Forensics of IP Based Security Surveillance Cameras

By

Rashid Masood Khan

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

Aug 2017

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by Mr/MS **Rashid Masood khan** Registration No.**NUST201463775MMCS25214F**, of **Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.

Signature: _____

Supervisor Maj Muhammad Faisal Amjad, PhD

Date: _____

Signature (HoD): _____

Date: _____

Signature (Dean): _____

Date: _____

Abstract

Recent years have seen tremendous increase in crime and terrorism all over the world which has necessitated continuous surveillance of public spaces, commercial entities and residential areas alike. CCTV cameras are an integral part of any surveillance system and have evolved significantly along with other technological advancements in image processing, storage as well as communication through Internet. They are a vital part of any investigation that follows a criminal or terrorism incident by providing invaluable evidence. However, preservation of the integrity of digital evidence is of paramount importance and must be guaranteed to be admissible in a court of law. Despite their ease of use and deployment, IP cameras have some vulnerabilities that can lead to compromised integrity of their videos. In this research, we show that the Advance Systems Format (ASF) file used in most IP cameras, which is also the main file containing metadata about the streaming packets, is vulnerable to forgery. This file is stored in plaintext and any technically savvy person can forge it therefore, a mechanism is needed to prevent it. To that end, we have gathered critical artifacts from an ASF file of IP cameras and carried out their forensic analysis. The analysis has shown that we have successfully detected forgery / tampering of evidence in IP cameras. To the best of our knowledge, this is the first research effort focusing on the forensic analysis and detection of forgery in an IP camera's ASF file.

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

Dedication

“In the name of Allah, the most Beneficent, the most Merciful"

I dedicate this thesis to my Father, mother, bother, and teachers who supported me in every step

Acknowledgments

All praises to Allah for the strengths and His blessing in completing this thesis.

I would like to convey my gratitude to my supervisor, Major. Muhammad Faisal Amjad, PhD,for his supervision and constant support. His invaluable help of constructive comments and suggestions throughout the experimental and thesis works are major contributions to the success of this research. Also, I would thank my committee members; Asst Prof Muhammad Waseem Iqbal, and Lecturer Waleed Bin Shahid for their support and knowledge regarding this topic.

Last, but not the least, I am highly thankful to my father and Mother (Mr and Mrs Masood Akhtar), and brother (Arslan Masood Khan). They have always stood by my dreams and aspirations and have been a great source of inspiration for me. I would like to thank them for all their care, love and support through my times of stress and excitement.

Table of Contents

List of Figures

List of Tables

Page

Chapter 1

Introduction

1.1 Overview

Every society in the world is suffering from crime and terrorism. Governments all over the world are looking towards technology to mitigate the threats against public safety and critical infrastructures [1]. Round the clock surveillance of assets is one such mechanism and due to the latest developments in the field, the attention has shifted from analog CCTV to modern digital cameras that are based on Internet Protocol (IP). In contrast with the analog CCTV technology, an IP Camera provides the flexibility of connecting to the Internet and being accessible across the world over the Internet. IP based Cameras can directly stream high resolution video either directly to computer or to a Network Video Recorder (NVR) for storage and archiving. IP cameras can be deployed using the centralized or a de-centralized approach [2]. In centralized approach, NVR has central video surveillance software installed which contains all functions including key management functions. In the decentralized approach, all the management is done inside the camera and there is no need for transferring the video to NVR [3]. Such IP cameras have the capabilities of NVR and store videos as sequences which can be accessed as files. One of the advantages of this approach is that one can directly attach an external Ethernet hard disk drive and download huge volumes of data without consuming any network bandwidth. By using the standard web browser, users can send video sequence searches based on date, time, and location and play the videos directly from the camera. Despite the advantages associated with IP cameras, organizations are still using analog cameras primarily due to the associated cost of replacing older systems [4].

With the flexibility of being accessible from across the world through the Internet, IP cameras are vulnerable to attacks and therefore, the data stored in them is susceptible to

forgery. The purpose of forensics in IP cameras is to analyze the data contained in them to ascertain occurrence of forgery and determine its admissibility in a court of law [5]. It involves analysis artifacts collected from the media data as well as its metadata that may be taken from hard disks connected to IP cameras or other storage devices to determine if its integrity has been compromised. E.g., Law Enforcement Agencies (LEA's) may need to identify faces or vehicle license plates to reach to perpetrators however, to ensure integrity of video data; they may need to perform forensic analysis of the video data [6]. This involves identifying patterns that are deployed by attackers for gaining unauthorized access to data as well as the actual forgery of video data. It may also help in identifying future threats that organizations face in terms of their video surveillance and relevant decision-making processes. With robust forensic techniques for IP cameras, their video evidence is expected to be upheld in the courts of law [7].

1.2 Motivation and Problem Statement

In today's world the attempts to forge the data is increasing day by day. So it is the duty of the law enforcement agencies to also beef up their efforts to stop these attempts to take place. The field of digital forensics is an evolving field and the victims don't know much about protecting their valuable data. There is very little research on forensics of IP based cameras and it is the need of the hour as the use IP cameras is increasing and it is becoming difficult to protect the integrity and availability of recorded surveillance video and images. Culprits easily get way with doing this digital crime as there is no proper laws and procedures that are in place that can apprehend the culprits who are involve in this crime which is getting bigger and bigger. So this research will help in identifying ways to protect the digital data which is in the form of ASF file which is the file of IP Cameras. The file of IP cameras includes lot of important information that culprits always want to remove to hide his/her identity from the law enforcement agencies (LEAs).

1.3 Objectives

Perform Forensic Analysis of video of IP based Camera. The Analysis will consist of ASF file structure.

- Determine all the changes that have occurred in the file.
- Comparing the forensic artifacts of file before and after it is forged.
- Developing different scenarios, how the media file can be forged and altered.
- Determining the Header, Data and Index Object of the media file.
- Finding out the Packets, Payloads and Stream within the Data Object.

1.4 Thesis Contribution

- Forensics of IP cameras uses proactive approaches to detect forgery or unauthorized access to the media data. Through forensics one can predict future events by looking into historical data or activities performed by the malign persons.
- Forensic video analysis highlights mainly on the case as it provides a concrete proof which can be used as evidence in the court of law. It makes the judges and the lawyers understand the complexities of the case and tackle the issues in an efficient manner
- The goal of forensics in IP based Cameras is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

1.5 Areas of Application

- Finding the all important evidence of a wrongdoing being done, examinations can likewise be utilized to demonstrate the goal behind the crime.
- Attributes of files and meta-information can be utilized to recognize the beginning of a specific bit of information. Demonstrating whether a document was prepared on the computerized gadget being analyzed or gotten from somewhere else.

- Document validation Related to "Assessment of source," metadata related with computerized reports can be effectively altered (for instance, by changing the PC clock you can influence the creation date of a record). Validation of the document identifies distortion of such points of interest.

1.6 Advantages of Research

- A video forensic analysis generally investigates the video which could be taken from computer hard disks or any other storage devices with adherence to standard policies and procedures to determine if those devices have been compromised by unauthorized access or not[8][9].
- The objective of digital forensics in IP based Cameras is to look at computerized media in a forensically stable way with the point of distinguishing, safeguarding, recuperating, dissecting and introducing certainties and conclusions about the data.
- Computer forensics is widely used by law enforcement agents in gathering evidence. Corporate entities use computer forensics to evaluate the usage of computer resources in office environments**.**

1.7 Conclusion

Forensics of IP Camera is one of the emerging fields and there is need of research in this area as the use of the IP cameras are increasing with every passing day and with the increase of use, the attempts are also increasing to forge the digital content by the malign person. The purpose of this research is identify the ways in which digital content can be forged and help LEA’s to apprehend the culprits involved

Chapter 2

Literature Review

2.1 Introduction

These days validating a given media content has turned out to be increasingly troublesome because of different causes and the potential modifications that could have been worked on it. This is because of the accessibility of modest and effectively operable advanced media gadgets (for example, cameras, cell phones, recorders etc.).

From these premises, a critical research has been as of late committed to the forensic examination of media information. These researches on video forensics are based on facts that forgers or malign persons always leave some clues that can be worked upon to build the processing history of the content. The investigation of these clues allows investigators to analyze the content that have gone through changes. An extensive examination exercises in this field are given to the investigation of still pictures. In any case, scientific research has been as of late concentrating on the crime scene investigation issues identified with video signals in view of their characteristics and the extensive variety of alterations/changes that can be connected to them. Some recent work that has been done on the forensics of video is discussed in [10]. [10] Has proposed different solutions that can be used by the investigators to build the history of the video data. These solutions include identification of acquisition device on which content is generated, it also include the concept of video re-encoding and the last solution that is given in the paper is about the doctoring of the videos as well as images.[11] discusses the techniques for identification of tempering in MPEG Videos. The techniques discussed in the paper exploit the fact that static and temporal artifacts are introduced, when video sequence is subjected to MPEG Compression. [12] Proposes a scheme that can be used in the detection of the forgery, it states that each content has unique characteristics that can be used to link media to its source. Proposed scheme attempts to

detect duplicate and modified copies of a video primarily based on peculiarities of imaging sensors rather than content characteristics only. [13] Discusses an approach for detecting video forgery based on ghost shadow artifact in this paper. The artifact Ghost shadow comes into action when object which is moving is removed by in-painting. In this approach, ghost shadow artifact is accurately detected by inconsistencies of the moving foreground segmented from the video frames and the moving track obtained from the accumulative frame differences, thus video forgery is exposed. [14] Discussed video forgery by giving two techniques by duplication. The first technique is based in detecting full frame duplication and second approach is based upon detecting only changed frames. The video crime scene investigation turns out to be amazingly harder than the investigation on still pictures since recovering of processing history could be substantially more intricate. Analysis of video metadata is given in [15]. The paper includes information on semantic content of the video; it includes differentiating between intrinsic metadata from ancillary metadata. The other problem that is associated with video investigation is that video content is always available in compressed format and can easily be forged or compromised, thus destroying the all-important footprints. This research examines the forensic artifacts of ASF file that are associated with IP Cameras. The examination of ASF file will help identifying the patterns of forgery or modifications that are done on the video content. Like different approaches that are proposed above in this section, this approach will be based on the forensic analysis of the video. The later part of research will focus on the test cases that are developed to show, how an ASF file can be forged or its integrity can be compromised.

2.2 Conclusion

There is very little research on the forensics of IP Cameras, this chapter includes the research papers that are on the detection of the forgery on videos. Video forensics is also one of the emerging fields and techniques to detect the forgery have been borrowed from image forensics. This research will focus on detecting forgery in the ASF file which is the main file of IP Cameras.

Chapter 3

IP CAMERA AND ASF FILE PRELIMINARIES

3.1 Introduction

There has been some work which is done on the ASF file of IP cameras. The work discussed the overall structure of the File. The structure includes three objects in which two are mandatory and one is optional object. The two mandatory objects are Header Object and Data Object and optional object is Simple index Object [16]. The work also included the description of the objects that reside in the ASF file. Microsoft discussed the properties of these objects and overall structure of the ASF file of IP cameras.

3.2 ASF FLE

ASF File which is commonly known as Advance systems Format is format for streaming audio and video content. The ASF file has the capability to allow single multimedia file to publish on wide series of bandwidth. The ASF file contains object which is further divided into three objects. [17]

Header Object	Data Object	Index
File Properties	Packet	Simple Index
Header Extension	. . .	
Stream Properties	Packet	
. . .		
Stream Properties		
Other Objects		

Table 1 ASF file Structure

3.3 Header Object

The header Object is compulsory object and it comes at the start of every ASF File. This object contains the global attributes and information regarding the streams that are available in the file. There is another feature of this object is that it is use to play data of the media file [18]. This object has further sub objects which are mandatory as well.

3.3.1 File Properties Object

The first sub object is file properties object that is global in nature contains the attribute such as file size, duration of the media data, data packets that are available in the file, minimum and maximum packet size.

3.3.2 Stream Properties Object

The second sub object is stream properties object which describes the information regarding the streams in the file. And its mandatory that ASF file must contain at least one stream therefore file will have one steam properties object.

3.3.3 Header Extension Object

The third sub object of header object is header extension which allows other functionality to be added plus maintaining backward compatibility.

3.4 Data Object

This object is mandatory too as header object is in the ASF file. Data object is considered to be most important object in structure of ASF File. This object contains the media data of the file. Data packets contain all the data of the file. All the stored packets have same length. All the data packets have data for single or many streams [19]. All these packets are arranged according to time on which they are received. There is header in data packet that contains all the parsing information. Content of the data object is stored in header object of the ASF File.

3.5 Simple Index Object

Among all the objects in ASF File, one object is optional and that is Index Object. In the file structure of ASF, this is the last object. And this object can contain more than one object. Basically it used to give to time based access to mandatory object that is data object. There are three other types of Index object which are Presentation time based index, time code Index, Frame based Index.

3.5.1 Presentation time based Index

It gives presentation based indexing to video and audio streams available in blocks. The main advantage of this indexing is that it provides space efficiency [20].

3.5.2 Time Code Index

Provides time based access to streams that contain metadata based on time code. The time code refers to SMPTE format. SMPTE formats supports (Hours, Minutes, Seconds, and Frames).

3.5.3 Frame Based Index

Frame based Index provides frame wise access to video streams. Indexing is based on the terms of frame numbers with first frame corresponds to entry number Zero in the Frame based Indexing.

3.6 Conclusion

The chapter includes the overall description of the ASF file which is main file of IP Cameras. As discussed earlier in this chapter the file includes the three objects in which two are mandatory and one object is optional. The two mandatory objects are Header Object and Data object and the optional object is Simple Index Object.

Chapter 4

Forensic Examination of Artifacts of ASF File

4.1 Introduction

To perform forensic analysis of the ASF file, there is need of ASF file which is file of an IP Camera, for that IP camera was used which had following specifications. The IP camera of 3 MP progressive scans with 7mm-35mm motorized lens was used [21] in the analysis phase of this research. The camera has capability of multiple network monitoring. The ASF file has size of 17. 4 MB (18,288,509bytes). The File on which analysis was done was recorded on 24th August 16 at 9:53:34 seconds.

The tool that was used for the analysis of the ASF file was Windows media ASF Viewer 9 series which is the certified tool of Microsoft for the analysis of ASF Files of IP Cameras [22]. The analysis of ASF file has covered all the objects that are part of the structure of the ASF File. This part of research will identify different artifacts of the objects that are in the ASF File and will also be focusing on sizes and locations of these artifacts.

4.2 Forensic Analysis of Header object Artifacts

The first artifact in this object is object ID which has size of 128 bits and describes the GUID of the object. The second artifact in this file is Object size which describes the size of the object and has size of 64 bits [23]. The other artifact that comes is of the header object which specifies, how many header objects are present in this object and it don't include the current one and has size of 32 bits. The last artifacts in this object are reserved fields which both have the size of 8 bits.

Field name	Size (bits)
Object ID	128
Object Size	64
Number of Header Objects	32
Reserved 1	8
Reserved 2	8

Table 2: Header Object

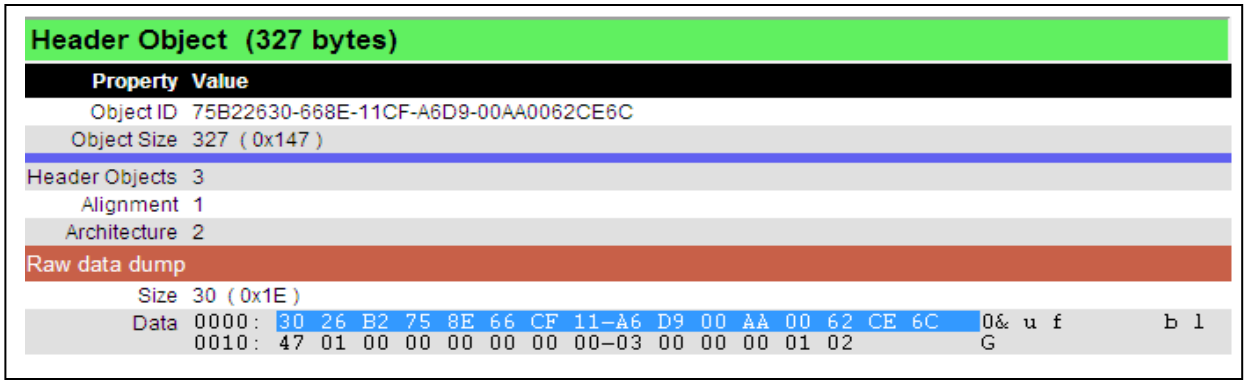


Figure 1: Data Object

The First 16 bits shows the Global Unique Identifier for the Header Object of the ASF file.

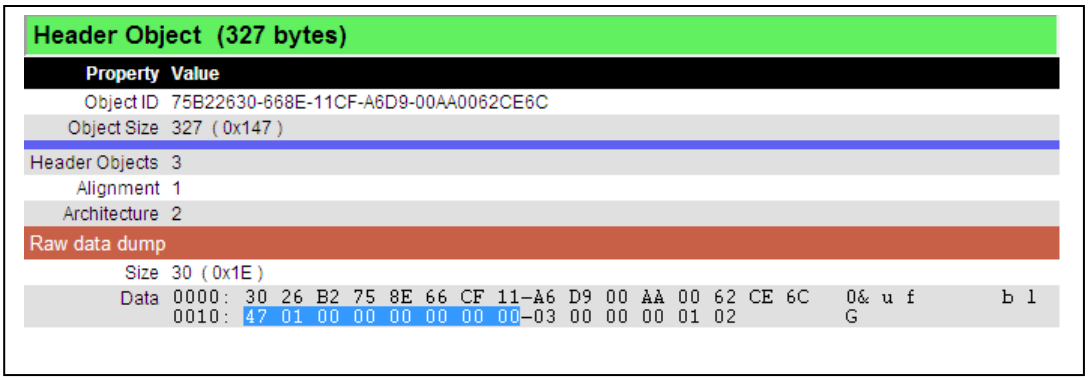


Figure 2: Object Size

The Next 64 bits describes the Object Size of the Header Object of the ASF File

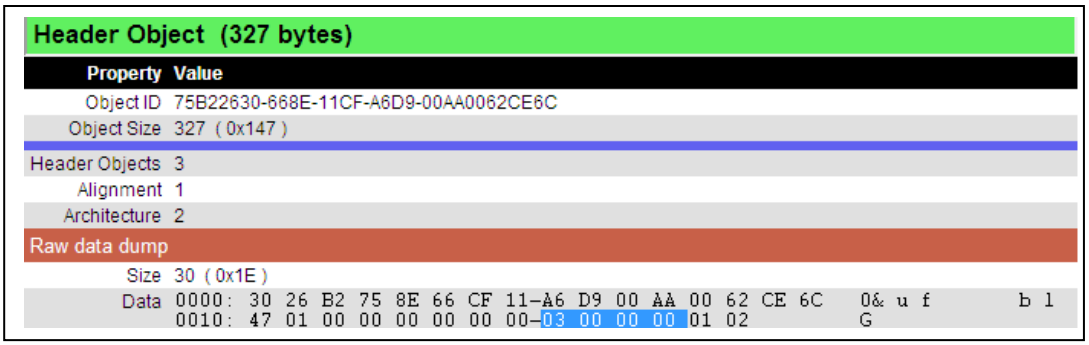


Figure 3: Number of Header Objects

The Highlighted 32 bits show the number of headers in the Header Object of the ASF.

And the current object is not included.

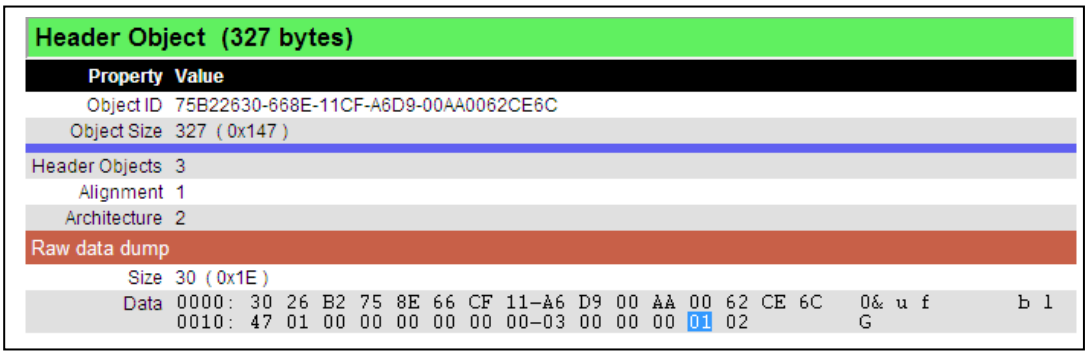


Figure 4: Reserved Field 1

The Highlighted part of the figure on the previous page shows the Reserved Field 1 which consist of 8 bits.

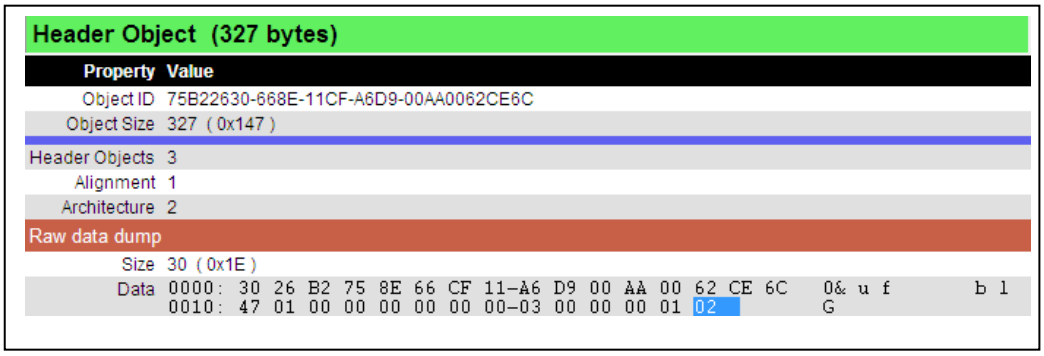


Figure 5: Reserved Field 2

The last 8 bits shows the Reserved Field 2 of the Header Object of the ASF file.

4.3 Forensic Analysis of File Properties Object Artifacts

As discussed earlier that Header object has sub objects as well which are also mandatory as the main object is. This part will focuses on the forensic artifacts of file properties object which is very important in the ASF file structure. The First artifact that comes in this object is Object ID which describes the GUID of the object and this artifact has the size of 128 bits. The next artifact that comes is the object size which describes the object size and has size of 64 bits. The third artifact in this file is file ID which is unique in every case and the ID of the file will be modified with slightest of the modifications in the file and it has size of 128 bits, then we have the file size of 64 bits which specifies the overall files size of the object [24]. After the file size, there is the artifact of the creation time (64 bits) which specifies the data and time for creation of the file.

The next artifact that comes is the data packets (64 bits) which describe data entries in the object. Play Duration (64 bits) is the other artifact that comes in the files properties object which describes the time needed to play the file. Value must include the estimated time if exact time is not specified. Send Duration (64 bits) is also one of the forensic artifacts which include the time needed for sending of the file, the time is in milliseconds. Then we have the Preroll (64 bits) that determines the time required to buffer before the media file is

played. The next artifacts are the flags (32 bits), there are multiple flags. Broadcast Flag (Determines the file is in process of Creation) .Seekable Flag (Determines the file, if it is seekable). Minimum data packet size (32 bits) describes the smallest available data packet available usually the size is given in bytes. The next artifact describes the maximum data packet size (32 bits) which is in bytes as well. Maximum bit rate (32 bits) is the last artifact in the file properties object which describes the total number of bits that can be transmitted for the complete ASF file.

Field Name	**Size (bits)**
Object ID	128
Object Size	64
File ID	128
File Size	64
Creation Time	64
Data Packets	64
Play Duration	64
Send Duration	64
Pre roll	64
Flags	32
Minimum Data Packet size	32
Maximum Data Packet Size	32
Maximum Bit rate	32

Table 3: File Properties Object

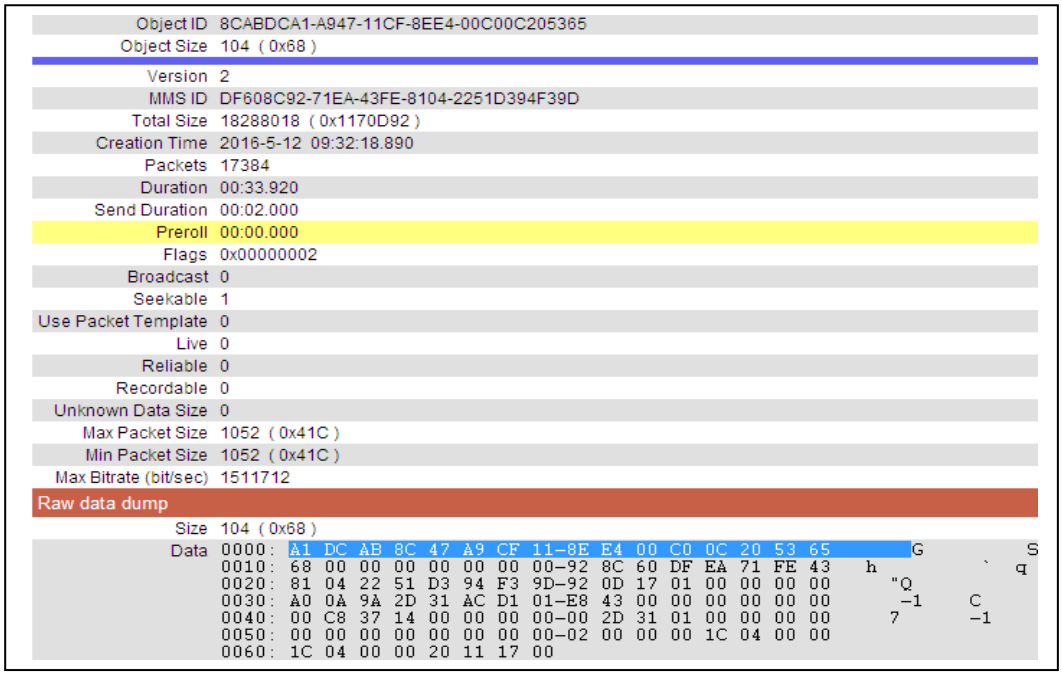


Figure 6: Object ID

The 128 bits specifies the Global Unique Identifier for the File Properties object.

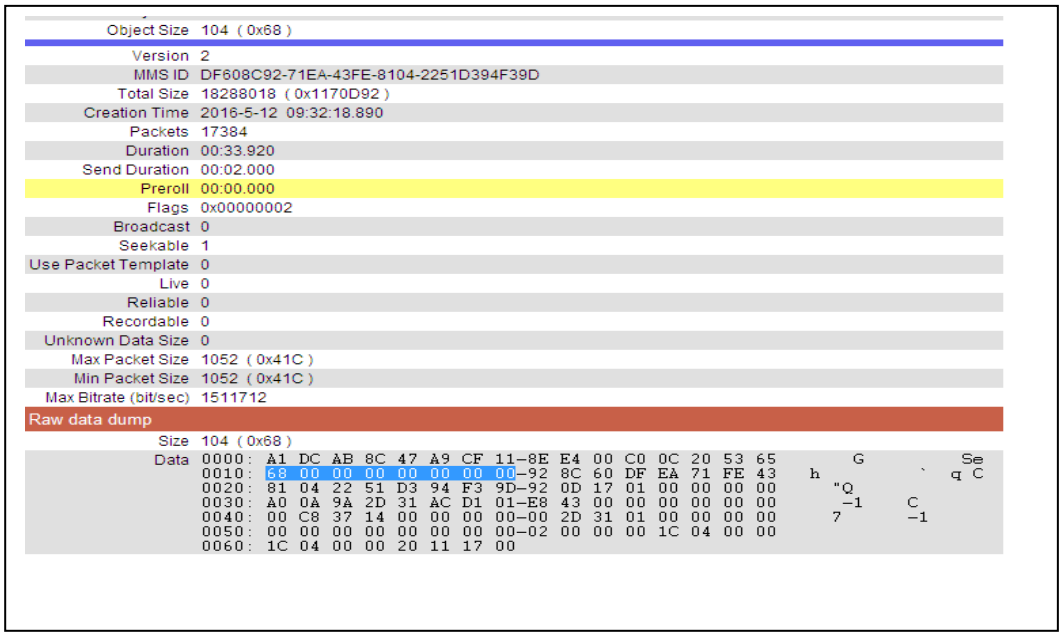


Figure 7: Object Size

The highlighted 64 bits specifies the Object size of the File Properties Object.

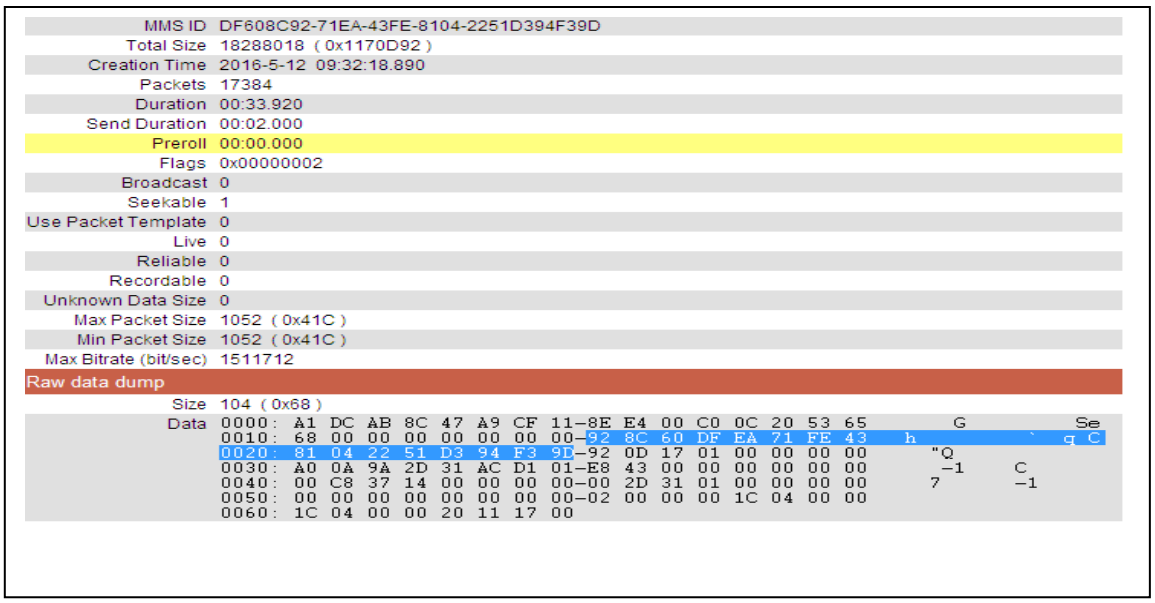


Figure 8: File ID

The Highlighted 128 bit specifies the File ID which is unique for this object and with slightest of the changes it will be modified.

