IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Study of Meta Data Properties of Image and Video Files of Android Based Smart Phones

A. Pathania[1*], D.P. Gangwar[2], A. Kumar[3]

[1] Central Forensic Science Laboratory, MHA, Govt. of India, Sector 36A, Chandigarh, UT, India
[2] Central Forensic Science Laboratory, MHA, Govt. of India, Sector 36A, Chandigarh, UT, India
[3] Central Forensic Science Laboratory, MHA, Govt. of India, Sector 36A, Chandigarh, UT, India

[*]*Corresponding Author: pathania.anju@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 13/Jul/2018, Published: 31/July/2018

Abstract: The metadata properties and the characteristic features of display structure of image/video files transferred/exchanged using Bluetooth, Wifi(Shareit) and WhatsApp among the android based smart phones have been analyzed. This metadata study involves the fundamentals of sharing image through Bluetooth, Wifi and the social networking application “WhatsApp”. From the findings of the study the originated source of image/video files could be identified or trace out, which could be very useful for forensic authentication of suspect image/video files as well as in police investigation of various types of the crime cases. Moreover, this research emphasizes the size, resolution and location of the image clicked and shared in different sharing media applications like Bluetooth, WiFi and WhatsApp. New technologies present both challenges and opportunities for the security professional, especially for areas such as digital forensics. It analyzes potential originated source with location of device as they may have used for the crime by criminals. The tests and analysis were performed with the aim of determining what metadata and information can be found on the device memory for sharing of images/video. The experiments and results show that the potential evidences and valuable data can be found on sharing of data in Android phones by forensic investigators.

Keywords— WhatsApp, Android and Windows Operating Systems, Smartphone, Image & Shareit.

I. INTRODUCTION

Mobile devices are increasingly utilized to access social media and instant messaging services, which allow users to communicate with others easily and quickly. Digital evidences in forensics, which contains information of files lying in Smartphone of different operating systems (IOS, *Android and Windows Operating Systems*) are designed to take advantage of both the 3rd Generation (3G) and 4G networks and in many types of criminal investigations. However, the misuse of social media (Facebook, WhatsApp, YouTube, Twitter) and instant messaging (Bluetooth, WiFi) services facilitated conducting different cybercrimes [1]. Therefore, mobile devices are an important evidentiary piece in digital investigation.

In this paper, we report the results of our study and analysis of Bluetooth, WiFi and WhatsApp messaging services in android phones. We have examined data (Image) transfer services (Bluetooth, WiFi and WhatsApp). Our analysis may pave the way for future forensic investigators to trace and examine the source of the generated image/video which can be transferd to another mobile phones through sharing via Bluetooth, WiFi and WhatsApp data sharing and social networking applications [2]. The information of image stored on and associated with mobile devices can help address the crucial questions in an investigation, revealing whom an individual has been in contact with, what they have been communicating about, and where they have been. Criminals can use a mobile device to make initial contact with victims, exchange photographs or videos, groom victims, creating a vivid cyber trail for digital investigators to follow. Most mobile devices are networked devices sending and receiving data through telecommunication systems, WiFi access points, internet and Bluetooth piconets.

II. RELATED WORK

Bluetooth is an open standard for short-range radio frequency (RF) ,with frequency 2.4 GHz and band width 800 Kbps. Bluetooth technology is used primarily to establish As wireless personal area networks (WPAN), commonly referred to as ad hoc or peer-to-peer (P2P) networks[3]. Whereas, WiFi is based on a local area networking (LAN) technology designed to provide in-building broadband coverage. WiFi offers remarkably higher peak data rates than do 3G systems, primarily since it operates over a larger 20 MHz bandwidth.

On the opposite side WhatsApp text messaging internet Application, through which users can send messages, images, videos and audio media as well as their location [4]. Through these web based social apps, information is becoming intertwined with our daily lives and could either enhance productivity, efficiency and intelligence or make users vulnerable to its side effects. WhatsApp, Messenger, Facebook, and Viber , have become dominant factor in today's digital world and are affecting how users communicate [5][6][7].

