Security Validation on WhatsApp and Facebook Messenger Mobile Applications against GIF Images that Incorporate Executable Code

Hilda Colón Martínez
IT Management and Information Assurance
Advisor: Dr. Jeffrey Duffany
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— Communication; Every day the messaging applications on mobile devices such as WhatsApp and Facebook Messenger are more common in the life of each user. With this in mind, we ask ourselves the question, how safe are these mobile applications for Android mobile devices? Stenography is a technique that allows to deliver camouflaged messages within an image, so that they cannot be detected and go unnoticed. Most of the research that has been done on this topic has focused only on laptops and PCs. The purpose of this paper was to design a schematic in which we use Steganography to get an idea of how some executable code could be spread instead of simply communicating a secret message. Additional to validate the security of the two most important application on these days which are WhatsApp and Facebook Messenger against image that use the stenography technique. Based on this, a questionnaire was carried out where users' knowledge about security issues in the mobile messaging applications WhatsApp and Facebook Messenger was analyzed.*

Key Terms *— Communication, GIF, Hiding Executable, Security, Smartphones, Steganography.*

INTRODUCTION

Instant messaging applications are the most requested and downloaded among Android users. The application that most convinces users is one that all friends and family use and summarizes all the messaging programs in one. Communicate with your friends and talk to them anytime from anywhere is the best option. That is what is happening daily, messaging applications are one of the top of the most required applications worldwide. But as the demand for these applications increases, also that leads to more people who go with bad intentions to steal the identity of people, to ask for money in exchange for their information or just to have fun destroying their operating system of the user's mobile devices.

Internet was a big breakthrough in the way we communicate with each other bringing a universe of information. This universe has a proliferation of digital images, being the most interchangeable kind of file. Multimedia data presents a highly redundant representation, which usually allows the hide of significantly large amounts of data. Due to this, image files are the ideal objects to hide information, especially executable code, besides other kind of information. [1] The study performed on paper [1] they hide information on an image where it was executed by itself. The basic technique that is used for these types of execution is known as steganography.

There are several projects, tools, etc., that can perform or have done that type of execution in the images, but these projects and tools have been based on personal desktop and laptops, but the question is, could this also happen in the smartphone? If that were the case, would this affect more than 85% of the people? How is this possible?

Based on these questions, my idea for this research is to validate the security of the two most import application on these days which are WhatsApp and Facebook Messenger. Also validate the capacity of the user on this type of subject to make them aware of the possible malicious program that can be used to steal their information, corrupt the mobile devices, etc.; via an executable image using GIF file format.

BACKGROUND

The term steganography is derived from the Greek words steganos that means, “covered” and graphia that means “writing”, (i.e. covered writing). Steganography refers to the art and science of concealing a communication; unlike cryptography, where conceals the message but the communication is often known [2]. Steganography has been used successfully in history with different procedures and purposes, particularly during World War II. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points [3].

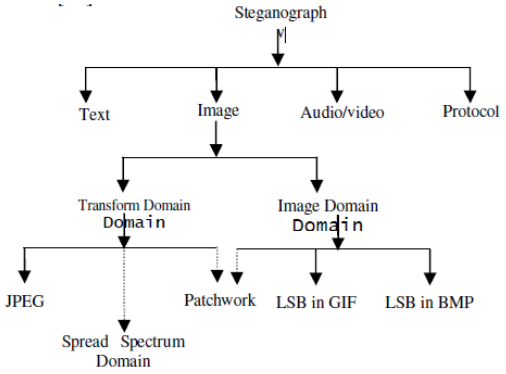


Figure 1
Variety Stenograph Techniques

Graphics Interchange Format, commonly known as GIF, this is a bitmapped image format widely used on the Web. Options include "progressive display" in which the rendering exploits interlaced lines, permitting recognizable images to appear before the whole file has downloaded; and short animations that exploit multiple images and control data within a single file. GIF uses LZW compression and palette-based color (256 or fewer shades) [4]. In other words, a GIF is multiple images in a single file. The GIF format is not associated with any type of application, but it was created for the visualization of data stored locally or on remote systems.

