Computer Forensics: A Forensic Approach to Recover Encrypted Data from Digital Evidences

VibhutiNarayanSingh[1] Shalini[2]
[1]M.Sc. (Forensic Sci.) [2]Assistant Professor
[1,2]Department of Forensic Sci. & Criminology
[1]Bundelkhand University, Jhansi, U.P. [2]BabasahebBhimraoAmbedkar University, Lucknow, U.P.

Abstract— Nowadays use of computers, mobile phones and external storage devices gain popularity among the population for storing their private data. To ensure privacy of these files user uses encryption software's such as bit locker, true crypt etc. These software encrypt data, storage devices etc. and once the data is encrypted it is impossible to read these files without decryption key. In this research we demonstrate a methodology for decryption and extractions of bit by bit information stored in these types of files by using appropriate tools under forensically sound condition and also discussed a method for recovery of password from these files using hibernating files.

Key words: Encryption, Decryption, True Crypt, Bit locker

I. INTRODUCTION

Encryption is derived from a Greek word "Krytos" which means "secret" or "hidden". It is a technique in which there is translation or conversion of electric data using encryption algorithm and an encryption key into a particular form called cipher text, which can be accessed when it is decrypted by using key files. Encryption of data is achieved by using some tools which encrypt data or create a separate protected containers or drives by using an encryption algorithm and key. These tools keep encryption key in system memory and facilitate easy access of encrypted file to user with a valid encryption key. The encrypted file can only be viewed, accessed, explored or modified by the user who has valid password to open it. All the encryption tools give strong level of protection which creates trouble to forensic investigator during analysis of these files. So it is necessary for forensic analyst to choose an appropriate and validated tool for examine these type of files.

A. Decryption:

Decoding of encrypted file using cryptographic key is known as decryption. A diagram of encryption and decryption process is presented in figure: 1.

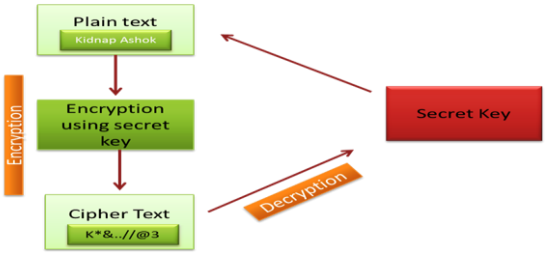

Fig. 1: Encryption and Decryption process

B. Type of Encryption:

Mainly two types of cryptographic algorithms are used i.e. Symmetric and Asymmetric key algorithms. But nowadays a new way of encryption is introduced named as Hybrid key algorithm. All the three types of key algorithm are presented in figure: 2 with their respective examples.

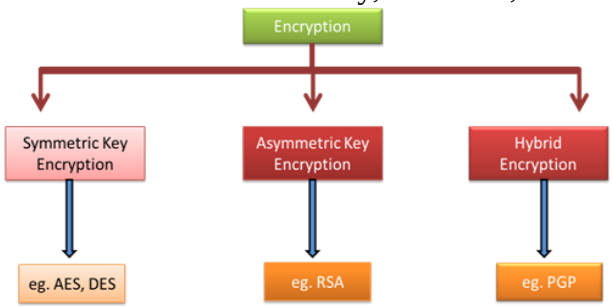

Fig. 2: Type of Encryption

1) Symmetric key algorithm:

It is also termed as Secret key cryptography. In this system cryptographic key is common for both encryption and decryption purpose. This encryption uses two cipher, one is Stream cipher and another is Block cipher. Process of symmetric key algorithm is shown below in figure: 3.

