SOURCE AND GENERATIONAL ANALYSIS OF TRANSMITTED VIDEO FILES TO AN APPLE IPHONE

by

BRANDON EVAN EPSTEIN

B.S., American Intercontinental University, 2017

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Master of Science

Recording Arts Program

2020

This thesis for the Master of Science degree by

Brandon Evan Epstein

has been approved for the

Recording Arts Program

by

Catalin Grigoras, Chair

Jeff M.Smith

Cole Whitecotton

Bertram Lyons

Date: December 12, 2020

Epstein, Brandon Evan (M.S., Recording Arts Program)

Source and Generational Analysis of Transmitted Video Files to an Apple iPhone

Thesis directed by Associate Professor Catalin Grigoras

ABSTRACT

Forensic video examiners are often asked to determine authenticity and provenance of unknown video files. Evaluation of an unknown video file's structure can give insight into the device that created the file as well as the way it was transmitted, independent of file metadata and visual content. Identifying common file structures among devices and transmission methods may allow for examiners to map a file back to an originating make and/or model of device and determine how it was transmitted. This methodology can be used as part of an overall authentication framework or when other avenues for authentication such as file metadata may be unavailable or unreliable.

The form and content of this abstract are approved. I recommend its publication.

Approved: Catalin Grigoras

DEDICATION

I dedicate this thesis to my wife Leigh Anne and my daughter Alex. Thank you for recognizing the importance of education and providing an unfathomable amount of support not only throughout this entire program and but in every part of life. Alex, I hope daddy makes you proud.

And to the memory of William “Billy” McCaw. The quest to provide justice for you and your family started my journey into video forensics and the path to the NCMF and this thesis.

ACKNOWLEDGEMENTS

I would like to thank to Dr. Catalin Grigoras and Jeff Smith to their dedication to providing a world class education both inside and outside the classroom, and for your continuing contributions to the media forensics community. You are epidemies of a true experts in the field and what we should all strive to be. I am also indebted to the work of Leah Haloin and Cole Whitecotton during my studies. Leah is the glue that holds the NCMF together and reason I was able to navigate the logistics of the program. If Leah is the glue, Cole is the oil that keeps it running smoothly. Thank you for not only your work inside the classroom but for your diligence and patience keeping the technology running smoothly.

I also want to express my deep appreciation and gratitude to Bertram Lyons for his assistance with completing this thesis. The development of the concept as well as the methodology would not have been possible without his tremendous insight and guidance along the way.

TABLE OF CONTENTS

CHAPTER

I. INTRODUCTION 1

Prior Research 1

ISO/IEC Base Media File Format File Structure 3

Research Focus/Limitations 7

II. MATERIALS AND METHODS 9

Transmitting Devices/Videos 9

Method of Transmission 14

Receiving Device/Data Acquisition 15

Structural Mapping/Signatures 16

III. RESULTS 21

On Device Analysis 21

iMessage Analysis 21

Facebook Messenger Analysis 22

WhatsApp Analysis 22

IV. CONCLUSIONS 23

V. FUTURE RESEARCH 25

REFERENCES 26

APPENDIX 28

LIST OF TABLES

TABLE

1. Specification Defined Boxes 5

2. Test Devices 9

3. iOS Video File Details 10

4. Android Video File Details 12

5. Comparison of Signatures A and B 17

6. File Signature by Device and Transmission 21

7. File Signature A Structural Map 28

8. File Signature B Structural Map 31

9. File Signature C Structural Map 34

10. File Signature D Structural Map 35

11. File Signature E Structural Map 37

12. File Signature F Structural Map 40

13. File Signature G Structural Map 43

14. File Signature H Structural Map 44

15. File Signature I Structural Map 46

16. File Signature J Structural Map 47

17. File Signature K Structural Map 49

18. File Signature L Structural Map 50

LIST OF FIGURES

FIGURE

1. Basic MP4 Box Construction.. 3

2. Basic MP4 Box Structure... 4

LIST OF ABBREVIATIONS

ISO – International Organization for Standardization

IEC – International Electrotechnical Commission

FBM – Facebook Messenger

CHAPTER I

INTRODUCTION

The smartphone has revolutionized the way people communicate around the world; advances in smartphone technology and cellular infrastructure has allowed for video files to be transmitted like never before. As such, transmitted video files often play an integral part in criminal investigations and legal proceedings. Video files can either be a record of critical events or themselves be prima facia contraband; either way, digital forensic examiners can be tasked with determining the source of a transmitted video file or the manner in which it was transmitted.

A common method employed by examiners is to evaluate a file's metadata to gain insight into many aspects of the file, including its source. However, certain metadata may become altered/removed during file transmission, complicating this approach. Unlike descriptive or administrative metadata, whose values display information to the user about a specific file, structural metadata is the organization and relationships of objects within a file, irrespective of their actual values [1]. This research and thesis will focus on the evaluation of a video file's structure, absent other metadata to determine the source and method of transmission of the file.

Prior Research

Using a structural analysis approach to evaluate video files is not a new concept. Prior research by Gloe, et al. [2] as well as Hall [3] have identified file structure as part of an overall approach to video file authenticity including other descriptive metadata. In a proposed framework for video authentication, Wales [4] identifies file structure as an initial step to optimize an overall authentication workflow. In the aforementioned research, structural analysis had focused on a one-to-one comparison and/or evaluation of authenticity from a specific source device. In contrast to a one-to-one comparison, Iuliani, Shullani, Fontani, S. Meucci, and Piva. [5] propose the use of structural analysis as part of an overall approach to authenticity by identifying the provenance of files without a known source.

While structural analysis has been explored as part of an overall authenticity and/or provenance evaluation, analysis of the effects of transmission to a video file's structure has not been fully addressed. As part of a comprehensive attempt to identify the source of video files transmitted to YouTube, Giammarrusco [6] examined elements of file structure that showed promise in determining provenance, but did not evaluate the entirety of the objects within a transmitted file. Wolanin [7] explored the structure of files downloaded from Facebook and identified specific structural consistencies/inconsistencies.

While the goal Wolanin's research was not to identify provenance or transmission method of video files uploaded to Facebook, the results showed promise that different platforms may use unique file structures, which may allow the mapping of those structures to a specific transmission method or group of devices.

Lyons and Fischer [8] explored the concept of using an unknown file's structure, absent administrative metadata, to identify its provenance without a reference file. This approach involves evaluating file structures and assigning unique signatures to structures in common. As part of this concept a forensic video examination tool, Medex, is used to automate this process by identifying structural signatures and comparing against a reference library. It should be noted that in addition to developing the concept, Bertram Lyons served as a member of this thesis committee and the Medex tool was utilized in order generate signatures and perform comparisons that were used to complete this thesis.

