ISSN 2349-0292
Impact Factor 2.365
GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

WHATSAPP FORENSICS AND ITS CHALLENGES FOR ANDROID SMARTPHONE

Mansur Zakariyya Shuaibu*, Alhassan Bala
* M.Sc. Students, CSE Department, Jodhpur National University, Jodhpur, India
M.Sc. Students, CSE Department, Jodhpur National University, Jodhpur, India

ABSTRACT
WhatsApp forensics has become an important area for legal issues due to its popularity and being number one social networking application among others and the increase in number of crimes that was committed using these applications. Like others it offers important opportunities and challenges in the world forensic. However, Forensic examiners are facing many difficulties during their investigation due to the high security measures WhatsApp Inc. took in order to protect the user data from unauthorized access. Our research will provide a comprehensive information about WhatsApp Application and the security issues regarding WhatsApp application. Our research will also give an outline on how Forensic examiners extract useful information from WhatsApp backup data on Android Smartphone.

KEYWORDS: WhatsApp Application, Android Smartphone, Forensic, Rooting, Encryption.

INTRODUCTION
According to Wikipedia **"WhatsApp Messenger** is an American proprietary cross-platform instant messaging client for smartphones. It uses the Internet to send text messages, documents, images, video, user location and audio media messages to other users using standard cellular mobile numbers. As of February 2016, WhatsApp had a user base of one billion, making it the most popular messaging application. **WhatsApp Inc.**, based in Mountain View, California, United States, was acquired by Facebook Inc. on February 19, 2014, for approximately US$19.3 billion [1]. Android smartphone forensics has evolved over time offering significant opportunities and exciting challenges. On one hand, being an open source platform Android is giving developers the freedom to contribute to the rapid growth of the Android market whereas on the other hand Android users may not be aware of the security and privacy implications of installing these applications on their phones. Users may assume that a password-locked device protects their personal information, but applications may retain private information on devices, in ways that users might not expect. Earlier WhatsApp databases were stored in a non-encrypted plain text format making it very easy for hackers to exploit the database files and extract chat conversations from them. Considering this a serious vulnerability, security experts at WhatsApp implemented a security mechanism by encrypting the stored backup files using a strong encryption algorithm to prevent or restrict unauthorized access. From a forensic investigation perspective, WhatsApp may contact volumes of evidentiary data that could be used in the court as evidence. Therefore, it is highly crucial to have a methodology to be able to parse these encrypted databases in human readable format [2]. Many research was conducted on how to acquire the encrypted backup files store on the Android Smartphones and decrypt them to obtain stored backup conversations from a suspect Android device and parse them in human readable format for both rooted and non-rooted Android Smartphones. This research paper tries to study the WhatsApp Application and security challenges faced for securing the user backup file from unauthorized access.

Why WhatsApp Forensics?
WhatsApp is a cross platform application with versions available for Android, BlackBerry, iPhone and Symbian operating systems. It is a widely used and universal application. WhatsApp as an application is not phone dependent, like certain applications that are only supported by certain phones e.g. Motoblur intended for specific Motorola phones. WhatsApp is not carrier dependent, like certain applications supported only by certain service providers, e.g. The 'Verizon Cloud' application that is intended only for users with Verizon Wireless phone service. WhatsApp is not operating system dependent, like certain apps that can be installed only on certain platforms, e.g. Symbian or iOS specific applications. WhatsApp is not factory installed (inbuilt-in). [3]

Global Market Scenario
According to a survey conducted by On Device Research, they surveyed 10,000 smartphone owners in 5 countries to get a global snapshot of popularity of particular apps but also how people use social messaging compared to calling, texting and emailing on their phones. The countries covered were the US, India, Brazil, South Africa, and China. [4]

