.264 High profile	960H/D1/CIF	USB 2 Backup	2	RJ45 Gigabit ethernet	TCP/IP, UDP, DHCP, DNS, PPPOE, DDNS	No
D14	M1	Rugged Cams 8 Channel advanced series DVR	Embedded	Embedded on Chip	2 HDD	1 TB	8-16	H.264 Audio G.732	352 x 240, 704 x 240, 704 x 480 (NTSC), 352 x 288, 704 x 576 (PAL)	USB 2 Backup	NA	Ethernet Backup	PSTN / ISDN / LAN (Ethernet) / Cable Modem / ADSL / Dynamic - IP / Private - IP / DDNS /Multi - Network Interface (Ethernet & PSTN)	DVD/CD Backup
D15	M1	Alibi 8-Channel HD-TVI 1080p / 960H Hybrid+ Security DVR	NA	NA	SATA 1HDD	NA	8	H.264	1920 × 1080 / 60 Hz, 1280 × 1024 / 60 Hz, 1280 × 720 / 60 Hz, 1024 × 768 / 60 Hz	NA	NA	RJ-45 port (10/100M)	TCP/IP, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, SNMP, NFS, iSCSI, UPnP™, HTTPS	No
D16	M1	1 TB "EXTREME SERIES" 16 Channel High Resolution Digital Video Recorder With DVD R/W - Internet & Cell Phone Viewing (FULL D1 High Definition HDMI	NA	NA	SATA 1-8HD/eSATA 1	up to 32 TB	16	H.264/G.711	D1, HD1, 2CIF, CIF, QCIF	USB 2 Backup	4	RJ-45 10/100/1000M Backup	HTTP, IPv4/IPv6, TCP/IP, UPNP, RTSP, UDP, SMTP, NTP, DHCP, DNS, PPPOE,DDNS, FTP, IP	No
D17	M1	8ch Hybrid DVR with HD-SDI & Analog as any combination	NA	Embedded Linux	3 – HDD/eSATA 1	500 GB - 2 TB	8	H.264/MJPEG/G.711	1920x1080p	NA	NA	10/100/1G	NA	DVD

Appendix B - Tables of Demonstrated DVR Capabilities by Device

The following tables provide details of the capabilities observed for each of the laboratory DVR systems examined in this study. "Onboard" indicates information obtained by examining video files stored on each DVR's hard drive. "Via GUI" indicates information obtained from an inspection of each DVR's GUI. "Export" indicates information obtained from an examination of each exported file type that a given DVR was capable of producing. Note that all observations recorded in these tables were made by *hands-on inspection*.

Table B-1. Demonstrated DVR Capabilities for Device D1M1

D1M1						
			YES	NO	UNKOWN	COMMENT
			(X)	(X)	(X)	(Other interesting facts and/or observations)
Onboard						
		1. Evidence of H.264 in use?	X			
		1.a Evidence of SEI messages?	X			SEI payload type 229 Unknown
		2. Evidence of Time Stamps?		X		
		3. Evidence of Camera Metadata?		X		
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		X		
Via GUI						
		1. Evidence of H.264 in use?		X		
		1.a Evidence of SEI messages?		X		
		2. Evidence of Time Stamps?	X			Capture identified with date and time.
		3. Evidence of Camera Metadata?		X		
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		x		
Export						
	File Type					
Type 1	NSF	1. Evidence of H.264 in file?	X			NSF - Propreitary Format Folder with h264 file, index file and video player file.
		1.a Evidence of SEI messages?	X			SEI payload type 229 Unknown
		2. Evidence of Time Stamps?		X		Export files placed in folder named with date.
		3. Evidence of Camera Metadata?		X		
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		X		
Type 2						
	AVI	1. Evidence of H.264 in file?	X			Integrated Subtitles Folder with video file and video player file.
		1.a Evidence of SEI messages?	X			SEI payload type 229 Unknown
		2. Evidence of Time Stamps?		X		Export files placed in folder named with date.
		3. Evidence of Camera Metadata?		X		
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		X		
Type 3						
	AVI	1. Evidence of H.264 in file?	X			Separated Subtile, MAC compatible Folder with video file and SMI file.
		1.a Evidence of SEI messages?	X			Export files placed in folder named with date.
		2. Evidence of Time Stamps?		X		SEI payload type 229 Unknown
		3. Evidence of Camera Metadata?		X		Export files placed in folder named with date.
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		X		