ISO/IEC Base Media File Format File Structure

In order for video files to be created by a multitude of devices and then played back on another, different device, established standards must be adhered to. One of the most common specifications for file formats encountered in smartphone video transmission is the ISO/IEC base media file format 14496-12 – MPEG-4 Part 12 [9]. The ISO base media file format specification was originally created in 2001 from the QuickTime file format specification for .MOV files by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Now in its fifth edition, the 2015 ISO/IEC base media file format specification extends coverage to the commonly encountered .MP4, .MOV and .3GP file formats as well as other lesser used formats.

At the core of the specification is the use of a sequence of objects, termed boxes, to construct a multimedia presentation (video file). All data encoded in the file is contained within boxes and there are specific requirements as to how a box is constructed [9].

	box size	**box type**	**version**	**flags**	**payload**
length	4 bytes	4 bytes	1 byte	3 bytes	variable
value	32 bit unsigned Big Endian	ASCII text	0 or 1 8 bit unsigned	24 bits	dependent on box type

Figure 1. Basic MP4 Box Construction

One of the requirements to build a valid box is a header with a four-byte code describing the type of box (i.e., what kind of information it contains) as well four additional bytes providing the length of the box (i.e., allows for the understanding of when the next box begins). Boxes may be sequential in their arrangement or nested within other boxes as the file is encoded as seen in figure 2 [8].

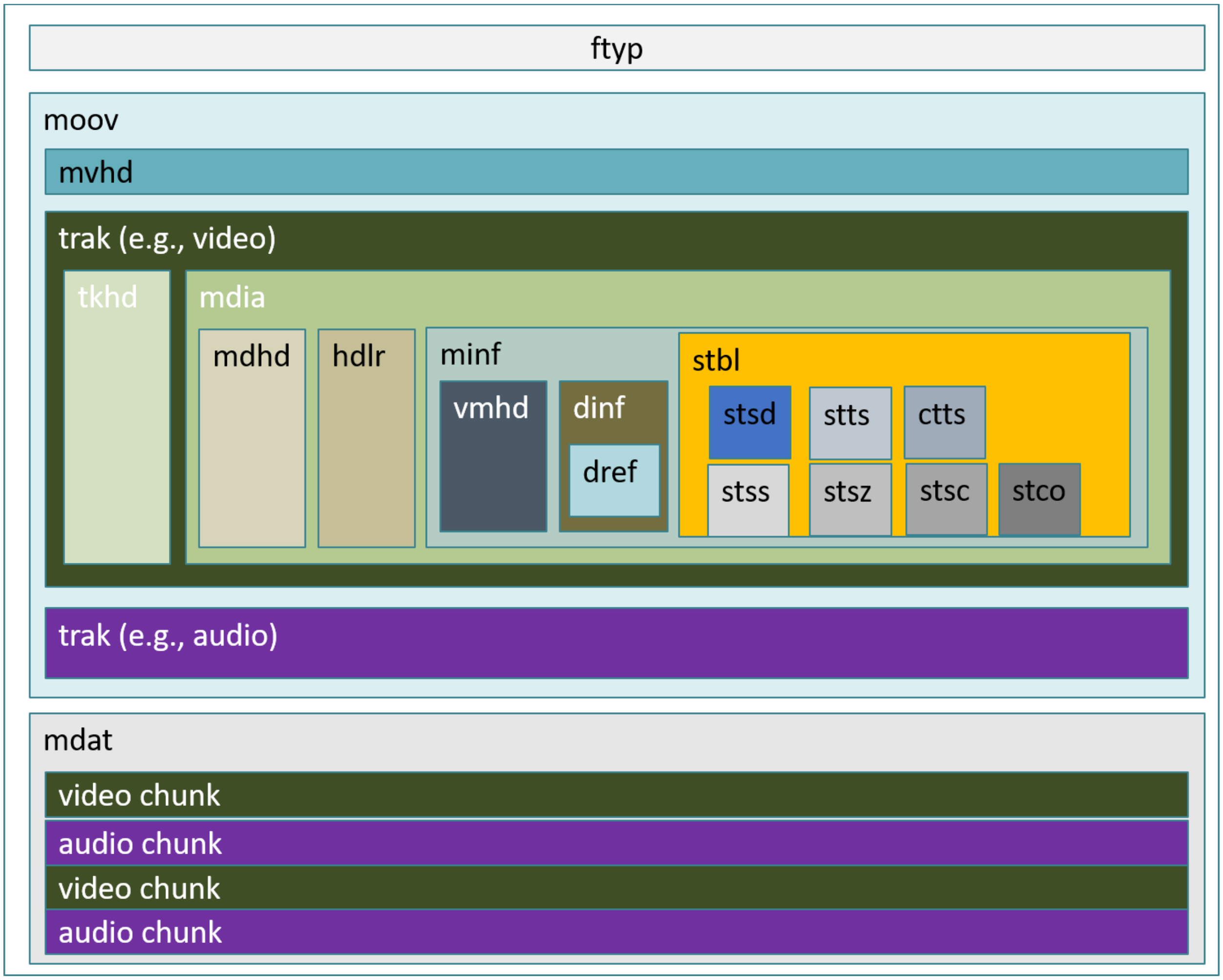

Figure 2. Basic MP4 Box Structure

While the ISO base media file format specification has rigid requirements for the construction of individual boxes, it is very flexible in regard to their presence and order within a file. For example, the file type ’ftyp’ box is typically required in all files and should be ordered first with very few exceptions. The specification also requires a singular movie ‘moov’ box but allows for the placement either at the beginning or end of the file. Even when boxes are required for playback, their arrangement is not strictly dictated by the specification. Additionally, there are a number of optional boxes that may or may not be present in a file whose order is flexible as well. Table 1 [9] provides greater detail of required and optional boxes and a sample arrangement. Users can also create custom boxes for inclusion in files that have not been specifically identified within the specification.

Table 1. Specification Defined Boxes

Box type						Description
ftyp						file type and compatibility
pdin						progressive download information
moov						container for all the metadata
	mvhd					movie header, overall declarations
	meta					metadata
	trak					container for an individual track or stream
		tkhd				track header
		tref				track reference container
		trgr				track grouping indication
		edts				edit list container
			elst			an edit list
		meta				metadata
		mdia				container for the media information in a track
			mdhd			media header
			hdlr			handler, declares the media (handler) type
			elng			extended language tag
			minf			media information container
				vmhd		video media header
				smhd		sound media header
				hmhd		hint media header (hint track only)
				sthd		subtitle media header (subtitle track only)
				nmhd		Null media header (some tracks only)
				dinf		data information box, container
					dref	data reference box
				stbl		sample table box
					stsd	sample descriptions
					stts	(decoding) time-to-sample
					ctts	(composition) time to sample
					cslg	composition to decode timeline mapping
					stsc	sample-to-chunk
					stsz	sample sizes
					stz2	compact sample sizes
					stco	chunk offset, partial data-offset information
					co64	64-bit chunk offset
					stss	sync sample table
					stsh	shadow sync sample table
					padb	sample padding bits