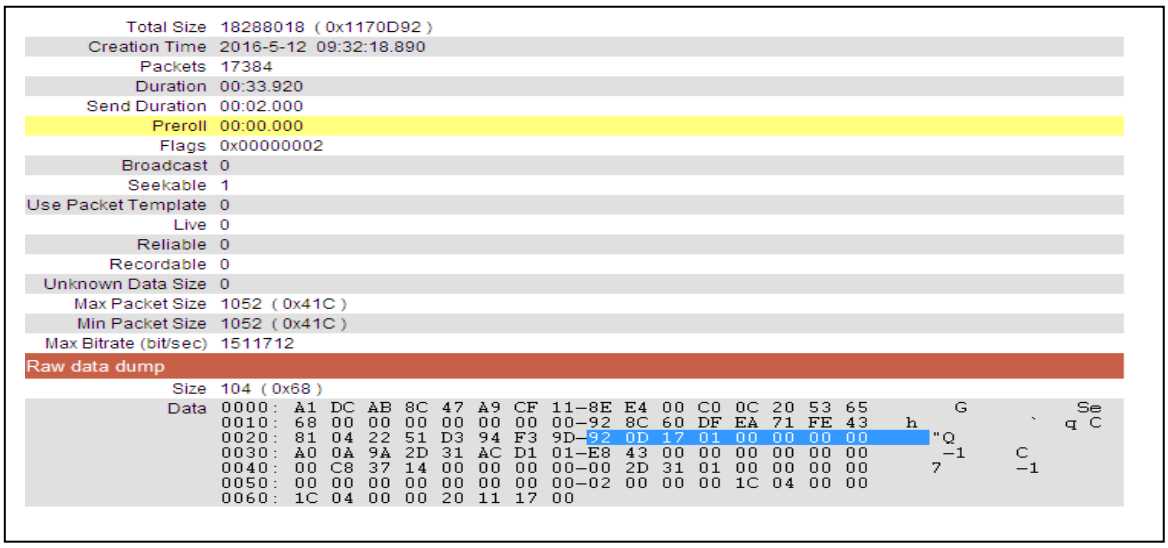


Figure 9: File Size

The Next 64 bits describes the File Size which is the File Size of an entire File

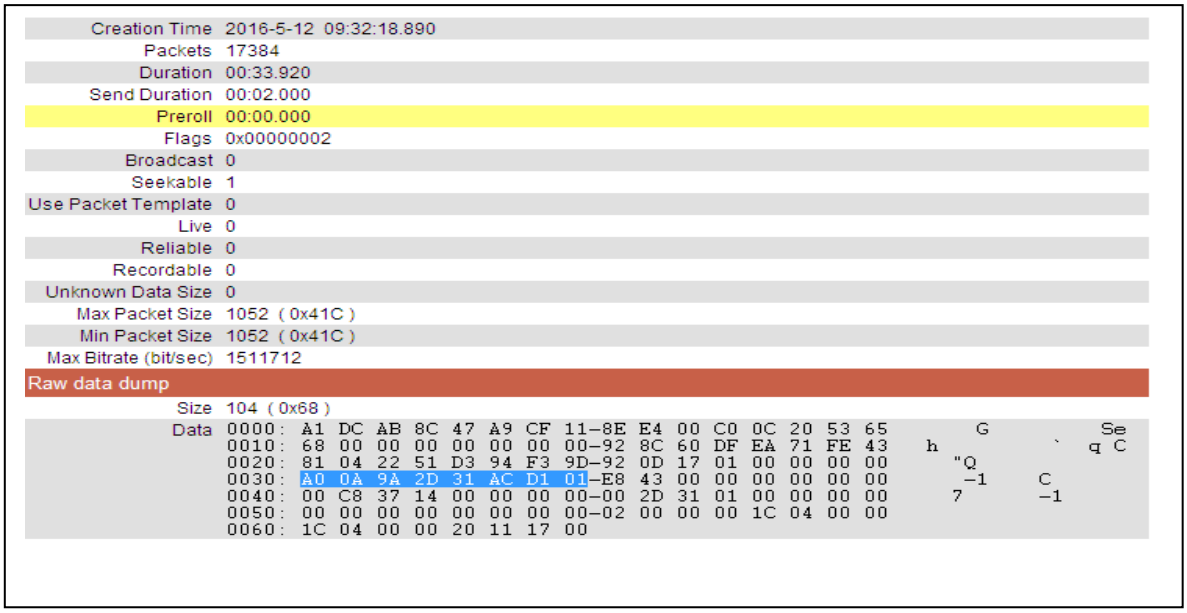


Figure 10: Creation Time

The highlighted 64 Bits determines the creation time of the ASF File being made.

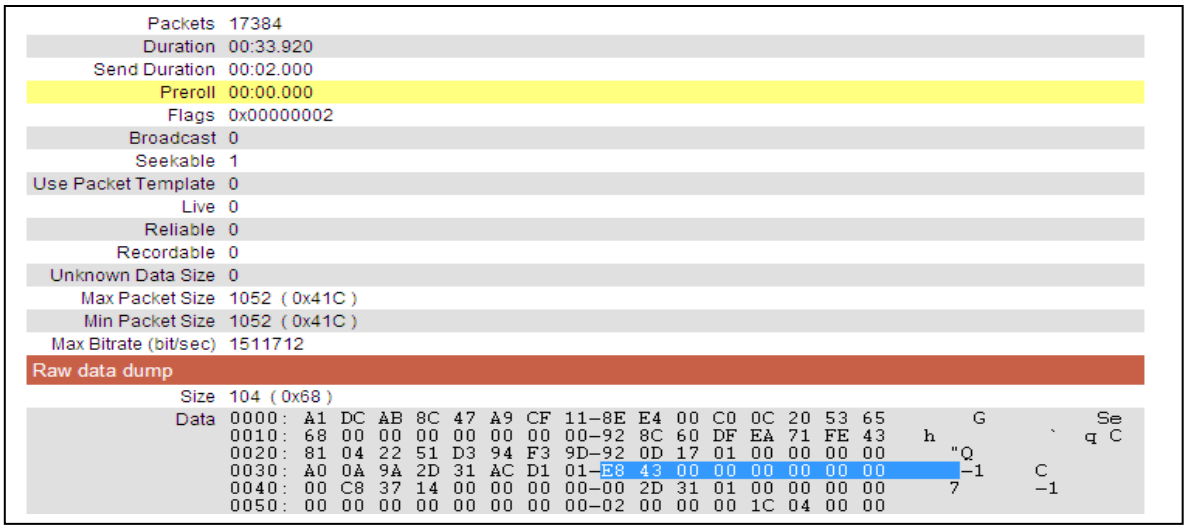


Figure 11: Data Packet Count

The 64 bits which are highlighted determines the data packet entries that exist in the Data Object of the ASF File

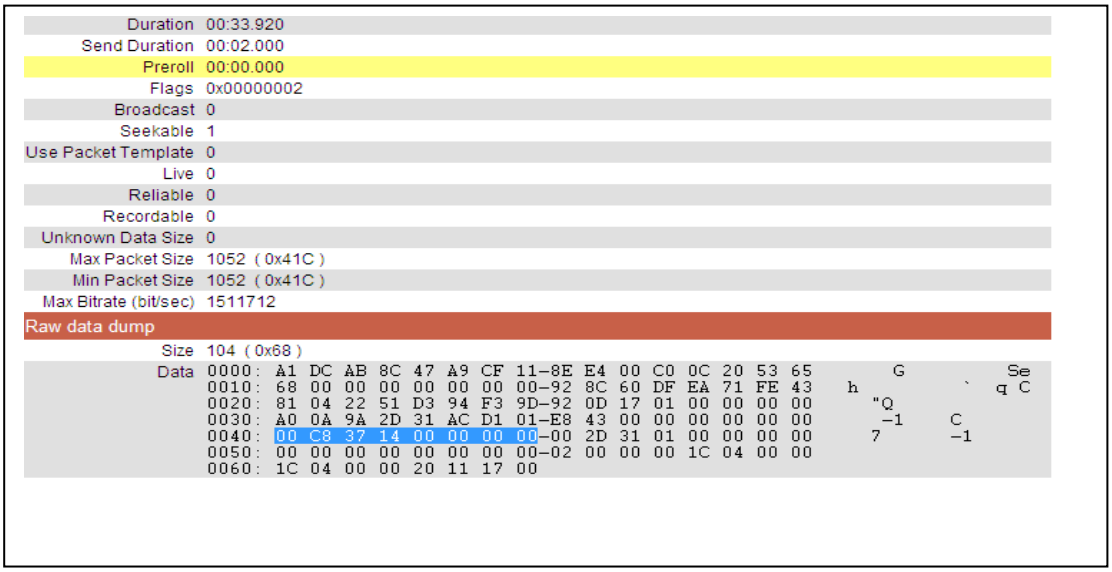


Figure 12: Play Duration

The Highlighted 64 bits determines the play Duration that is the time required to play the file

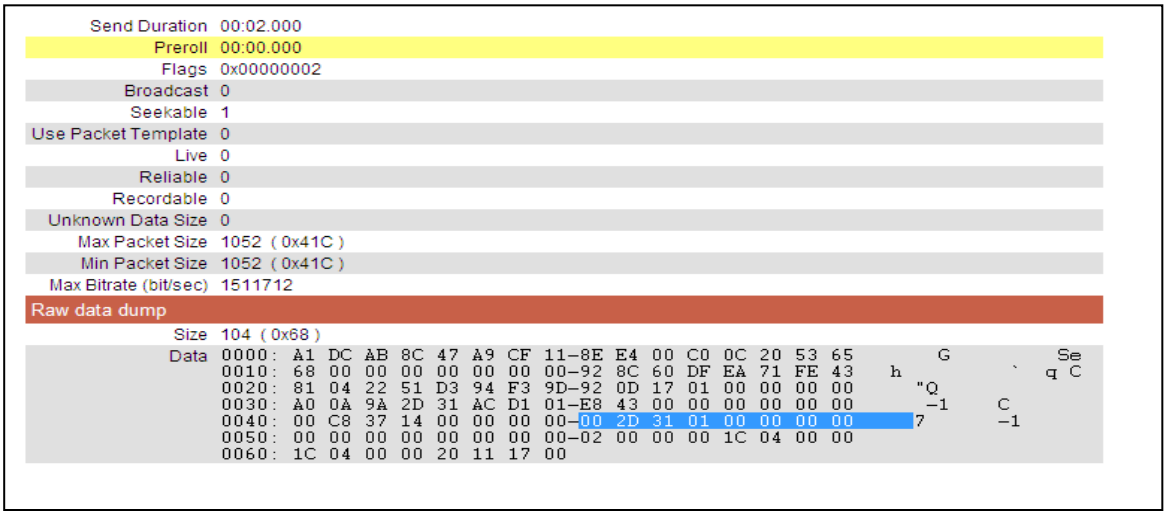


Figure 13: Send Duration

Send Duration is specified by the highlighted 64 bits of File Properties Object of the ASF File.

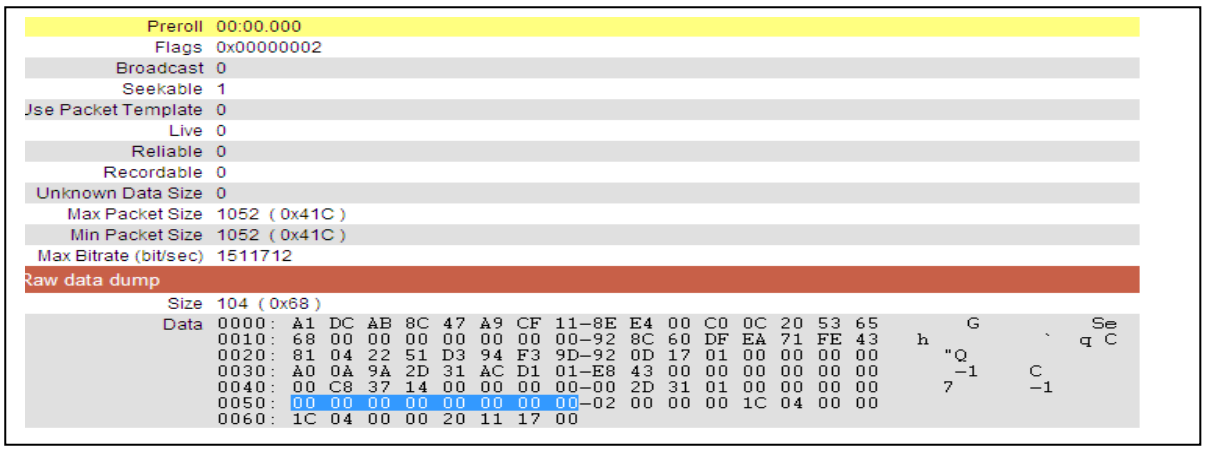


Figure 14: Preroll

The 64 bits determines the Preroll. Preroll is time needed to buffer before the media file is played.

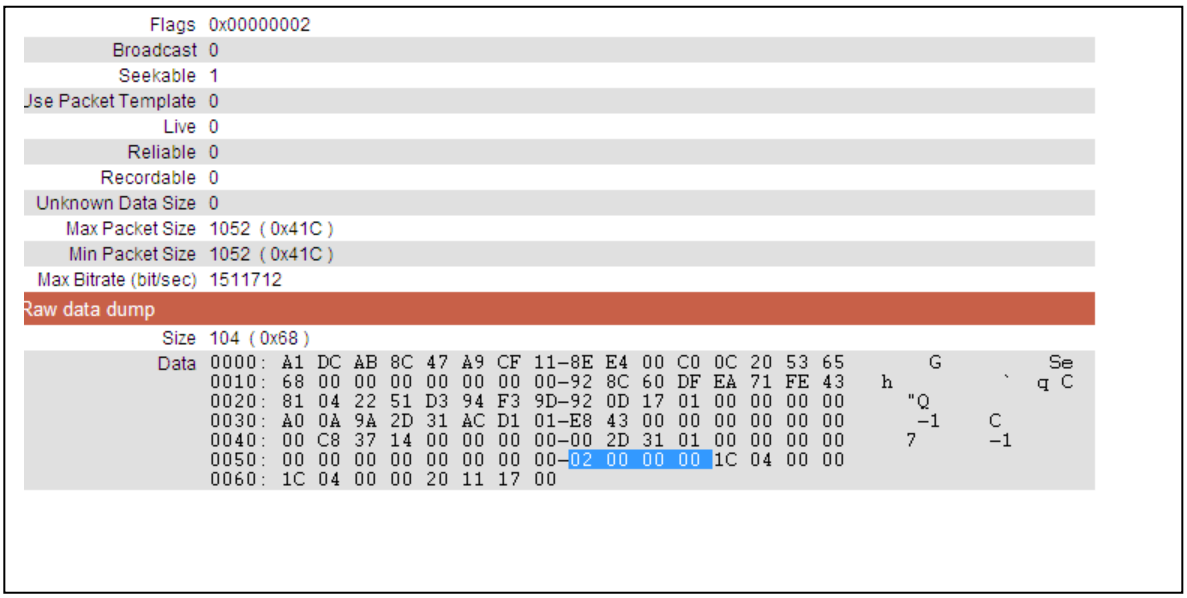


Figure 15: Flags

The Highlighted 32 bits specifies the Flags In LSB (Least Significant Byte)

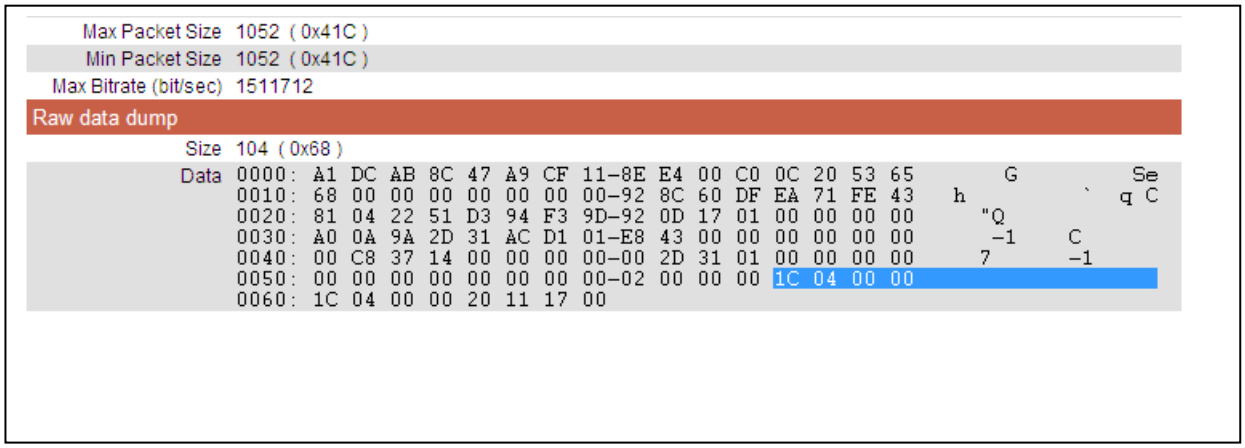


Figure 16: Minimum Data Packet Size

The Highlighted 32 bits determine the minimum packet size of the File Properties Object.

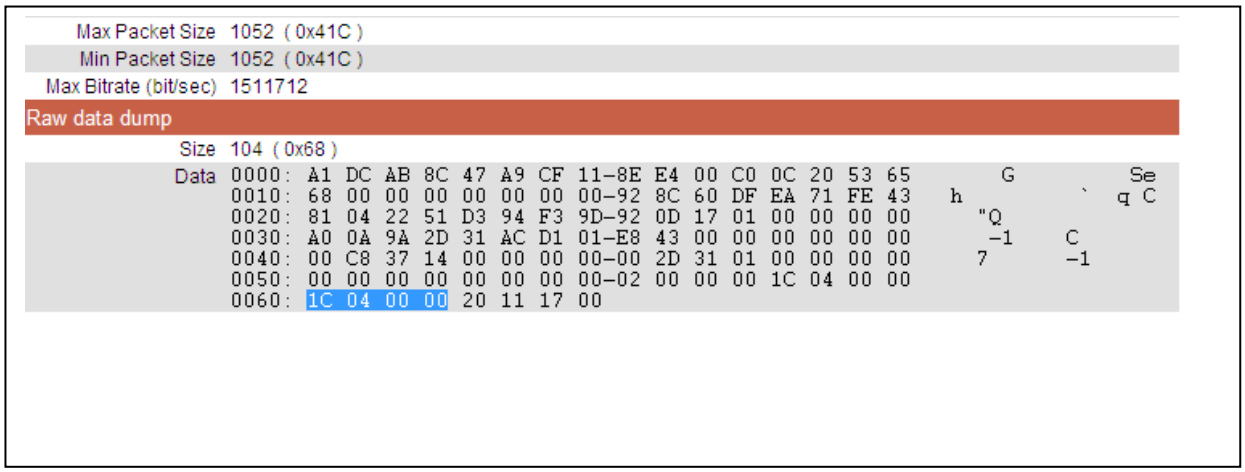


Figure 17: Maximum Packet Size

The Highlighted 32 bits determine the maximum packet size.

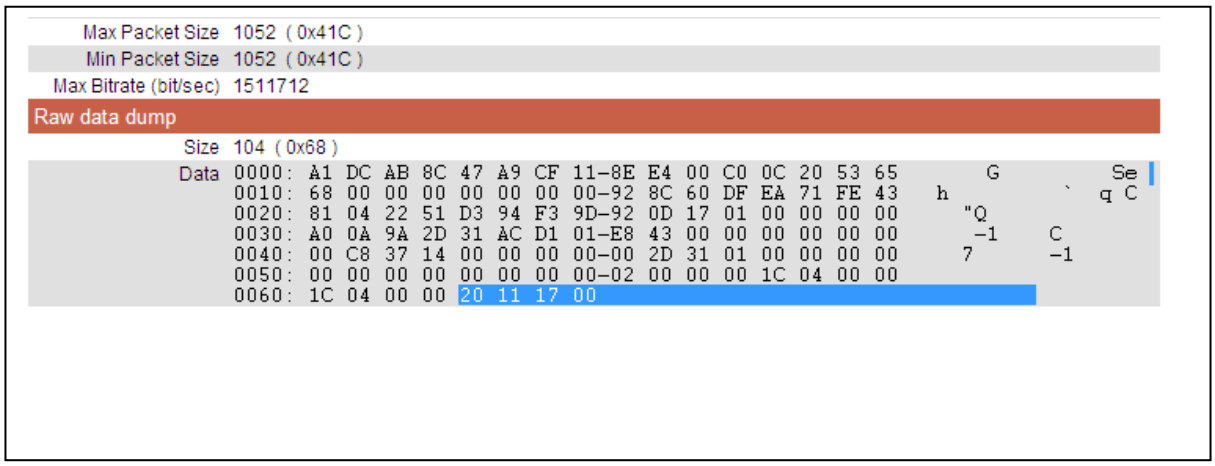


Figure 18: Maximum Bit Rate

The Highlighted 32 bits determine the bit rate in per second of the entire file.

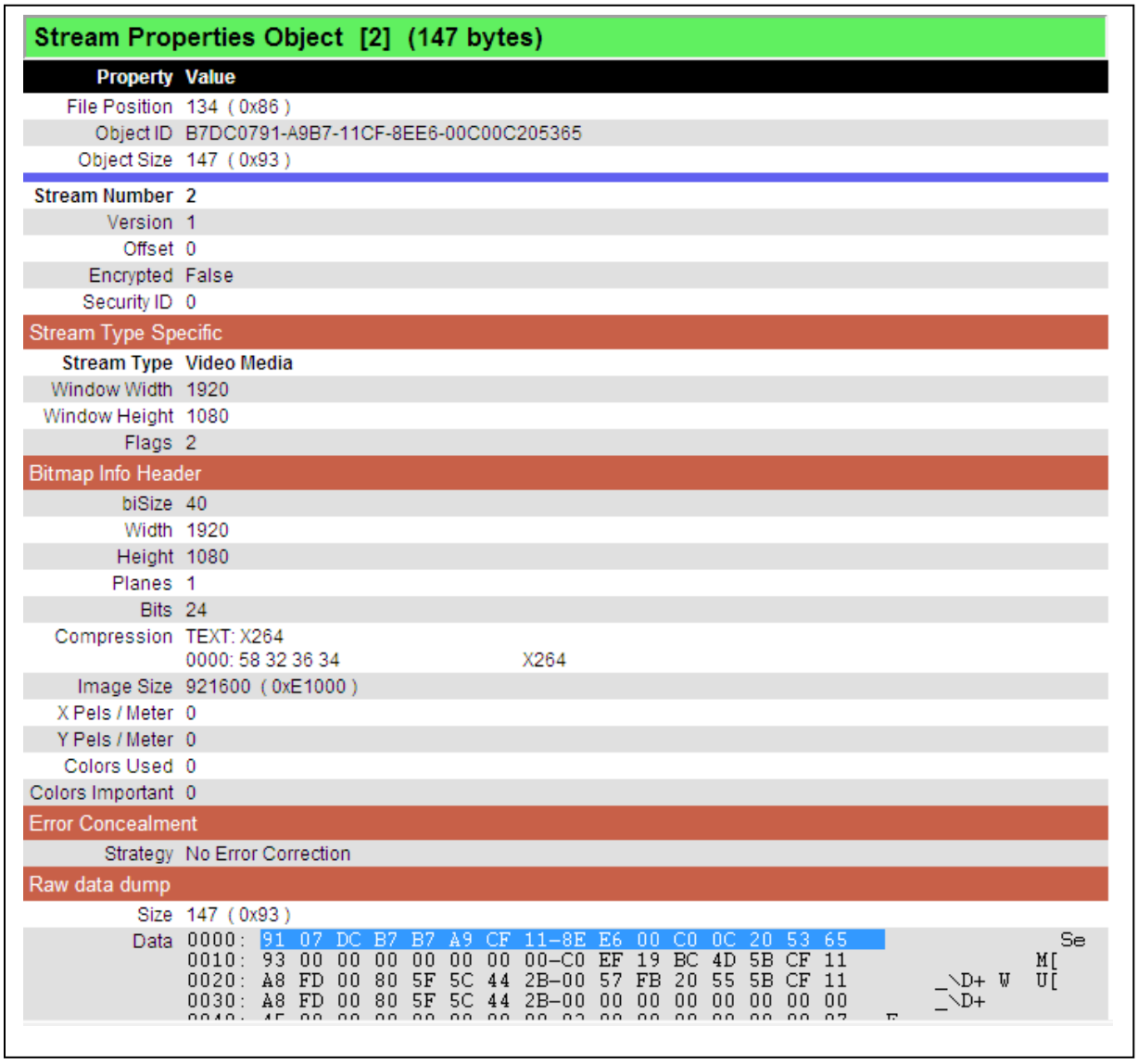
4.4 Forensic Analysis of Stream Properties Object Artifacts

This is another sub object of the header object and like previous sub-object, this is also mandatory object. The first artifact in this object is the object ID (128 bits) which describes the GUID of file properties object. The next artifact in this object is the object size (64 bits) which describes the size of the object in the file properties object. After the object size there is an artifact, the stream type (128 bits) artifact which determines the type of stream available, there must be one stream available and therefore one stream Properties object [25]. The next artifact is the error rectification type (128 bits) which specifies the type of error used by the media files. Time offset (64 bits) is another artifact which determines the presentation time of the media stream. The value of the time offset is included to all the timestamps of the media in the stream. Then is the artifact regarding the data length (32 bits) which is considered to type oriented and this artifact describes the bytes in the field. Another data length which is error correction specific (32 bits) specifies total number of bytes in this field. Like file properties object there is field of flag (16 bits) in the stream properties object. The flag which is available determines Stream number (number of streams), then there are some reserved bits (32 bits) in this field, Encrypted Flag (which describes the data which is encrypted and it can't be read until the data is in unencrypted

form). After these there are some reserved bits. The second last object in this object is the type specific data that determines the type specific data. The Last artifact in this object is the error correction type which determines data which is related to this artifact. The overall structure of this artifact depends on the value that is stored in this field.