Table B-2. Demonstrated DVR Capabilities for Device D2M1

D2M1						
			YES	NO	UNKOWN	COMMENT
			(X)	(X)	(X)	(Other interesting facts and/or observations)
Onboard						
		1. Evidence of H.264 in use?	X			
		1.a Evidence of SEI messages?	X			SEI payload type 0Buffering period
		2. Evidence of Time Stamps?		X		
		3. Evidence of Camera Metadata?		X		
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		X		
Via GUI						
		1. Evidence of H.264 in use?		X		
		1.a Evidence of SEI messages?		X		
		2. Evidence of Time Stamps?	X			Name of capture on device contains time data
		3. Evidence of Camera Metadata?		X		
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		X		
Export						
	File Type					
Type 1	AVI	1. Evidence of H.264 in file?	X			
		1.a Evidence of SEI messages?	X			SEI payload type 0Buffering period
		2. Evidence of Time Stamps?		X		Name of exported file contains date and time data
		3. Evidence of Camera Metadata?		X		
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		X		

Table B-3. Demonstrated DVR Capabilities for Device D3M1

D3M1						
			YES	NO	UNKOWN	COMMENT
			(X)	(X)	(X)	(Other interesting facts and/or observations)
Onboard						
		1. Evidence of H.264 in use?	X			
		1.a Evidence of SEI messages?	X			SEI payload type 175 Unknown
		2. Evidence of Time Stamps?		X		
		3. Evidence of Camera Metadata?		X		
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		X		
Via GUI						
		1. Evidence of H.264 in use?	X			Specified in GUI
		1.a Evidence of SEI messages?		X		
		2. Evidence of Time Stamps?	X			Capture time recorded in a table on screen
		3. Evidence of Camera Metadata?		X		
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		X		
Export						
	File Type					
Type 1	DAV	1. Evidence of H.264 in file?			X	Codec not identified with analysis tools. Bundled video file and player
		1.a Evidence of SEI messages?			X	
		2. Evidence of Time Stamps?			X	
		3. Evidence of Camera Metadata?			X	
		3.a Evidence of Camera Type?			X	
		4. Evidence of Location Metadata?			X	
Type 2						
	ASF	1. Evidence of H.264 in file?	X			
		1.a Evidence of SEI messages?		X		
		2. Evidence of Time Stamps?		X		
		3. Evidence of Camera Metadata?		X		
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		X		

Table B-4. Demonstrated DVR Capabilities for Device D4M1

D4M1						
			YES	NO	UNKOWN	COMMENT
			(X)	(X)	(X)	(Other interesting facts and/or observations)
Onboard						
		1. Evidence of H.264 in use?	X			Unable to carve playable filestream from the hard drive.
		1.a Evidence of SEI messages?			X	Unable to ascertain from partial bitstream
		2. Evidence of Time Stamps?			X	Unable to ascertain from partial bitstream
		3. Evidence of Camera Metadata?			X	Unable to ascertain from partial bitstream
		3.a Evidence of Camera Type?			X	Unable to ascertain from partial bitstream
		4. Evidence of Location Metadata?			X	Unable to ascertain from partial bitstream
Via GUI						
		1. Evidence of H.264 in use?		X		
		1.a Evidence of SEI messages?		X		
		2. Evidence of Time Stamps?		X		
		3. Evidence of Camera Metadata?	X			User can specify brand name in camera settings during system setup
		3.a Evidence of Camera Type?	X			
		4. Evidence of Location Metadata?		X		
Export						
	File Type					
Type 1	NSF	1. Evidence of H.264 in file?	X			NSF - Proprietary Format. Folder with h264 file, index file and video player.
		1.a Evidence of SEI messages?	X			SEI payload type 229 Unknown
		2. Evidence of Time Stamps?		X		Export files placed in folder named with date.
		3. Evidence of Camera Metadata?		X		
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		X		
Type 2						
	AVI	1. Evidence of H.264 in file?	X			AVI -Separated Subtile, MAC Compatible. Folder with video file and SMI file.
		1.a Evidence of SEI messages?	X			SEI payload type 229 Unknown
		2. Evidence of Time Stamps?		X		Export files placed in folder named with date.
		3. Evidence of Camera Metadata?		X		
		3.a Evidence of Camera Type?		X		
		4. Evidence of Location Metadata?		X		

Appendix C - Investigation of H.265 Readiness for Recommendation

This appendix contains general information gathered as part of an investigation into H.265 (High Efficiency Video Coding (HEVC)). H.265 is a potential successor to H.264 and was developed by the JCT-VC organization, a collaboration between the ISO/IEC MPEG and ITU-U VCEG. Improvements to H264 are a doubling of the compression rate at the same level of video quality, and improved video quality at the same bit rate. H.265 also supports 4K resolution.

C.1 H.265 Profiles

H.265 does support profiles. A profile is a defined set of coding tools used to create the bitstream that conforms to that profile. An encoder may choose which coding tools to use as long as it produces a conforming bitstream. A decoder must support all coding tools that can be used in that profile.