Table 1. Continued

					stdp	sample degradation priority
					sdtp	independent and disposable samples
					sbgp	sample-to-group
					sgpd	sample group description
					subs	sub-sample information
					saiz	sample auxiliary information sizes
					saio	sample auxiliary information offsets
		udta				user-data
	mvex					movie extends box
		mehd				movie extends header box
		trex				track extends defaults
		leva				level assignment
moof						movie fragment
	mfhd					movie fragment header
	meta					metadata
	traf					track fragment
		tfhd				track fragment header
		trun				track fragment run
		sbgp				sample-to-group
		sgpd				sample group description
		subs				sub-sample information
		saiz				sample auxiliary information sizes
		saio				sample auxiliary information offsets
		tfdt				track fragment decode time
		meta				metadata
mfra						movie fragment random access
	tfra					track fragment random access
	mfro					movie fragment random access offset
mdat						media data container
free						free space
skip						free space
	udta					user-data
		cprt				copyright etc.
		tsel				track selection box
		strk				sub track box
			stri			sub track information box
			strd			sub track definition box
meta						metadata
	hdlr					handler, declares the metadata (handler) type
	dinf					data information box, container
		dref				Data reference box
	iloc					item location

Table 1. Continued

	ipro					item protection
		sinf				protection scheme information box
			frma			original format box
			schm			scheme type box
			schi			scheme information box
	iinf					item information
	xml					XML container
	bxml					binary XML container
	pitm					primary item reference
	fiin					file delivery item information
		paen				partition entry
			fire			file reservoir
			fpar			file partition
			fecr			FEC reservoir
		segr				file delivery session group
		gitn				group id to name
	idat					item data
	iref					item reference
meco						additional metadata container
	mere					metabox relation
		meta				metadata
styp						segment type
sidx						segment index
ssix						subsegment index
prft						producer reference time

Research Focus/Limitations

Due to the nature of the ISO base media file format specification, it is feasible that different recording devices, software platforms and transmission methods may use differing sets of boxes, and may present those boxes in differing sequences and hierarchies when creating files of the same format. The absence or presence of these boxes as well as their arrangement may be used to develop unique structural signatures that correlate to a specific device, software, or transmission method [8]. This thesis will look at the ability to use a structural signature alone to provide insight into provenance or method of transmission of an unknown file. The specific hypothesis being that file structure alone will show some degree of file provenance and/or the transmission method. While this thesis focuses on structural evaluation and exploring the limits of using file structure to identify the source and transmission methods, file structure analysis is already a recognized approach when performing video authentication examinations, particularly in one to one evaluations [4]. Rather, this thesis will examine what effects certain methods of video file transmission have on file structure and if these effects produce unique signatures. The intent of this thesis is not to have structural analysis replace any other forms of authentication, rather be incorporated as part of an overall workflow/triage for file authentication from unknown sources (without a known or reference file for comparison).

CHAPTER II

MATERIALS AND METHODS

Transmitting Devices/Videos

Eight devices (detailed in table 2) were used to capture sample videos (detailed in tables 3 and 4) to be transmitted. The specific devices were chosen based upon their popularity among users in North America [10]. To maintain consistency between devices, the forward camera was used to record videos that included background audio for 20 seconds. The device's GPS was disabled and the native camera app that records directly to the phone's DCIM folder was utilized.

Table 2. Test Devices

Make	Model	OS	Version/Revision	Chipset
Apple	iPhone 7	iOS	13.6	A10
Apple	iPhone 8	iOS	13.5	A11
Apple	iPhone X	iOS	13.5.1	A11
Apple	iPhone XR	iOS	13.6	A12
Apple	iPhone 11	iOS	13.6	A13
Samsung	Galaxy Note 9	Android	10.QP1A.190711.020.N960U1UES4DTD1	Qualcomm Snapdragon 845
Samsung	Galaxy S10	Android	10.QP1A.190711.020.G973U1UES3DTDD	Qualcomm Kryo 845
LG	Stylo 5	Android	9.PKQ1.190302.001.201561850950d	Qualcomm Snapdragon 450

Table 3. iOS Video File Details

Device	iPhone 7	iPhone 8	iPhone X	iPhone XR	iPhone 11
Format	MPEG-4	MPEG-4	MPEG-4	MPEG-4	MPEG-4
Format profile	QuickTime	QuickTime	QuickTime	QuickTime	QuickTime
File size	19.8 MiB	17.9 MiB	19.1 MiB	19.5 MiB	19.0 MiB
Duration	21 s 188 ms	20 s 722 ms	20 s 688 ms	20 s 685 ms	20 s 435 ms
Overall bit rate mode	Variable	Variable	Variable	Variable	Variable
Overall bit rate	7 825 kb/s	7 254 kb/s	7 749 kb/s	7 910 kb/s	7 782 kb/s
Video Data					
Track ID	1	1	1	1	1
Format	HEVC	HEVC	HEVC	HEVC	HEVC
Codec ID	hvc1	hvc1	hvc1	hvc1	hvc1
Duration	21 s 188 ms	20 s 722 ms	20 s 688 ms	20 s 685 ms	20 s 435 ms
Bit rate	7 722 kb/s	7 153 kb/s	7 649 kb/s	7 724 kb/s	7 588 kb/s
Width	1 920 pixels	1 920 pixels	1 920 pixels	1 920 pixels	1 920 pixels
Height	1 080 pixels	1 080 pixels	1 080 pixels	1 080 pixels	1 080 pixels
Display aspect ratio	16:9	16:9	16:9	16:9	16:9
Rotation	90°	90°	90°	90°	90°
Frame rate mode	Variable	Variable	Variable	Variable	Variable
Frame rate	29.970 FPS	29.970 FPS	29.970 FPS	29.970 FPS	30.000 FPS
Minimum frame rate	28.571 FPS	28.571 FPS	28.571 FPS	28.571 FPS	28.571 FPS

Table 3. Continued

Maximum frame rate	30.000 FPS	30.000 FPS	30.000 FPS	30.000 FPS	30.000 FPS
Color space	YUV	YUV	YUV	YUV	YUV
Chroma subsampling	4:2:0	4:2:0	4:2:0	4:2:0	4:2:0
Bit depth	8 bits	8 bits	8 bits	8 bits	8 bits
Bits/(Pixel*Frame)	0.124	0.115	0.123	0.124	0.122
Stream size	19.5 MiB	17.7 MiB	18.9 MiB	19.0 MiB	18.5 MiB
Color range	Limited	Limited	Limited	Limited	Limited
Color primaries	BT.709	BT.709	BT.709	BT.709	BT.709
Transfer characteristics	BT.709	BT.709	BT.709	BT.709	BT.709
Matrix coefficients	BT.709	BT.709	BT.709	BT.709	BT.709
Audio Data					
Track ID	2	2	2	2	2
Format	AAC	AAC	AAC	AAC	AAC
Format profile	LC	LC	LC	LC	LC
Codec ID	40	40	40	40	40
Duration	21 s 188 ms	20 s 720 ms	20 s 687 ms	20 s 685 ms	20 s 433 ms
Source duration	21 s 246 ms	20 s 782 ms	20 s 759 ms	20 s 735 ms	20 s 503 ms
Bit rate mode	Variable	Variable	Variable	Variable	Variable
Bit rate	88.6 kb/s	87.6 kb/s	85.9 kb/s	152 kb/s	162 kb/s