Field Name	**Size(Bits)**
Object ID	128
Object Size	64
Stream Type	128
Error Correction Type	128
Time offset	64
Type Specific Data length	32
Error Correction Data length	32
Flags	16
Reserved	32
Type Specific Data	Varies
Error Correction Data	Varies

Table 4: Stream Properties Object

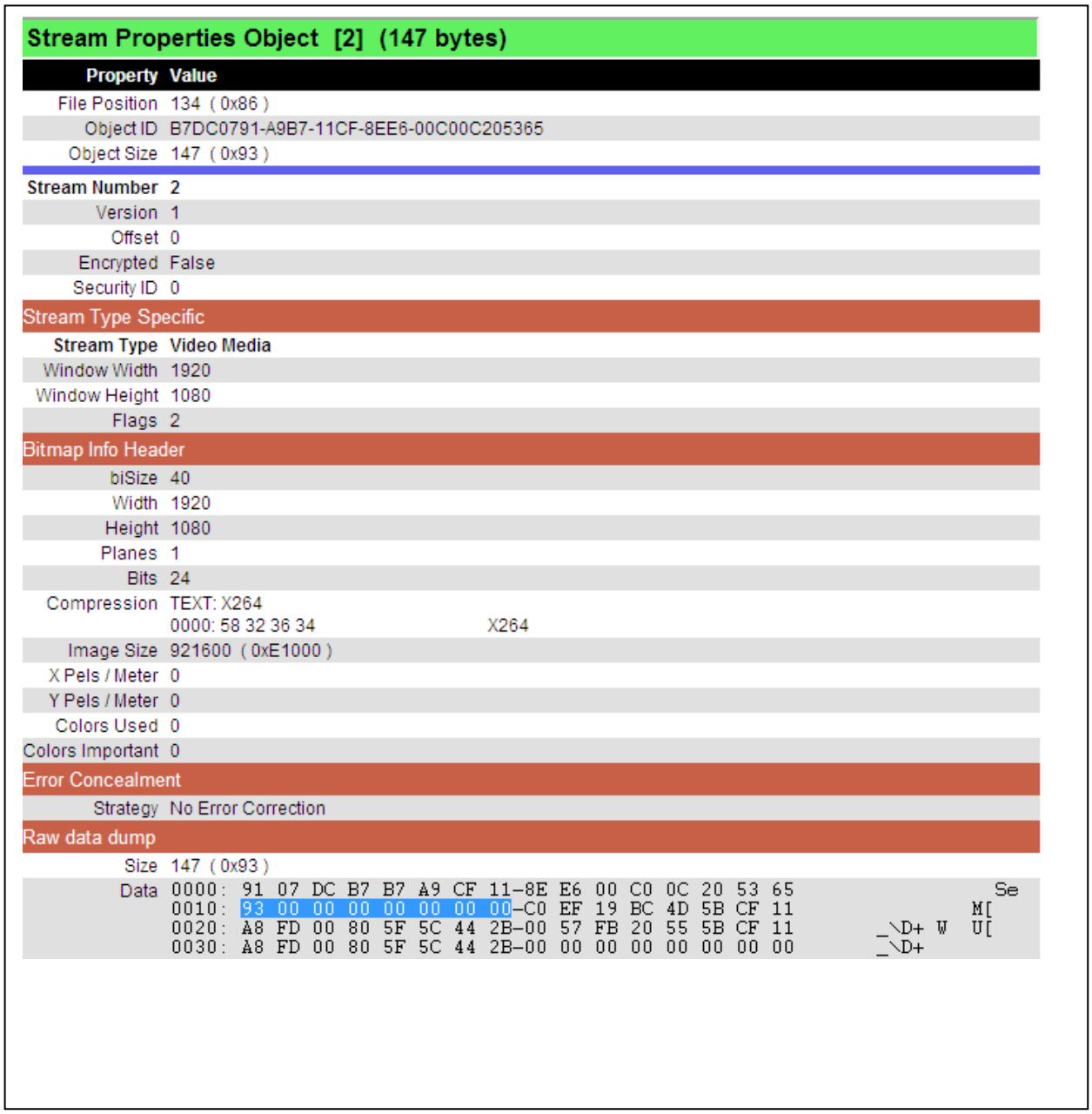


Stream Properties Object [2] (147 bytes)

Property	Value
File Position	134 (0x86)
Object ID	B7DC0791-A9B7-11CF-8EE6-00C00C205365
Object Size	147 (0x93)
Stream Number	**2**
Version	1
Offset	0
Encrypted	False
Security ID	0
Stream Type Specific	
Stream Type	**Video Media**
Window Width	1920
Window Height	1080
Flags	2
Bitmap Info Header	
biSize	40
Width	1920
Height	1080
Planes	1
Bits	24
Compression	TEXT: X264 0000: 58 32 36 34 X264
Image Size	921600 (0xE1000)
X Pels / Meter	0
Y Pels / Meter	0
Colors Used	0
Colors Important	0
Error Concealment	
Strategy	No Error Correction
Raw data dump	
Size	147 (0x93)
Data	0000: 91 07 DC B7 B7 A9 CF 11-8E E6 00 C0 0C 20 53 65 Se 0010: 93 00 00 00 00 00 00 00-C0 EF 19 BC 4D 5B CF 11 M[0020: A8 FD 00 80 5F 5C 44 2B-00 57 FB 20 55 5B CF 11 _\D+ W U[0030: A8 FD 00 80 5F 5C 44 2B-00 00 00 00 00 00 00 00 _\D+

Figure 19: Object ID

The 128 bits which are highlighted determines the GUID for the Stream Properties object of ASF

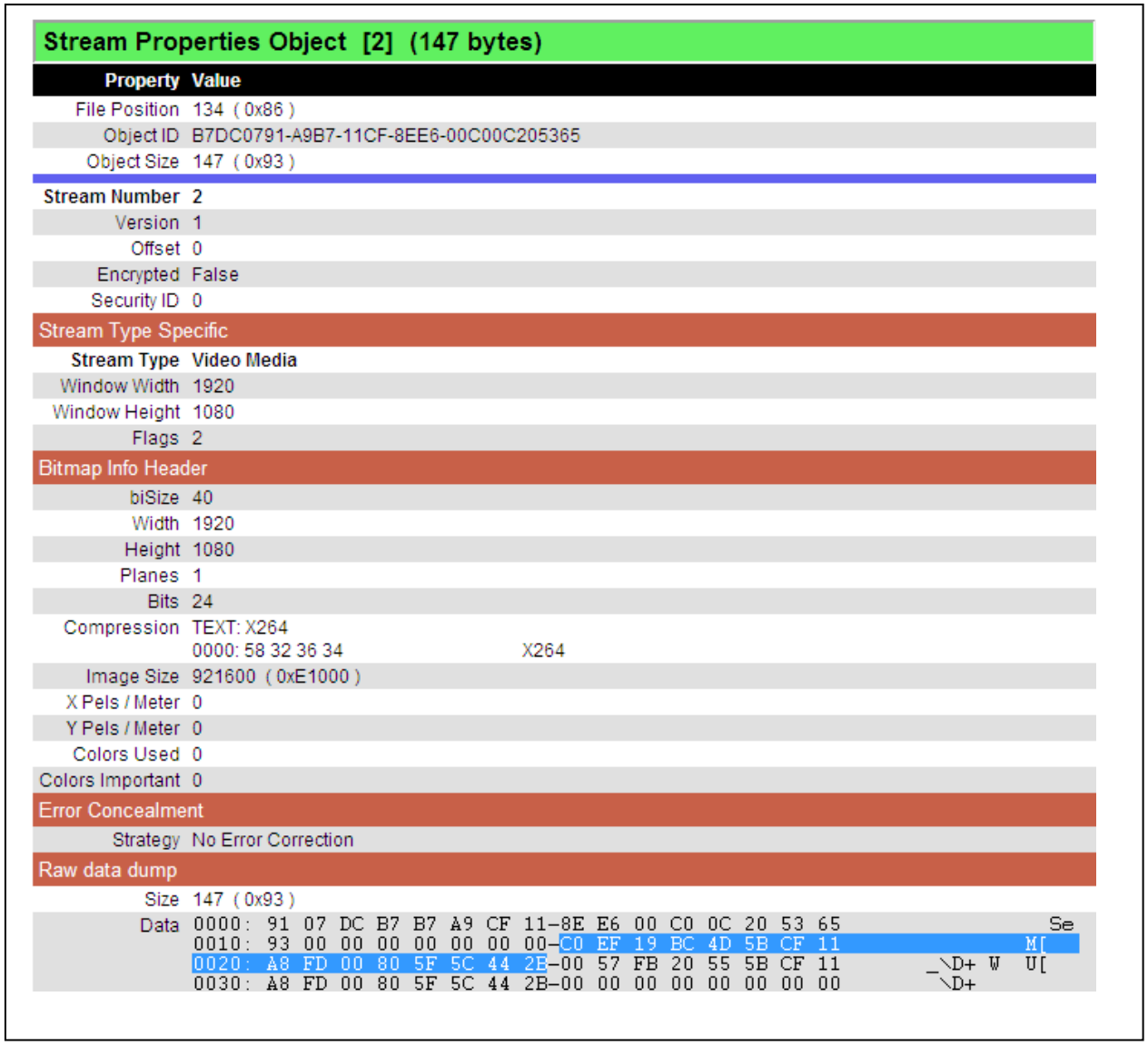


Stream Properties Object [2] (147 bytes)

Property	Value
File Position	134 (0x86)
Object ID	B7DC0791-A9B7-11CF-8EE6-00C00C205365
Object Size	147 (0x93)
Stream Number	**2**
Version	1
Offset	0
Encrypted	False
Security ID	0
Stream Type Specific	
Stream Type	**Video Media**
Window Width	1920
Window Height	1080
Flags	2
Bitmap Info Header	
biSize	40
Width	1920
Height	1080
Planes	1
Bits	24
Compression	TEXT: X264 0000: 58 32 36 34 X264
Image Size	921600 (0xE1000)
X Pels / Meter	0
Y Pels / Meter	0
Colors Used	0
Colors Important	0
Error Concealment	
Strategy	No Error Correction
Raw data dump	
Size	147 (0x93)
Data	0000: 91 07 DC B7 B7 A9 CF 11-8E E6 00 C0 0C 20 53 65 Se 0010: 93 00 00 00 00 00 00 00-C0 EF 19 BC 4D 5B CF 11 M[0020: A8 FD 00 80 5F 5C 44 2B-00 57 FB 20 55 5B CF 11 _\D+ W U[0030: A8 FD 00 80 5F 5C 44 2B-00 00 00 00 00 00 00 00 _\D+

Figure 20: Object Size

The 64 bits determine the Object Size of the Stream Properties object of ASF File.

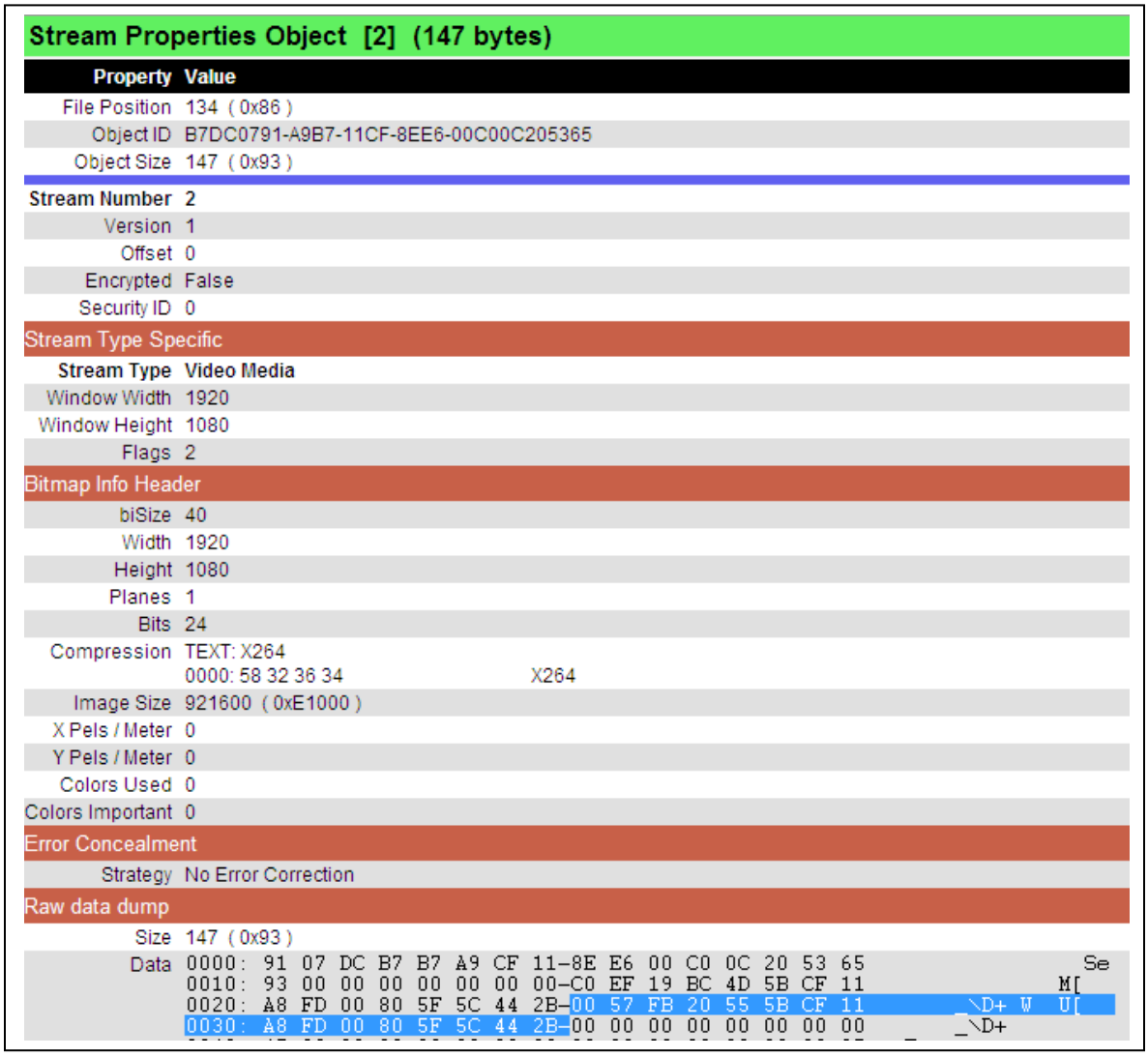


Stream Properties Object [2] (147 bytes)

Property	Value
File Position	134 (0x86)
Object ID	B7DC0791-A9B7-11CF-8EE6-00C00C205365
Object Size	147 (0x93)
Stream Number	**2**
Version	1
Offset	0
Encrypted	False
Security ID	0
Stream Type Specific	
Stream Type	**Video Media**
Window Width	1920
Window Height	1080
Flags	2
Bitmap Info Header	
biSize	40
Width	1920
Height	1080
Planes	1
Bits	24
Compression	TEXT: X264 0000: 58 32 36 34 X264
Image Size	921600 (0xE1000)
X Pels / Meter	0
Y Pels / Meter	0
Colors Used	0
Colors Important	0
Error Concealment	
Strategy	No Error Correction
Raw data dump	
Size	147 (0x93)
Data	0000: 91 07 DC B7 B7 A9 CF 11-8E E6 00 C0 0C 20 53 65 Se 0010: 93 00 00 00 00 00 00 00-C0 EF 19 BC 4D 5B CF 11 M[0020: A8 FD 00 80 5F 5C 44 2E-00 57 FB 20 55 5B CF 11 _\D+ W U[0030: A8 FD 00 80 5F 5C 44 2E-00 00 00 00 00 00 00 00 _\D+

Figure 21: Stream Type

The 128 bits determines the Stream type present in the ASF File.

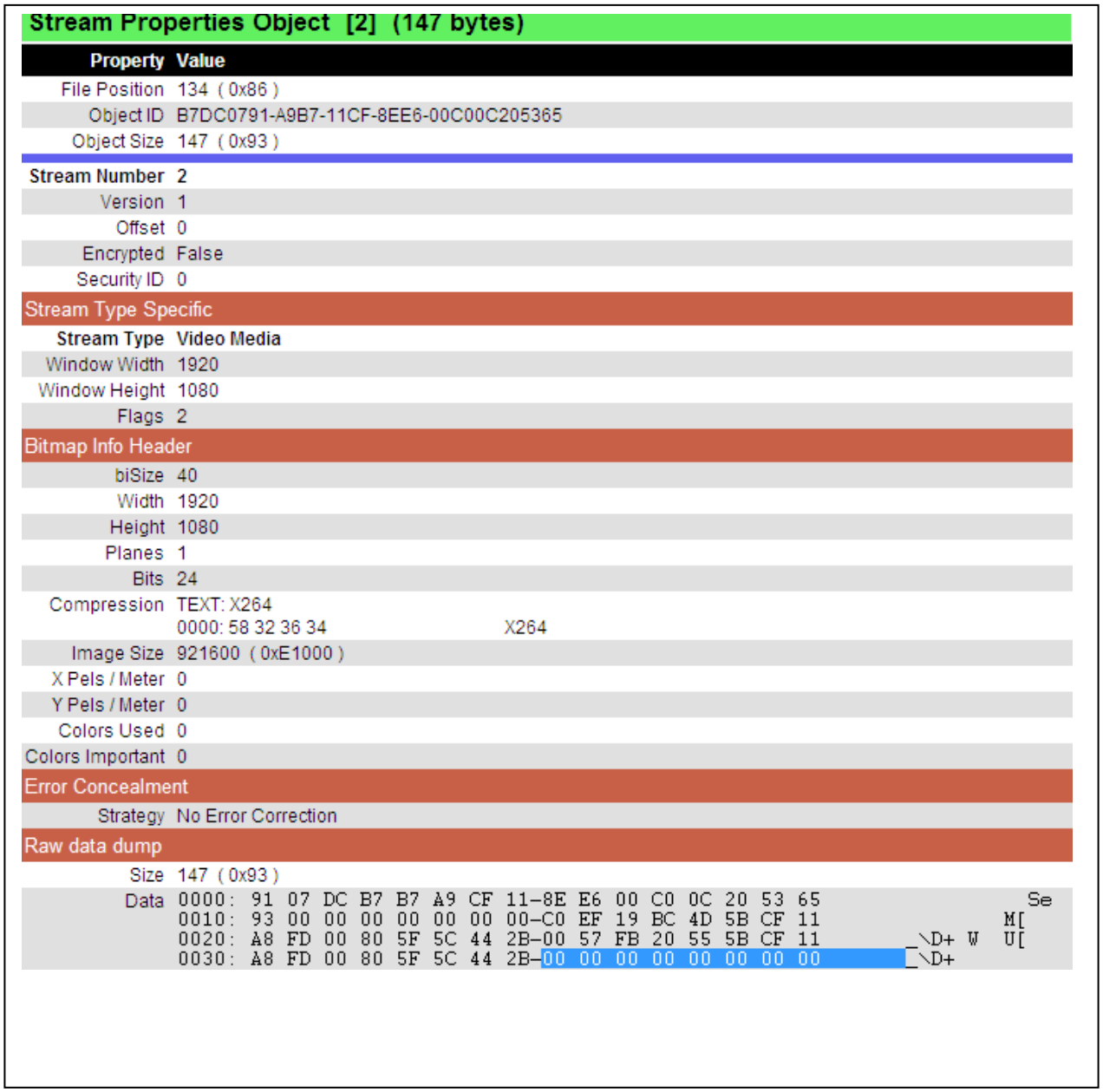


Stream Properties Object [2] (147 bytes)

Property	Value
File Position	134 (0x86)
Object ID	B7DC0791-A9B7-11CF-8EE6-00C00C205365
Object Size	147 (0x93)
Stream Number	**2**
Version	1
Offset	0
Encrypted	False
Security ID	0
Stream Type Specific	
Stream Type	**Video Media**
Window Width	1920
Window Height	1080
Flags	2
Bitmap Info Header	
biSize	40
Width	1920
Height	1080
Planes	1
Bits	24
Compression	TEXT: X264 0000: 58 32 36 34 X264
Image Size	921600 (0xE1000)
X Pels / Meter	0
Y Pels / Meter	0
Colors Used	0
Colors Important	0
Error Concealment	
Strategy	No Error Correction
Raw data dump	
Size	147 (0x93)
Data	0000: 91 07 DC B7 B7 A9 CF 11-8E E6 00 C0 0C 20 53 65 Se 0010: 93 00 00 00 00 00 00 00-C0 EF 19 BC 4D 5B CF 11 M[0020: A8 FD 00 80 5F 5C 44 2B-00 57 FB 20 55 5B CF 11 _\D+ W U[0030: A8 FD 00 80 5F 5C 44 2B-00 00 00 00 00 00 00 00 _\D+

Figure 22: Error Correction Type

The 128 bits represent the Error Correction type used by the digital media Stream.



Stream Properties Object [2] (147 bytes)

Property	Value
File Position	134 (0x86)
Object ID	B7DC0791-A9B7-11CF-8EE6-00C00C205365
Object Size	147 (0x93)
Stream Number	2
Version	1
Offset	0
Encrypted	False
Security ID	0
Stream Type Specific	
Stream Type	**Video Media**
Window Width	1920
Window Height	1080
Flags	2
Bitmap Info Header	
biSize	40
Width	1920
Height	1080
Planes	1
Bits	24
Compression	TEXT: X264 0000: 58 32 36 34 X264
Image Size	921600 (0xE1000)
X Pels / Meter	0
Y Pels / Meter	0
Colors Used	0
Colors Important	0
Error Concealment	
Strategy	No Error Correction
Raw data dump	
Size	147 (0x93)
Data	0000: 91 07 DC B7 B7 A9 CF 11-8E E6 00 C0 0C 20 53 65 Se 0010: 93 00 00 00 00 00 00 00-C0 EF 19 BC 4D 5B CF 11 M[0020: A8 FD 00 80 5F 5C 44 2B-00 57 FB 20 55 5B CF 11 _\D+ W U[0030: A8 FD 00 80 5F 5C 44 2B-00 00 00 00 00 00 00 00 _\D+

Figure 23: Time Offset

The 8 bits represents the presentation time offset of the stream in 100 Nano Seconds.

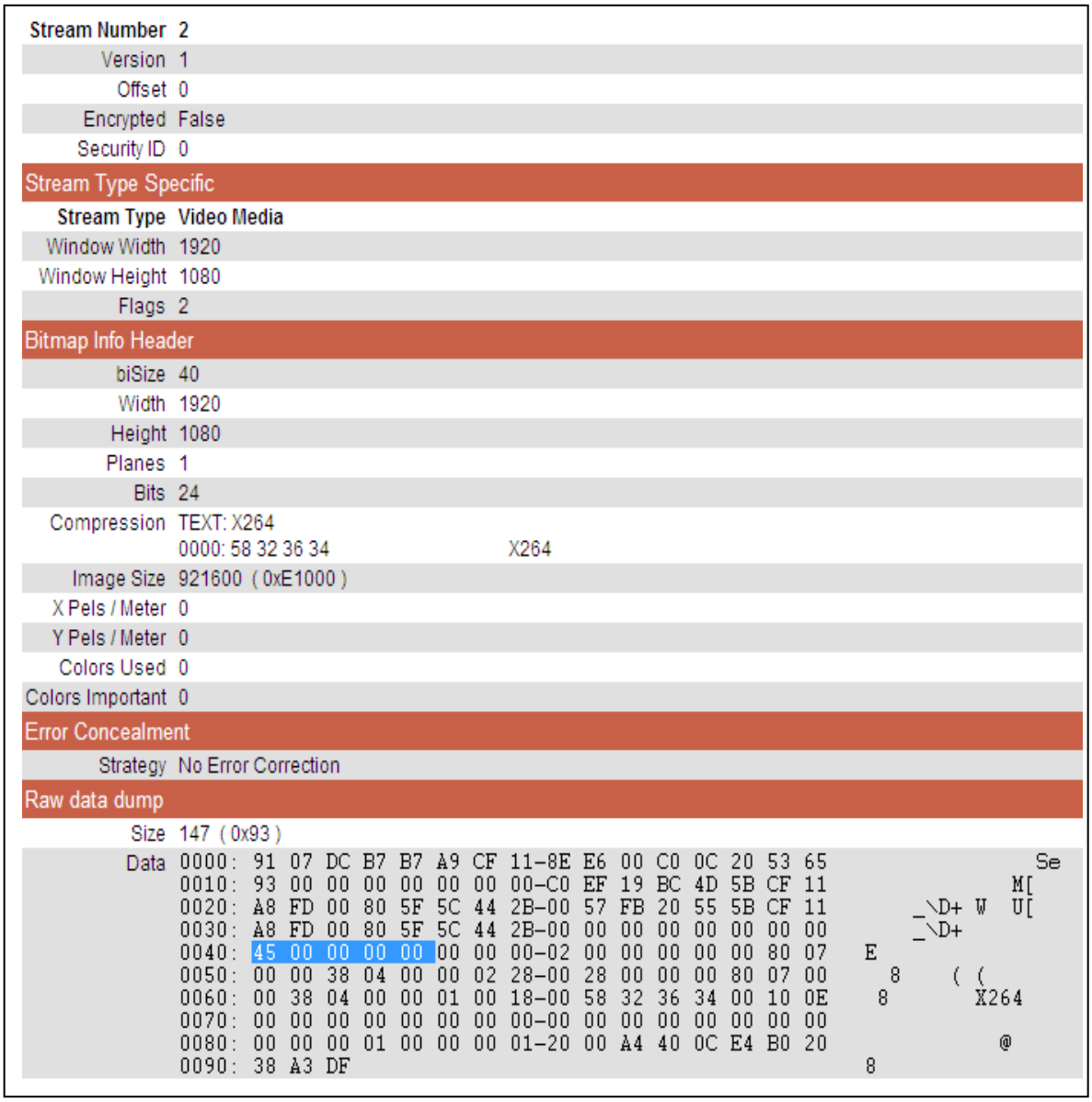


Figure 24: Type Specific Data Length

Highlighted part determines time Specific data length in number of bytes.

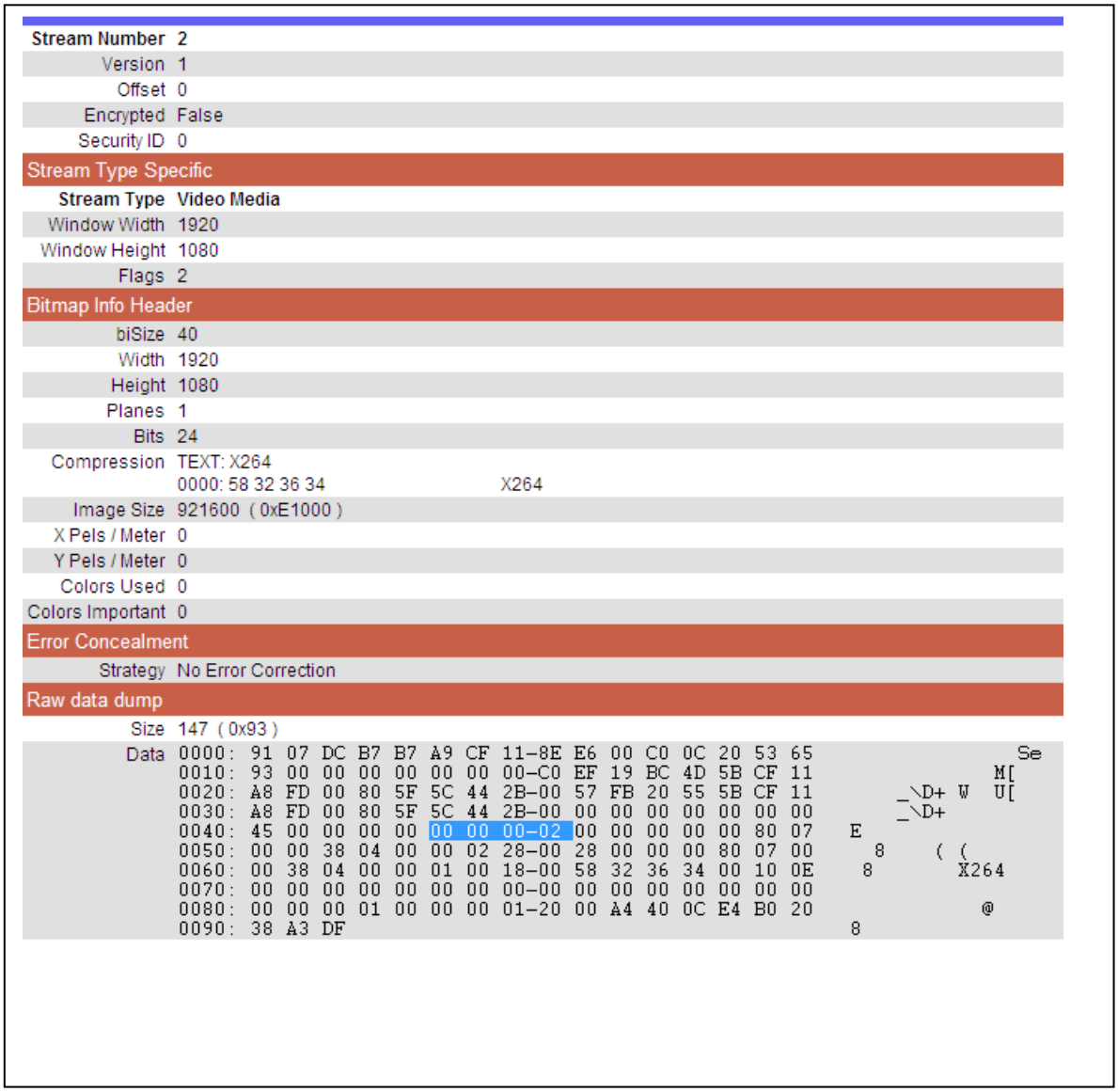


Figure 25: Error Correction Data Length

32 bits determine Error Correction data length in number of bytes.

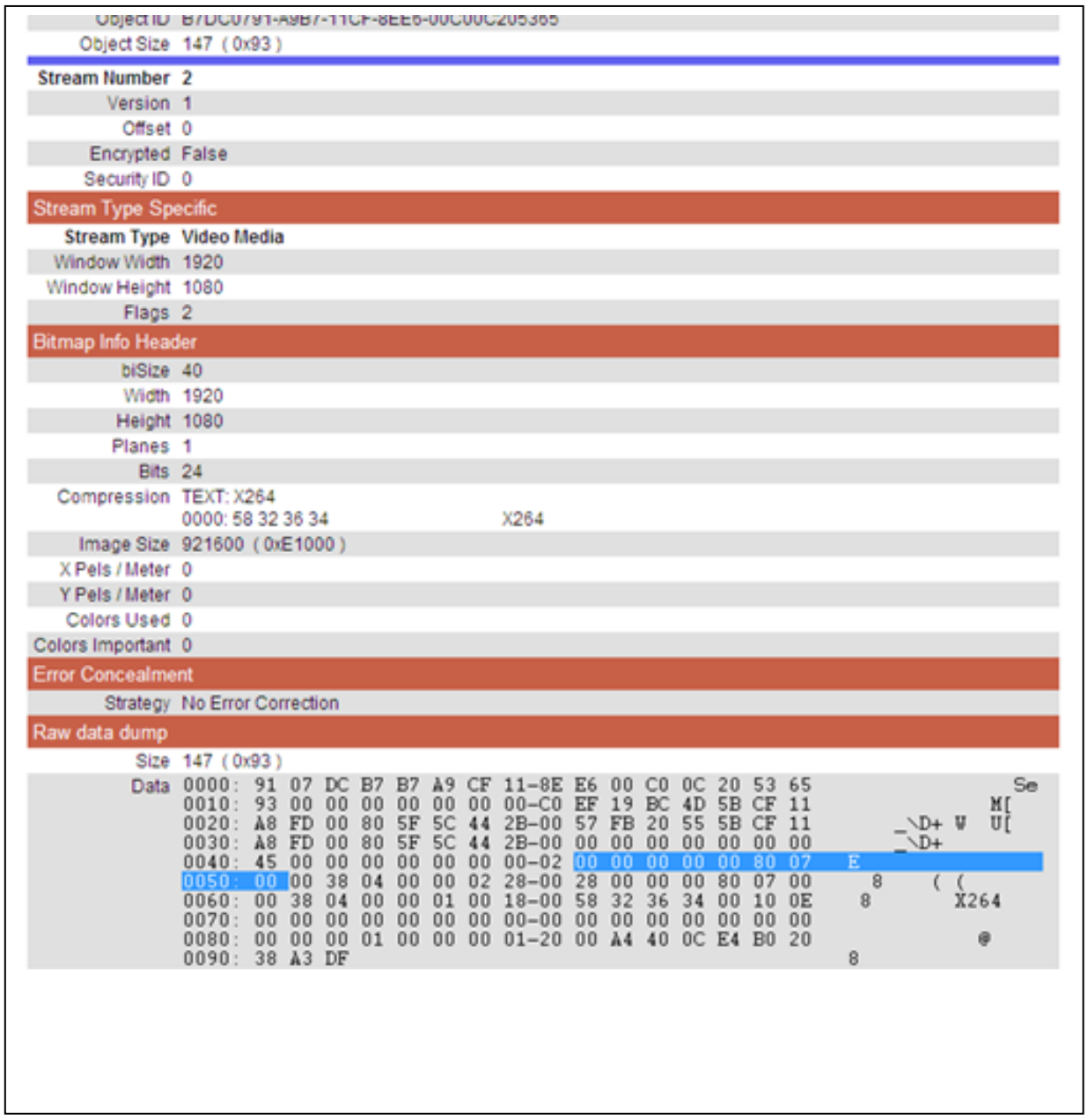


Figure 26: Flags

The Highlighted part shows the Flags which stores in LSB order.