ISSN 2349-0292
Impact Factor 2.365

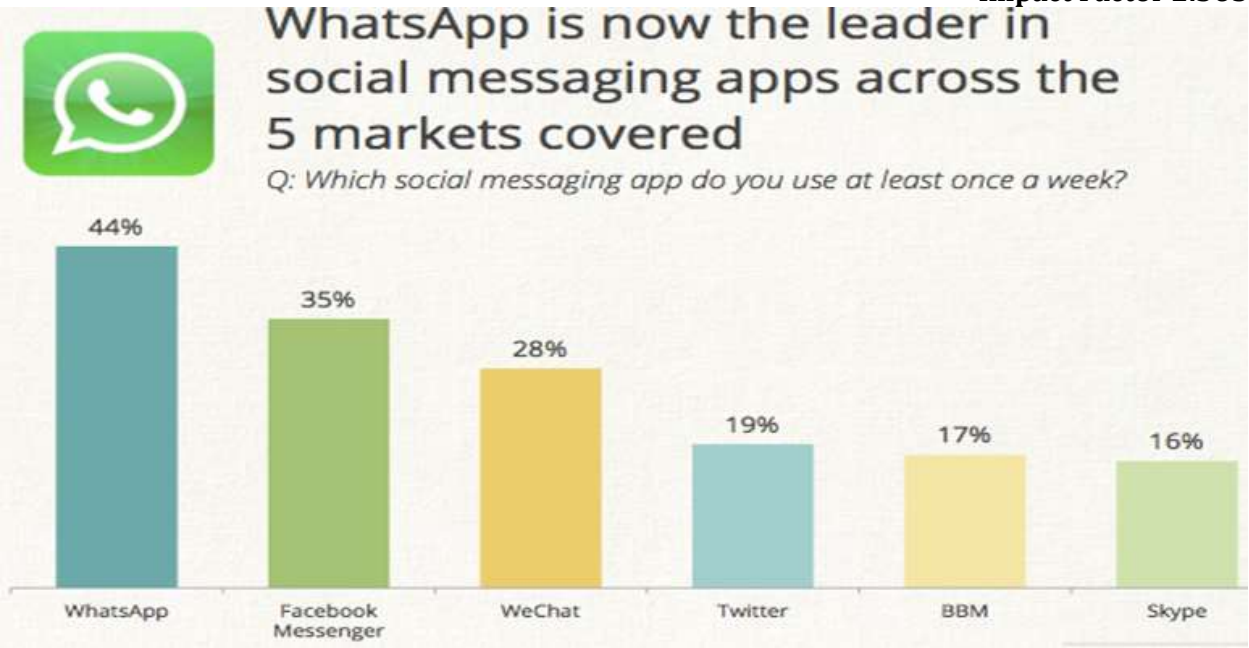

Figure 1: global snapshot of popularity among 5 social networking apps

Through these various data security issues were identified in instant messaging applications on the Android and other Mobile platform which aid in forensic investigations.

WHATSAPP APPLICATION

WhatsApp allows to text messaging, send images, video, and audio media messages. The application is available for Android, Blackberry, iOS, Symbian (s60), and Windows phone. WhatsApp Inc. was founded in 2009 by Brian Acton and Jan Koum, both veterans of Yahoo! People are exchanging information like images, videos, activities and events. But despite of getting connected with friends for more and more time, their privacy is also getting more vulnerable to threats by hackers and cyber criminals. There is no restriction on the length and number of messages one can exchange and no carrier fees apply. One does not need to install a sim-card to use WhatsApp; the only requirements are a supported phone, internet connection and storage space on the phone to download the application. WhatsApp uses a customized version of the open standard Extensible Messaging and Presence Protocol (XMPP). After WhatsApp is installed in any mobile, it creates a user account using the phone number as the username (ID: phone number@s.whatsapp.net). WhatsApp automatically synchronizes all the phone numbers from user's phonebook with its centralized database of WhatsApp users to add contacts to the user's WhatsApp contact list. Previously, WhatsApp messages were not encrypted, that means data which was sent and received was in plaintext, meaning messages could easily be read easily if packet traces were available. [5]

WhatsApp Application Now and Before

WhatsApp data is stored in the Internal Memory of the mobile phone. After it is installed, it automatically synchronizes with the phone's contacts showing users who are already using WhatsApp. When a mobile with WhatsApp installed is turned on, "*com.whatsapp*" process receives a signal to start the '*ExternalMediaManage*' and '*MessageService*' services which runs in the phone's background till the phone is turned on.