Table 3. Continued

Channel(s)	1 channel	1 channel	1 channel	2 channels	2 channels
Channel positions	Front: C	Front: C	Front: C	Front: L R	Front: L R
Sampling rate	44.1 kHz	44.1 kHz	44.1 kHz	44.1 kHz	44.1 kHz
Frame rate	43.066 FPS	43.066 FPS	43.066 FPS	43.066 FPS	43.066 FPS
Compression mode	Lossy	Lossy	Lossy	Lossy	Lossy
Stream size	229 KiB	222 KiB	217 KiB	385 KiB	404 KiB
Source stream size	230 KiB	222 KiB	217 KiB	385 KiB	405 KiB

Table 4. Android Video File Details

Device	**Galaxy Note 9**	**Galaxy S10**	**Stylo 5**
Format	MPEG-4	MPEG-4	MPEG-4
Format profile	Base Media / Version 1	Base Media / Version 1	Base Media / Version 1
File size	36.7 MiB	43.0 MiB	40.4 MiB
Duration	20 s 878 ms	20 s 922 ms	19 s 733 ms
Overall bit rate	14.8 Mb/s	17.2 Mb/s	17.2 Mb/s
Video Data			
Track ID	1	1	1
Format	AVC	AVC	AVC
Codec ID	avc1	avc1	avc1
Duration	High@L4	High@L4	High@L4
Format Settings	CABAC / 1 Ref Frames	CABAC / 1 Ref Frames	CABAC / 1 Ref Frames

Table 4. Continued

GOP	M=1, N=30	M=1, N=30	M=1, N=30
Duration	20 s 878 ms	20 s 922 ms	19 s 556 ms
Bit rate	14.5 Mb/s	17.0 Mb/s	17.0 Mb/s
Width	1 920 pixels	1 920 pixels	1 920 pixels
Height	1 080 pixels	1 080 pixels	1 080 pixels
Display Aspect Ratio	16:9	16:9	16:9
Rotation	90°	90°	270°
Frame Rate Mode	Variable	Variable	Variable
Frame Rate	29.970 FPS	30.000 FPS	30.000 FPS
Minimum Frame Rate	20.404 FPS	15.048 FPS	21.162 FPS
Maximum Frame Rate	30.010 FPS	30.100 FPS	30.303 FPS
Color Space	YUV	YUV	YUV
Chroma Subsampling	4:2:0	4:2:0	4:2:0
Bit Depth	8 bits	8 bits	8 bits
Scan Type	Progressive	Progressive	Progressive
Bits/(Pixel*Frame)	0.233	0.273	0.273
Stream Size	36.1 MiB	42.3 MiB	39.7 MiB
Color range	Limited	Limited	Limited

Table 4. Continued

Transfer characteristics	BT.709	BT.709	BT.709
Audio Data			
Track ID	2	2	2
Format	AAC LC	AAC LC	AAC LC
Codec ID	mp4a-40-2	mp4a-40-2	mp4a-40-2
Duration	20 s 779 ms	20 s 885 ms	19 s 733 ms
Bit rate mode	Constant	Constant	Constant
Bit rate	256 kb/s	256 kb/s	156 kb/s
Channels	2 channels	2 channels	2 channels
Channel layout	L R	L R	L R
Sampling rate	48.0 kHz	48.0 kHz	48.0 kHz
Frame rate	46.875 FPS	46.875 FPS	46.875 FPS
Compression mode	Lossy	Lossy	Lossy

Method of Transmission

After capture, a total of 21 video files were then transmitted – 15 files from 5 iPhones using the iMessage app , WhatsApp, and Facebook Messenger (FBM) and 6 files from 3 Android devices using WhatsApp and FBM. Video files were attached to messages from their stored location in the DCIM folder. It should be noted that the apps utilized allow the user to record video within the app and directly transmit it without being stored in the DCIM folder. Those methods of transmission were outside the scope of this research and were not considered.

Receiving Device/Data Acquisition

All files were transmitted to an Apple iPhone 6S (iOS 13.2) for evaluation. Once received, the iPhone 6S was connected to a computer and the 21 transmitted video files were copied from the phone's DCIM folder for analysis. Prior to copying files from the device, testing was conducted to ensure that the method of acquisition did not affect any file attributes.

Initial acquisition testing was conducted by acquiring video files from the iPhone 6S in the following manner:

- Cellebrite UFED Physical Analyzer (v.7.35.2.16) Advanced Logical extraction - Method 1&2
- Cellebrite UFED 4PC Checkm8 Filesystem extraction (v.7.34.1.133)
- Copy from DCIM folder
- iTunes backup

Once acquired, SHA256 hash values were created for the test video files for each method of extraction. Those hash values were compared and it was found that the corresponding video file's hash values matched regardless of acquisition method. Once confirmed that acquisition method did not affect video files, copying from the DCIM folder was selected for its ease of use and speed.

To ensure that the receiving iPhone 6S did not process or change the received files in any way, video files were downloaded using alternate methods as well. Files transmitted through iMessage were accessed through the Messages application in the Mac operating system and downloaded to a MacBook. Files transmitted through Facebook Messenger and WhatsApp were accessed on a Windows operating system though provider's web application and downloaded. SHA256 checksums of all files acquired using the aforementioned methods were calculated and compared to the files acquired from the iPhone 6S. Those hash values were found to be the same, confirming that the receiving device did not alter any video files.

Structural Mapping/Signatures

Medex forensic video examination software (developer version) [11] was utilized to parse and visualize the box structure of all files. While manually decoding and noting the file's box structure within a hex editor is possible, it is inefficient and time consuming to evaluate video files in this manner without a known reference to compare the data to. The use of automated tools, such as MediaTrace [12], AtomicParsley [13], and Medex is preferred as they will analyze a video file and report the order of the structural boxes to the user without the need for manual decoding. In addition to reporting the box structure of files, the Medex software will assign a specific structural signature based upon the presence of unique boxes and their order within a file. These structural signatures and the method employed by the Medex software were utilized in the analysis of all files for this thesis.

The creation of a unique signature based upon box structure allows for efficient comparison of file structures. Instead of performing a comparison against multiple box structures, unique signatures can be evaluated to identify like structures [14]. To demonstrate how box structure allows for attribution of signature to a specific group of devices, Table 5 shows a comparison of the structural composition of between Signature A (iPhone 7, iPhone 8, and iPhone X) and Signature B (iPhone XR and iPhone 11). Tables 7-18 (see appendix) contain the 12 unique structural signature maps from the 29 analyzed files (8 directly from the source device and 21 transmitted).