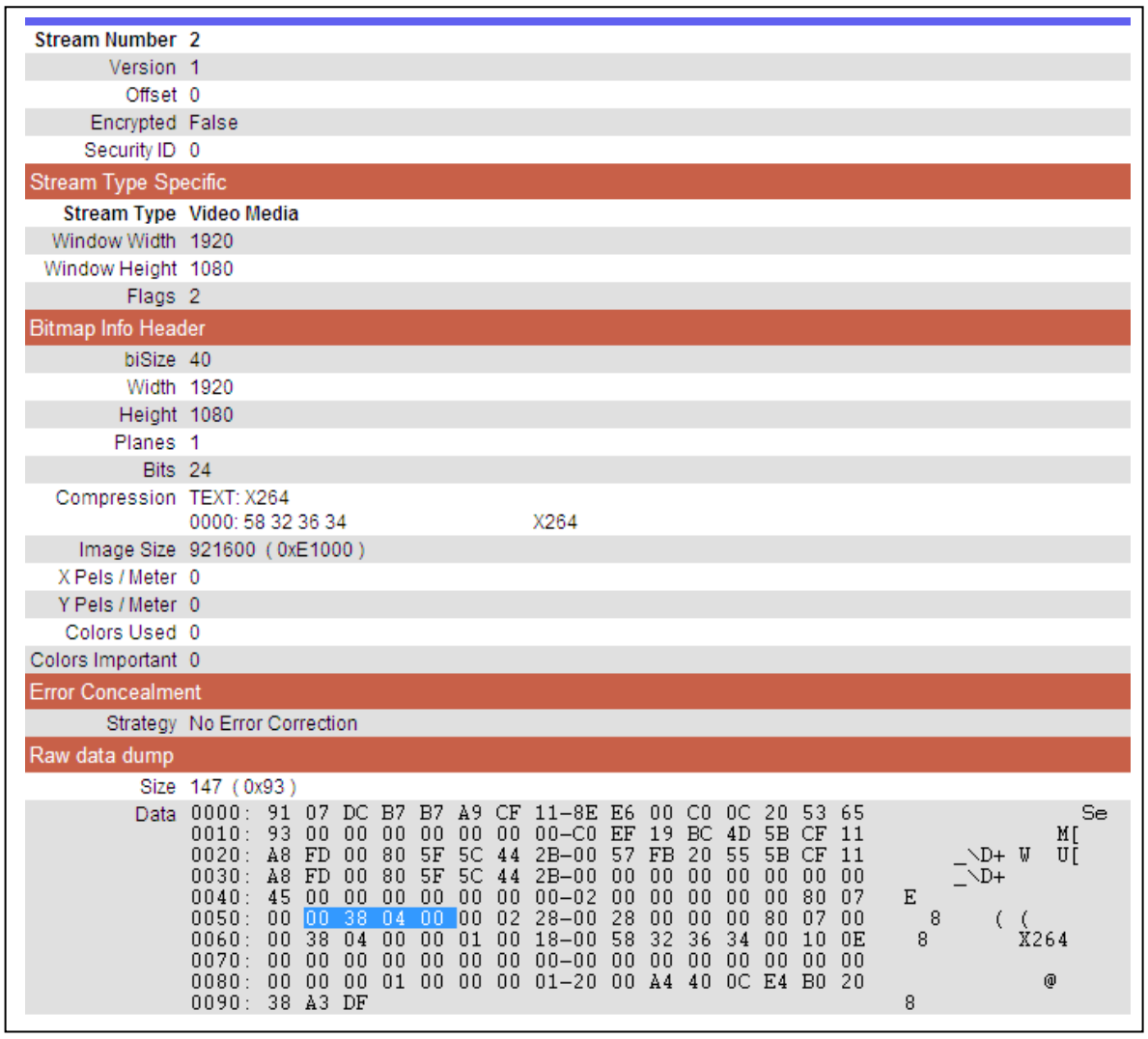


Figure 27: Reserve Field

The last 8 bits represent the reserved field in Stream Properties Object.

4.5 Forensic Analysis of Header Extension Object Artifacts

Like Header Object, the header extension object is mandatory object. The first artifact in this object is the object ID (128 bits) which determines the GUID for the header extension object. The next artifact is the object size (64 bits) of the object which specifies the size of the object for the header extension. Then there are the reserved fields. First field is 128 bits and the second field is of 16 bits. After the reserved fields then there is size of header extension (32 bits) which determines the total number of bytes stored in the field. The last object in this header extension (Size Varies) is the header extension data which determines bytes having extended header data.

Field Name	**File Size(bits)**
Object ID	128
Object Size	64
Reserved Field 1	128
Reserved Field 2	16
Header Extension Data Size	32
Header Extension Data	varies

Table 5: Header Extension Object

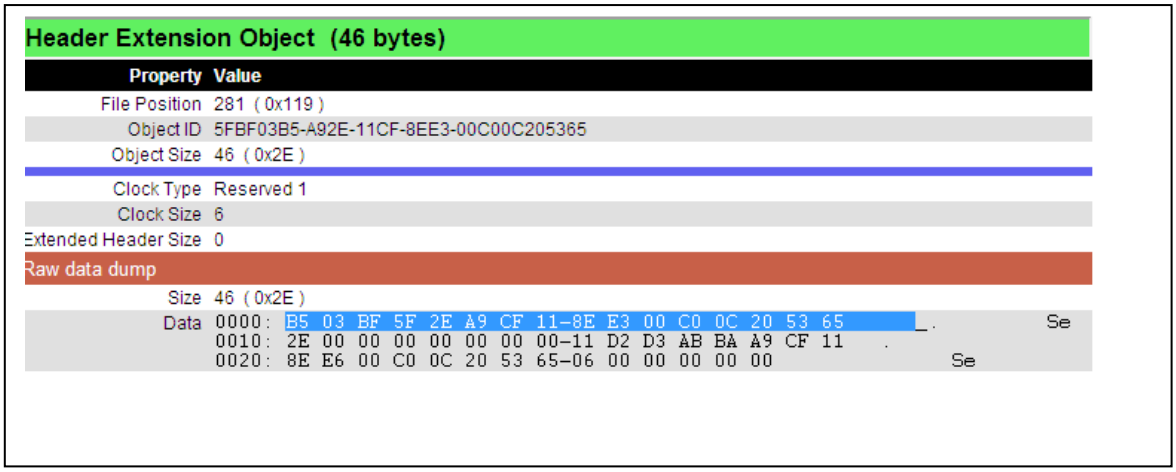


Figure 28: Object ID

The 128 bit shows the object ID which is GUID of the Header Extension Object.

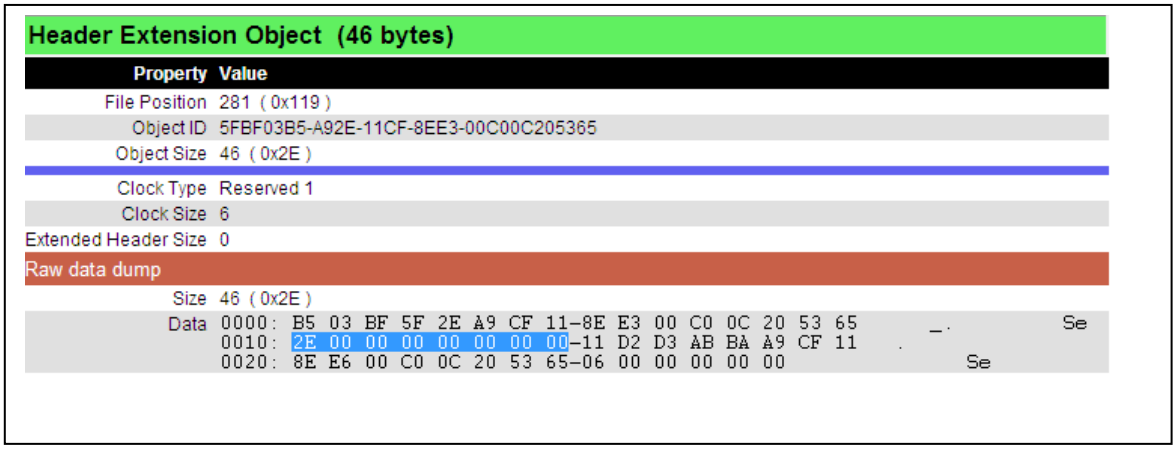


Figure 29: Object Size

The 64 bits shows the Size of Header Extension Object.

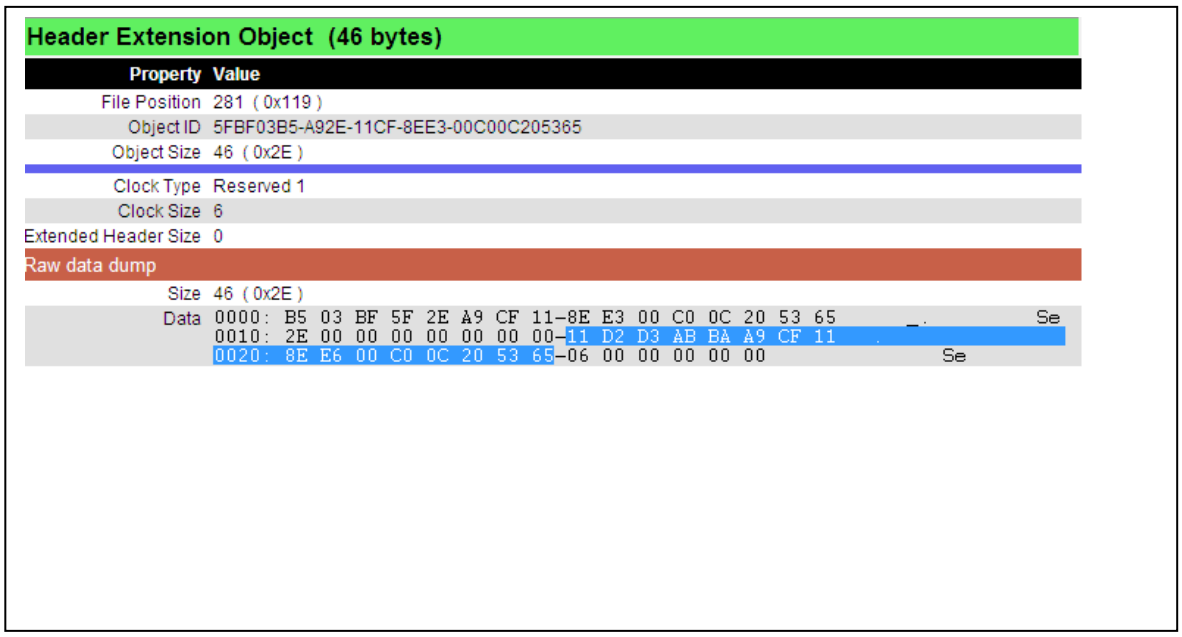


Figure 30: Reserved Field 1

The Highlighted 128 bits represent the Reserved Field 1.

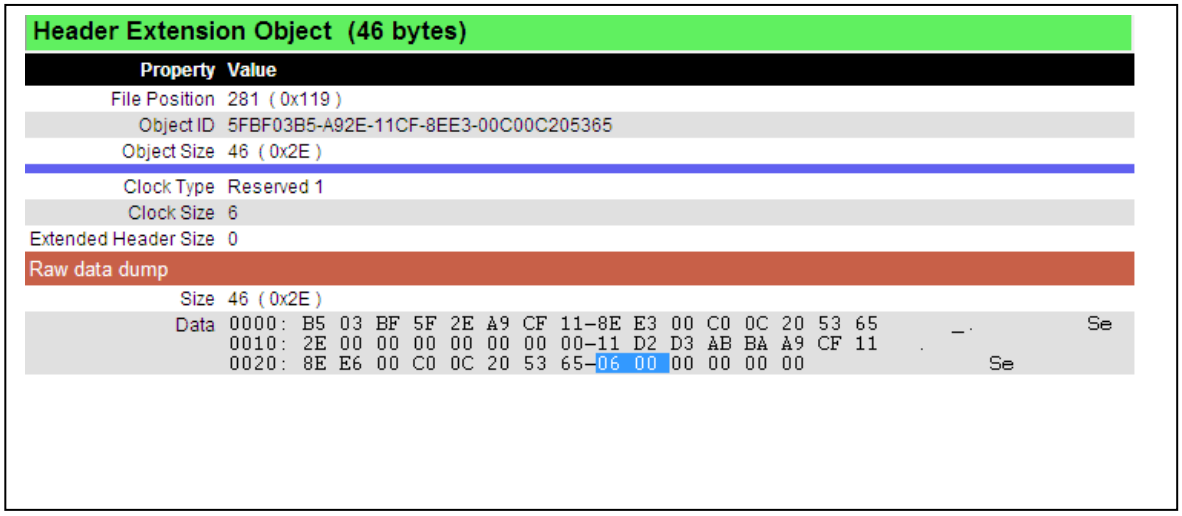


Figure 31: Reserved Field 2

The Highlighted 16 bits represent the Reserved Field 2.

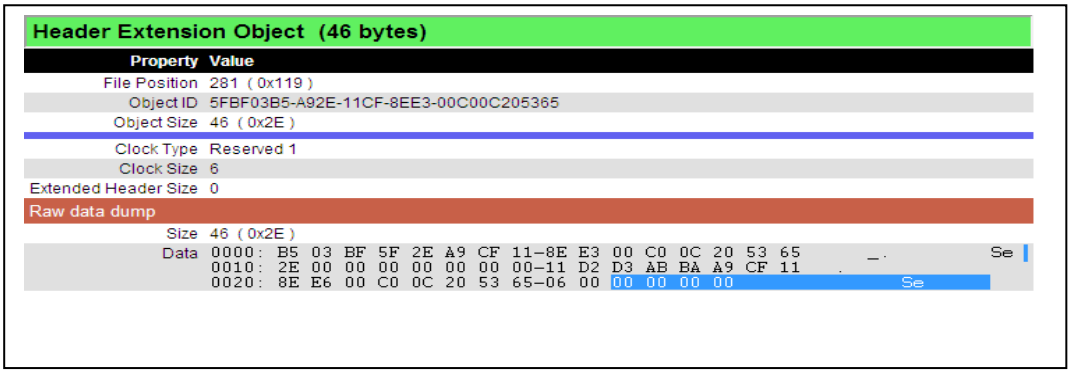


Figure 32: Header Extension Data Size

The last 32 bits represents Header Extension data which includes the Extended objects present in the Header Extension Object

4.6 Forensic Analysis of Data object Artifacts

This object is important object in file structure of ASF file as it contains all the data packets of the media file. The first artifact is the object ID (128 bits) which determines the GUID of the data object. The second artifact is the object size (64 bits) which describes the size of object. Then comes the artifact which is ID (128 bits) of the file which is unique for every file and with slightest of the modifications or changes the file ID will be changed. Then there is the artifact of data packets (64 bits) which specifies the total number of packets in the data object. Then there are some reserved bits. The last artifact is regarding the type of data packets (Varies in Size). Some of the data packets are as follows, there could be two schemes of data packets .The first scheme consist of Error correction data (optional), then there is Payload parsing [26].Then comes the payload (the digital data follows the payload parsing data), the last is the Padded data (optional).The second scheme consist of error correction data (optional), the second data type could be opaque data and the last is padded data which is optional.

Field name	Size (bits)
Object ID	128
Object Size	64
File ID	128
Total Data Packets	64
Reserved	16
Data Packets	Varies

Table 6: Data Object

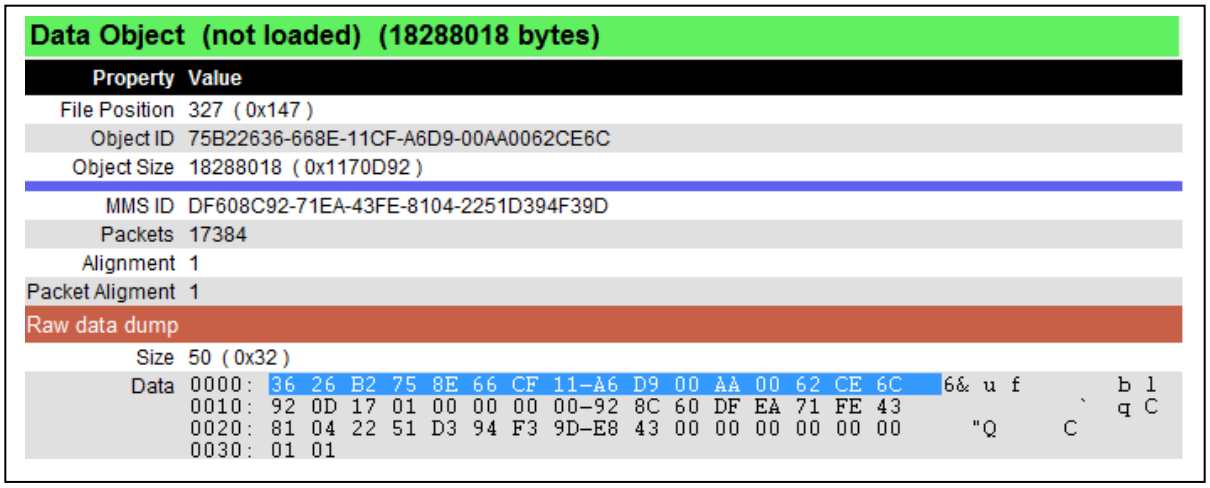


Figure 33: Object ID

The 128 bits represents the GUID of the Data Object.

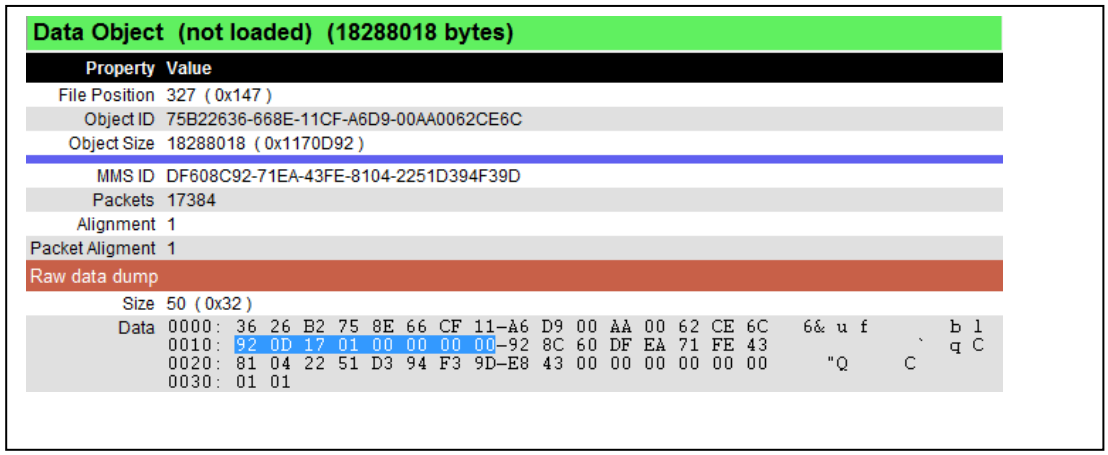


Figure 34: Object Size

The next artifact is the object size which describes the object size of the Data Object

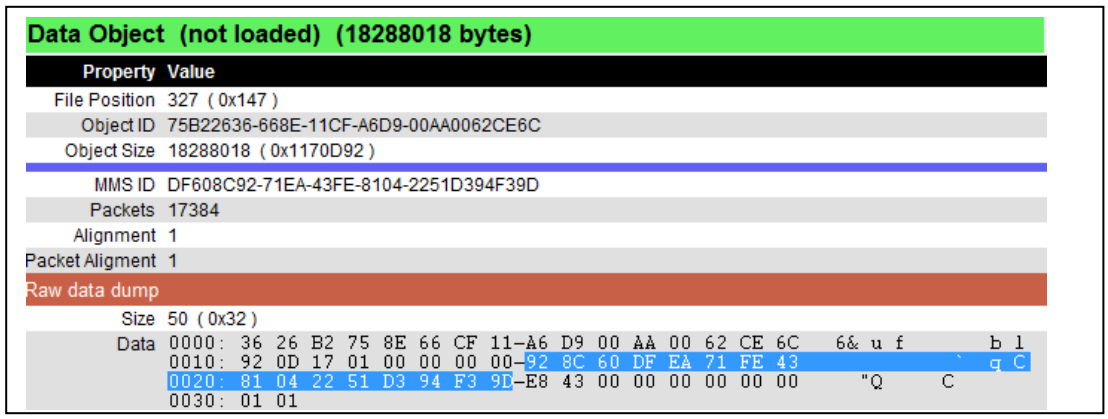


Figure 35: File ID

The128 bits represent the File Id which is unique and with the slightest of changes it get modified.

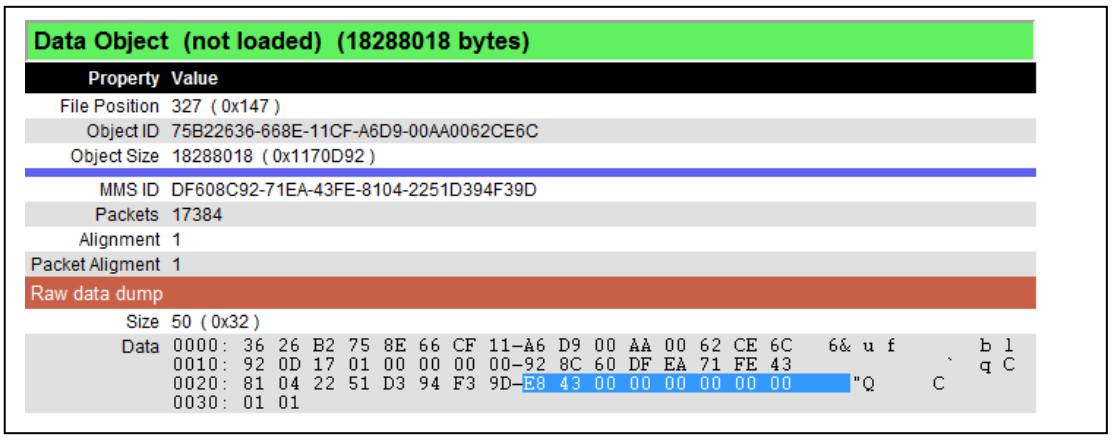


Figure 36: Total Data Packets

The 64 bits represents the total number of packets that exist in the data object of the ASF File

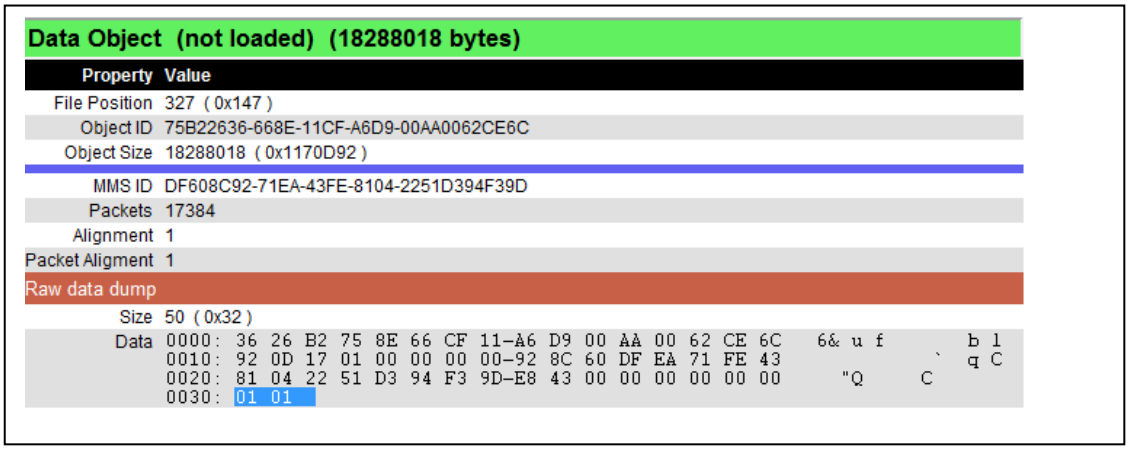


Figure 37: Reserved

The Highlighted 16 bits represent the Reserved Field of Data Object.

4.7 Forensic Analysis of Simple Index Object Artifacts

This object in this file is optional object. The first artifact in this object is the object Id (128 bits) which specifies the GUID of Index object. The second is the object size (64 bits). Then comes the File ID (128 bits) which is unique for every file with modifications it will be changed. Time interval between different entries is specified by the index entry time (64 bits). The next artifact is the maximum packet count (32 bits) which specifies total number of packets. Number of index entries (32 bits) is determined by the artifact of index entries count. The last artifact in this object is Index entries (Varies in Size) which are divided into packet number and packet count.

Field name	**Size (bits)**
Object ID	128
Object Size	64
File ID	128
Index Entry Time Interval	64
Maximum Packet Count	32
Index Entries Count	32
Index Entries	varies

Table 7: Simple Index Object

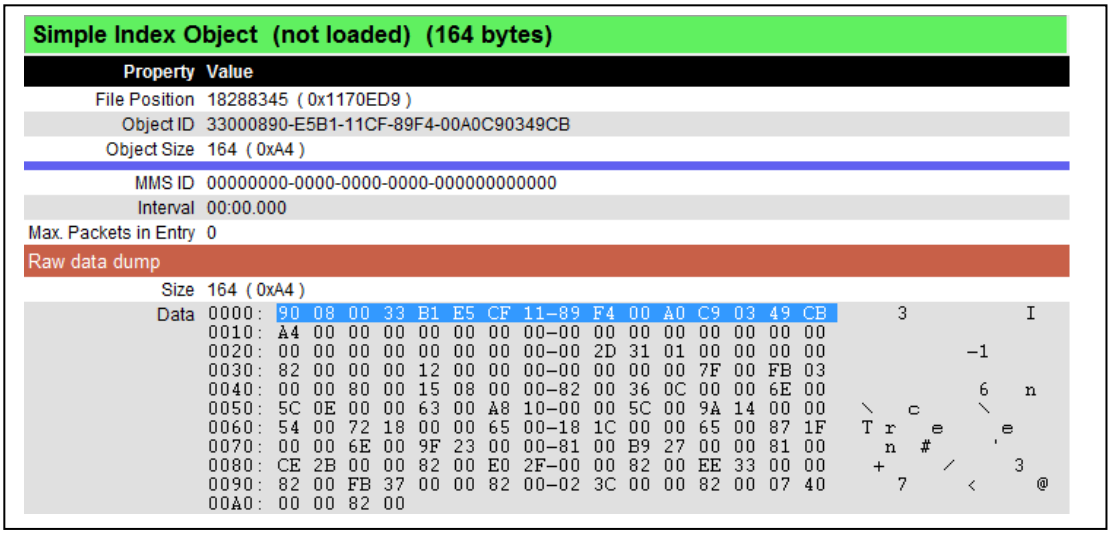


Figure 38: Object ID

The 128 bit highlighted part represents the object ID which is GUID of the Simple Index Object.

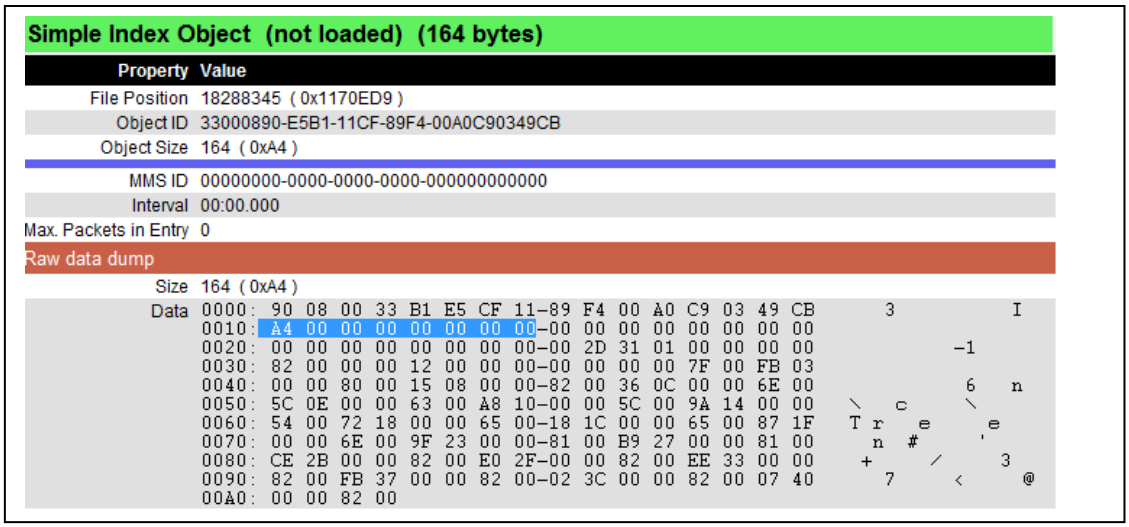


Figure 39: Object Size

The 64 bit represents the object Size of the Simple Index Object.