In the paper [5] they provide the general GIF format properties which are:

- Can be compressed to a small size.
- Are commonly used for images presented on the web.
- GIF files allow only 8-bit indexed color.
- GIF files use lossless LZW compression.
- GIF files support transparency.
- Animated GIF files can be created by sequences of single images.
- GIF files can be saved in an interlaced format that allows progressive download of web images (low resolution version of an image first then gradually comes into focus the rest of the data is downloaded).

PROBLEM

The importance of this research is due to the high demand that exists in the daily life of every users, regarding on how to properly use the mobile devices and the security on each one since these artifacts contains a lot of personal information. Most people use GIF images to express any feeling. That is why this project was chosen because we want to continue working on the realization or preparation of a GIF image that executes any type of command configured without the person noticing it, this is for the security validation in the messaging applications (WhatsApp and Facebook Messenger). The main objectives are to ensure the safety of users in the messaging applications WhatsApp and Facebook Messenger against GIF images containing executable content using the basic concept of Steganography and to educate users about the images that they shared since most of them do not know the origin of the same and the danger it could pose in their mobile phones.

METHODOLOGY

Due to several situations that affected the process to carry out this research, several schemes were created and used to help us continue the preparation of the executable GIF file for future work.

The general idea I want to stablish is to inject an executable X file into a GIF image. After it is obtained, several tests will be carried out on the

WhatsApp and Facebook Messenger applications within the devices that contain the Android operating system for educational purposes for the validation of security in both applications.

In the image that is presented below, is being observed a basic diagram of what would be the process of testing the executable GIF images:

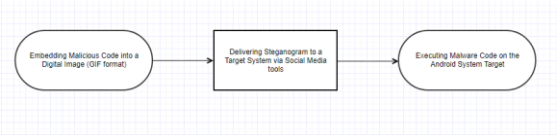


Figure 2
Basic Process Diagram

In this image we see the components of the GIF file of an image. In which we will be working on the decomposition of the GIF images to be able to add the executable file on the future works.

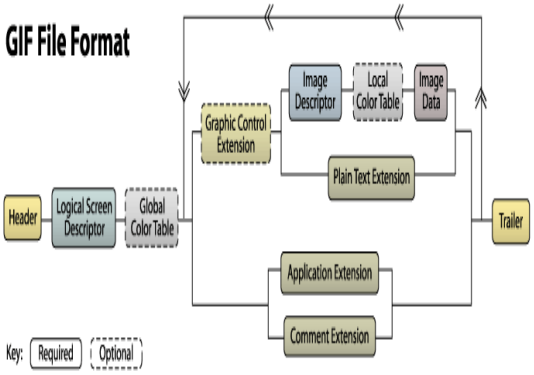


Figure 3
Basic GIF File Format Diagram

Several tests were performed with numerous applications of Steganography to start with the security evaluation of the WhatsApp and Facebook Messenger applications, but only using images with hidden messages. These tests were conducted to obtain data to see the behavior of the applications on how it will differentiate two type of image that contain secret messages in them. In the tests was used two Samsung Galaxy S7 Edge mobile devices with the version of Android 7.0. Also, the Steganography and Steganography Master tools where use. These two tools are free and can be downloaded from the Play Store application on any Android system. Both tools were installed on both mobile devices. Several images were used to encode the following message: "This is a test with educational purposes developed". Then both images were shared on the WhatsApp and Facebook Messenger messaging applications. The versions of both applications are as follows: WhatsApp is 2.17.395 and Facebook Messenger is 145.0.0.25.203.

Additional for this project, 75 people over 18 years of age were surveyed. For the survey, the online program used was the Google Form which is free for any user that has a Google account. The requirement for choose the survey participants was that each participant had a mobile device and the WhatsApp and Messenger applications installed in their device. Several questions were asked about age, gender, type of mobile technology used, level of education, use of Antivirus in mobile phones, frequency in which it uses messaging applications, etc. Each person was asked the same questions and the intention of this interview was indicated. It was explained to them that a survey and an analysis of the GIF images were being carried out and how these images could affect the mobile devices through the WhatsApp and Facebook Messenger messaging applications, this to be used for educational purposes. The questions asked during the survey were the following:

1. Gender
2. Age
3. What is your level of your Education?
4. Do you have a mobile device that contains the Android operating system?
5. You have some kind of Antivirus program on your mobile device?
6. How often do you use messaging applications (WhatsApp or Messenger)?
7. Do you have the knowledge of what GIF (Graphics Interchange Format) images are?
8. Do you share GIF (Graphics Interchange Format) images that are not created by you or by someone you know?
9. Do you know what the Malwares are?
10. Do you know what Ransomware is?