Table 5. Comparison of Signatures A and B

Signature A				Signature B		
Box Sequence	Box Depth	Box Name		Box Sequence	Box Depth	Box Name
1	1	ftyp		1	1	ftyp
2	1	wide		2	1	wide
3	1	mdat		3	1	mdat
4	1	moov		4	1	moov
5	2	mvhd		5	2	mvhd
6	2	trak		6	2	trak
7	3	tkhd		7	3	tkhd
8	3	tapt		8	3	tapt
9	4	clef		9	4	clef
10	4	prof		10	4	prof
11	4	enof		11	4	enof
12	3	edts		12	3	edts
13	4	elst		13	4	elst
14	3	mdia		14	3	mdia
15	4	mdhd		15	4	mhdh
16	4	hdlr		16	4	hdlr
17	4	mif		17	4	minf
18	5	vmhd		18	5	vmhd
19	5	hdlr		19	5	hdlr
20	5	dinf		20	5	dinf
21	6	dref		21	6	dref
22	7	alis		22	7	alis
23	5	stbl		23	5	stbl
24	6	stsd		24	6	stsd
25	6	sgpd		25	6	sgpd
26	6	sgpd		26	6	sgpd
27	6	sbgp		27	6	sbgp
28	6	stts		28	6	stts
29	6	ctts		29	6	ctts
30	6	cslg		30	6	cslg
31	6	stss		31	6	stts
32	6	sdtp		32	6	sdtp
33	6	stsc		33	6	stsc
34	6	stsz		34	6	stsz
35	6	stco		35	6	stco
36	2	trak		36	2	trak
37	3	tkhd		37	3	tkhd
38	3	edts		38	3	edts

Table 5. Continued

39	4	elst		39	4	elst
40	4	mdia		40	3	mdia
41	5	mdhd		41	4	mdhd
42	5	hdlr		42	4	hdlr
43	5	minf		43	4	minf
44	6	smhd		44	5	smhd
45	6	hdlr		45	5	hdlr
46	6	dinf		46	5	dinf
47	7	dref		47	6	dref
48	8	alis		48	7	alis
49	6	stbl		49	5	stbl
50	7	stsd		50	6	stsd
51	7	stts		51	6	stts
52	7	stsc		52	6	stsc
53	7	stsz		53	6	stsz
54	7	stco		54	6	stco
55	2	trak		55	2	trak
56	3	tkhd		56	3	tkhd
57	3	edts		57	3	edts
58	4	elst		58	4	elst
59	3	tref		59	3	tref
60	4	cdsc		60	4	cdsc
61	4	cdep		61	4	cdep
62	3	mdia		62	4	mdia
63	3	mdhd		63	5	mdhd
64	3	hdlr		64	5	hdlr
65	3	minf		65	5	minf
66	4	gmhd		66	6	gmhd
67	5	gmin		67	7	gmin
68	4	hdlr		68	6	hdlr
69	4	dinf		69	6	dinf
70	5	dref		70	7	dref
71	6	alis		71	8	alis
72	4	stbl		72	5	stbl
73	5	stsd		73	6	stsd
74	5	stts		74	6	stts
75	5	stsc		75	6	stsc
76	5	stsz		76	6	stsz
77	5	stco		77	6	stco
78	2	trak		78	2	trak
79	3	tkhd		79	3	tkhd
80	3	edts		80	3	edts

Table 5. Continued

81	4	elst		81	4	elst
82	3	tref		82	3	tref
83	4	cdsc		83	4	csdsc
84	4	cdep		84	4	cdep
85	3	mdia		85	3	mdia
86	4	mdhd		86	4	mdhd
87	4	hdlr		87	4	hdlr
88	4	minf		88	4	minf
89	5	gmhd		89	5	gmhd
90	6	gmin		90	6	gmin
91	5	hdlr		91	5	hdlr
92	5	dinf		92	5	dinf
93	6	dref		93	6	dref
94	5	alis		94	7	alis
95	4	stbl		95	5	stbl
96	5	stsd		96	6	stsd
97	5	stts		97	6	stts
98	5	stsc		98	6	stsc
99	5	stsz		99	6	stsz
100	5	stco		100	6	stco
101	2	meta		101	2	trak
102	3	hdlr		102	3	tkhd
103	3	keys		103	3	edts
104	4	mdta		104	4	elst
105	4	mdta		105	3	tref
106	4	mdta		106	4	cdsc
107	4	mdta		107	4	cdep
108	3	ilst		108	3	mdia
109	4	data		109	4	mdhd
110	4	data		110	4	hdlr
111	4	data		111	4	minf
112	4	data		112	5	gmhd
				113	6	gmin
				114	5	hdlr
				115	5	dinf
				116	6	dref
				117	7	alis
				118	5	stbl
				119	6	stsd
				120	6	stts
				121	6	stsc
				122	6	stsz

Table 5. Continued

	123	6	stco
	124	2	meta
	125	3	hdlr
	126	3	keys
	127	4	mdta
	128	4	mdta
	129	4	mdta
	130	4	mdta
	131	3	ilst
	132	4	data
	133	4	data
	134	4	data
	135	4	data

CHAPTER III

RESULTS

Twelve unique structural signatures were identified from the 29 video files (8 acquired directly from the originating device and 21 transmitted) evaluated. Those unique signatures were then analyzed for any possible correlation between device and/or method of transmission. Table 17 identifies the individual unique signatures and their corresponding video file(s).

Table 6. File Signature by Device and Transmission

	iPhone 7	**iPhone 8**	**iPhone X**	**iPhone XR**	**iPhone 11**	**Galaxy Note 9**	**Galaxy S10**	**Stylo 5**
On Device	Sig A	Sig A	Sig A	Sig B	Sig B	Sig C	Sig C	Sig D
iMessage	Sig E	Sig E	Sig F	Sig F	Sig F			
FBM	Sig G	Sig G	Sig G	Sig G	Sig G	Sig H	Sig I	Sig H
WhatsApp	Sig J	Sig J	Sig J	Sig J	Sig J	Sig K	Sig L	Sig L

On Device Analysis

It was found that video recorded to the DCIM folders of the iPhone 7, iPhone 8, and iPhone X shared the same signature while the iPhone XR and iPhone 11 shared another. It should be noted that the iOS version of the devices varied. While the iPhone 8 and iPhone X share the same chipset, the other devices do not. Videos recorded to the DCIM folder of the Samsung Note 9 and Galaxy S10 also shared the same signature. Those devices had similar operating systems and chipsets were from the same manufacturer, but not the same model. The LG Stylo 5 exhibited its own unique signature. It should be noted that the chipset for the LG Stylo 5 is the same brand as in the Samsung devices used, but a different model.

iMessage Analysis

When files were transmitted between iPhones via iMessage, the file signature changed from when the file was stored in the DCIM folder. The iPhone 7 and iPhone 8 shared the same signature while the iPhone X, iPhone XR, iPhone 11 shared a different signature. Additionally, it was found that the signatures in common between devices when transmitted between devices by iMessage is different than the signatures in common between devices when the video file is stored in the DCIM folder without transmission.