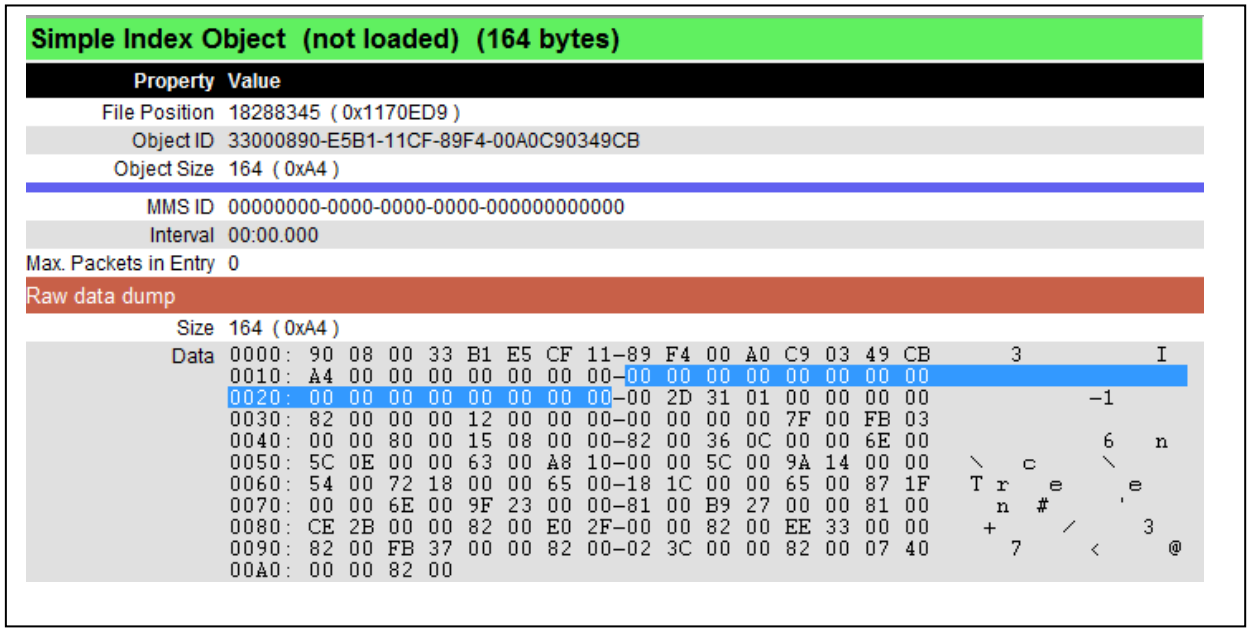


Figure 40: File ID

The128 bits represent the File Id which is unique and with the slightest of changes it gets modified.

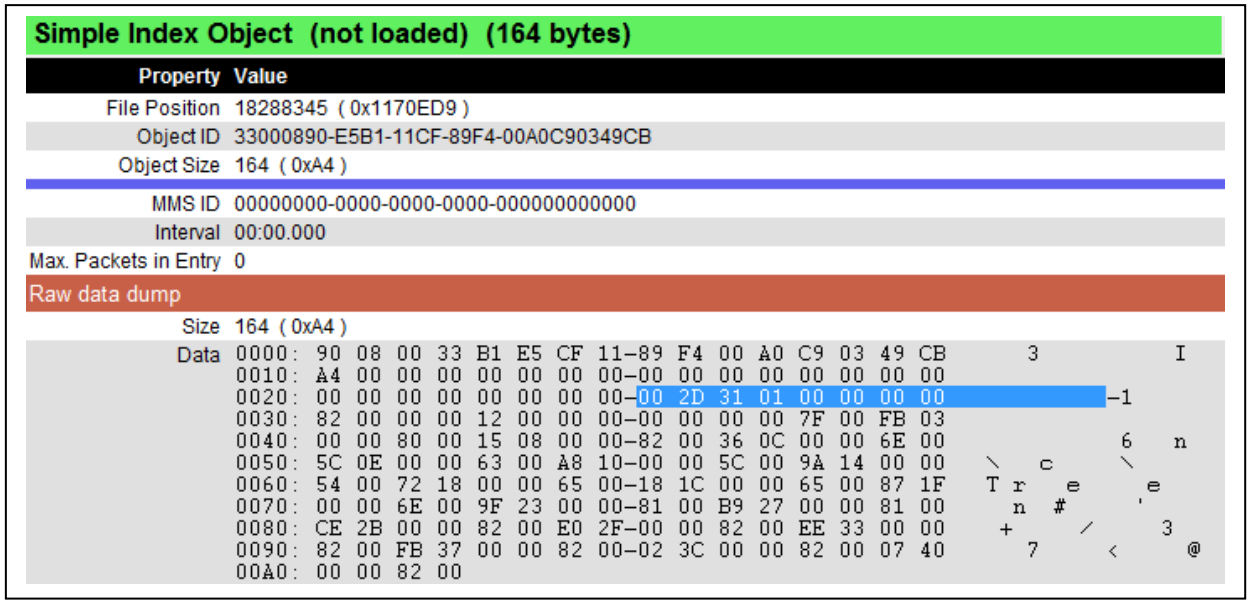
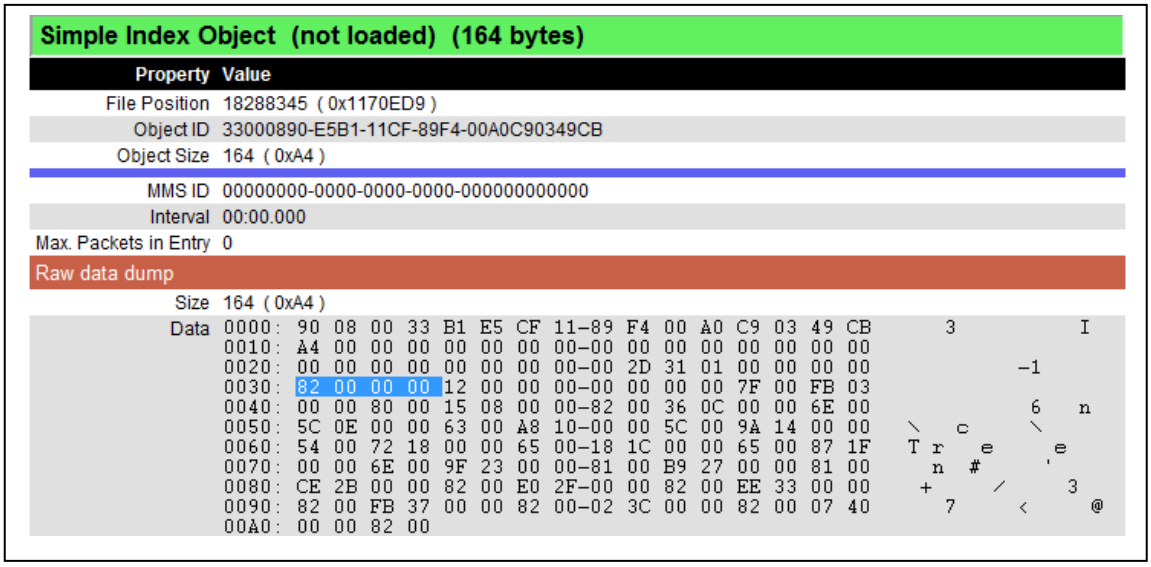


Figure 41: Index Entry Time Interval

Specify the time interval between different index entries in the Simple Index Object.



Simple Index Object (not loaded) (164 bytes)

Property	Value
File Position	18288345 (0x1170ED9)
Object ID	33000890-E5B1-11CF-89F4-00A0C90349CB
Object Size	164 (0xA4)
MMS ID	00000000-0000-0000-0000-000000000000
Interval	00:00.000
Max. Packets in Entry	0

Raw data dump

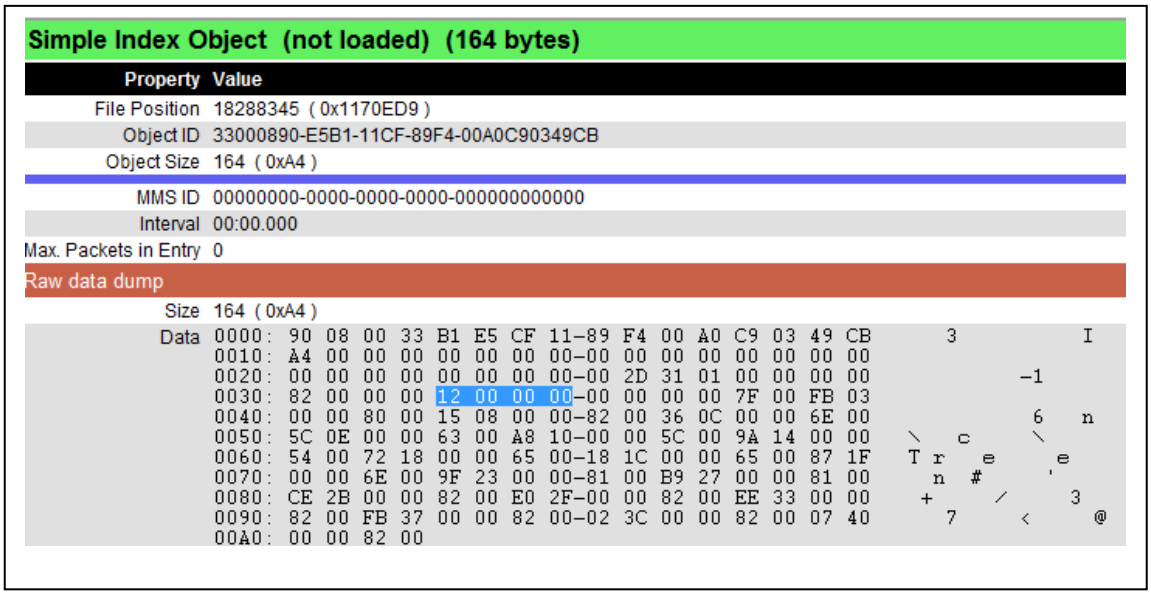
Size 164 (0xA4)

Data

```
0000: 90 08 00 33 B1 E5 CF 11-89 F4 00 A0 C9 03 49 CB
0010: A4 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0020: 00 00 00 00 00 00 00 00-00 2D 31 01 00 00 00 00
0030: 82 00 00 00 12 00 00 00-00 00 00 00 7F 00 FB 03
0040: 00 00 80 00 15 08 00 00-82 00 36 0C 00 00 6E 00
0050: 5C 0E 00 00 63 00 A8 10-00 00 5C 00 9A 14 00 00
0060: 54 00 72 18 00 00 65 00-18 1C 00 00 65 00 87 1F
0070: 00 00 6E 00 9F 23 00 00-81 00 B9 27 00 00 81 00
0080: CE 2B 00 00 82 00 E0 2F-00 00 82 00 EE 33 00 00
0090: 82 00 FB 37 00 00 82 00-02 3C 00 00 82 00 07 40
00A0: 00 00 82 00
```

Figure 42: Maximum Packet Count

The 32 bits represent the maximum packets in the Simple Index Object.



Simple Index Object (not loaded) (164 bytes)

Property	Value
File Position	18288345 (0x1170ED9)
Object ID	33000890-E5B1-11CF-89F4-00A0C90349CB
Object Size	164 (0xA4)
MMS ID	00000000-0000-0000-0000-000000000000
Interval	00:00.000
Max. Packets in Entry	0

Raw data dump

Size 164 (0xA4)

Data

```
0000: 90 08 00 33 B1 E5 CF 11-89 F4 00 A0 C9 03 49 CB
0010: A4 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0020: 00 00 00 00 00 00 00 00-00 2D 31 01 00 00 00 00
0030: 82 00 00 00 12 00 00 00-00 00 00 00 7F 00 FB 03
0040: 00 00 80 00 15 08 00 00-82 00 36 0C 00 00 6E 00
0050: 5C 0E 00 00 63 00 A8 10-00 00 5C 00 9A 14 00 00
0060: 54 00 72 18 00 00 65 00-18 1C 00 00 65 00 87 1F
0070: 00 00 6E 00 9F 23 00 00-81 00 B9 27 00 00 81 00
0080: CE 2B 00 00 82 00 E0 2F-00 00 82 00 EE 33 00 00
0090: 82 00 FB 37 00 00 82 00-02 3C 00 00 82 00 07 40
00A0: 00 00 82 00
```

Figure 43: Index Entries Count

The highlighted 32 bits represents the Index Entries in Simple Index Object

4.8 Conclusion

This chapter includes the forensic analysis of Artifacts of ASF file. ASF file was recorded and analysis was done on it. Analysis includes highlighting all the artifacts that exist within the objects of ASF File. Analysis was done on the Header Object (File properties Object, Stream Properties object and Header Extension Object), Data Object and Simple Index Object which are the objects of ASF file. This is the first phase of the research which includes highlighting the artifacts; next phase includes highlighting the artifacts of the forged file and comparing them with the original file.

Chapter 5

Implementation and Evaluation

5.1 Introduction

This part of research will cover the test scenarios that are specifically designed to help law enforcements agencies (LEAs) investigating different cases involving forgery and gaining unauthorized access to the data by the culprits and malign persons. The scenarios are mounted on ASF file which was used earlier to study the forensic artifacts of the file.

The ASF file has been edited to look into the artifacts which were changed after the editing was done on the file. A forger can do anything to hide his/her identity. So he/she can make changes to original media file. This part will look into those changes forensically. Some basic properties of the ASF file were changed to develop different scenarios that a forger can do to hide himself him the law enforcement agencies (LEAs). After the changes were done, some of the artifacts of the different objects will be seen as changed and it can develop from that, file has been forged deliberately. Some of the properties that were changed are the total size of the file by deleting some of the segments of the media file to hide or conceal some important information from the forensic investigators. Then the creation time of the file has been changed. File ID of ASF file was changed during the editing part. The nest property that was changed of the ASF file was the bit rate which is used to send number of bits per unit of the video. The flags in the video were edited. The other properties that were changed during the editing were the time specific data length. There are some other properties that were changed similarly to hide the details.

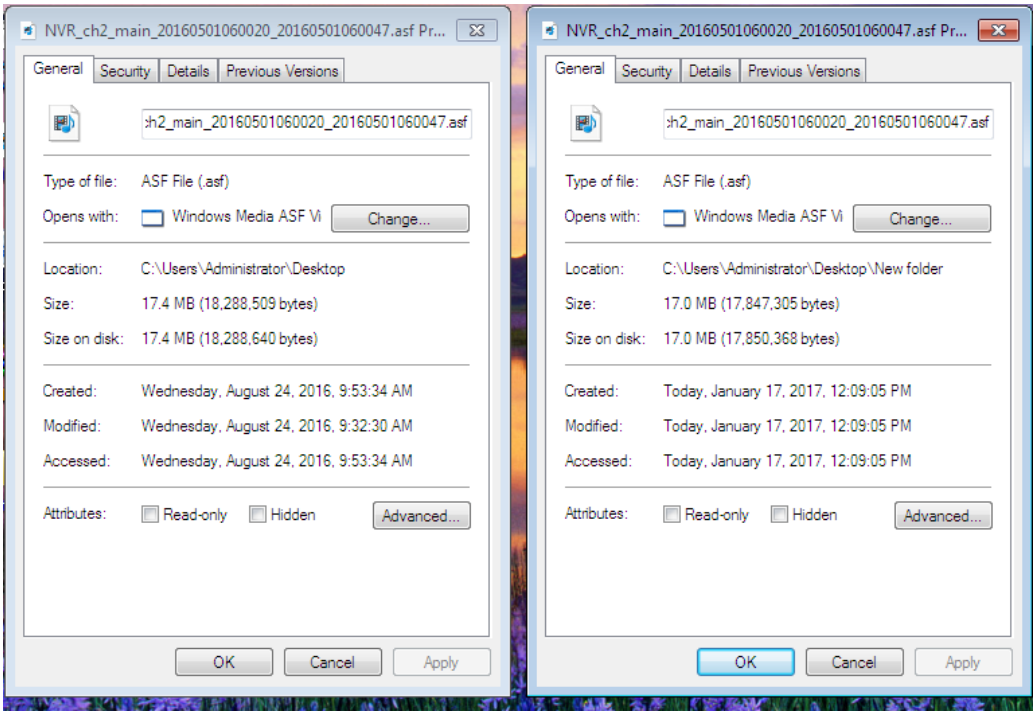


Figure 44: Comparsion of General Properties of both files

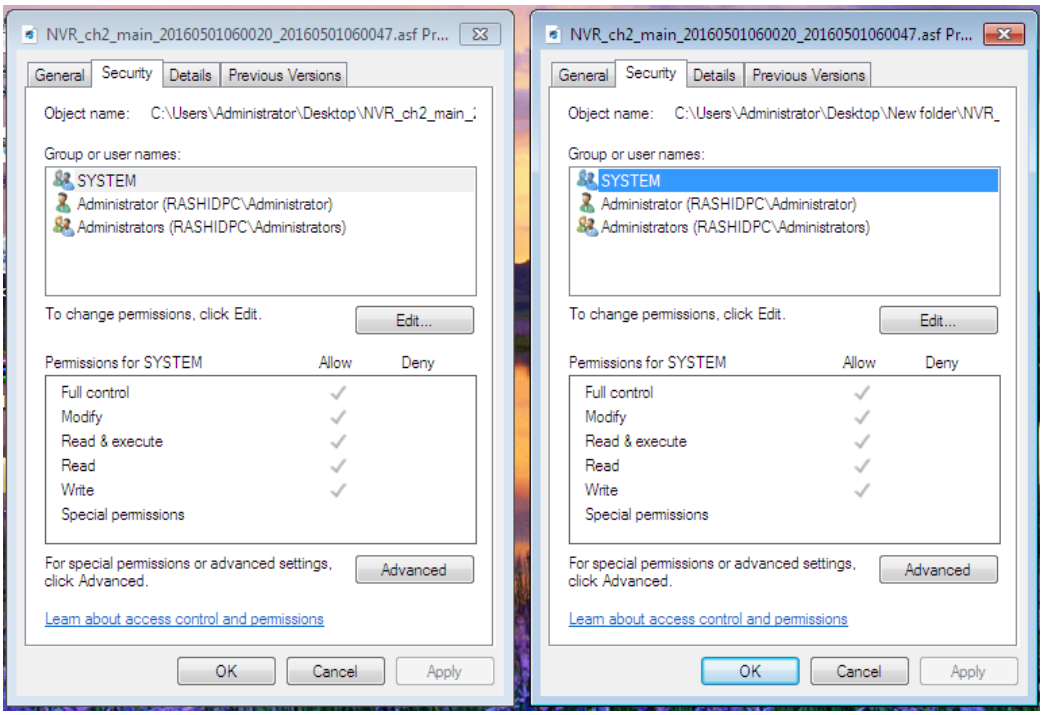


Figure 45: Comparsion of Security of both files

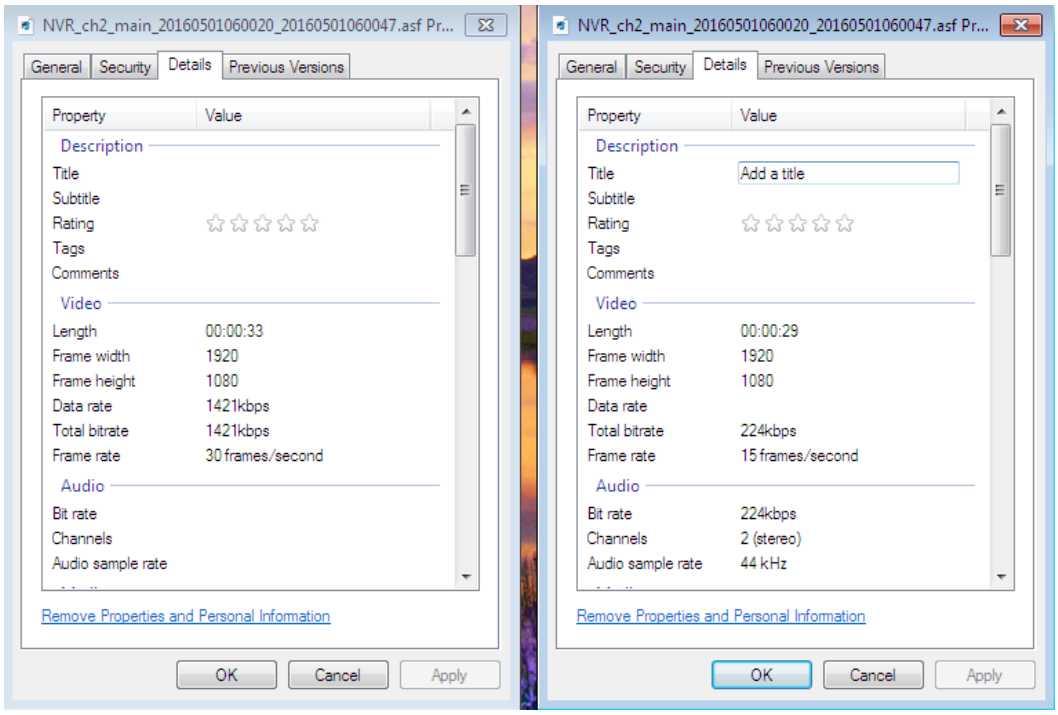


Figure 46: Comparison of details of both files

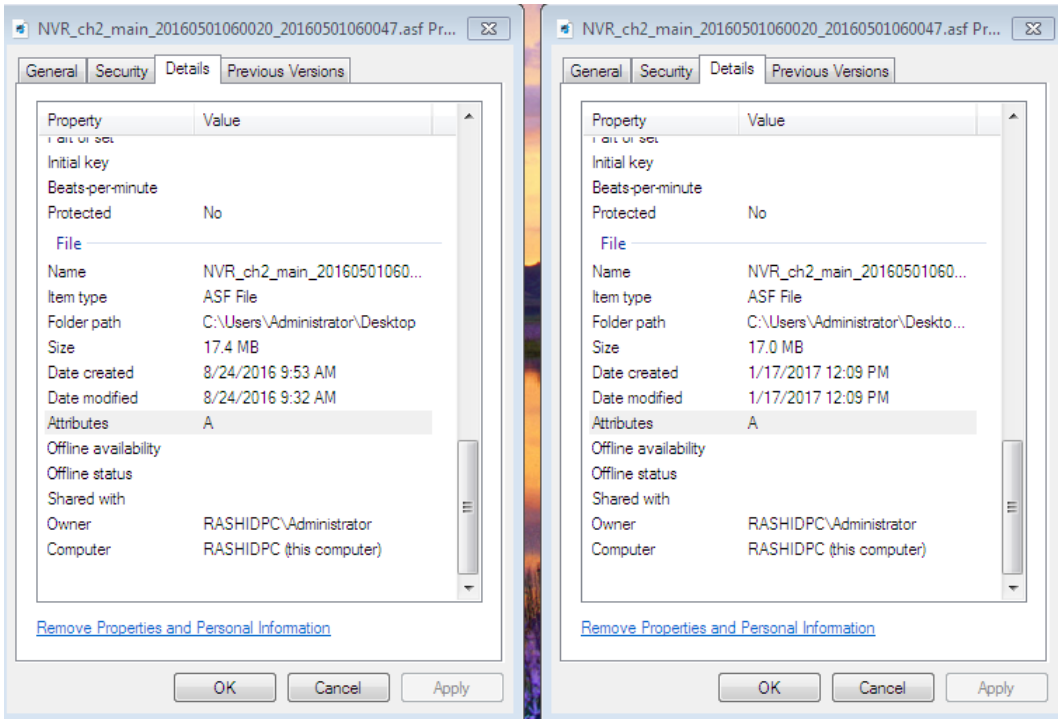


Figure 47: Comparison of details of both files

ASF File Objects	Modified Artifacts
Header Object	Object Size
Header Object	Number of Header Objects
File Properties Object	File ID
File Properties Object	File Size
File Properties Object	Creation Time
File Properties Object	Data Packets
File Properties Object	Play Duration
File Properties Object	Send Duration
File Properties Object	Preroll
File Properties Object	Maximum and minimum Data packets
File Properties Object	Maximum Bit Rate
Stream Properties object	Object Size
Stream Properties object	Flags
Stream Properties object	Time Specific Data Length
Stream Properties object	Object Size
Header Extension Object	File Position
Data Object	Object Size
Data Object	File ID
Data Object	Total Data Packets
Simple Index Object	Object Size
Simple Index Object	Index entry time Interval
Simple Index Object	Maximum Packet Count
Simple Index Object	Index Entries Count

Table 8: All the Modified Artifacts of ASF File

5.2 Modified Properties of Header Object

The artifacts that were changed are the object size. Before the editing was done the size of the object was 327 and afterwards it was changed to 625. Header object was another artifact that was changed after the editing was done on the ASF file. The artifacts that were changed can be seen in table 9.

Objects	Properties	Status
Header Object	File Size	Changed
Header Object	Number of Header Objects	Changed

Table.9: Changed Artifacts of Header Object

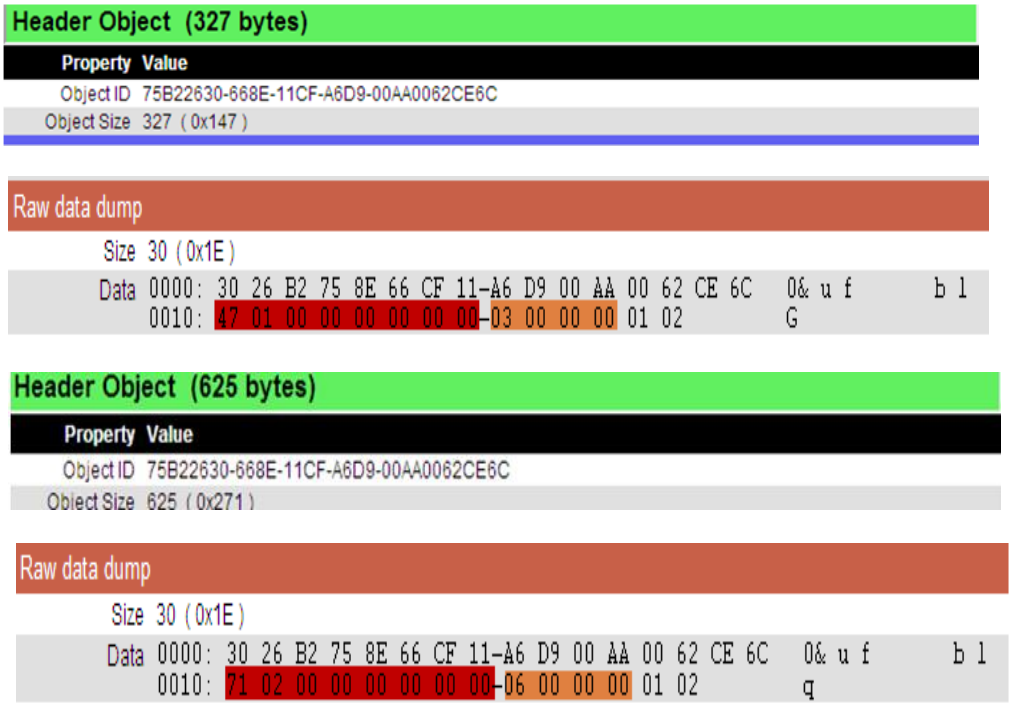


Figure 48: Comparison between Artifacts before and after Editing of Header Object

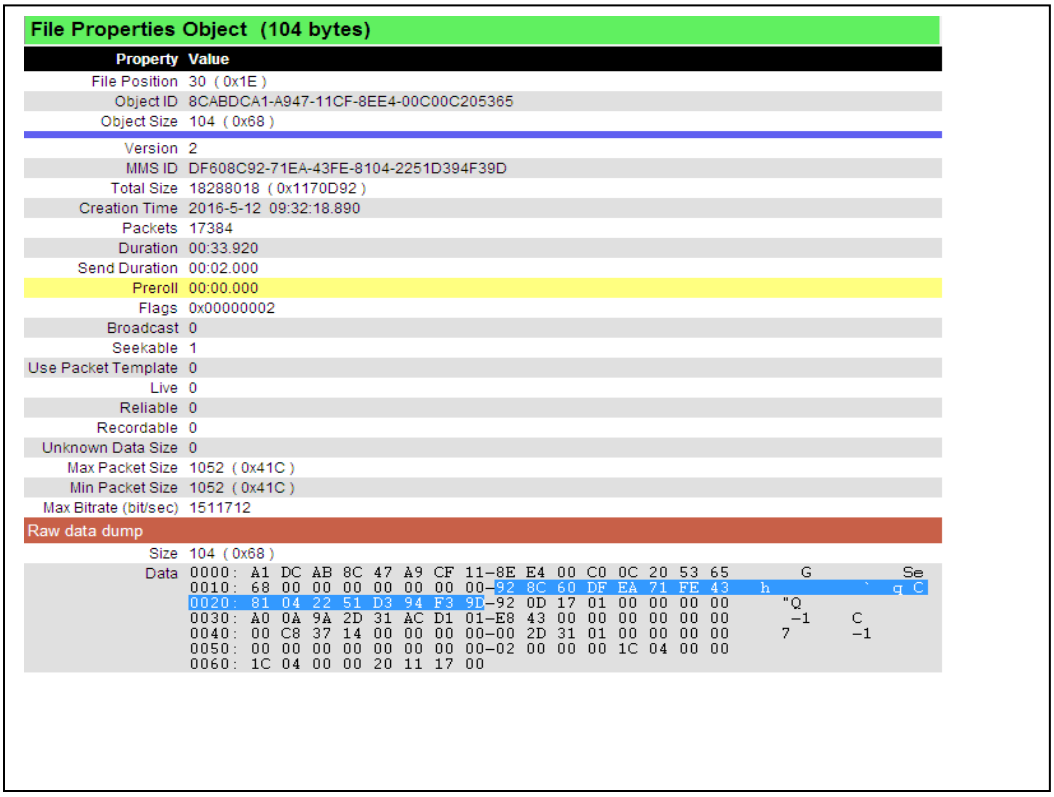
The artifacts that can be seen as changed in the header object are File Size and number of header objects.