Before

With the starting version of WhatsApp 2.9 the messages exchanged was stored in 'msgstore.db' which is SQLite databases. But in early versions security researchers found that the chat records which was handled by WhatsApp was vulnerable, because the database file which saves the chat conversations was not encrypted and can easily accessible through many ways to get the whole conversation chat details including images, videos, contacts and so on. As this news hits the internet, security researchers started researching with WhatsApp database (msgstore.db) to retrieve the conversation even the deleted ones from the chat option. But WhatsApp reacted soon and came up with an encryption mechanism to protect its database.

Now

- Now, according to officials of WhatsApp they are taking the conversation database security in a very serious manner, now WhatsApp database encryption having custom AES encryption algorithm with above 192-bit encryption key mainly used for WhatsApp Android Platform. So now the previous file *msgstore.db* is converted to *msgstore.db.crypt*, *msgstore.db.crypt*5, *msgstore.db.crypt*7, and finally *msgstore.db.crypt*8 which is encrypted by AES algorithm with 256-bit key. [5]

WhatsApp Encryption: (The Most Secure Instant Messenger)
WhatsApp is easily the most widely-used instant messaging service for Smartphones and Tablets. Founded in 2009, the service has now exploded to more than 700 million active users – almost 250 million more than the second-placed alternative, China's WeChat. Since being acquired by Facebook for an eye-watering $19 billion, the firm has been forced to clean up its approach to security and privacy, which resulted in the news last year that it has introduced new encryption measures. [6]

What was the Problem?
WhatsApp had suffered countless embarrassments and exposures over their poor security. The problems started as long ago as May 2011, when a security flaw was discovered that allowed users' accounts to have their session hijacked (gaining unauthorized access to information by exploiting a valid usage session), and have their traffic intercepted and logged by a package sniffer. A new version of the app was released, but data continued to be sent and received in plaintext. Their difficulties continued into 2012. At the start of the year a hacker published WhatsAppStatus.net, which allowed people to change the status of any user of WhatsApp, and the developers of the app were slow to respond – initially claiming the flaw had been fixed when in reality they had merely blocked the website's IP address. Unsurprisingly, similar tools soon popped up, and the firm was forced to respond in a more robust way. By the late spring, WhatsApp finally stopped using plaintext for data, but its replacement a cryptographic method was widely criticized for being broken at launch.

In late 2013 a security researcher in The Netherlands claimed anyone with enough technical knowledge could decrypt communications sent within the app thanks to several "long documented weaknesses" – mainly the fact WhatsApp used the same encryption key on both sides of a conversation. Thijs Alkemade, the student at the University of Utrecht who discovered the flaw, said *"You should assume that anyone who is able to eavesdrop on your WhatsApp connection is capable of decrypting your messages, given enough effort ".* Adding, *"There is nothing a WhatsApp user can do about this… except to stop using it until the developers can update it ".* As recently as November 2014, WhatsApp scored a mere two out of seven on the Electronic Frontier Foundation's secure messaging scorecard – losing points thanks the fact it used an encryption which the provider had the key for, there was no way to verify a user's identity, and its security design was not well-documented. [6]

What was the Response?
On the 18th November last year, WhatsApp's new owners Facebook decided enough was enough. Although Facebook isn't exactly well-regarded in terms of its own transparency about privacy and security, they didn't want to jeopardize their expensive new acquisition and risk losing users to a rival service such as Viber or Tango. As a result, they announced a new partnership with Open Whisper Systems in a deal that would finally bring end-to-end encryption to the service, hopefully banishing the gremlins of the previous three years. Open Whisper said the new encryption would be the largest of its kind anywhere in the world, and would use Text-Secure a service which uses a cryptographic key that's unique to individual devices to protect its giant user base. Experts were quickly impressed, as Wired claimed the solution was *"practically uncrack able".* [6]

How Does It Work?
Instead of storing the keys for unscrambling the encryption on a centralized server that's owned and operated by the WhatsApp developers, end-to-end encryption works by instead only storing the keys on a user's device. When combined with Text Secure, which uses a protocol called "forward secrecy" to issue a fresh key for every new message, it's easy to see why WhatsApp's CEO Jan Koum claimed they had *"now built WhatsApp around the goal of knowing as little about you as possible… Respect for your privacy is coded into our DNA".*

The encryption now used by the service differs hugely from that used by similar instant messaging apps and social networks, who mostly still store the keys on their own servers as well as a person's device. This means companies and governments can access the contents of your messages and data on demand, as well making it easier for hackers to

gain access to private and personal information. In fact, the move by WhatsApp is part of a larger movement towards increased privacy by leading tech firms, though not everyone is happy. When Apple and Google both expanded their encryption services in the run up to the WhatsApp announcement, FBI Director James Comey criticised the move. [6]

Are All the Problems Fixed?