Facebook Messenger Analysis

When files were transmitted by Facebook Messenger all Apple devices tested shared the same unique signature which was different than that stored on the device or transmitted by other methods. The Galaxy Note 9 and the LG Stylo 5 also shared a unique signature for transmission by Facebook Messenger while the Galaxy S10 had its own unique signature specific to this method.

WhatsApp Analysis

Like Facebook Messenger, the iPhones shared a unique signature specific to WhatsApp for the transmission method. Unlike the Facebook Messenger results, the Galaxy S10 and LG Stylo 5 shared a unique signature while the Galaxy Note 9 exhibited its own unique file signature for WhatsApp transmittal.

CHAPTER IV

CONCLUSIONS

The results of the research conducted for this thesis support the hypothesis that file structure alone will show some degree of file provenance and/or the manner it was transmitted. Three distinct on-device, two distinct iMessage, three distinct FBM, and 3 distinct WhatsApp signatures were found during this analysis. Given this finding, and the supposition that these distinct signatures would not be found elsewhere or in common between each other, it could be determined with confidence that, evidence characterized by one of these twelve signatures could be attributed to either an iPhone or Android device as well as iMessage, FBM, or WhatsApp. While devices of the same operating system did share some of the same signatures, no single signature found to be shared by both iOS and Android operating systems.. The lack of any similarity between iOS vs Android files lends support that structural analysis can be an effective approach when triaging unknown files for analysis. Additionally, each transmission method showed a different structural signature, giving unique insight into if the file was transmitted and/or method of transmission.

When looking at files that were captured on a device and not transmitted, file structure can also be used to further narrow potential source devices. Even though devices like the iPhone 7, iPhone 8, and iPhone X shared a signature, it was different than the signature for the iPhone XR and iPhone 11. Additionally, the iOS versions on the devices did not appear to affect the structure of files as different signatures shared the same iOS version. While both Samsung devices tested did share a common signature, the LG device exhibited a different one, showing promise that file structure could be used to discern between manufacturers of Android devices.

Apple devices that send video files via iMessage were also found to have a unique signature to the method of transmittal. This unique signature can not only be used to identify a video file transmitted by iMessage, but identify a potential group of device models that it originated from. Even though the Apple devices exhibited 2 different signatures for videos stored to the DCIM folder and 2 different signatures for files sent by iMessage, the signatures shared by devices are not the same for both scenarios. Identifying the cause for these differences was outside the scope of this thesis but could aid in a deeper understanding of determining provenance from unknown files.

File signatures of videos transmitted by Facebook Messenger may allow for the identification of Facebook Messenger as the method of transmission and identification of operating system of the originating device. Apple devices were found to share the same unique signature when video files were transmitted in this manner. Again, those signatures were different than Android devices, allowing structural analysis to limit potential methods of transmission and narrow down source devices. Android devices can also be further narrowed down as the Galaxy Note 9 and LG Stylo 5 exhibited the same signature while the Galaxy S10 displayed a different unique signature.

WhatsApp signatures may also allow the identification of WhatsApp as a method of transmission and identification of operating system of the originating device. Android device make and model may be further narrowed as evidenced by the Galaxy S10 and LG Stylo 5 sharing a unique signature to WhatsApp transmittal while the Galaxy Note 9 had its own unique signature.

CHAPTER V

FUTURE RESEARCH

The results of this thesis show promise in using an unknown file's structure to identify a source device and/or method of transmission. Expanded testing and structural signature identification with a larger number of iOS and Android as well as other recording devices such as security digital video recorders and camcorders could help to demonstrate validity to this approach. Additional testing involving an expanded group of applications and software could allow for structural signatures to be used on a broader scale.

To be increasingly effective against unknown files sources, a library of known file structure signatures could expedite authentication examinations by identifying the source device and method of transmission [11]. This could aid in developing investigative leads as well as conduct authenticity examinations. Once established, any library would have to be consistently updated as new devices and operating system versions are introduced.

REFERENCES

[1] J. Riley, "Understanding Metadata." National Information Standards Organization, 2017, Accessed: Sep. 24, 2020. [Online]. Available: https://groups.niso.org/apps/group_public/download.php/17446/Understanding%20Metadata.pdf.

[2] T. Gloe, A. Fischer, and M. Kirchner, "Forensic analysis of video file formats," *Digit. Investig.*, vol. 11, pp. S68–S76, May 2014, doi: 10.1016/j.diin.2014.03.009.

[3] J. R. Hall, "MPEG-4 Video authentication using file structure and metadata," University of Colorado, Denver, 2015.

[4] G. S. Wales, "Proposed framework for digital video authentication," University of Colorado, Denver, 2019.

[5] M. Iuliani, D. Shullani, M. Fontani, S. Meucci, and A. Piva, "Video Forensic Framework for the Unsupervised Analysis of MP4-Like File Container," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 3, pp. 635–45, Mar. 2019.

[6] Z. Giammarrusco, "Source identification of high definition videos: A forensic analysis of downloaders and YouTube video compression using a group of action cameras," University of Colorado, Denver, 2014.

[7] J. Wolanin, "Analysis of Facebook's video encoders," University of Colorado, Denver, 2018.

[8] B. Lyons and D. Fischer, "Structural signatures: Using source-specific format structures to identify the provenance of digital video files," presented at the Joint Technical Symposium, Hilverum, Netherlands, Oct. 05, 2019.

[9] "ISO/IEC 14496-12 Information technology - Coding of audio-visual objects - Part 12: ISO base media file format." ISO/IEC, 2015.

[10] A. Werner, "Global Handest Market by Region." Cellebrite Digital Intelligence, May 2020.

[11] B. Lyons and D. Fischer, *Medex*. Medex Forensics. https://www.medexforensics.com/.

[12] MediaArea, *MediaTrace*. https://mediaarea.net/MediaTrace.

[13] wez, *AtomicParsley*. http://atomicparsley.sourceforge.net/.

[14] B. Lyons and W. Bruehs, “Structural signatures: Using source-specific format structures to identify the provenance of digital video files,” presented at the 104th IAI International Educational Conference, Reno, Aug. 2019.