There are three standard versions of H.265.

H.265 Version 1 (April 2013)

- Main profile supporting 8-bit 4:2:0 chroma sampling.
  This is the most common type of video used with consumer devices.
- Main 10 profile with 10-bit support.
  Decoders must support decoding bitstreams made with the Main and Main 10 profiles. The higher bit rate allows for use of greater number of colors, improved video quality and improved coding efficiency.
- Main Still Picture profile.
  This profile allows for a single still picture to be encoded with the same constraints as the Main profile. As a subset of the main profile it allows for a bit depth of 8-bits with a 4:2:0 chroma sampling.

Version 2 (October 2014)

- Twenty-one range extensions profiles.
- Two scalable extensions profiles.
- One multi-view extensions profiles.

Version 3 (April 2015)

- 3D Main profile.

H.265 defines two tiers, Main and High, and thirteen levels. A level is defined to be a set of constraints for a bitstream. The Main tier applies to levels below four. The tiers where added to deal with applications that differ in terms of the maximum bitrate. A decoder that conforms to a given tier/level is required to be capable of decoding all bitstreams that are encoded at that level and below.

C.2 H.265 Bitstream

The H.265 bitstream is an ordered sequence of syntax elements that are placed into logical packets called NAL (Network Abstraction Layer) Units. Support for NAL units is similar to H.264.

Comparison of NAL Unit Classes

H.265 NAL Units	H.264 NAL Units
VPS - Video parameter set	---
SPS - Sequence parameter set	SPS - Sequence parameter set
PPS - Picture parameter set	PPS - Picture parameter set
Slice (different types)	Slice (different types)
AUD - Access unit delimiter	AUD - Access unit delimiter
EOS - End of sequence	EOS - End of sequence
EOB - End of bitstream	EOB - End of bitstream
FD - Filler data	FD - Filler data
SEI - Supplemental enhancement information	SEI - Supplemental enhancement information
Reserved and unspecified	Reserved and unspecified

H.265 defines an additional video parameter set (VPS). The VPS, SPS, and PPS contain general video parameters. These provide a robust mechanism for conveying data that are essential to the decoding process. This is similar to H.264, which supports the SPS and PPS.

The slice NAL unit contains data from an encoded video frame. It can contain a full frame or its part. Each slice can be decoded independently, that is, without using information from any other slice. Thereby, slices can be used as a tool to support parallel encoding/decoding.

There are three slice types as follows:

1. I-slice - slice with only intra prediction
2. P-slice - slice with inter prediction from one I or P slice
3. B-slice - slice with inter prediction from two I or P slices

Note that in H.265 there is no special slice type called IDR slice. In H.264 the IDR (Instantaneous Decoder Refresh) slice is a specific type of I-slice that makes locating data within the H.264

stream more responsive to the player. The IDR slice specifies that no frame that comes after can reference frames before that point.

AUD can be used for signaling about start of video frame. FD can be used for bitrate smoothing. SEI provides support for different types of metadata. It includes picture timing, color space information, etc.

C.3 Standard Adoption

A challenge for broad industry adoption of H.265 is that the standard is protected by patents owned by various parties [OZER]. Commercial use of this standard requires payment of royalties to the different license holders such as MPEG LA, HEVC Advance and Technicolor SA. This differs from the licensing of H.264 where a single organization Moving Picture Experts Group License Agreement (MPEG LA) administered the license rights related to the collection of patents through a pool mechanism. A company who wanted to implement this technology could pay MPEG LA for the patent pool instead of negotiating individually with each individual patent holder.

Patent holders for H.265 want to pursue royalties outside of this patent pool model making it more challenging for users who license this technology. This licensing situation is one of the reasons for the development of an alternative format, for example VP10. VP10 is an open source and royalty-free video coding format developed by Google.

The decoding of H.265 video is more processor intensive, relying on hardware and software for support of efficient HEVC playback. There is a limited number of dedicated media players that currently support H.265. The VLC player does support HEVC files but the playback may suffer from poor quality, especially 4K videos.

C.4 SEI Message Support

As noted above, SEI messages used in H.264 are also supported in the H.265 specification. The MISB standard 604.3, which utilizes SEI messages, has been revised to include the precision time stamp definition in an H.265 video stream (see MISB standard - 604.4, Timestamps for Class 1 / Class 2 Motion Imagery, February 25, 2016). Similarly, NISTIR 8161 also leverages SEI messages for transmission of metadata exported from surveillance systems. The inclusion of SEI messages within H.265 is essential for application of the recommendations provided in NISTIR 8161 to H.265 in the future.