Providing effective security isn't easy. While WhatsApp were clearly a long way behind the game at the turn of the decade, the late 2014 update sounds entirely hacker-proof. Sadly, that's rarely the case, and in recent days more negative press has emerged for the Mountain View-based firm. Although the contents of a user's message seemingly remain secure, a simple piece of software has been released that can be used by hackers to circumnavigate various privacy settings – thus giving them a way to see whether a user is online or offline, a way to monitor a person's profile picture, a way to see a user's status, and the ability to see someone's personalized privacy settings. The software, called WhatsSpy Public, has been created by a Dutch developer and can reveal the timeline of a tracked-user's online status, even if the user has the strictest privacy controls enabled. *"You may think now you've set all options to 'nobody' you are safe, privacy-wise, but nevertheless I can still track your moves on WhatsApp"* said the software's designer Maikel Zweerink. The good news for users is that the software is hard to set up, and will only be able to track users on rooted Androids or jail-broken iPhones so if you use a "vanilla" OS you should be ok. WhatsApp have not yet responded to the allegations officially, though an insider moves to play down the breach when he told the UK media that *"This is not a hack… in essence he built a program that just records and monitors information he has access to anyway ".*

Despite that, given WhatsApp's poor track record its users are unlikely to take much solace in the statement. Whatever the truth may be, the issue simply points to the overriding fact that security in a digital age can never be taken for granted; even when you think you're protected you can be certain there is a hacker or criminal looking for the next bug or flaw with which to compromise you. [6]

ROOTING ANDROID SMARTPHONES DURING FORENSIC INVESTIGATION

The Android Smartphone that you have learned to love and enjoy is running an operating system that was designed for commercial and private use. Like most any operating system, several features have been disabled, either for future use or to prevent the casual user from causing permanent damage to the operating system. "Rooting" is the process in which the limitations are removed and full access is allowed. Once rooted, the Android phone owner will have more control over many settings, features and performance of their phone [7]. Basically, *"rooting" means to get to the root of the operating system and to have the ability to make global changes.*

- 90% of forensics trick depends on the root?
- Not enabled even in a single device.
- Not possible on all devices without altering the evidence.
- Gaining root will leave a lot of traces.
- Many data's they get altered.
- Takes lot of time searching for the correct exploits.
- Root could make the device more vulnerable for future exploits.

Types of rooting:

Temporary root: -

- Temp root gives you root access till you reboot the device.
- Temp root is something essential when it comes to forensic (z4root.apk).
- Doesn't work on all devices, test it first before using.

Permanent root: -

- not good as far as forensic is concerned.
- Leaves a huge footprint altering the evidence.

ISSN 2349-0292
Impact Factor 2.365

Figure 2: Snapshot of Z4root Application

HOW TO PERFORM FORENSICS ANALYSIS ON WHATSAPP DATA USING ANDROID SMARTPHONE?

Tools:

1) WhatsApp Application
2) Android Smartphone
3) Computer System
4) WhatsApp-Crypt-DB Converter
5) WhatsApp extract + Python
6) USB Cable (for Data Transfer)

Methodology

Locating WhatsApp Database files

- The first step to perform acquisition of WhatsApp database file is by connecting the Android device to the Computer System using the corresponding data cable.
- Browse to the folder named WhatsApp and then browse in a folder named Databases.
- Displayed below are the lists of encrypted database backups which are present on the Android Smartphone.