APPENDIX

Table 7. File Signature A Structural Map

Signature A iPhone 7 (source) / iPhone 8 (source) / iPhone X (source)							
ftyp							
wide							
mdat							
moov							
	mvhd						
	trak						
		tkhd					
		tapt					
			clef				
			prof				
			enof				
		edts					
			elst				
		mdia					
			mdhd				
			hdlr				
			minf				
				vmhd			
				hdlr			
				dinf			
					dref		
						alis	
				stbl			
					stsd		
					sgpd		
					sgpd		
					sbgp		
					stts		
					ctts		
					cslg		
					stss		
					sdtp		
					stsc		
					stsz		
					stco		
	trak						
		tkhd					
		edts					

Table 7. Continued

			elst				
			mdia				
				mdhd			
				hdlr			
				minf			
					smhd		
					hdlr		
					dinf		
						dref	
							alis
					stbl		
						stsd	
						stts	
						stsc	
						stsz	
						stco	
	trak						
		tkhd					
		edts					
			elst				
		tref					
			cdsc				
			cdep				
		mdia					
			mdhd				
			hdlr				
			minf				
				gmhd			
					gmin		
				hdlr			
				dinf			
					dref		
						alis	
				stbl			
					stsd		
					stts		
					stsc		
					stsz		
					stco		
	trak						
		tkhd					
		edts					

Table 7. Continued

			elst				
		tref					
			cdsc				
			cdep				
		mdia					
			mdhd				
			hdlr				
			minf				
				gmhd			
					gmin		
				hdlr			
				dinf			
				dref			
					alis		
			stbl				
				stsd			
				stts			
				stsc			
				stsz			
				stco			
	meta						
		hdlr					
		keys					
			mdta				
			mdta				
			mdta				
			mdta				
		ilst					
			data				
			data				
			data				
			data				

Table 8. File Signature B Structural Map

Signature B **iPhone XR (source) / iPhone 11 (source)**							
ftyp							
wide							
mdat							
moov							
	mvhd						
	trak						
		tkhd					
		tapt					
			clef				
			prof				
			enof				
		edts					
			elst				
		mdia					
			mhdh				
			hdlr				
			minf				
				vmhd			
				hdlr			
				dinf			
					dref		
						alis	
				stbl			
					stsd		
					sgpd		
					sgpd		
					sbgp		
					stts		
					ctts		
					cslg		
					stts		
					sdtp		
					stsc		
					stsz		
					stco		
	trak						
		tkhd					
		edts					
			elst				

Table 8. Continued

		mdia					
			mdhd				
			hdlr				
			minf				
				smhd			
				hdlr			
				dinf			
					dref		
						alis	
				stbl			
					stsd		
					stts		
					stsc		
					stsz		
					stco		
	trak						
		tkhd					
		edts					
			elst				
		tref					
			cdsc				
			cdep				
			mdia				
				mdhd			
				hdlr			
				minf			
					gmhd		
						gmin	
					hdlr		
					dinf		
						dref	
							alis
					stbl		
						stsd	
						stts	
						stsc	
						stsz	
						stco	
	trak						
		tkhd					
		edts					
			elst				

Table 8. Continued

		tref					
			csdsc				
			cdep				
		mdia					
			mdhd				
			hdlr				
			minf				
				gmhd			
					gmin		
				hdlr			
				dinf			
					dref		
						alis	
				stbl			
					stsd		
					stts		
					stsc		
					stsz		
					stco		
	trak						
		tkhd					
		edts					
			elst				
		tref					
			cdsc				
			cdep				
		mdia					
			mdhd				
			hdlr				
			minf				
				gmhd			
					gmin		
				hdlr			
				dinf			
					dref		
						alis	
				stbl			
					stsd		
					stts		
					stsc		
					stsz		
					stco		

Table 8. Continued

	meta						
		hdlr					
		keys					
			mdta				
			mdta				
			mdta				
			mdta				
		ilst					
			data				
			data				
			data				
			data				

Table 9. File Signature C Structural Map

Signature C Galaxy Note 9 (source) / Galaxy S10 (source)							
ftyp							
mdat							
moov							
	mvhd						
	udta						
		SDLN					
		smrd					
		smta					
			saut				
	meta						
		hdlr					
		keys					
			mdta				
			mdta				
		ilst					
			data				
	trak						
		tkhd					
		mdia					
			mdhd				
			hdlr				
			minf				
				vmhd			
					dinf		
						dref	

Table 9. Continued

							url
					stbl		
						stsd	
						stts	
						stss	
						stsz	
						stsc	
						stco	
	trak						
		tkhd					
		mdia					
			mdhd				
			hdlr				
			ound				
			minf				
				smhd			
				dinf			
					dref		
						url	
				stbl			
					stsd		
					stts		
					stsz		
					stsc		
					stco		

Table 10. File Signature D Structural Map

Signature D LG Stylo 5 (source)						
ftyp						
moov						
	mvhd					
	udta					
		auth				
		stvd				
		vhdr				
	meta					
		hdlr				
		keys				
			mdta			
		ilst				

Table 10. Continued

			data			
	trak					
		tkhd				
		mdia				
			mdhd			
			hdlr			
			minf			
				vmhd		
				dinf		
					dref	
						url
				stbl		
					stsd	
					stts	
					stss	
					stsz	
					stsc	
					stco	
	trak					
		tkhd				
		mdia				
			hdlr			
			ound			
			minf			
				smhd		
				dinf		
					dref	
						url
				stbl		
					stsd	
					stts	
					stsz	
					stsc	
					stco	
free						
mdat						

Table 11. File Signature E Structural Map

Signature E iPhone 7 (iMessage) / iPhone 8 (iMessage)							
ftyp							
wide							
mdat							
moov							
	mvhd						
	trak						
		tkhd					
		edts					
			elst				
		mdia					
			mdhd				
			hdlr				
			minf				
				smhd			
				hdlr			
				dinf			
					dref		
						alis	
				stbl			
					stsd		
					stts		
					stsc		
					stsz		
					stco		
	trak						
		tkhd					
		tapt					
			clef				
			prof				
			enof				
		edts					
			elst				
				Entry			
		mdia					
			mdhd				
			hdlr				
			minf				
				vmhd			
				hdlr			

Table 11. Continued

				dinf			
					dref		
						alis	
				stbl			
					stsd		
					stts		
					ctts		
					cslg		
					stss		
					sdtp		
					stsc		
					stsz		
					stco		
	trak						
		tkhd					
		edts					
			elst				
		tref					
			cdsc				
			cdeo				
		mdia					
			mdhd				
			hdlr				
			minf				
				gmhd			
					gmin		
				hdlr			
				minf			
					gmhd		
						gmin	
					hdlr		
					dinf		
						dref	
							alis
					stbl		
						stsd	
						stts	
						stsc	
						stsz	
						stco	
	trak						
		tkhd					

Table 11. Continued

		edts					
			elst				
		tref					
			cdsc				
			cdep				
		mdia					
			mdhd				
			hdlr				
			minf				
				mdhd			
				hdlr			
				minf			
					gmhd		
						gmin	
					hdlr		
					dinf		
						dref	
							alis
					stbl		
						stsd	
						stts	
						stsc	
						stsz	
						stco	
	meta						
		hdlr					
		keys					
			mdta				
			mdta				
			mdta				
			mdta				
		ilst					
			data				
			data				
			data				
			data				