5.3 Modified Properties of File Properties Object

The first artifact that was changed after the editing was the File ID, as with slightest of the changes the ID of the file was changed. Creation time was another artifact that was edited and results could be seen with change of the values in the edited file..The number of packets was also edited and could be seen in the edited file. Before the file was edited the numbers of packets were 17384 and after editing was done the numbers of packets were 5577. Play duration of the file was another artifact that was changed after changes were made to the file. The other artifacts that changed were the send duration, maximum and minimum data packets and maximum bit rate as the numbers of bits transmitted were changed as the result of editing on the file. Changed Artifacts of File Properties Object can be seen in table 10.

Objects	Properties	Status
File Properties Object	File ID	Changed
File Properties Object	File Size	Changed
File Properties Object	Creation Time	Changed
File Properties Object	Data Packets	Changed
File Properties Object	Play Duration	Changed
File Properties Object	Send Duration	Changed
File Properties Object	Maximum and minimum Data packets	Changed
File Properties Object	Maximum Bit Rate	Changed

Table.10: Changed Artifacts of File Properties Object



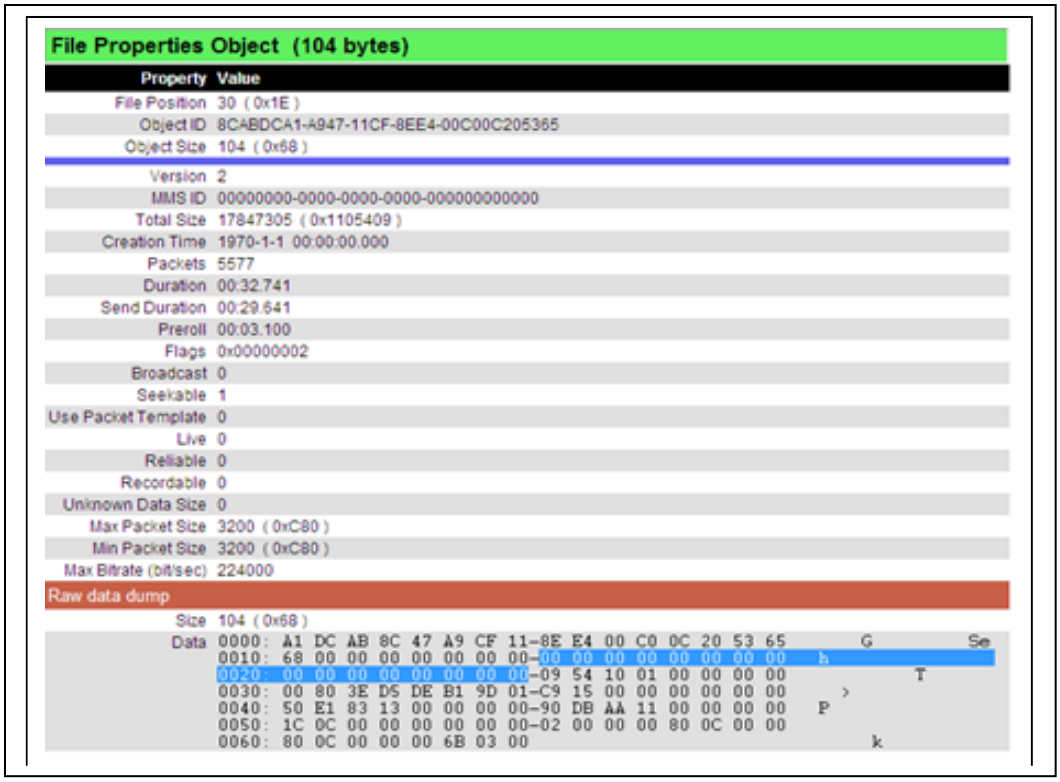
File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	DF608C92-71EA-43FE-8104-2251D394F39D
Total Size	18288018 (0x1170D92)
Creation Time	2016-5-12 09:32:18.890
Packets	17384
Duration	00:33.920
Send Duration	00:02.000
Preroll	00:00.000
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	1052 (0x41C)
Min Packet Size	1052 (0x41C)
Max Bitrate (bit/sec)	1511712

Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65       G          Se
0010: 68 00 00 00 00 00 00 00-92 8C 60 DF EA 71 FE 43   h            `  q C
0020: 81 04 22 51 D3 94 F3 9D-92 0D 17 01 00 00 00 00     "Q
0030: A0 0A 9A 2D 31 AC D1 01-E8 43 00 00 00 00 00 00      -1     C
0040: 00 C8 37 14 00 00 00 00-00 2D 31 01 00 00 00 00     7       -1
0050: 00 00 00 00 00 00 00 00-02 00 00 00 1C 04 00 00
0060: 1C 04 00 00 20 11 17 00
```



File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	00000000-0000-0000-0000-000000000000
Total Size	17847305 (0x1105409)
Creation Time	1970-1-1 00:00:00.000
Packets	5577
Duration	00:32.741
Send Duration	00:29.641
Preroll	00:03.100
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	3200 (0xC80)
Min Packet Size	3200 (0xC80)
Max Bitrate (bit/sec)	224000

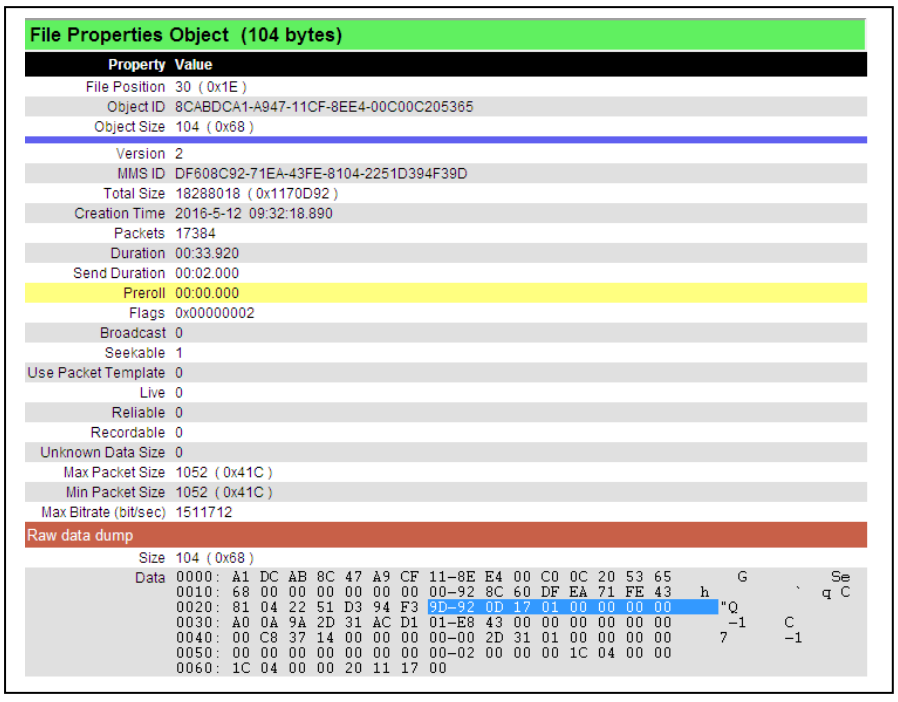
Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65       G          Se
0010: 68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    h
0020: 00 00 00 00 00 00 00 00-09 54 10 01 00 00 00 00            T
0030: 00 80 3E D5 DE B1 9D 01-C9 15 00 00 00 00 00 00      >
0040: 50 E1 83 13 00 00 00 00-90 DB AA 11 00 00 00 00    P
0050: 1C 0C 00 00 00 00 00 00-02 00 00 00 80 0C 00 00
0060: 80 0C 00 00 00 6B 03 00                                    k
```

Figure 49: File ID Changed

As it can be seen the first artifact that was changed in the file properties object after the modifaication is File ID.



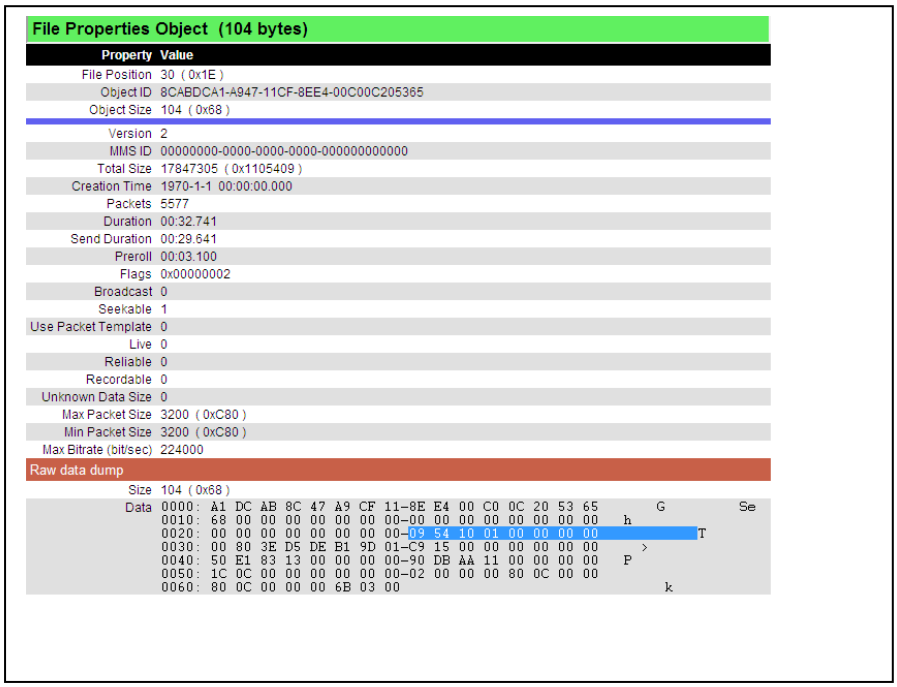
File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	DF608C92-71EA-43FE-8104-2251D394F39D
Total Size	18288018 (0x1170D92)
Creation Time	2016-5-12 09:32:18.890
Packets	17384
Duration	00:33.920
Send Duration	00:02.000
Preroll	00:00.000
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	1052 (0x41C)
Min Packet Size	1052 (0x41C)
Max Bitrate (bit/sec)	1511712

Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65       G          Se
0010: 68 00 00 00 00 00 00 00-92 8C 60 DF EA 71 FE 43    h          `  q C
0020: 81 04 22 51 D3 94 F3 9D-92 0D 17 01 00 00 00 00      "Q
0030: A0 0A 9A 2D 31 AC D1 01-E8 43 00 00 00 00 00 00       -1    C
0040: 00 C8 37 14 00 00 00 00-00 2D 31 01 00 00 00 00      7      -1
0050: 00 00 00 00 00 00 00 00-02 00 00 00 1C 04 00 00
0060: 1C 04 00 00 20 11 17 00
```



File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	00000000-0000-0000-0000-000000000000
Total Size	17847305 (0x1105409)
Creation Time	1970-1-1 00:00:00.000
Packets	5577
Duration	00:32.741
Send Duration	00:29.641
Preroll	00:03.100
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	3200 (0xC80)
Min Packet Size	3200 (0xC80)
Max Bitrate (bit/sec)	224000

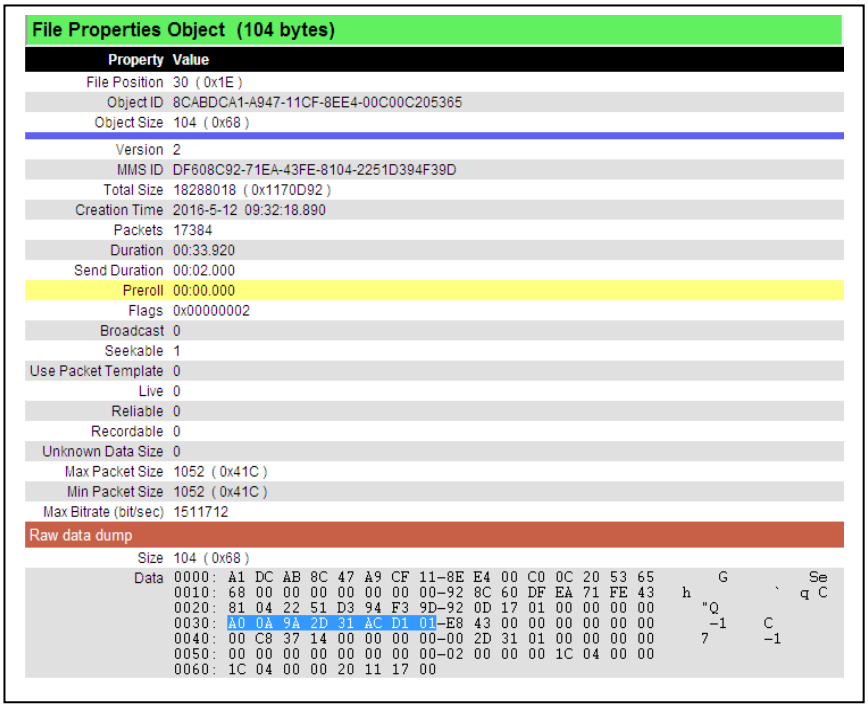
Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65       G          Se
0010: 68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   h
0020: 00 00 00 00 00 00 00 00-09 54 10 01 00 00 00 00                T
0030: 00 80 3E D5 DE B1 9D 01-C9 15 00 00 00 00 00 00     >
0040: 50 E1 83 13 00 00 00 00-90 DB AA 11 00 00 00 00   P
0050: 1C 0C 00 00 00 00 00 00-02 00 00 00 80 0C 00 00
0060: 80 0C 00 00 00 6B 03 00                          k
```

Figure 50: Total Sizes of File-Changed

The next artifact that was changed is the total size of file.



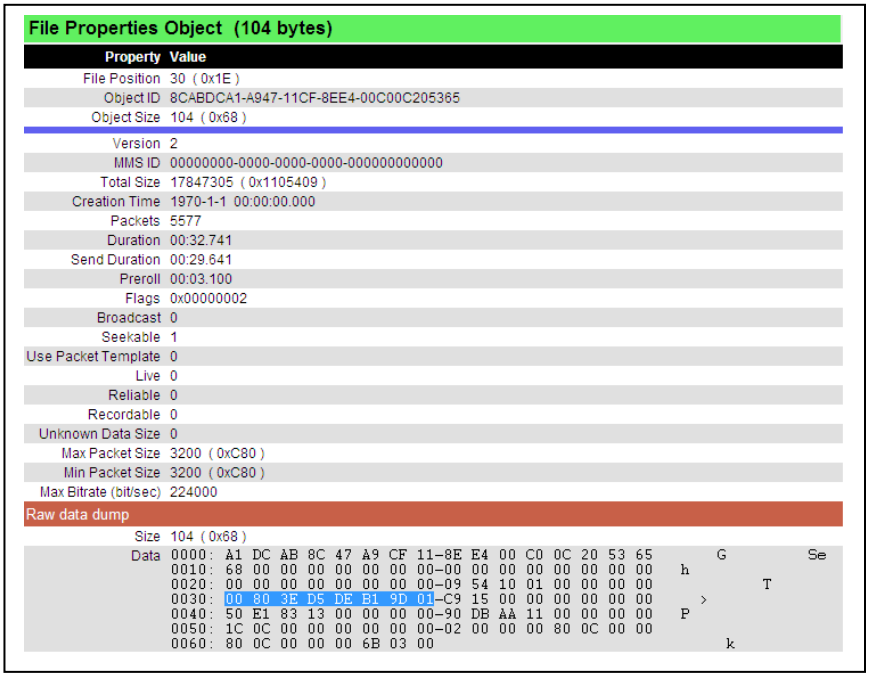
File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	DF608C92-71EA-43FE-8104-2251D394F39D
Total Size	18288018 (0x1170D92)
Creation Time	2016-5-12 09:32:18.890
Packets	17384
Duration	00:33.920
Send Duration	00:02.000
Preroll	00:00.000
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	1052 (0x41C)
Min Packet Size	1052 (0x41C)
Max Bitrate (bit/sec)	1511712

Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65       G          Se
0010: 68 00 00 00 00 00 00 00-92 8C 60 DF EA 71 FE 43   h         `  q C
0020: 81 04 22 51 D3 94 F3 9D-92 0D 17 01 00 00 00 00     "Q
0030: A0 0A 9A 2D 31 AC D1 01-E8 43 00 00 00 00 00 00      -1    C
0040: 00 C8 37 14 00 00 00 00-00 2D 31 01 00 00 00 00     7      -1
0050: 00 00 00 00 00 00 00 00-02 00 00 00 1C 04 00 00
0060: 1C 04 00 00 20 11 17 00
```



File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	00000000-0000-0000-0000-000000000000
Total Size	17847305 (0x1105409)
Creation Time	1970-1-1 00:00:00.000
Packets	5577
Duration	00:32.741
Send Duration	00:29.641
Preroll	00:03.100
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	3200 (0xC80)
Min Packet Size	3200 (0xC80)
Max Bitrate (bit/sec)	224000

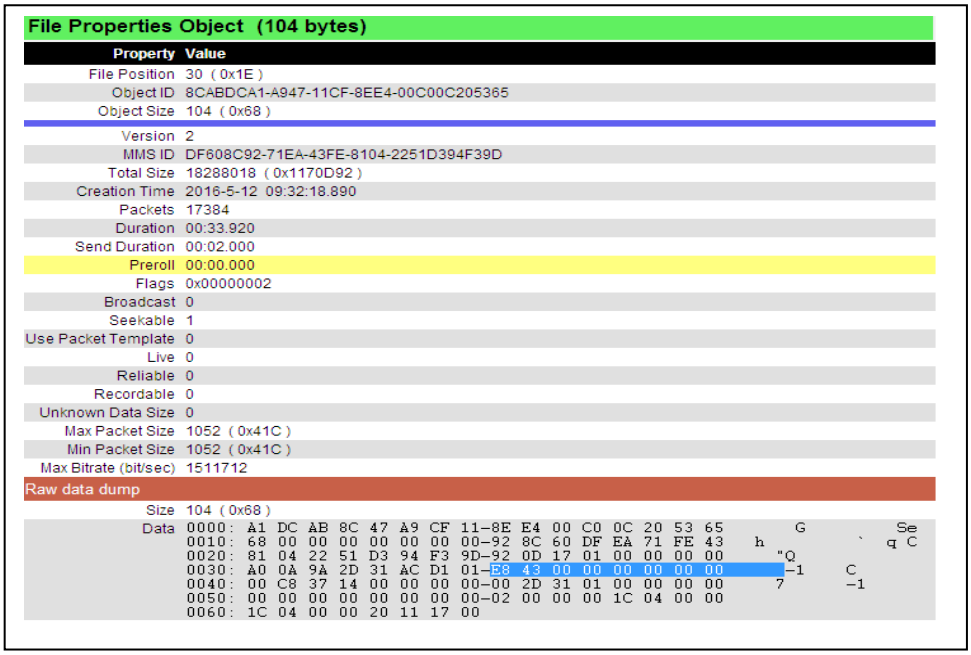
Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65       G          Se
0010: 68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   h
0020: 00 00 00 00 00 00 00 00-09 54 10 01 00 00 00 00             T
0030: 00 80 3E D5 DE B1 9D 01-C9 15 00 00 00 00 00 00     >
0040: 50 E1 83 13 00 00 00 00-90 DB AA 11 00 00 00 00   P
0050: 1C 0C 00 00 00 00 00 00-02 00 00 00 80 0C 00 00
0060: 80 0C 00 00 00 6B 03 00                              k
```

Figure 51: Creation Time Changed

The next artifact after the total file size that can be seen as changed is the creation time as with slightest of the changes,this artifact is modified.



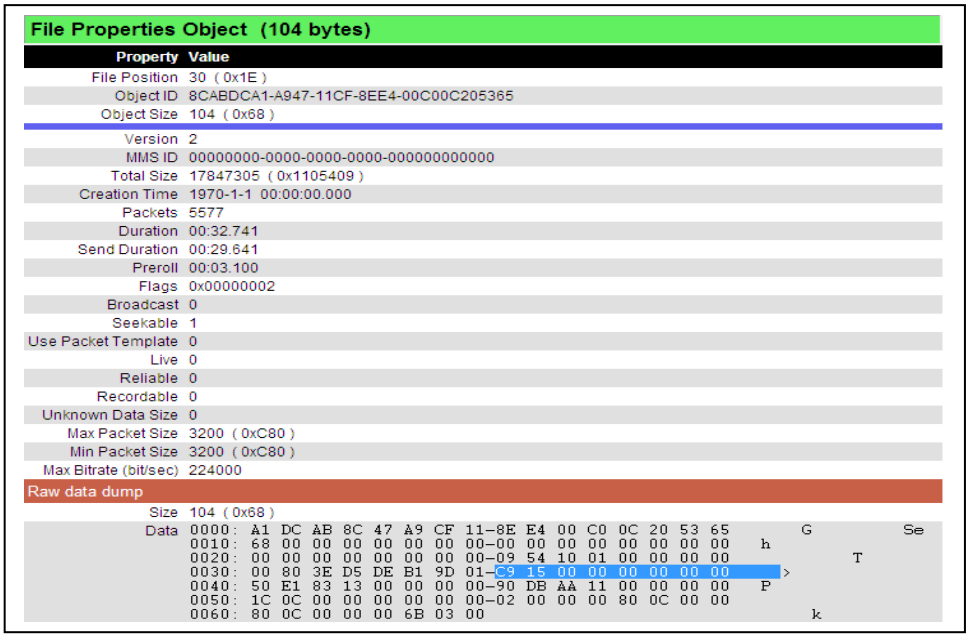
File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	DF608C92-71EA-43FE-8104-2251D394F39D
Total Size	18288018 (0x1170D92)
Creation Time	2016-5-12 09:32:18.890
Packets	17384
Duration	00:33.920
Send Duration	00:02.000
Preroll	00:00.000
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	1052 (0x41C)
Min Packet Size	1052 (0x41C)
Max Bitrate (bit/sec)	1511712

Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65       G          Se
0010: 68 00 00 00 00 00 00 00-92 8C 60 DF EA 71 FE 43   h         `  q C
0020: 81 04 22 51 D3 94 F3 9D-92 0D 17 01 00 00 00 00     "Q
0030: A0 0A 9A 2D 31 AC D1 01-E8 43 00 00 00 00 00 00       -1     C
0040: 00 C8 37 14 00 00 00 00-00 2D 31 01 00 00 00 00      7      -1
0050: 00 00 00 00 00 00 00 00-02 00 00 00 1C 04 00 00
0060: 1C 04 00 00 20 11 17 00
```



File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	00000000-0000-0000-0000-000000000000
Total Size	17847305 (0x1105409)
Creation Time	1970-1-1 00:00:00.000
Packets	5577
Duration	00:32.741
Send Duration	00:29.641
Preroll	00:03.100
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	3200 (0xC80)
Min Packet Size	3200 (0xC80)
Max Bitrate (bit/sec)	224000

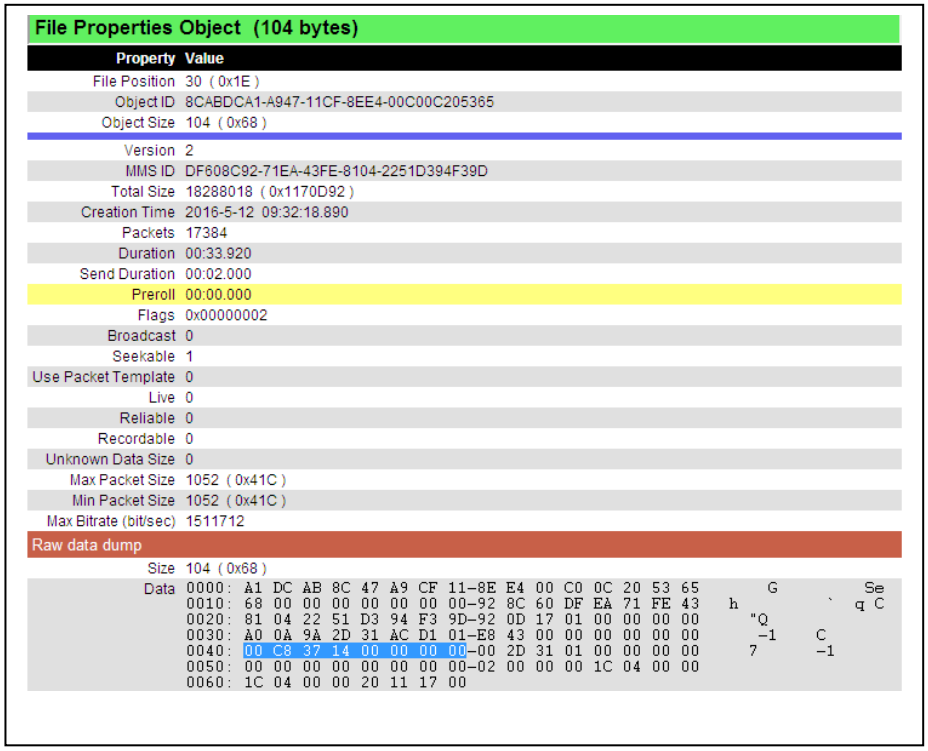
Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65        G           Se
0010: 68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00    h
0020: 00 00 00 00 00 00 00 00-09 54 10 01 00 00 00 00              T
0030: 00 80 3E D5 DE B1 9D 01-C9 15 00 00 00 00 00 00    >
0040: 50 E1 83 13 00 00 00 00-90 DB AA 11 00 00 00 00    P
0050: 1C 0C 00 00 00 00 00 00-02 00 00 00 80 0C 00 00
0060: 80 0C 00 00 00 6B 03 00                                    k
```

Figure 52: Data Packets of File

After the creation time, the next artifact that can be ssen as changed is the data packets of file.



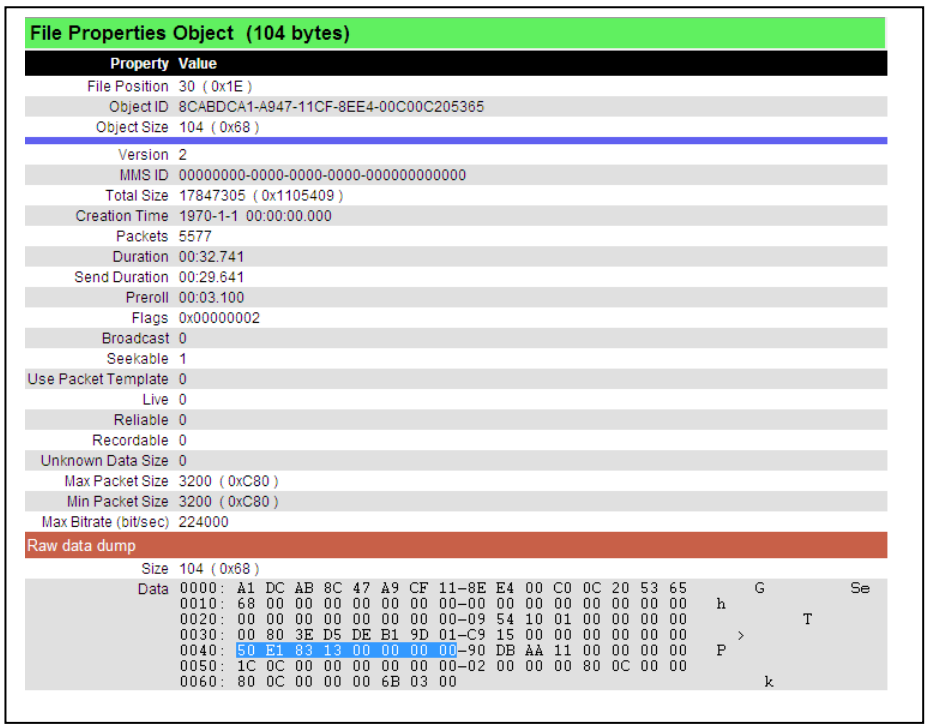
File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	DF608C92-71EA-43FE-8104-2251D394F39D
Total Size	18288018 (0x1170D92)
Creation Time	2016-5-12 09:32:18.890
Packets	17384
Duration	00:33.920
Send Duration	00:02.000
Preroll	00:00.000
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	1052 (0x41C)
Min Packet Size	1052 (0x41C)
Max Bitrate (bit/sec)	1511712

Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65        G           Se
0010: 68 00 00 00 00 00 00 00-92 8C 60 DF EA 71 FE 43    h           `  q C
0020: 81 04 22 51 D3 94 F3 9D-92 0D 17 01 00 00 00 00      "Q
0030: A0 0A 9A 2D 31 AC D1 01-E8 43 00 00 00 00 00 00       -1     C
0040: 00 C8 37 14 00 00 00 00-00 2D 31 01 00 00 00 00      7       -1
0050: 00 00 00 00 00 00 00 00-02 00 00 00 1C 04 00 00
0060: 1C 04 00 00 20 11 17 00
```



File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	00000000-0000-0000-0000-000000000000
Total Size	17847305 (0x1105409)
Creation Time	1970-1-1 00:00:00.000
Packets	5577
Duration	00:32.741
Send Duration	00:29.641
Preroll	00:03.100
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	3200 (0xC80)
Min Packet Size	3200 (0xC80)
Max Bitrate (bit/sec)	224000

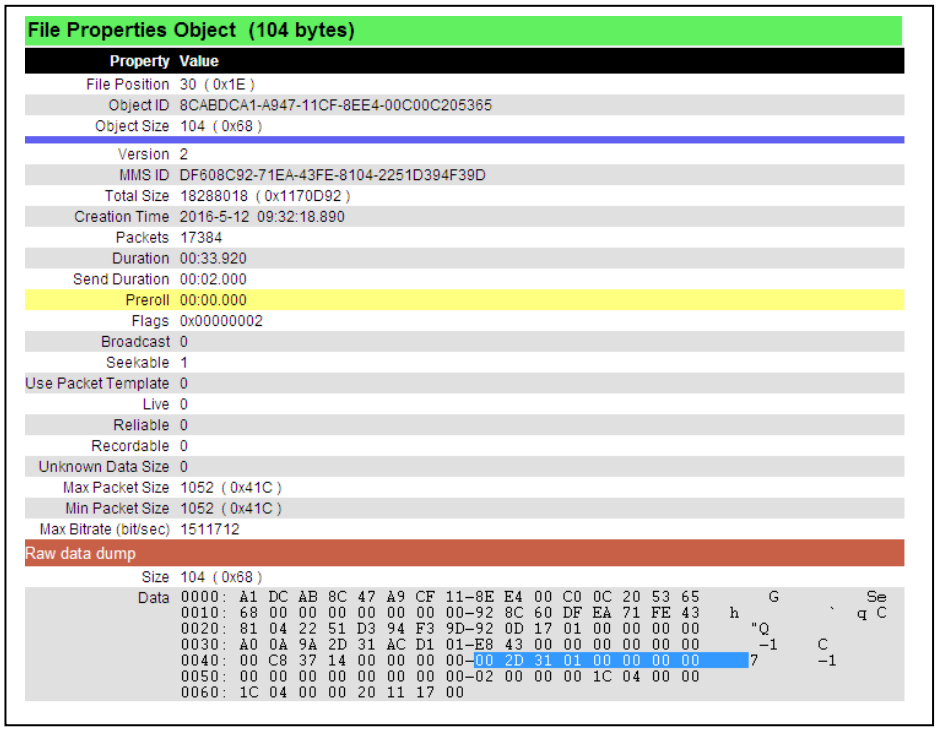
Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65
0010: 68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0020: 00 00 00 00 00 00 00 00-09 54 10 01 00 00 00 00
0030: 00 80 3E D5 DE B1 9D 01-C9 15 00 00 00 00 00 00
0040: 50 E1 83 13 00 00 00 00-90 DB AA 11 00 00 00 00
0050: 1C 0C 00 00 00 00 00 00-02 00 00 00 80 0C 00 00
0060: 80 0C 00 00 00 6B 03 00
```

Figure 53: Play Duration of File -Changed

Play duration is the other artifact that can be seen as changed. This is the artifact which specifies the time needed to play the media file.