msgstore.db.crypt8	3/30/2016 2:00 AM	CRYPT8 File	6,734 KB
msgstore-2016-03-23.1.db.crypt8	3/22/2016 2:00 AM	CRYPT8 File	6,589 KB
msgstore-2016-03-24.1.db.crypt8	3/23/2016 2:00 AM	CRYPT8 File	6,612 KB
msgstore-2016-03-25.1.db.crypt8	3/24/2016 2:00 AM	CRYPT8 File	6,652 KB
msgstore-2016-03-26.1.db.crypt8	3/25/2016 2:00 AM	CRYPT8 File	6,663 KB
msgstore-2016-03-27.1.db.crypt8	3/26/2016 2:00 AM	CRYPT8 File	6,673 KB
msgstore-2016-03-28.1.db.crypt8	3/27/2016 2:00 AM	CRYPT8 File	6,708 KB
msgstore-2016-03-29.1.db.crypt8	3/28/2016 2:00 AM	CRYPT8 File	6,723 KB
msgstore-2016-03-30.1.db.crypt8	3/29/2016 2:00 AM	CRYPT8 File	6,729 KB

Figure 3: List of encrypted databases present in the memory.

Note: WhatsApp in its recent update stores database in crpyt8 format, so for decrypting database you need to convert crypt8 to crypt file. So first you have to convert crypt8 file to crypt using *WhatsApp-Crypt-DB Converter*.

Here are the procedures for converting Crypt8 files into Crypt files in Android Smartphones by using WhatsApp Crypt-DB Converter Application

- Open WhatsApp Crypt-DB Converter and Click on ***Convert cryptataba8/7/5 to database***.

ISSN 2349-0292
Impact Factor 2.365

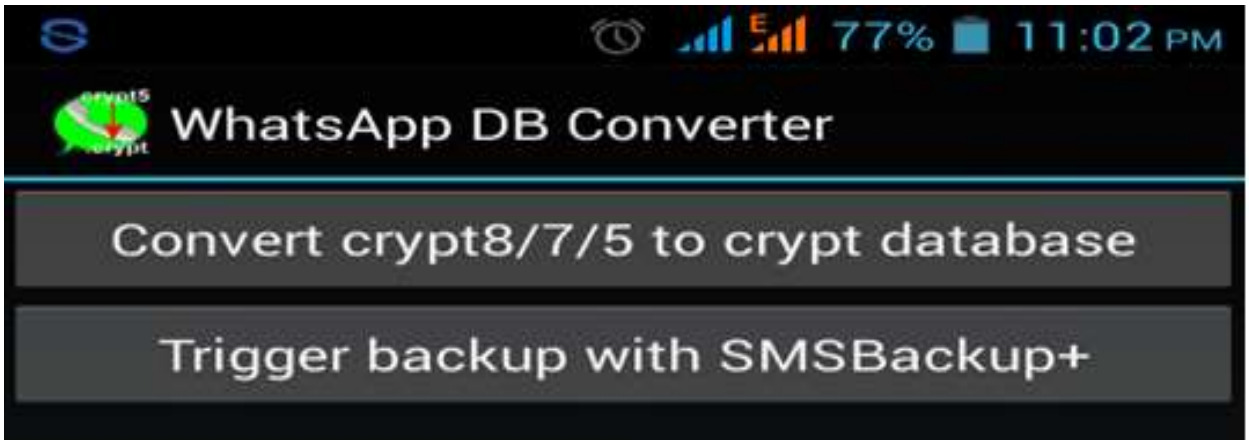

Figure 4: Snapshot of WhatsApp Crypt-DB Converter.

- Then transfer the WhatsApp databases in */sdcard/whatsapp/Databases* files from your mobile device to PC using USB cable.
- First, make a folder in your PC i.e. Backup chat. And Copy and paste the backup database into the Backup Chat Folder.

Since these backup databases are encrypted and cannot be viewed directly, we require a software package WhatsApp Xtract Tool [8] and Python that decrypt the database files in order to be displayed in human readable format.

Performing the decryption

- Step 1: Download WhatsApp Xtract package on your computer and extract it.
- Step 2: Download and install Python programming language environment on your computer.
- Step 3: Open the folder where you downloaded the What Sapp Xtract archive. Find a file with name *!install pyCrypto.bat*, right click on it and click run as administrator. This bat file will execute the following Python command, *pypm install pycrypto*. This common automatically installs the pycrypto library on your compter, which will be used to decrypt the WhatAapp backup data.