Table 12. File Signature F Structural Map

Signature F iPhone X (iMessage) / iPhone XR (iMessage) / iPhone 11 (iMessage)							
ftyp							
wide							
mdat							
moov							
	mvhd						
	trak						
		tkhd					
		edts					
			elst				
		mdia					
			mdhd				
			hdlr				
			minf				
				smhd			
				hdlr			
				dinf			
					dref		
						alis	
				stbl			
					stsd		
					stts		
					stsc		
					stsz		
					stco		
	trak						
		tkhd					
		tapt					
			clef				
			prof				
			enof				
		edts					
			elst				
		mdia					
			mdhd				
			hdlr				
			minf				
				vmhd			
				hdlr			
				dinf			

Table 12. Continued

					dref		
						alis	
				stbl			
					stsd		
					stts		
					ctts		
					cslg		
					stss		
					sdtp		
					stsc		
					stsz		
					stco		
	trak						
		tkhd					
		edts					
			elts				
		tref					
			cdsc				
			cdep				
			mdia				
				mdhd			
				hdlr			
				minf			
					gmhd		
						gmin	
					hdlr		
					dinf		
						dref	
							alis
					stbl		
						stsd	
						stts	
						stsc	
						stsz	
						stco	
	trak						
		tkhd					
		edts					
			elst				
		tref					
			cdsc				
			cdep				

Table 12. Continued

		mdia					
			mdhd				
			hdlr				
			minf				
				gmhd			
					gmin		
				hdlr			
				dinf			
					dref		
						alis	
				stbl			
					stsd		
					stts		
					stsc		
					stsx		
					stco		
	trak						
		tkhd					
		edts					
			elst				
		tref					
			cdsc				
			cdep				
		mdia					
			mdhd				
			hdlr				
			minf				
				gmhd			
					gmin		
				hdlr			
				minf			
					gmhd		
						gmin	
					hdlr		
					dinf		
						dref	
							alis
					stbl		
						stsd	
						stts	
						stsc	
						stsz	

Table 12. Continued

						stco	
	meta						
		hdlr					
		keys					
			mdta				
			mdta				
			mdta				
			mdta				
		ilst					
			data				
			data				
			data				
			data				

Table 13. File Signature G Structural Map

Signature G iPhone 7 (FBM) / iPhone 8 (FBM) / iPhone X (FBM) iPhone XR (FBM) / iPhone 11 (FBM)						
ftyp						
moov						
	mvhd					
	trak					
		tkhd				
		edts				
			elst			
		mdia				
			mdhd			
			hdlr			
			minf			
				vmhd		
				dinf		
					dref	
						url
				stbl		
					stsd	
					stts	
					ctts	
					stsc	
					stsz	
					stco	
	trak					

Table 13. Continued

		tkhd				
		edts				
			elst			
		mdia				
			mdhd			
			hdlr			
			minf			
				smhd		
				dinf		
					dref	
						url
				stbl		
					stsd	
					stts	
					stsc	
					stsz	
					stsco	
					sgpd	
					sbgp	
	udta					
		meta				
			hdlr			
			ilst			
				data		
free						
mdat						

Table 14. File Signature H Structural Map

Signature H Galaxy Note 9 (FBM) / LG Stylo 5 (FBM)						
ftyp						
moov						
	mvhd					
	trak					
		tkhd				
		edts				
			elst			
		mdia				
			mdhd			
			hdlr			

Table 14. Continued

			minf			
				vmhd		
				dinf		
					dref	
						url
				stbl		
					stsd	
					stts	
					stss	
					ctts	
					stsc	
					stsz	
					stco	
	trak					
		tkhd				
		edts				
			elst			
		mdia				
			mdhd			
			hdlr			
			ound			
			minf			
				smhd		
				dinf		
					dref	
						url
				stbl		
					stsd	
					stts	
					stsc	
					stsz	
					stco	
					sgpd	
					sbgp	
	udta					
		meta				
			hdlr			
			ilst			
				data		
free						
mdat						

Table 15. File Signature I Structural Map

Signature I Galaxy S10 (FBM)						
ftyp						
moov						
	mvhd					
	trak					
		tkhd				
		edts				
			elst			
		mdia				
			mdhd			
			hdlr			
			minf			
				vmhd		
				dinf		
					dref	
						url
				stbl		
					stsd	
					stts	
					stss	
					ctts	
					stsc	
					stsz	
					stco	
	trak					
		tkhd				
		edts				
			elst			
		mdia				
			mdhd			
			hdlr			
			minf			
				smhd		
				dinf		
					dref	
						url
				stbl		
					stsd	

Table 15. Continued

					stts	
					stsc	
					stsz	
					stco	
	udta					
		meta				
			hdlr			
			ilst			
				data		
free						
mdat						

Table 16. File Signature J Structural Map

Signature J iPhone 7 (WhatsApp) / iPhone 8 (WhatsApp) iPhone X (WhatsApp) / iPhone XR (WhatsApp) iPhone 11 (WhatsApp)						
ftyp						
moov						
	mvhd					
	trak					
		tkhd				
		free				
		mdia				
			mdhd			
			hdlr			
			minf			
				vmhd		
				dinf		
					dref	
						url
				stbl		
					stsd	
					stts	
					stss	
					sdtp	
					stsc	
					stsz	
					stco	
	trak					

Table 16. Continued

		tkhd				
		free				
		mdia				
			mdhd			
			hdlr			
			minf			
				smhd		
				dinf		
					dref	
						url
				stbl		
					stsd	
					sgpd	
					sbgp	
					stts	
					stsc	
					stsz	
					stco	
mdat						

Table 17. File Signature K Structural Map

Signature K Galazy Note 9 (WhatsApp)						
ftyp						
beam						
moov						
	mvhd					
	trak					
		tkhd				
		mdia				
			mdhd			
			hdlr			
			minf			
				vmhd		
				dinf		
					dref	
						url
				stbl		
					stsd	
					stts	
					stsc	
					stsz	
					stco	
					stss	
	trak					
		tkhd				
		mdia				
			mdhd			
			hdlr			
			gmin			
			smhd			
			dinf			
				dref		
					url	
			stbl			
				stsd		
				stts		
				stsc		
				stsz		
				stco		
mdat						

Table 18. File Signature L Structural Map

Signature L Galaxy S10 (WhatsApp) / LG Stylo 5 (WhatsApp)						
ftyp						
beam						
moov						
	mvhd					
	trak					
		tkhd				
		mdia				
			mdhd			
			hdlr			
			minf			
				vmhd		
				dinf		
					dref	
						url
				stbl		
					stsd	
					stts	
					stsc	
					stsz	
					stco	
					stss	
	trak					
		tkhd				
		mdia				
			mdhd			
			hdlr			
			minf			
				smhd		
				dinf		
					dref	
						url
				stbl		
					stsd	
					stts	
					stsc	
					stsz	
					stco	
mdat						