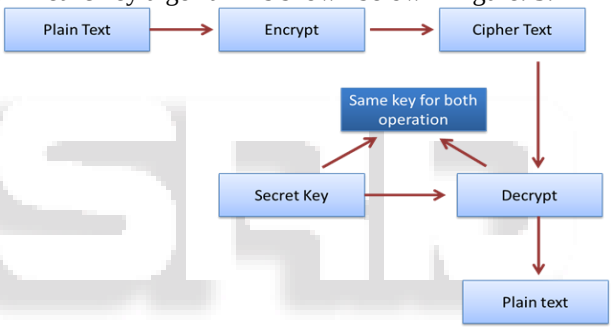

Fig. 3: Symmetric Key Algorithms

2) Asymmetric Key Algorithm:

It is also known as Public key cryptography. In this system two different cryptographic keys are used. One of which is private and another is public. Public key is used to encrypt plain text or verify the digital signature and it is shared with everyone, while private key is used to decrypt cipher text or create digital signature. This technique not only provides a new way for assuring the confidentiality of the electronic data but also maintains authenticity and integrity of these data through the use of digital signature. Process of Asymmetric key algorithm is shown below in figure: 4.

3) Hybrid key algorithm

In this encryption both symmetric and asymmetric key algorithms are used for encryption.

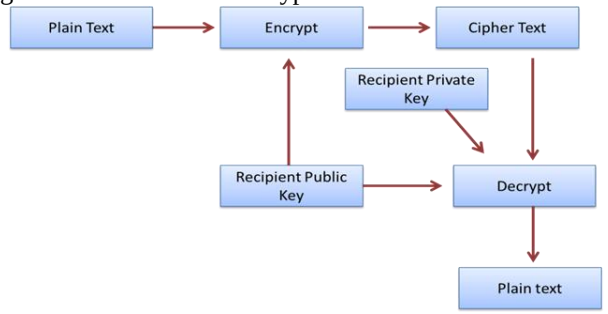

Fig. 4: Asymmetric Key Algorithms

C. Encrypted File Extension:

File extension is commonly a set of few characters separate from the main filename by a dot (.) added to the end of the filename. File extension give detailed explanation about the parent program from which these file are generated. Encrypted file extension vary according to the encryption software program. There are many encryption software and they are only identified on the basis of their file extension. Some of the file extensions are listed below in table: 1.

File extension	File type description	File extension	File type description
.crypt	Whatsapp messenger encrypted database backup file	.sef	Stegnous encrypted file
.crypt5	Whatsapp messenger encrypted database backup file	.afp	File protector encrypted file
.crypt6	Whatsapp messenger message database file	.ecr	Ecrypt encrypted file
.crypt7	Whatsapp messenger encrypted database backup file	.hid	Keysafe encrypted file
.crypt8	Whatsapp messenger message database file	.flkw	Folder lock encrypted file
. db.crypt7	Whatsapp messenger encrypted database backup file	.sdc	Microsoft secure archive cabinet file
.jpgens	Egis encrypted JPG file	.pwl	Microsoft window software file
.jpgx	Egis encrypted bitmap image file	.sdoc	Microsoft word sealed document file
.tc	True crypt disc volume file	.etxt	Encrypted text file
.bioexcess	My win locker protected file	.pst	Microsoft outlook personal folder
.cip	Crypto-buddy encrypted file	.mbs	Opera mail box
.hid2	Keep safe encrypted file	.asc	PGP signature file
.egisenc	Egis encrypted file	.gng	GNU privacy guard encrypted file
.flk	Folder lock encrypted file	.pgp	PGP encrypted file
.kdbx	Keypass password database file	.sig	GNU privacy guard signature file
.dcv	Drive crypt encrypted volume file	.jbc	Best crypt
.if	Software key license file		

Table 1: Encrypted file extension list

II. MATERIAL AND METHODOLOGY

Digital evidence such as computer hard disc, memory card, pen drive, and external hard disc has many type of electronic data in which some have forensic value. Here we proposed an authentic method for recovering data from encrypted files. For analysis of this kind of evidence a set of tools which is mentioned below is used.