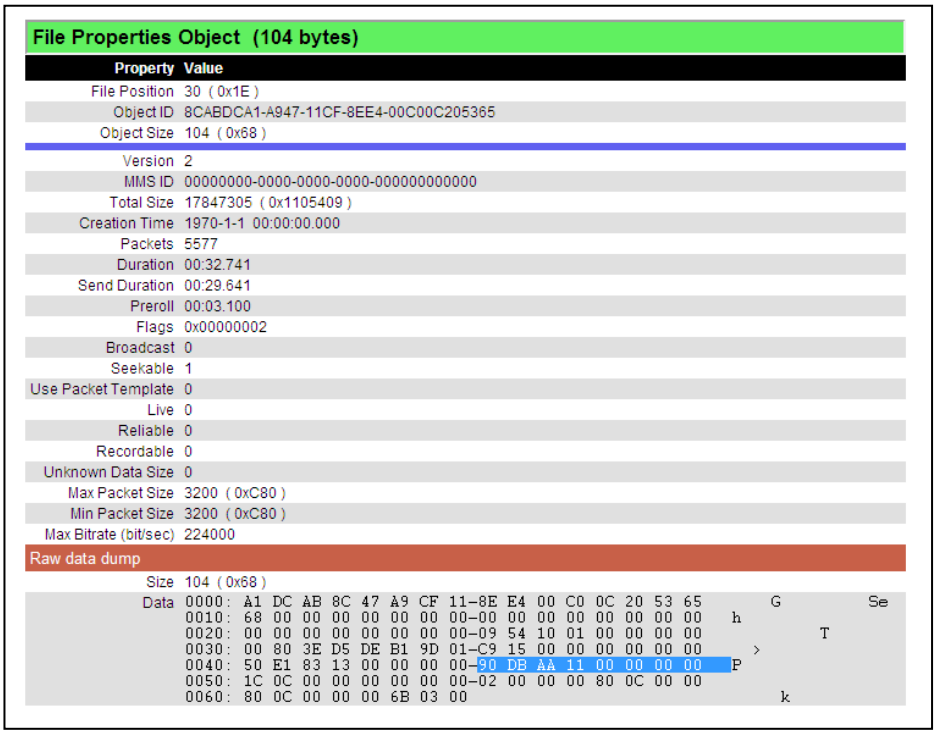
File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	DF608C92-71EA-43FE-8104-2251D394F39D
Total Size	18288018 (0x1170D92)
Creation Time	2016-5-12 09:32:18.890
Packets	17384
Duration	00:33.920
Send Duration	00:02.000
Preroll	00:00.000
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	1052 (0x41C)
Min Packet Size	1052 (0x41C)
Max Bitrate (bit/sec)	1511712

Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65
0010: 68 00 00 00 00 00 00 00-92 8C 60 DF EA 71 FE 43
0020: 81 04 22 51 D3 94 F3 9D-92 0D 17 01 00 00 00 00
0030: A0 0A 9A 2D 31 AC D1 01-E8 43 00 00 00 00 00 00
0040: 00 C8 37 14 00 00 00 00-00 2D 31 01 00 00 00 00
0050: 00 00 00 00 00 00 00 00-02 00 00 00 1C 04 00 00
0060: 1C 04 00 00 20 11 17 00
```



File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	00000000-0000-0000-0000-000000000000
Total Size	17847305 (0x1105409)
Creation Time	1970-1-1 00:00:00.000
Packets	5577
Duration	00:32.741
Send Duration	00:29.641
Preroll	00:03.100
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	3200 (0xC80)
Min Packet Size	3200 (0xC80)
Max Bitrate (bit/sec)	224000

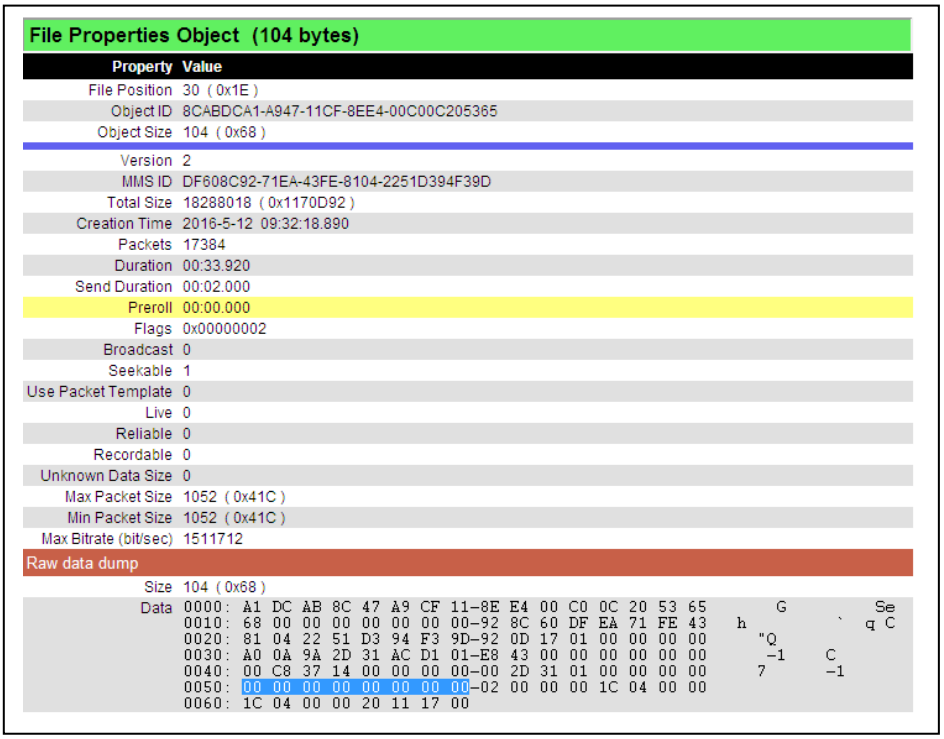
Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65       G          Se
0010: 68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   h
0020: 00 00 00 00 00 00 00 00-09 54 10 01 00 00 00 00            T
0030: 00 80 3E D5 DE B1 9D 01-C9 15 00 00 00 00 00 00     >
0040: 50 E1 83 13 00 00 00 00-90 DB AA 11 00 00 00 00   P
0050: 1C 0C 00 00 00 00 00 00-02 00 00 00 80 0C 00 00
0060: 80 0C 00 00 00 6B 03 00                             k
```

Figure 54: Send Duration of File- Changed

The next artifact that can be seen as changed in file properties object is the Send duration.



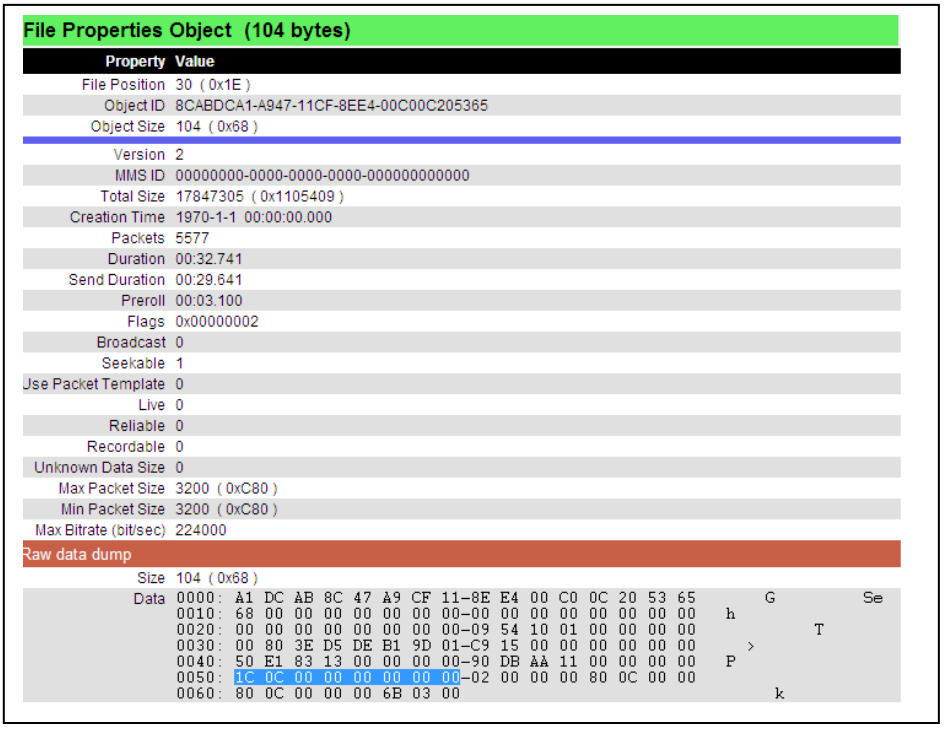
File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	DF608C92-71EA-43FE-8104-2251D394F39D
Total Size	18288018 (0x1170D92)
Creation Time	2016-5-12 09:32:18.890
Packets	17384
Duration	00:33.920
Send Duration	00:02.000
Preroll	00:00.000
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	1052 (0x41C)
Min Packet Size	1052 (0x41C)
Max Bitrate (bit/sec)	1511712

Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65       G          Se
0010: 68 00 00 00 00 00 00 00-92 8C 60 DF EA 71 FE 43   h          `  q C
0020: 81 04 22 51 D3 94 F3 9D-92 0D 17 01 00 00 00 00     "Q
0030: A0 0A 9A 2D 31 AC D1 01-E8 43 00 00 00 00 00 00      -1    C
0040: 00 C8 37 14 00 00 00 00-00 2D 31 01 00 00 00 00     7      -1
0050: 00 00 00 00 00 00 00 00-02 00 00 00 1C 04 00 00
0060: 1C 04 00 00 20 11 17 00
```



File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	00000000-0000-0000-0000-000000000000
Total Size	17847305 (0x1105409)
Creation Time	1970-1-1 00:00:00.000
Packets	5577
Duration	00:32.741
Send Duration	00:29.641
Preroll	00:03.100
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	3200 (0xC80)
Min Packet Size	3200 (0xC80)
Max Bitrate (bit/sec)	224000

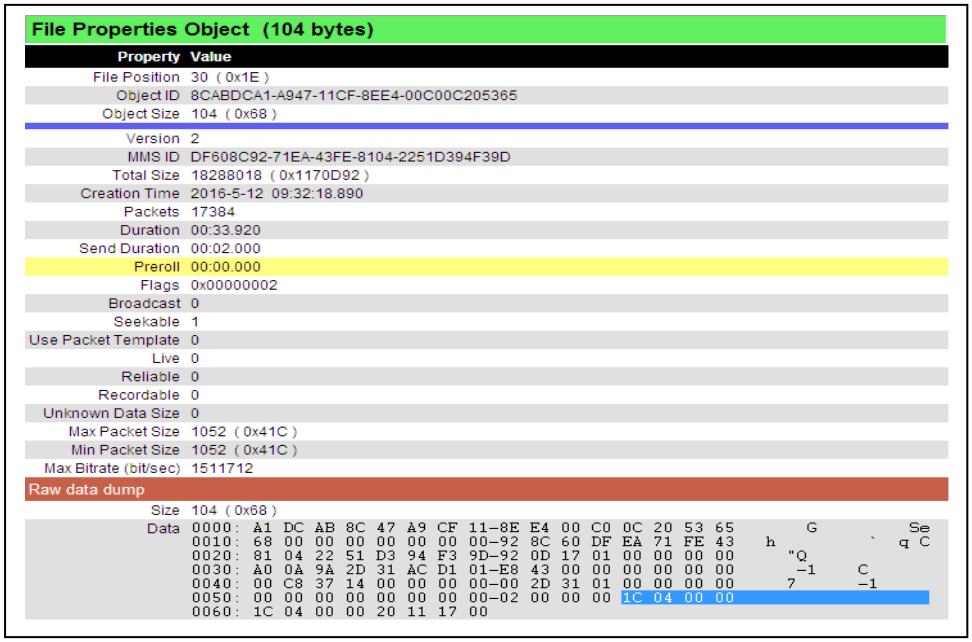
Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65
0010: 68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0020: 00 00 00 00 00 00 00 00-09 54 10 01 00 00 00 00
0030: 00 80 3E D5 DE B1 9D 01-C9 15 00 00 00 00 00 00
0040: 50 E1 83 13 00 00 00 00-90 DB AA 11 00 00 00 00
0050: 1C 0C 00 00 00 00 00 00-02 00 00 00 80 0C 00 00
0060: 80 0C 00 00 00 6B 03 00
```

Figure 55: Preroll- Changed

Preroll is the other artifact that is modified after the changes are made to the file.



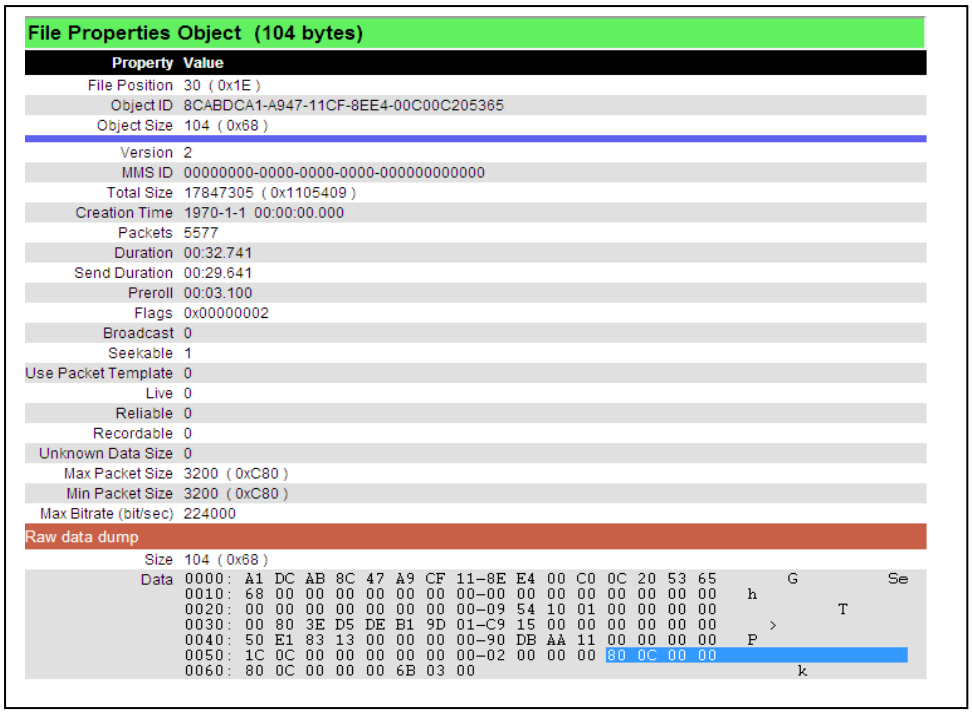
File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	DF608C92-71EA-43FE-8104-2251D394F39D
Total Size	18288018 (0x1170D92)
Creation Time	2016-5-12 09:32:18.890
Packets	17384
Duration	00:33.920
Send Duration	00:02.000
Preroll	00:00.000
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	1052 (0x41C)
Min Packet Size	1052 (0x41C)
Max Bitrate (bit/sec)	1511712

Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65
0010: 68 00 00 00 00 00 00 00-92 8C 60 DF EA 71 FE 43
0020: 81 04 22 51 D3 94 F3 9D-92 0D 17 01 00 00 00 00
0030: A0 0A 9A 2D 31 AC D1 01-E8 43 00 00 00 00 00 00
0040: 00 C8 37 14 00 00 00 00-00 2D 31 01 00 00 00 00
0050: 00 00 00 00 00 00 00 00-02 00 00 00 1C 04 00 00
0060: 1C 04 00 00 20 11 17 00
```



File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	00000000-0000-0000-0000-000000000000
Total Size	17847305 (0x1105409)
Creation Time	1970-1-1 00:00:00.000
Packets	5577
Duration	00:32.741
Send Duration	00:29.641
Preroll	00:03.100
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	3200 (0xC80)
Min Packet Size	3200 (0xC80)
Max Bitrate (bit/sec)	224000

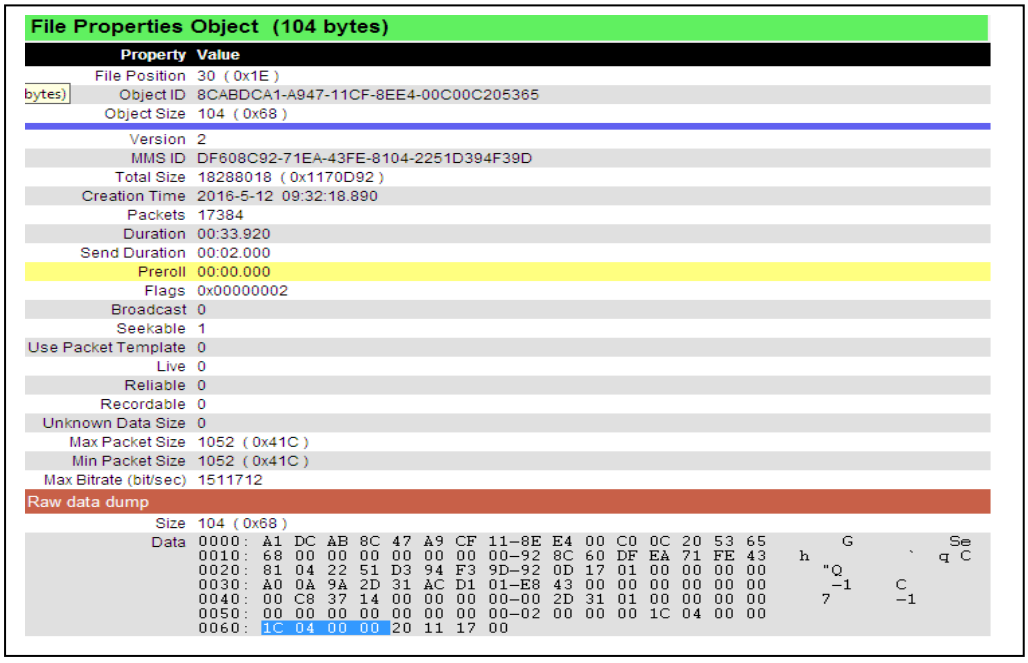
Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65      G          Se
0010: 68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   h
0020: 00 00 00 00 00 00 00 00-09 54 10 01 00 00 00 00             T
0030: 00 80 3E D5 DE B1 9D 01-C9 15 00 00 00 00 00 00     >
0040: 50 E1 83 13 00 00 00 00-90 DB AA 11 00 00 00 00   P
0050: 1C 0C 00 00 00 00 00 00-02 00 00 00 80 0C 00 00
0060: 80 0C 00 00 00 6B 03 00                                 k
```

Figure 56: Minimum Data Packet Size-Changed

The third last artifact that is changed is the Minimum data packet size which specifies size of packets in the Data object



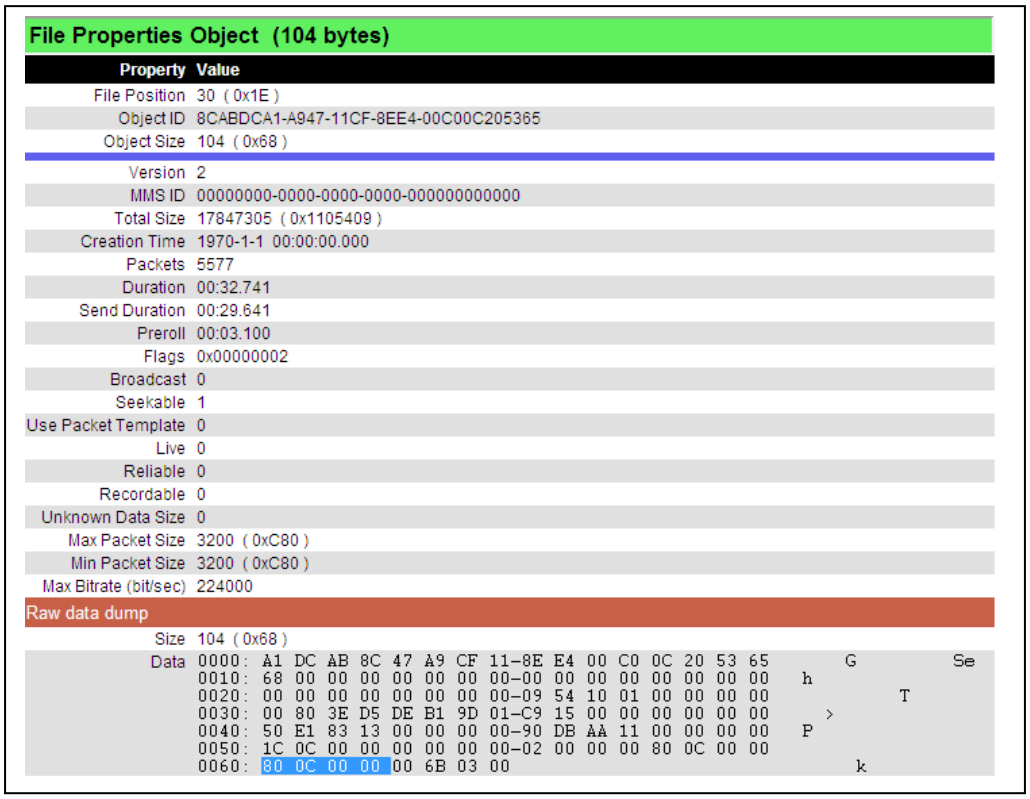
File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
bytes) Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	DF608C92-71EA-43FE-8104-2251D394F39D
Total Size	18288018 (0x1170D92)
Creation Time	2016-5-12 09:32:18.890
Packets	17384
Duration	00:33.920
Send Duration	00:02.000
Preroll	00:00.000
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	1052 (0x41C)
Min Packet Size	1052 (0x41C)
Max Bitrate (bit/sec)	1511712

Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65      G          Se
0010: 68 00 00 00 00 00 00 00-92 8C 60 DF EA 71 FE 43   h         `  q C
0020: 81 04 22 51 D3 94 F3 9D-92 0D 17 01 00 00 00 00     "Q
0030: A0 0A 9A 2D 31 AC D1 01-E8 43 00 00 00 00 00 00      -1     C
0040: 00 C8 37 14 00 00 00 00-00 2D 31 01 00 00 00 00      7      -1
0050: 00 00 00 00 00 00 00 00-02 00 00 00 1C 04 00 00
0060: 1C 04 00 00 20 11 17 00
```



File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	00000000-0000-0000-0000-000000000000
Total Size	17847305 (0x1105409)
Creation Time	1970-1-1 00:00:00.000
Packets	5577
Duration	00:32.741
Send Duration	00:29.641
Preroll	00:03.100
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	3200 (0xC80)
Min Packet Size	3200 (0xC80)
Max Bitrate (bit/sec)	224000

Raw data dump

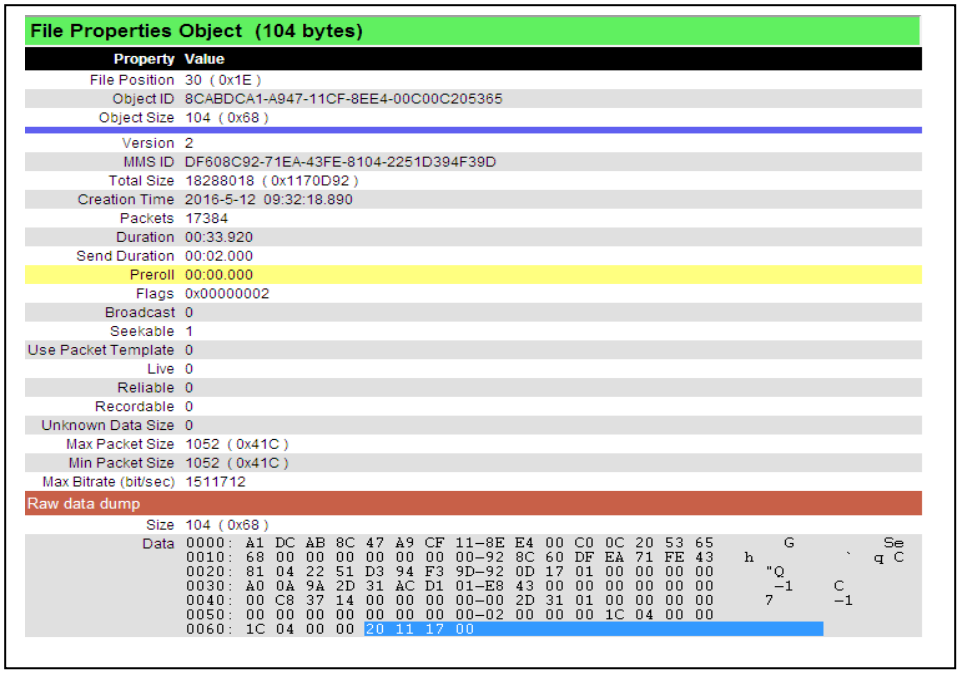
Size 104 (0x68)

Data

```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65      G          Se
0010: 68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   h
0020: 00 00 00 00 00 00 00 00-09 54 10 01 00 00 00 00             T
0030: 00 80 3E D5 DE B1 9D 01-C9 15 00 00 00 00 00 00     >
0040: 50 E1 83 13 00 00 00 00-90 DB AA 11 00 00 00 00   P
0050: 1C 0C 00 00 00 00 00 00-02 00 00 00 80 0C 00 00
0060: 80 0C 00 00 00 6B 03 00                                 k
```

Figure 57: Maximum Data Packet Size-Changed

The above figure shows the modified artifact in the file properties object



File Properties Object (104 bytes)

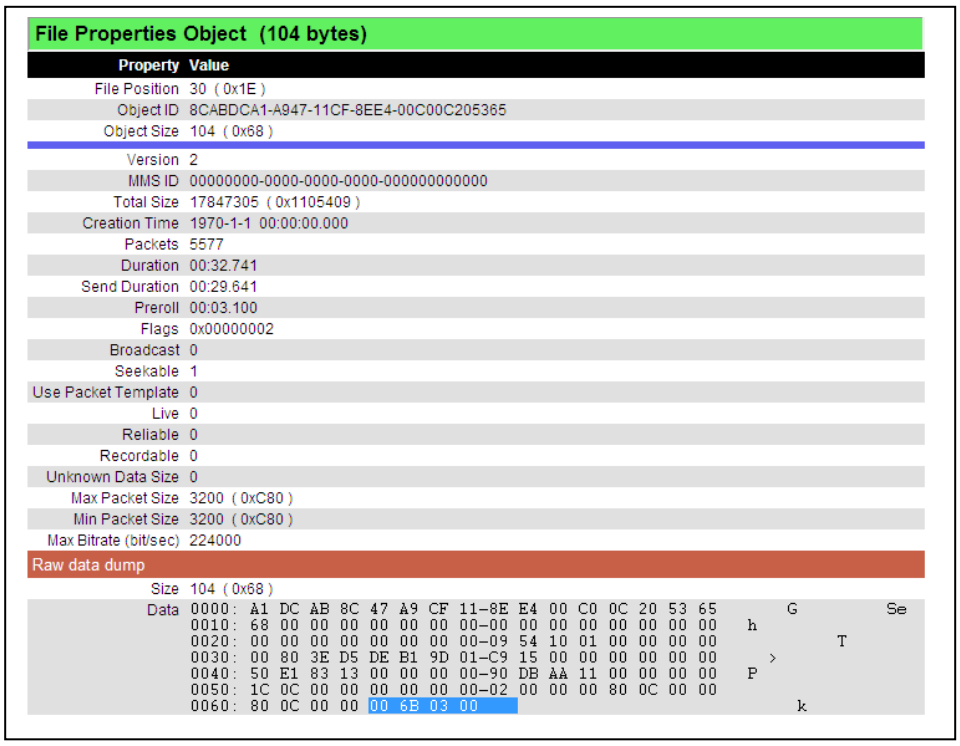
Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	DF608C92-71EA-43FE-8104-2251D394F39D
Total Size	18288018 (0x1170D92)
Creation Time	2016-5-12 09:32:18.890
Packets	17384
Duration	00:33.920
Send Duration	00:02.000
Preroll	00:00.000
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	1052 (0x41C)
Min Packet Size	1052 (0x41C)
Max Bitrate (bit/sec)	1511712

Raw data dump

Size 104 (0x68)

Data