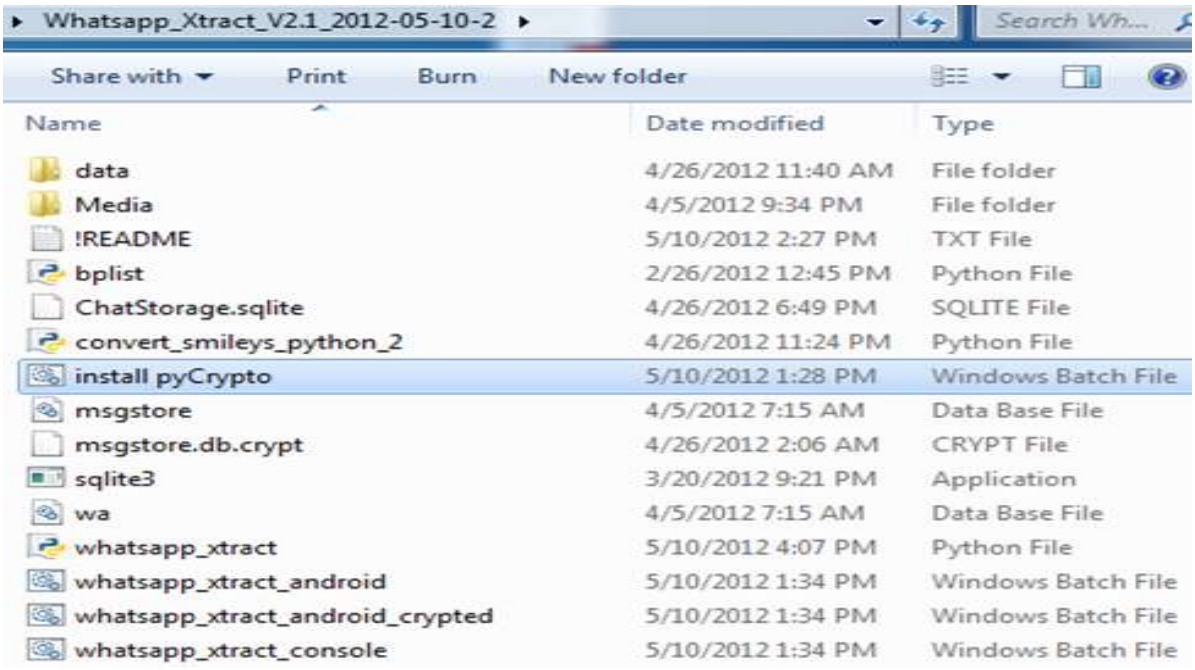

Figure 5: Locating !install pyCrypto.bat file.