11. Do you know if the messaging applications (WhatsApp or Messenger) are safe?
12. Both applications protect against Malwares, Virus, Ransomware, etc?
13. Both applications protect you from identity theft?
14. Both applications protect you from dishonest images?
15. Can an image harm your mobile device?

RESULTS AND DISCUSSION

After having sent the images with hidden information in them to the messaging applications WhatsApp and Facebook Messenger, the two tools mentioned above were used to decode the text. The result was observed that in the WhatsApp messaging application the images were received perfectly, but at the time of decoding the message, none was detected unlike Facebook Messenger the decoded message could be observed.

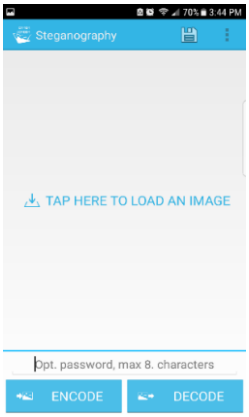


Figure 4
Steganography Tool

These tests give us a little knowledge of how both messaging applications are managing security through their tools. We see how WhatsApp can identify the images with hidden messages and perform some type of conversion in the image that returns it to its origin state unlike Facebook Messenger that received as it has been sent. Another situation that was observed in the WhatsApp application was that, if the same image that went through the Steganography process is sent more than twice, the application does not allow to send the image. Below is the illustration of each steps that has been worked with their results:

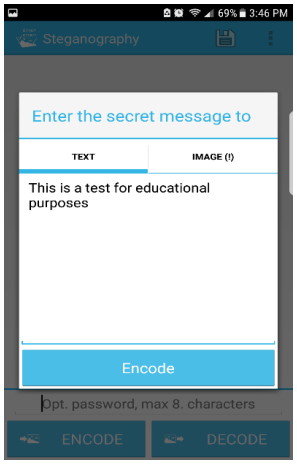


Figure 5
Steganography Tool Encode Message

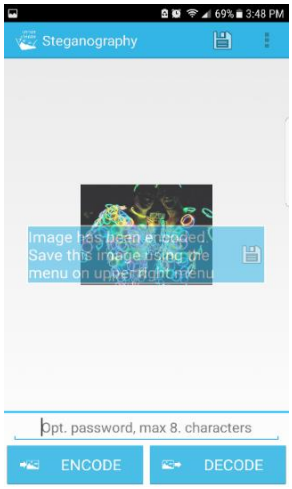


Figure 6
Steganography Tool

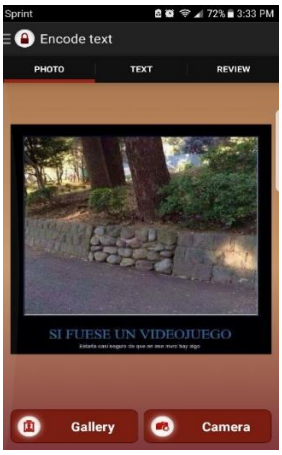


Figure 7
Steganography Master Tool

Figure 8
Steganography Master Tool Encode Message

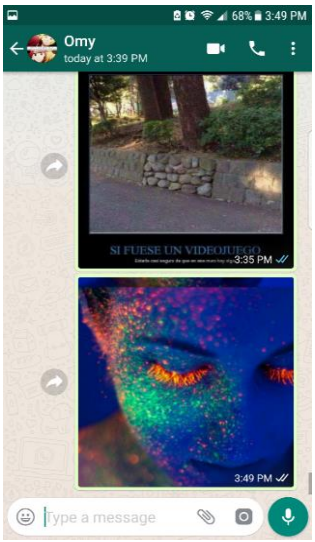


Figure 9
Sending Message WhatsApp

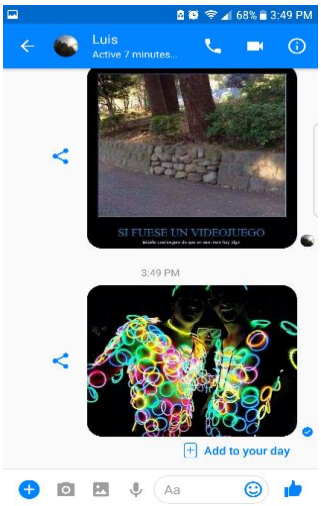


Figure 10
Sending Message Facebook Messenger

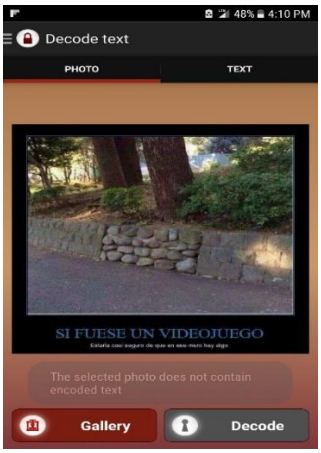


Figure 11
Decode Message from WhatsApp Image on Steganography Master

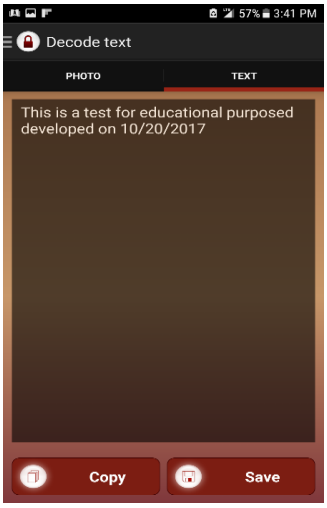


Figure 12
Decode Message from Facebook Messenger Image on Steganography Master

Figure 13
Decode Message from WhatsApp Image on Steganography

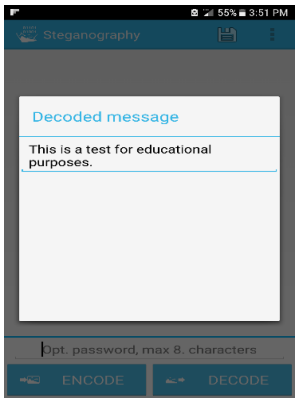


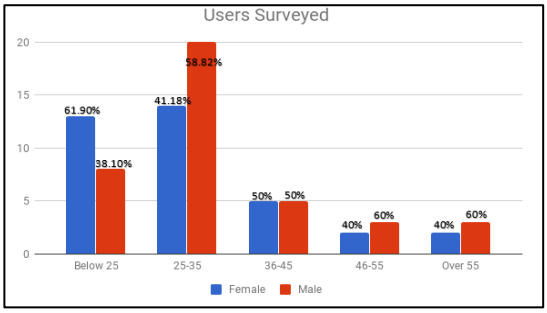
Figure 14
Decode Message from Facebook Messenger Image on Steganography

After tabulating the data collected in the interviews, the following data was obtained:

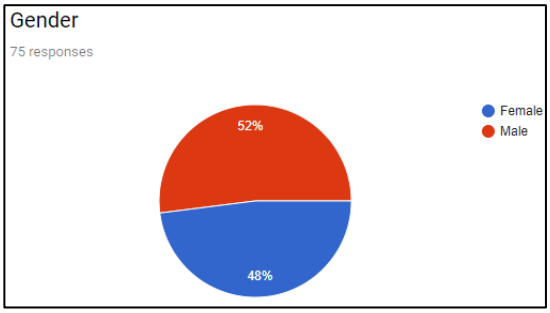
a. The people interviewed were divided in the following way with reference to their age and gender:

Table 1
Number of People Interviewed by Age and Gender

	Below 25	25-35	36-45	46-55	Over 55
Female	13	14	5	2	2
Male	8	20	5	3	3



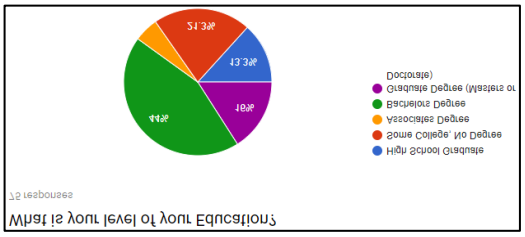
Graph 1
Users Surveyed Percentage



Graph 2
Users Gender Surveyed Percentage

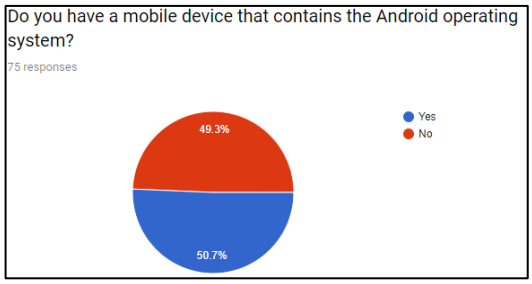
The data tells us that 52% of those interviewed were men and the rest were female. It also lets us see that, of the men interviewed, 58.2% are between the ages of 25-35 years while the largest group in the females is between the ages of below 25 years.

b. The data of the third question shows us that 44% of the people interviewed indicated that their level of education is Bachelor's Degree and the rest is divided between Some College, No Degree, Associates Degree, High School and Graduate Degree.



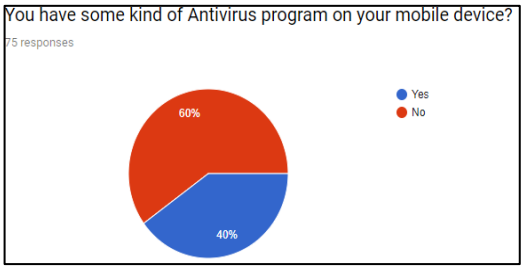
Graph 3
Users Level Educational Surveyed Percentage

c. The data of the fourth question shows us that 50.7% of the people interviewed indicated that their mobile device contains the Android operating system.



Graph 4
Users Mobile Operating System

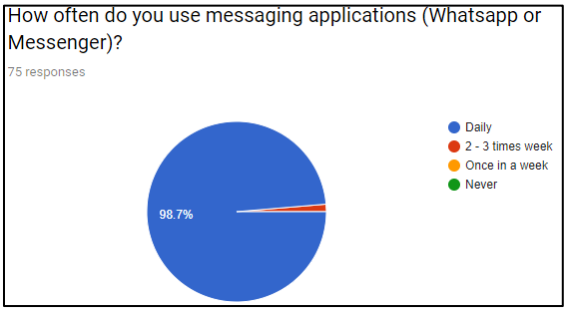
d. The results of the fifth question were the following:



Graph 5
Users with Antivirus Mobile Devices

As can be seen in the graph, 60% of respondents indicated that their mobile devices do not have an Antivirus program.

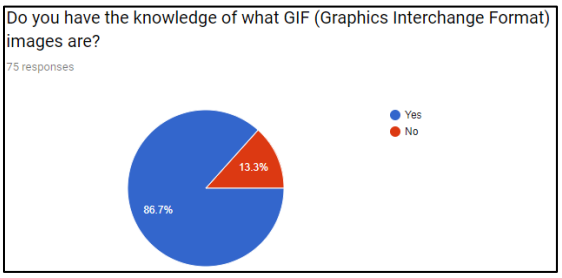
e. The results of the sixth question were the following:



Graph 6
Users using Messaging Applications

As can be seen in the graph, 98.7% of the respondents indicated that they use the WhatsApp or Facebook Messenger messaging applications daily.

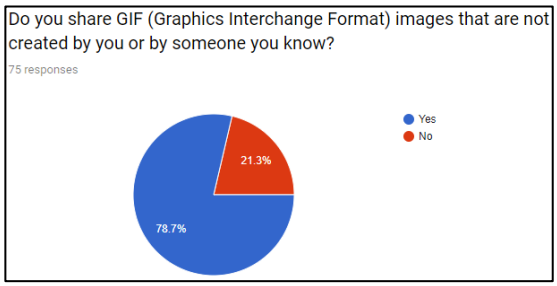
f. The results of the seventh question were the following:



Graph 7
User's GIF Knowledge Survey Percentage

As can be seen in the graph, 86.7% of respondents indicated that they have knowledge of what GIF images are.