III. METHODOLOGY

The questioned image file was captured by using Xiomi Redmi Note3, V5.1.1 (Android operating system) smart phone. Then the same image was sent to five different android based smart phones of different brands and versions (as shown in the Table.1) by using three different modes of data sharing applications ie. Bluetooth, Wifi(Shareit) and Web based social networking application WhatsApp, to determine the source information along with the location of mobile device. The image taken via the mobile phone contains the metadata property of the source mobile phone, record the location of cellular towers, potentially providing a media information.

Table. 1(Source mobile phone along with targeted phones)

Source of Image	**Images receiving devices/mobiles**		
	Make	*Model*	***Version***
Xiomi	Redmi	Note 3	V5.1.1
	Samsung	Galaxy on7Pro SM-G600FY	6.0.1
	Lenovo	A7000148	6.0
	Xiomi	Redmi	7.0
	Oppo	A57	6.0.1
	Vivo	V3	5.1

Table. 2(Metadata properties of image file)

Source	Taken On	File Name	Exif Data		Location	Device name
			Resolution	***Size***		
Redmi Note 3(Source)	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18 MB	205,Dakshin Marg,36A,Sec 36,chd	Xiomi Redmi Note 3
Redmi Note 4	(Mod Dt.) 19.1.18/17:03	IMG_20171214_162341.jpg	3456 x4608	2.18 MB	-	-
Vivo	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18 MB	205,Dakshin Marg,36A,Sec 36,chd	Xiomi Redmi Note 3
Lenovo	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18 MB	Chandigarh 30.737.76.759	Redmi Note 3
oppo	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18 MB	-	Redmi Note 3
Samsung	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18 MB	30.736837.76758987	-

ExifViewer, MediaInfo, JPEG-snoop and Amped Five were used to extract the metadata properties of the image and video files. The Hash calculator was used to calculate hash value of image files.

The XiomiRedmi Note 2, V5.11 was used as the source/capturing device of image file and captured file was transferred/shared with other mobile i.e. Samsumg, Lenovo, Oppo, Vivo and Redmi note 4 as image receiving android smart phones as shown in Table1. The metadata properties which are being extracted from the media files are shown in Table.2.

Table.3(Metadata Properties of received Image Through Bluetooth)

Source	Taken On	File Name	Exif Data		Location	Device name
			Resolution	***Size***		
Redmi Note 3(Source)	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18 MB	205,Dakshin Marg,36A ,Sec 36,chd	Xiomi Redmi Note 3
Redmi Note 4	(Mod Dt.) 19.1.18 /17:03	IMG_20171214_162341.jpg	3456 x4608	2.18 MB	-	-
Vivo	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18 MB	205,Dakshin Marg,36A ,Sec 36,chd	Xiomi Redmi Note 3
Lenovo	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18 MB	Chandigarh 30.737.76.759	Redmi Note 3
oppo	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18 MB	-	Redmi Note 3
Samsung	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18 MB	30.736837 .76758987	-

Table.4(Metadata Properties of received Image Through ShareIt)

	Taken On	**File Name**	**Exif Data**		**Location**	**Device name**
			Resolution	***Size***		
Redmi Note 3(Source)	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18MB	205,Dakshin Marg,36A,Sec 36,chd	Xiomi Redmi Note 3
Redmi Note 4	(Mod Dt.) 19.1.18 /17:03	IMG_20171214_162341.jpg	3456 x4608	2.18MB	-	-
Vivo	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18MB	205,Dakshin Marg,36A,Sec 36,chd	Xiomi Redmi Note 3
Lenovo	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18MB	Chandigarh 30.737.76.759	Redmi Note 3
oppo	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18MB	-	Redmi Note 3
Samsung	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456 x4608	2.18MB	30.736837.76758987	-

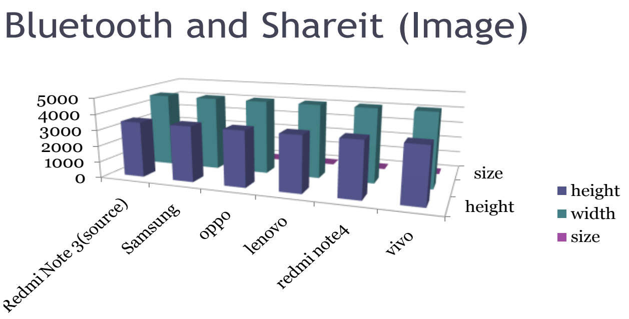

Figure 1. Block Chart of Bluetooth and Shareit properties(Height,Width and Size)