A. Software:

- FTK imager
- Access Data Forensic Toolkit
- Passware Password Recovery Kit Forensic
- OSF mount

B. Hardware:

- Window 7 with core i3 processor, Write protector

C. Analysis:

Connect the hard disk to computer through write protector device and image of hard disk was created using FTK imager in (dd) format. Image was mounted by the same tool (Fig.5). Here a .doc file named as “manual” and a .pdf file named as “Essential_ of_Hindutva by Sawarkar” was found. These both files were encrypted. A true crypt volume named as “Imp”was also found. All these encrypted files were copied to analysis computer.

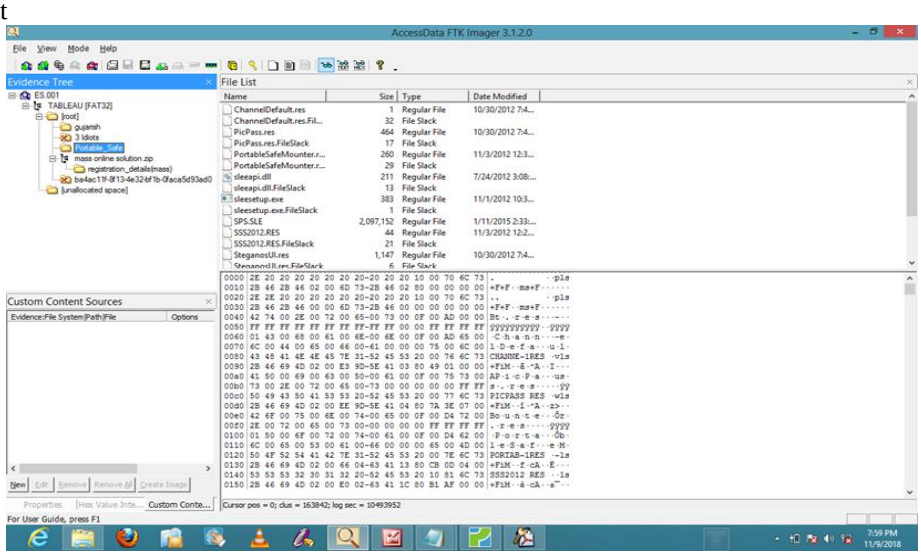

Fig. 5: Image of Hard disk

In next step this dd image was mounted using Access Data Forensic Toolkit for data carving (Fig.6). After carving one more encrypted file was found. It was also extracted for the analysis of computer.

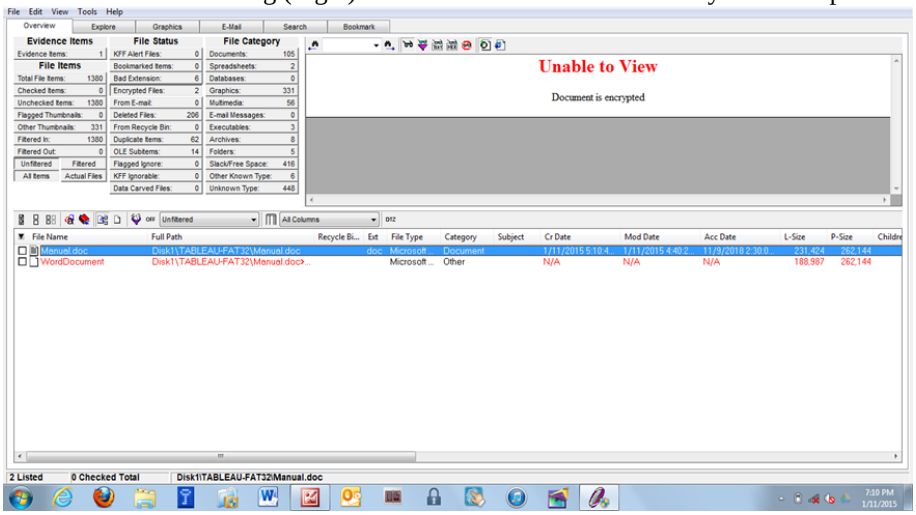

Fig. 6: Data Carving

D. Decryption of encrypted ".doc" and ".pdf" file:

The control of passware password recovery kit forensic are shown in figure: 7. Here 6 interfaces are present in this tool which recovered password of file, internet, window and hard disk and also scan password protected files present in the storage medium.