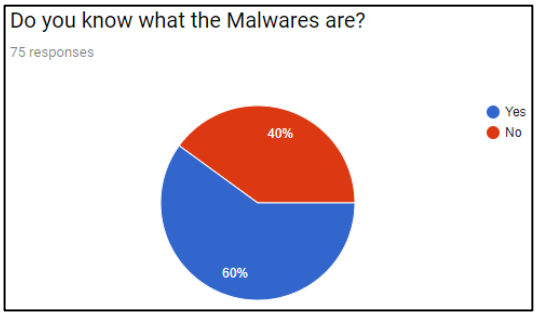
g. The results of the eighth question were the following:



Graph 8
Users Sharing GIF in Percentage

As can be seen in the graph, 78.7% of respondents indicated that they share GIF images that belong to third parties.

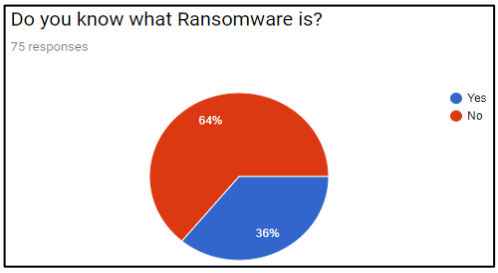
h. The results of the ninth question were the following:



Graph 9
User's Malware Knowledge Survey Percentage

As you can see in the graph, 60% of the respondents indicated that they have knowledge of what the Malwares are.

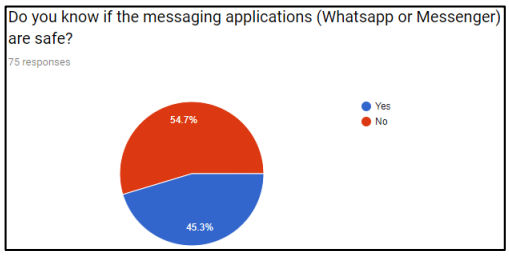
i. The results of the tenth question were the following:



Graph 10
User's Ransomware Knowledge Survey Percentage

As can be seen in the graph, 64% of respondents indicated that they have no knowledge of what infections with Ransomware are.

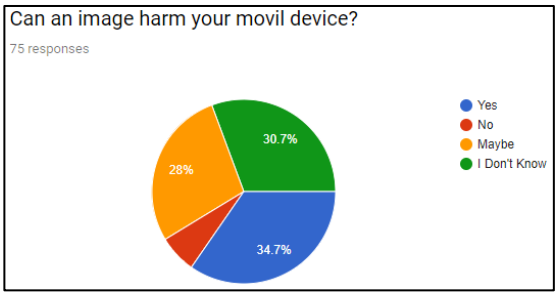
j. The results of the eleventh question were the following:



Graph 11
User's Safe Messaging Applications (WhatsApp or Facebook Messenger)

As can be seen in the graph, 54.7% of respondents indicated that none of the messaging applications (WhatsApp or Facebook Messenger) are safe.

k. The results of the twelfth question were the following:

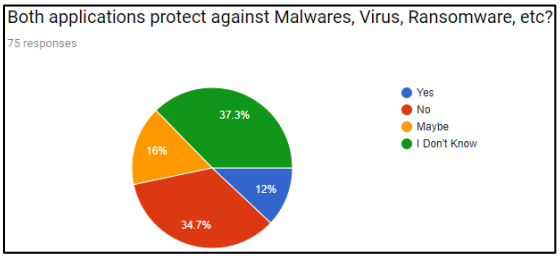


Graph 12
User's Harm Image Mobile Device

As can be seen in the graph, for this question three answers were obtained with quite similar percentages. The majority of respondents with 34.7% indicated that an image could damage a mobile phone. While 30.7% indicated that they were not aware if an image could damage their mobile device and 28% indicated that it could be possible.

The following questions are based on different scenarios to know users' knowledge about the security of WhatsApp and Facebook Messenger messaging applications.

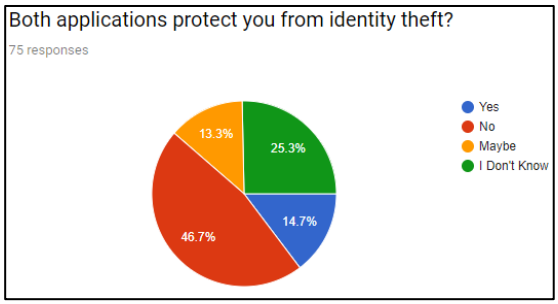
l. The results of the thirteenth question were the following:



Graph 13
Application Protect against Malwares, Virus, Ransomware, etc.