IV. Results and Discussion

The test Image was exchanged via Bluetooth, shareIt and WhatsApp v2.17.41 using different 6 android phones of different operating system. We decided to use only three mobile-applications instead of the too many net based applications are here. We used an Android Phone since it produces an image file that is more compressed than the iPhone one. In this way, we provided an equilibrate spectrum of BlueTooth, WiFi and Whatsapp contents qualities: namely high-low resolution and file size. The metadata properties of image file of source mobile and receiving mobiles using Bluetooth, ShareIt and Whatsapp data sharing applications as shown in Table.3,4 & 5.

Table.5(Metadata Properties of received Image Through WA)

Source	Taken On	File Name	Exif Data		Location	Device name
			Resolution	***Size***		
Redmi Note 3(Source)	14.12.17/16:23:14	IMG_20171214_162341.jpg	3456x4608	2.18 MB	205,Dakshin Marg,36A ,Sec 36,chd	Xiomi Redmi Note 3
Redmi Note 4	(Mod Dt.) 19.1.18/17:03	IMG-20180119-WA0019	864X1152	97.41KB	-	-
Vivo	14.12.17/16:23:14	IMG-20180119-WA0015	IMG-20180119-WA0015	97.41KB	-	-
Lenovo	14.12.17/16:23:14	IMG-20180119-WA0008	3456x4608	97.41KB	-	-
oppo	14.12.17/16:23:14	IMG-20180119-WA0026	3456x4608	97.41KB	-	Redmi Note 3
Samsung	14.12.17/16:23:14	IMG-20180119-WA0003	3456x4608	97.41KB	-	-

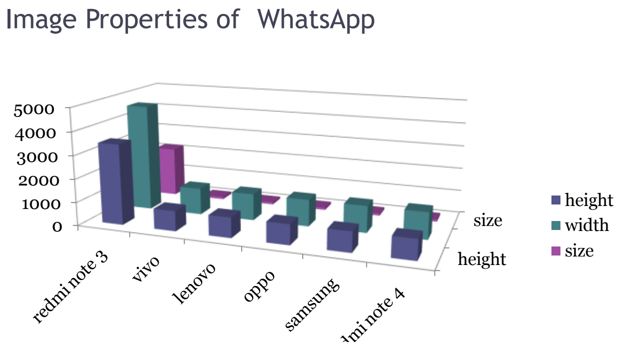

Figure 2. Block Chart of WhatsApp properties(Height,Width and Size)

Their comparison pictorial charts are shown in **Fig**ure 1 and 2 shows the resolution (pixels,height and width) and size of the test image.

GPS-enabled devices may also contain locations or maps and when that clicked image is being shared via Bluetooth or Shareit then the receiver will also get the same location along with the same metadata properties of image clicked by source mobile phone that can be very useful in an investigation.

Additionally, EXIF data embedded in digital image providing the date and time of the photograph was created, file name, resolution, size, device name and potentially the GPS coordinates/locations address of source of where the photograph was taken as shown in Table 3 and 4. GPS along with the metadata properties may also provide the user with mapping functionality, while transferring the data from Bluetooth and WiFi **only**

On the other hand whole metadata properties of image get compressed while sharing via WhatsApp as shown in Table.5.

V. Conclusion

The main purpose of the research is to identify source in media sharing applications on the Android platform which aid in forensic investigations. The study of metadata properties of image and video files of source and receiving mobiles were studied indicated that the image and video files sent between the source and other android mobile phones using the Bluetooth Data transfer and WiFi data Transfer applications, contained the same metadata properties hence the source identification is possible. If the GPS is in ON condition then location of the image will be identified while sending it through Bluetooth and WiFi sharing application ShareIt.

The metadata properties of image and video files source and other phone is not same in case of the files sent using the Web-based application i.e. WhatsApp. Therefore, the source identification may not be possible due to the compression and privacy protocol (ie.E2EE, Asynchronous communication Signal Protocol, and Curve25519) of the file size at present juncture.