```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65      G          Se
0010: 68 00 00 00 00 00 00 00-92 8C 60 DF EA 71 FE 43   h          `  q C
0020: 81 04 22 51 D3 94 F3 9D-92 0D 17 01 00 00 00 00     "Q
0030: A0 0A 9A 2D 31 AC D1 01-E8 43 00 00 00 00 00 00      -1    C
0040: 00 C8 37 14 00 00 00 00-00 2D 31 01 00 00 00 00     7      -1
0050: 00 00 00 00 00 00 00 00-02 00 00 00 1C 04 00 00
0060: 1C 04 00 00 20 11 17 00
```



File Properties Object (104 bytes)

Property	Value
File Position	30 (0x1E)
Object ID	8CABDCA1-A947-11CF-8EE4-00C00C205365
Object Size	104 (0x68)
Version	2
MMS ID	00000000-0000-0000-0000-000000000000
Total Size	17847305 (0x1105409)
Creation Time	1970-1-1 00:00:00.000
Packets	5577
Duration	00:32.741
Send Duration	00:29.641
Preroll	00:03.100
Flags	0x00000002
Broadcast	0
Seekable	1
Use Packet Template	0
Live	0
Reliable	0
Recordable	0
Unknown Data Size	0
Max Packet Size	3200 (0xC80)
Min Packet Size	3200 (0xC80)
Max Bitrate (bit/sec)	224000

Raw data dump

Size 104 (0x68)

Data
```
0000: A1 DC AB 8C 47 A9 CF 11-8E E4 00 C0 0C 20 53 65      G          Se
0010: 68 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   h
0020: 00 00 00 00 00 00 00 00-09 54 10 01 00 00 00 00            T
0030: 00 80 3E D5 DE B1 9D 01-C9 15 00 00 00 00 00 00     >
0040: 50 E1 83 13 00 00 00 00-90 DB AA 11 00 00 00 00   P
0050: 1C 0C 00 00 00 00 00 00-02 00 00 00 80 0C 00 00
0060: 80 0C 00 00 00 6B 03 00                                  k
```

Figure 58: Minimum Bit Rate-Changed

The last artifact in the file properties object that can be seen as change sis the Minimum Bit rate

5.4 Modified Properties of Stream Properties Object

There are also some artifacts that were changed in this object of ASF file.. First artifact that changed was the object size. Initially it was 147 and after editing the object size was 129. Number of streams which were described by the number of flags were also one of the artifacts that was changed in this object. Table 11 shows changed Artifacts of Stream Properties Object.

Objects	Properties	Status
Stream Properties object	Object Size	Changed
Stream Properties object	Type Specific Length	Changed
Stream Properties object	Error Correction Data Length	Changed

Table.11: Changed Artifacts of Stream Properties Object

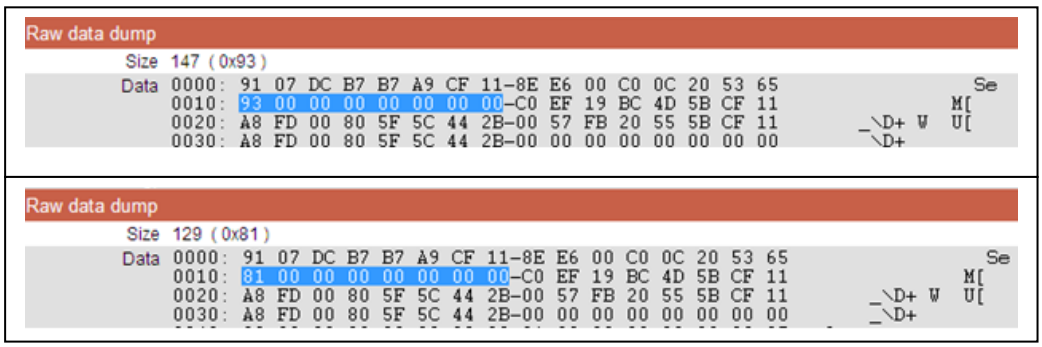


Figure 59: Object Size-Changed

The first artifact that is changed in the stream Properties Object is the Object Size which specifies the total object size of the stream Properties Object.

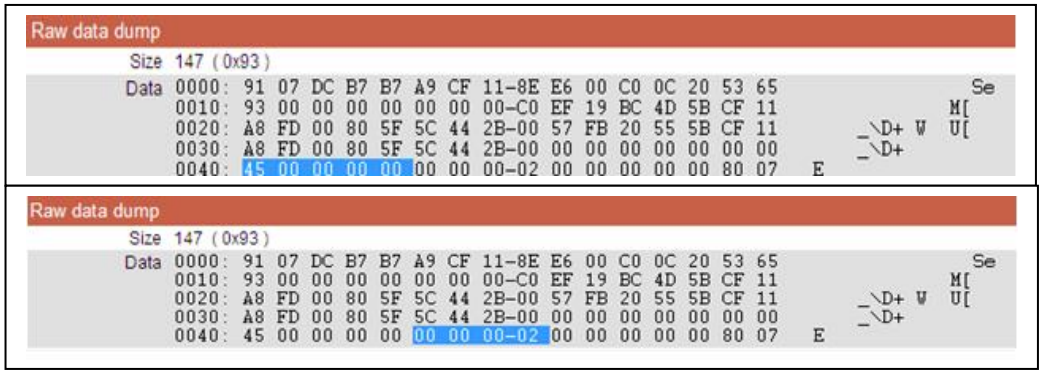


Figure 60: Type Specific Length- changed

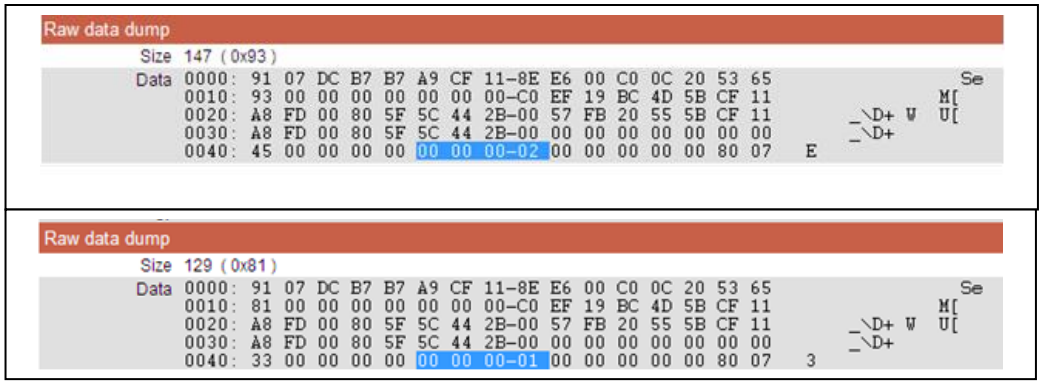


Figure 61: Error Correction Data Length-Changed

The last artifact in stream properties object that can be seen as changed is the error correction Data length which specifies the bytes.

5.5 Modified Properties of Header Extension Object

The only artifact that was changed in the header extension object was the file position. Before the editing it was 281 and after the editing it was changed to 134. Figure 62 shows comparison between artifacts before and after Editing of Header Extension Properties Object. Table 12 can be used to see the changed Artifacts of Header Extension Object.

Objects	Properties	Status
Header Extension Object	File Position	Changed

Table 12: Changed Artifacts of Header Extension Object

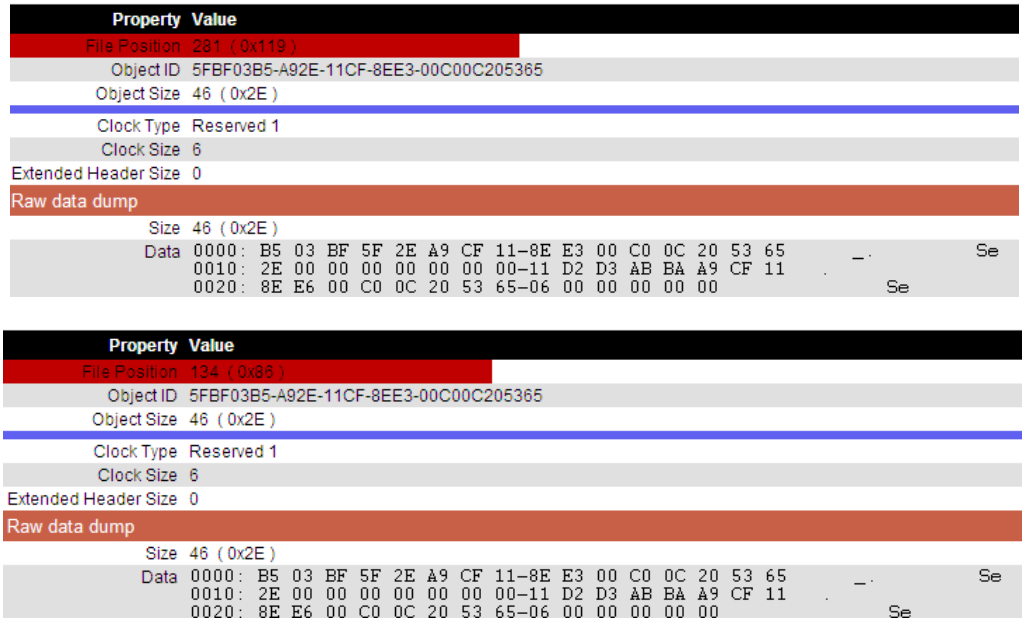


Figure 62: Header Object Changed

The only artifact that can be seen changed as the file position between two files.

5.6 Modified Properties of Data Object

The artifacts that were changed in this mandatory object were the object size which was having a value of 18828018 and afterwards it was having a value of 17846450. The other artifact that was edited was the file ID of the object. Total data packets were 17384 before the editing and afterward the packets were 5577.Total payload was also changed. The other artifact that changed was packet and payload overheads. Table 13 shows the Changed Artifacts of Data Object.

Objects	Properties	Status
Data Object	Object Size	Changed
Data Object	File ID	Changed
Data Object	Total Data Packets	Changed
Data Object	Total Payload Data	Changed
Data Object	Packet and Payload Overheads	Changed

Table 13: Changed Artifacts of Data Object

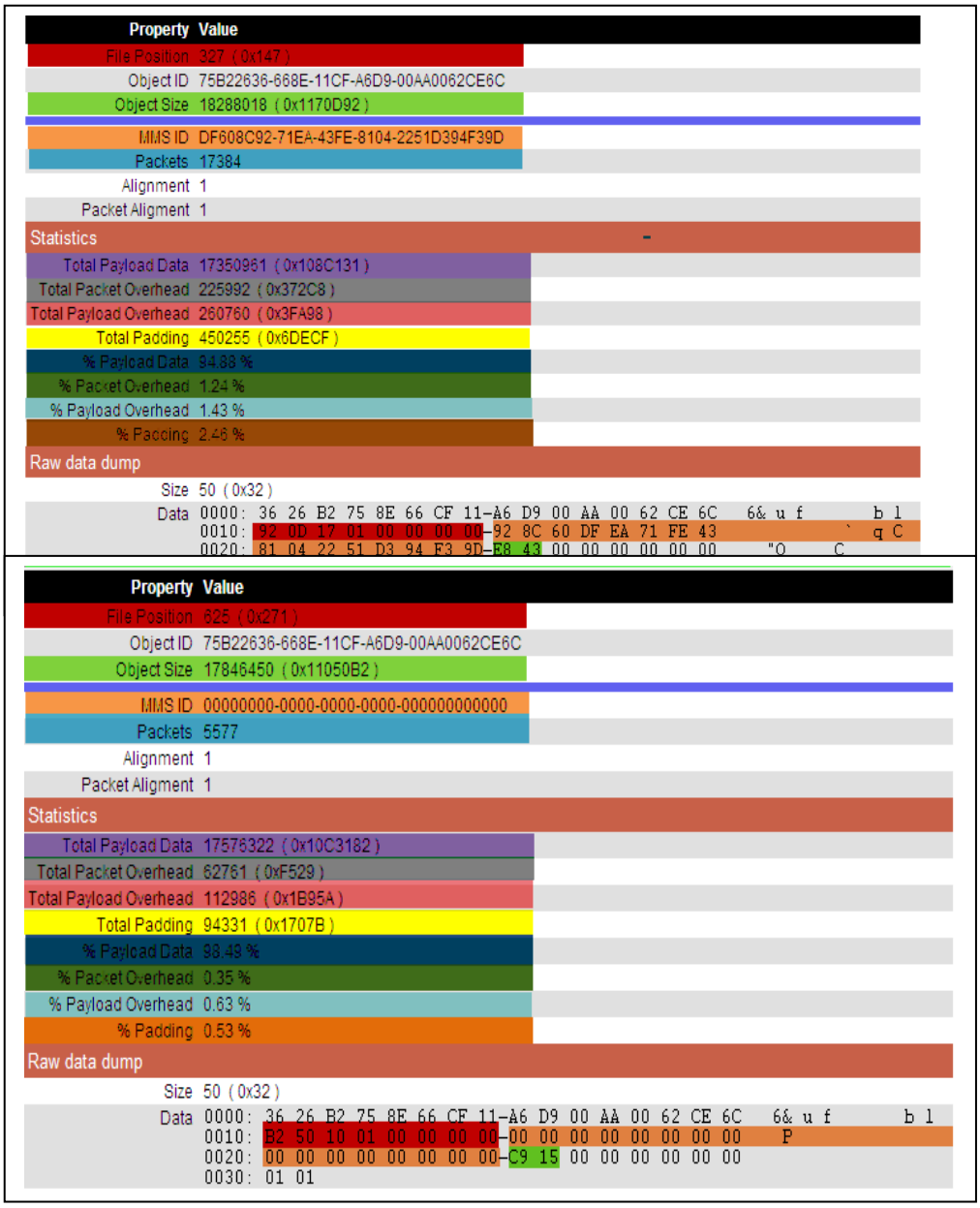


Figure 63: Data Object Changed

5.7 Modified Properties of Simple Index Object

Object Size was the first artifact that was seen as changed in the edited file. Time interval between two entries was also changed as result of editing on the file. The other artifacts

that were changed in index object were packet count and index entries count. Changed Artifacts of Simple Index Object can be seen in table 14.

Objects	Properties	Status
Simple Index Object	Object Size	Changed
Simple Index Object	Index entry time Interval	Changed
Simple Index Object	Maximum Packet Count	Changed
Simple Index Object	Index Entries Count	Changed

Table 14 Changed Artifacts of Simple Index Object

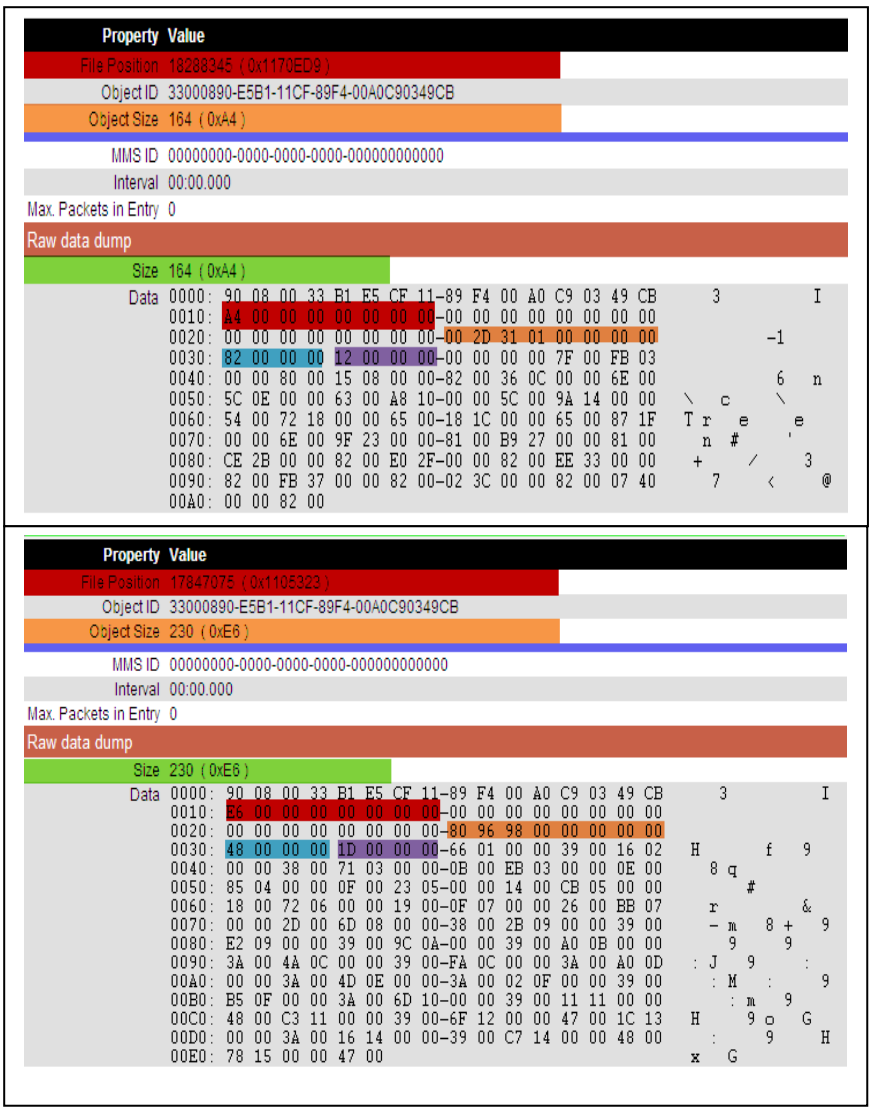


Figure 64: Simple Index Object Changed

From the above it can be seen that following artifacts were changes after the modifications ere made on the file. The artifacts inlucdes object size which specifies the size of simple index object of file, index entry time interval, maximum packet count and last artifact that is changed after the modification is Index entries count.

5.8 Conclusion

These Tables of different objects and comparison figures illustrates the artifacts that were changed after the editing was done on the file. Editing was done as part of the analysis to highlight the growing number cases of alterations that take place every day by the culprits to steal important information and edit the all important information to hide their identity from the LEA's. This research will also help agencies to identify the change that are made in the file.

Chapter 6

Proposed Policies and Recommendations

6.1 Introduction

The industry involving the IP cameras have grown extensively over past few years. From simple cameras to quite sophisticated ones. The Technology of using the IP cameras is getting easier to use and everyone is installing the surveillance cameras to watch their homes or properties. With ease of use technology there are also some disadvantages that follow which come in shape of data breaches that are taking place in high rate than ever before in the history of internet connectivity. Now the question arises here from the security point of view is that how can one keep away hackers from finding your cameras on the network.

Forensics of IP cameras use proactive approach in detecting or identify forgery and it can also help in identifying different patterns that are used by the forgers in committing forgery. This study on the forensics of IP cameras will help predict future activities that can be committed by the forgers by seeking historical activities of same nature.

The forensic analysis of video revolves around the video that has been taken from hard disks are desktop computer to check whether the video has been compromised or edited by gaining unauthorized access. This research will help the agencies to submit the data in the court which was not acceptable earlier because its validity could not proved in the court.

Firmware in the IP cameras plays very important role as far as security is concerned and they need up-gradation.[27] There is good news for all the cameras users is that firmware of IP cameras is updatable and can be updated by the vendors if there is some vulnerability to be seen in security of the cameras on the network. Unattended vulnerability can be exploited by the hackers to gain unauthorized to the cameras. The

other thing that user of the cameras is to look for is to keep the IP cameras local otherwise the feed of the camera will end up on the internet. Non-routable IP's should be given to cameras if you are interested in securing your cameras. Most cameras don't have password protected feeds. There is always a basic mistake that is done by the camera user are that they set up the cameras and they think they will set password later and they will end up forgetting to set the password and they leave the cameras for everyone to access[28]. The other security aspect is that the computers or hard drives on which videos are being saved for later access should be protected and no unauthorized access should be given to anyone where all the important data/content lies. Renaming the default admin account and default password of the cameras is also an important thing one should do to protect the cameras. As in most occasions the default admin account and password is set by the manufacturers can be available on the website. If your camera is wireless capable you need to put on encryption, to save your cameras from intruders which can gain access to your cameras and can lot of tricky stuff [29]. If your cameras are attached to main network, it can pave way for the attackers to gain access to your network through the surveillance system, so it is advised to put the security camera to separate network.

Video Management software (VMS's) considered to be backbone of every IP based cameras. It is the part where all the logic resides, so VMS's need proactive measures for its protection [30]. There are many components involve in VMS that includes the Operating system, Microsoft databases. As for operating system itself it needs upgrades, so users must remain in contact with Vendors of VMS for up gradation. And it must be the responsibility of vendor to send you updates because with un-patched vulnerability it can be disastrous.

6.2 Conclusion

The use of IP cameras is increasing, so are the attempts to forge the digital content. IP cameras come with lot of advantages but there are also disadvantages that come with the cameras which are network based. This chapter discussed the vulnerabilities that can be used by the hackers to get access to your surveillance cameras.

Chapter 7

Future Work

7.1 Introduction

As discussed in the above sections that video forensics is one of the hot research topics and recently lot of research is being carried out in this field generating lot of complex problems as far as the investigation of different videos are concerned.

Despite lot of techniques have been borrowed from image forensics, video forensics always comes with the problems that are usually complex and always takes time build the processing history of the video content that is being investigated

Currently it is believed that processing history of the video content can be built under the impression that it will not distort the results and will maintain the authenticity of the content.

Future research will focus on the video content that is being forged or modified multiple times by the forger and it will be difficult to work on its processing history. In order to deal with this problem analysis and different techniques should be introduced as the knowledge of malign persons or forgers are increasing with every passing day [31].

7.2 Objectives Achieved

- Performed Forensic Analysis of video of IP based Camera. The Analysis consisted of ASF file structure.
- Determined all the changes that were occurred in the file.
- Compared the forensic artifacts of file before and after it was forged.
- Developed different scenarios, how the media file was forged and altered.
- Determined the Header, Data and Index Object of the media file.
- Found out the Packets, Payloads and Stream within the Data Object.

7.3 Concluding Remarks

The research discussed the current problems that are faced by the law enforcement agencies in validating the integrity/authenticity of multimedia data in the court of law. The research discussed different scenarios that can be used by culprits in forging the data. Few have studied the forensic analysis of ASF file of IP Camera. This research will pave a way that could lead towards more analysis of ASF files.

In this research we analyzed different artifacts of the ASF file of an IP based camera. The discussed analysis can be used to gather all important forensic evidence. The analysis can also help find similarities or differences to the ASF file, if the file is forged by the forger. The research also gave recommendations that can be used to safeguard the data of the IP cameras, so hackers or forgers couldn't get hold of it.

References

1. Cletus O. Ohaneme , James Eke , Augustine C.O. Azubogu , Emmanuel N. Ifeagwu and Louisa C. Ohaneme. Design and Implementation of an IP-Based Security Surveillance System. International Journal of Computer Science;2012 Sep;9(5):391-400
2. “Centralized vs Decentralized Cameras” Available at http://vs-us.com/centalized-and-decentralized-ip-cameras/ /(Accessed at 10th Jan, 17).
3. "Storage Servers-Difference between Centralized Surveillance cameras and Decentralized Surveillance cameras", Available at https://storageservers.wordpress.com/2015/05/25/difference-between-centralized-surveillance-cameras-and-decentralized-surveillance-cameras/ (Accessed at 10th Jan, 17).
4. "White paper-Total cost comparison study of analog and IP-based video surveillance", Available at: https://www.axis.com/files/whitepaper/wp_cost_comparison_41264_en_1012_lo.pdf. (Accessed at 12 Jan, 17).
5. “Presenting digital evidence to court”, Available at: http://www.bcs.org/content/ConWebDoc/7372 (Accessed at 13 Jan, 17).
6. "Improving Video Surveillance with Megapixel Cameras-The advantages of using megapixel cameras with advanced IP video surveillance management software",

Available at: file:///C:/Users/NLC%20User/Downloads/IP_VSwMC%20 (1).pdf. (Accessed at 14th Jan,17)

7. Ashwin Swaminathen, Min Wu and K. J. Ray Liu. "Component forensics of digital cameras: A non-intrusive approach."
8. Ashwin Swaminathen, Min Wu and K. J. Ray Liu. "Component forensics of digital cameras: A non-intrusive approach.".
9. "White paper-Understanding Compression Technologies for HD and Megapixel Surveillance." (Accessed at 20th Jan,17)
10. P. Bestagini, M. Fontani, S. Milani, M. Barni, A. Piva, M. Tagliasacchi, S. Tubaro. "An Overview on Video Forensics". 20th European Signal Processing Conference (EUSIPCO 2012).
11. Weihong Wang and Hany Farid, "Exposing digital forgeries in video by detecting double MPEG compression," in MM&Sec, 2006.
12. Sevinc Bayram, Husrev T. Sencar, and Nasir D. Memon, "Video copy detection based on source device characteristics: a complementary approach to content-based methods," in Proceedings of the 1st ACM international conference on Multimedia information retrieval, 2008.
13. Jing Zhang, Yuting Su, and Mingyu Zhang, "Exposing digital video forgery by ghost shadow artifact," in Proceedings of the First ACM workshop on Multimedia in forensics, 2009.
14. Weihong Wang and Hany Farid, "Exposing digital forgeries in video by detecting duplication," in MM&Sec, 2007.

15. D. M. Shotton,A. Rodríguez,N. Guil,O. Trelles,"A metadata classification schema for semantic content analysis of videos". DOI: 10.1046/j.0022-2720.2001.00966.2002 January 28
16. "Advanced Systems Format" , Available at : https://en.wikipedia.org/wiki/Advanced_Systems_Format (Accessed at 24th Jan,17)
17. "Overview of the ASF Format", Available at: https://msdn.microsoft.com/en-us/library/windows/desktop/dd757562 (v=vs.85).aspx (Accessed at 24th Jan, 17).
18. "Advance System Format-Header Object", Available at: https://wiki.libav.org/Format/ASF (Accessed at 31st Jan, 17).
19. Advance System Format-Data Object, Available at": https://wiki.libav.org/Format/ASF#Data_Object (Accessed at 31st Jan, 17).
20. "Advance System Format-Index Object", Available at: https://wiki.libav.org/Format/ASF#Index_objects (Accessed at 31st Jan, 17).
21. Dahua-Network Camera, Available at : http://www.dahuasecurity.com/products/ipc-hfw8331e-z5-11681.html (3rd Jan,17).
22. "ASF Windows Media Player 9 series ", Available at: https://www.microsoft.com/en-us/download/details.aspx?id=12826 (Accessed at 5th Feb, 17).
23. Artifacts of Header Object, Available at: https://msdn.microsoft.com/en-us/library/windows/desktop/ee663575 (v=vs.85).aspx (Accessed at 8th Feb,17).

24. "Artifacts of File Properties Object", Available at: http://tech-insider.org/digital-video/research/1997/asf/asfwp.htm (Accessed at 17th Feb, 17).
25. "Artifacts of Stream Properties Object", https://msdn.microsoft.com/en-us/library/windows/desktop/bb970440 (v=vs.85).aspx (Accessed at 17th Feb,17).
26. Qing Wei ,Yongqiang Zhang, Mohua Zhang ,Mingyi Cui, Study on Synchronization for Streaming Media Based on ASF Format for E-learning. Proceedings of Web International Conference on Information Systems and Mining (WISM), 2010 23-24 Oct; Sanya, China.
27. Firmware of IP cameras, Available at : https://www.cnet.com/how-to/how-to-prevent-your-security-camera-from-being-hacked/ (Accessed at 2nd March,17).
28. 10 Easy Tips to Secure Your WiFi Home Security Camera", Available at: https://reolink.com/how-to-secure-your-wifi-enabled-home-camera/ (Accessed at 3rd March, 17).
29. Video Management Software", Available at: https://kintronics.com/solutions/ip-camera-systems/video-recording-systems/video-management-software/ (Accessed at 2nd March, 17).
30. "Encryption of IP Cameras", Available at: https://security.stackexchange.com/questions/56779/securing-remotely-accessible-ip-cameras-that-do-not-support-https (Accessed at 3rd March, 17).
31. Michael G. Noblett, Mark M. Pollitt, Lawrence A. Presley. Recovering and Examining Computer Forensic Evidence. Forensic science Communication, October 2000.