As can be seen in the graph, for this question two answers were obtained with quite similar percentages. The majority of the respondents with 37.3% indicated that they did not know if the messaging applications WhatsApp and Facebook Messenger protected their mobile devices from Malwares, Viruses, Ransomware, etc. While 34.7% said that these applications do not protect their mobile devices.

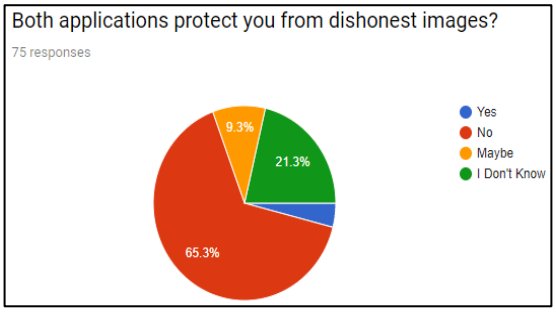
m. The results of the fourteenth question were the following:



Graph 14
Application Protect against Identity Theft

As can be seen in the graph, 46.7% of respondents indicated that none of the messaging applications (WhatsApp or Facebook Messenger) protect against identity theft.

n. The results of the fifteenth question were the following:



Graph 15
Application Protect against Dishonest Images

As can be seen in the graph, 65.3% of respondents indicated that none of the messaging applications (WhatsApp or Facebook Messenger) protect against dishonest images.

Based on all the results obtained, we can see that most of the respondents have mobile devices with Android operating systems. Which most do not contain Antivirus programs. Additionally, we observe that most people have knowledge about what Malwares, GIF, etc. are. With this survey we realize the importance of continuing to guide people

on the different dangers that occur every day on mobile devices.

CONCLUSION

In this work we have been able to observe the importance of messaging applications in mobile devices especially WhatsApp and Facebook Messenger since they are one of the most used worldwide. Therefore, we must keep in mind the importance of security in each of the messaging applications because if we successfully send an image with a hidden message through one of the most important and used applications worldwide, imaging what will happen if an attack occurs with a GIF image with a executable file without having an application installed in the receiver?

For reasons of time, the section of the GIF format with the executable file could not be completed to carry out the security tests in the applications. Hopefully this research will continue to be able to help all the companies that works in communication to continue innovating in their cybersecurity departments.

FUTURE WORK

For future work we will be continuing with the development of the GIF format with the executable file to continue performing security tests in all social network applications.

On the other hand, if we find any vulnerability in any operating system or any application related to GIF images, we want to help these companies to improve their security systems or be able to generate some kind of program that can detect this type of GIF images with malicious codes.

ACKNOWLEDGEMENTS

I would like to acknowledge all the users that contributed on the survey and to Dr. Jeffrey Duffany with his guidance during the project.

REFERENCES

[1] R. Gomez and G. Ramirez. (2015, February 19). *Using Digital Images to spread Executable Code on Internet* [Online]. Available: https://www.researchgate.net/publication/221221682_Using_Digital_Images_to_spread_Executable_Code_on_Internet.

[2] K. Rabah, "Steganography - The Art of Hiding Data," in *Information Technology Journal*, vol. 3, no. 3, Jan. 2004, pp. 245–269.

[3] R. Reddy and R. Ramani, "The Process of Encoding and Decoding of Image Steganography using LSB Algorithm," in *IJCSET*, vol. 2, no. 11, November 2012, pp. 1488-1492.

[4] J. Murray and W. VanRyper. (2006, October 4). "Sustainability of Digital Formats: Planning for Library of Congress Collections," in *GIF Graphics Interchange Format, Version 89a* [Online]. Available: https://www.loc.gov/preservation/digital/formats/fdd/fdd000133.shtml.

[5] E. Elgabar and F. Mohammed. (2013, December). *JPEG versus GIF Images in forms of LSB Steganography* [Online]. Available: http://ijcsn.org/articles/0206/JPEG-versus-GIF-Images-in-forms-of-LSB-Steganography.html. [Accessed: December 11, 2017].