VI. Acknowledgment

Support from the Head of Department, Physics and Director Central Forensic Science Laboratory, Chandigarh is gratefully acknowledged.

REFERENCES

[1] Cosimo Anglano , *“Forensic analysis of WhatsApp Messenger on Android smartphones*” Digital Investigation. Volume 11, Issue 3, *pp* 201-213, 2014.

[2] Breeuwsma. M, “*Forensic Imaging of embedded systems using JTAG*”, Digital Investigation. Volume 3, Issue 1, March 2006, Pages 32-42,2006

[3] Neha S. Thakur, *“Forensic Analysis of WhatsApp on Android Smartphones,”* University of New Orleans Theses and Dissertations pp.1706

[4] Kehinde Funmilayo Mefolere , “*WhatsApp and Information Sharing: Prospect and Challenges”,* International Journal of Social Science and Humanities Research, Vol. 4**,** (Issue 1), pp: (615-625), 2016,

[5] Shubham Sahu, *“An Analysis of WhatsApp Forensics in Android Smartphones”,* International Journal of Engineering Research, Volume No.3, (Issue No.5), pp: 349-350, 01 May 2014

[6] Umesh Kumar Singh, ShivlalMewada, Lokesh Laddhani & Kamal Bunkar, “*An Overview & Study of Security Issues in Mobile Ado Networks*”, International Journal of Computer Science and Information Security (IJCSIS) USA, Volume-9, No.4, pp (106-111), April 2011.ISSN: 1947-5500

[7] R. Nathiya, S.G. Santhi, *“Energy Efficient Routing with Mobile Collector in Wireless Sensor Networks (WSNs)”,* International Journal of Computer Sciences and Engineering, Vol.2, Issue.2, pp.36-43, 2014.

Authors Profile

Anju Pathania pursed Bachelor of Science from University of HP(Simla), India in 2004 and Master of Science(Physics) from BarkatUllah University in year 2008. She has done M.Tech(NS&NT) from Panjab University, Chandigarh and currently working as Senior Scientific Assistant(Physics) in Department of Foresic Science, Central Forensic Science Laboratory, Chandigarh, India since 2011. She has published one research papers in reputed international journal “Solar Energy Materials & Solar Cells” it’s also available online and one conference 24th AIFSC. Her main research work focuses on source identification which could be used in crime in digital forensics. She has 1year of teaching experience and 1 year of Research Experience before joining Forensic field(Before 2011). Myself is starting research work in digital forensics and area of interest are mobile forensics and crime related to it.

Durga Prasad Gangwar pursed B.Sc and M.Sc.(Physics) from Rohilkhand University bareilly(UP). He is currently working as Senior Scientific Officer(Physics) in Department of Foresic Science, Central Forensic Science Laboratory, Chandigarh, India since 1991. He has 27 years of experince in the filed of Forensic Science. He has solved many crime cases. He has published many research papers in reputed national Journals including Indian Acedemy of Forensic sciences,Kolkatta and Indian Police journal etc. ie. Codec Impact on Voice Spectrographic Features: A Forensic Study, ii. Characterization of Facial Features for Human Identification, iii. Decoding the code of the Disc combination lock of VIP brief case, Forensic Discrimination of Alkyd paint by Fourier Transform Infrared (FTIR) spectrometer etc. He has got best scientific paper awards from home ministery in 2014.

Akhlesl Kumar B.Sc.(Physics,Chemistry&Forensic Science**)** and M.Sc.(Forensic Science) from Dr. H.S. Gaur University Sagar (MP). He is currently working as Senior Scientific Officer(Physics) in Department of Foresic Science, Central Forensic Science Laboratory, Chandigarh, India since 1998. He has 20 years of experince in the filed of Forensic Science. He has solved many crime cases. He has published and presented 7 research papers in reputed national Journals including Indian Acedemy of Forensic sciences, Kolkatta, Indian Science Congress Delhi and All India Forensic Science Conference,etc and one book on Forensic science practical hand book published in the year of 1997. He has got Best Worker Award 2003, from Director,CFSL, MHA, Govt. of India, Kolkata in 2003. He got training from the FBI, Verginia USA on Digital Forensic in the year of 2010.