ISSN 2349-0292
Impact Factor 2.365

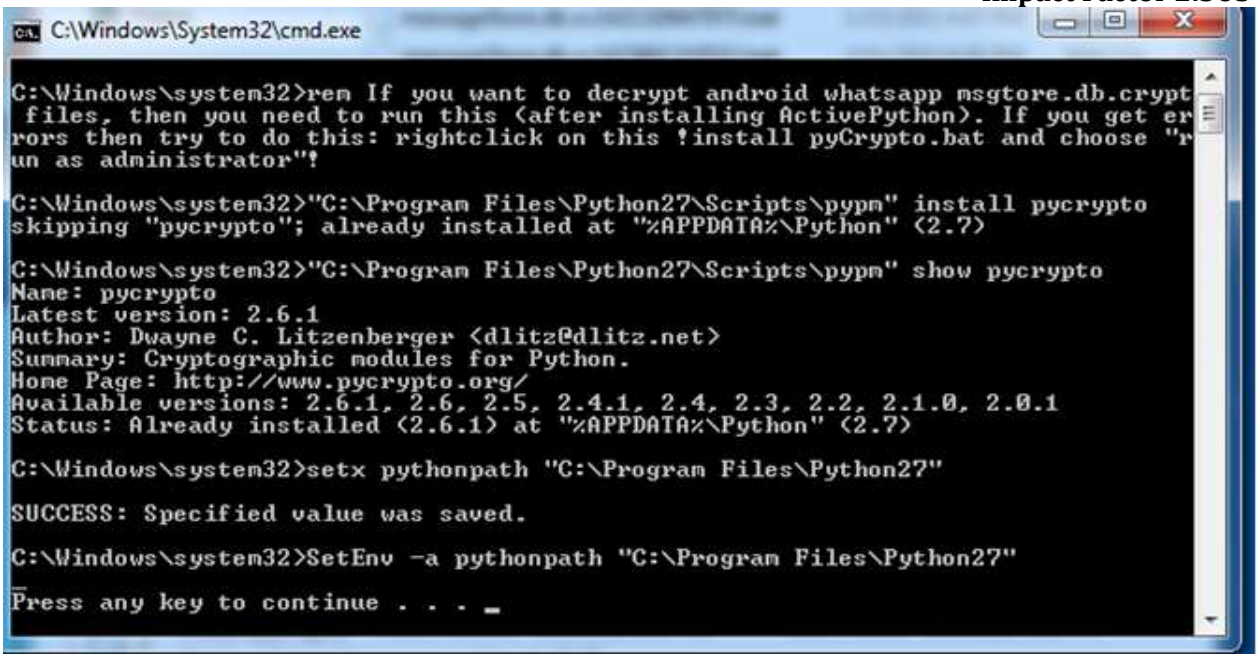

Figure 6: Snapshot of Successful installation of !install pyCrypto.bat file.

- Step 4: In the same folder, run whatsapp_xtract_android.bat. To run any of these files, simply right click on it and click run as administrator.
- Step 5: As soon as the execution of the bat file or command is completed, all your WhatsApp backup data will be decrypted and displayed in the default browser on your computer system.

CHALLENGES

- ✓ The major challenge for any forensic examiner is the frequent updating of encryption standards that WhatsApp uses to protect these backups from unauthorized access.
- ✓ Now, WhatsApp database encryption having custom AES encryption algorithm with 256-bit encryption key mainly used for WhatsApp Android Platform which is hardly to break.
- ✓ Therefore, it is highly important for forensic investigators to keep themselves updated with the changes in technology pertaining WhatsApp backup databases in order to be able to extract pieces of chat conversations that may be present on suspect device.
- ✓ Another challenge is that WhatsApp has added end-to-end encryption to all of its messages – meaning that the company couldn't give information to governments, even if it required.
- ✓ Due to its strong encryption WhatsApp has already run into issues around encryption in Brazil, where a Facebook executive was arrested after WhatsApp failed to hand over user messages in court.

CONCLUSION

WhatsApp Application now is the leading Application among all other social networking Applications for which people use to exchange their personal and business information. In our research we discussed some important issues about WhatsApp Application and its security. We also mentioned some of the challenges regarding WhatsApp Forensics as well as the procedures on how to extract pieces of evidence on suspect Android Smartphone.

REFERENCES

[1] [Online]. Available: https://en.wikipedia.org/wiki/WhatsApp
[2] Gudipaty and Jhala. WhatsApp Forensics: Decryption of Encrypted WhatsApp Databases on Non Rooted Android Devices. J Inform Tech Softw Eng. 2015 Available at: http://dx.doi.org/10.4172/2165-7866.1000147.
[3] Thakur, Neha S., "Forensic Analysis of WhatsApp on Android Smartphones" (2013). *University of New Orleans Theses and Dissertations.* Paper 1706. Available at: http://scholarworks.uno.edu/td

[4] Sean Rodrigues, "A study about the current market scenario & the success factors for What Sapp", A Project Report, 2015.
[5] Mr. Shubham Sahu, An Analysis of WhatsApp Forensics in Android Smartphones, International Journal of Engineering Research ISSN:2319-6890 Volume No.3, Issue No.5, pp : 349-350 01 May 2014
[6] [Online]. Available at: http://www.makeuseof.com/tag/whatsapp-encryption-now-secure-instant-messenger/ visited on 14/03/2016.
[7] [Online]. Available: http://google.about.com/od/androidphonescat/qt/Why-Do-People-Root-Android-Phones.html.
[8] Zena Forensics "WhatsAppXtract_v2.1_2012-05-10-2" [Online]. Available at: http://code.google.com/p/hotoloti/downloads/list.