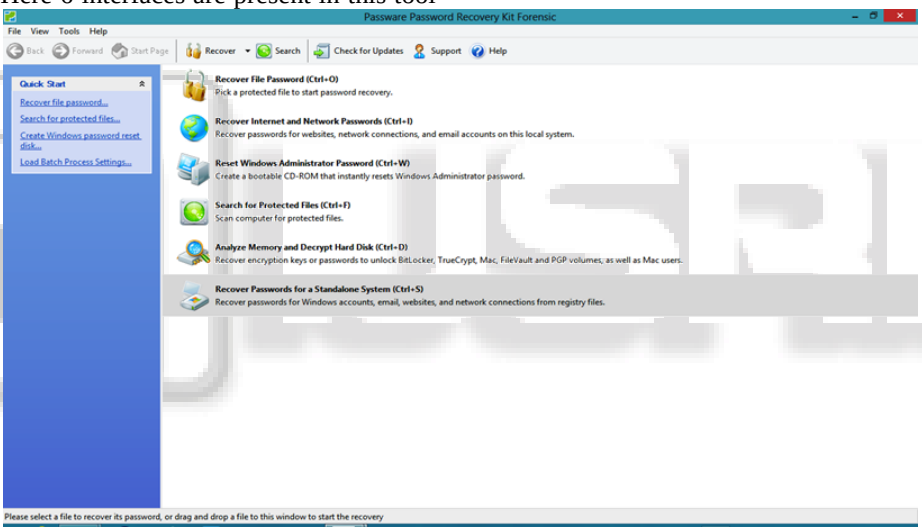

Fig. 7: Passware Password Recover Kit Forensic Interface

Both encrypted .doc and .pdf files were mounted respectively by clicking on recover file password interface and then run wizard for recovery of the password. Decryption took 0 sec for .doc (Fig.8) file and 15 min 26 sec for .pdf (fig.9) file.

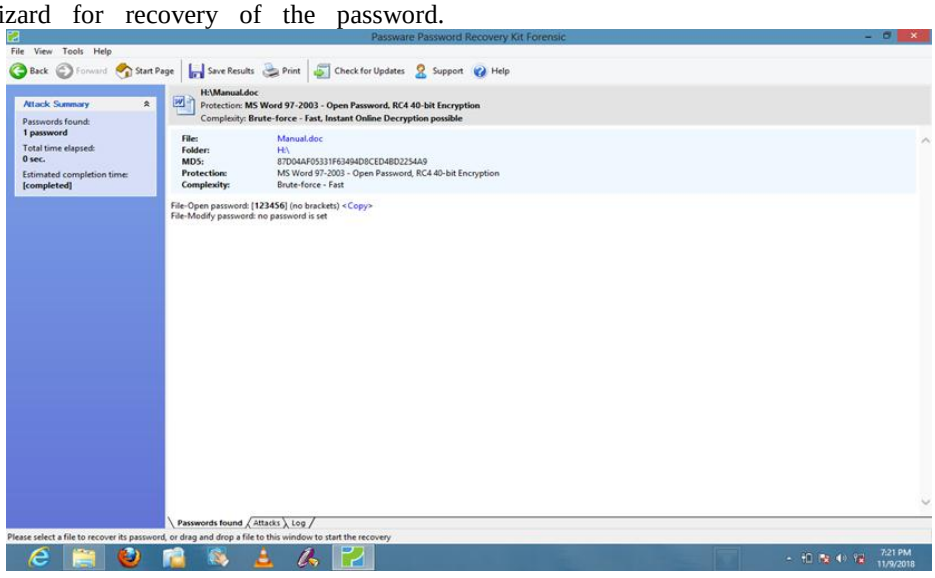

Fig. 7: Password recovery of .doc file

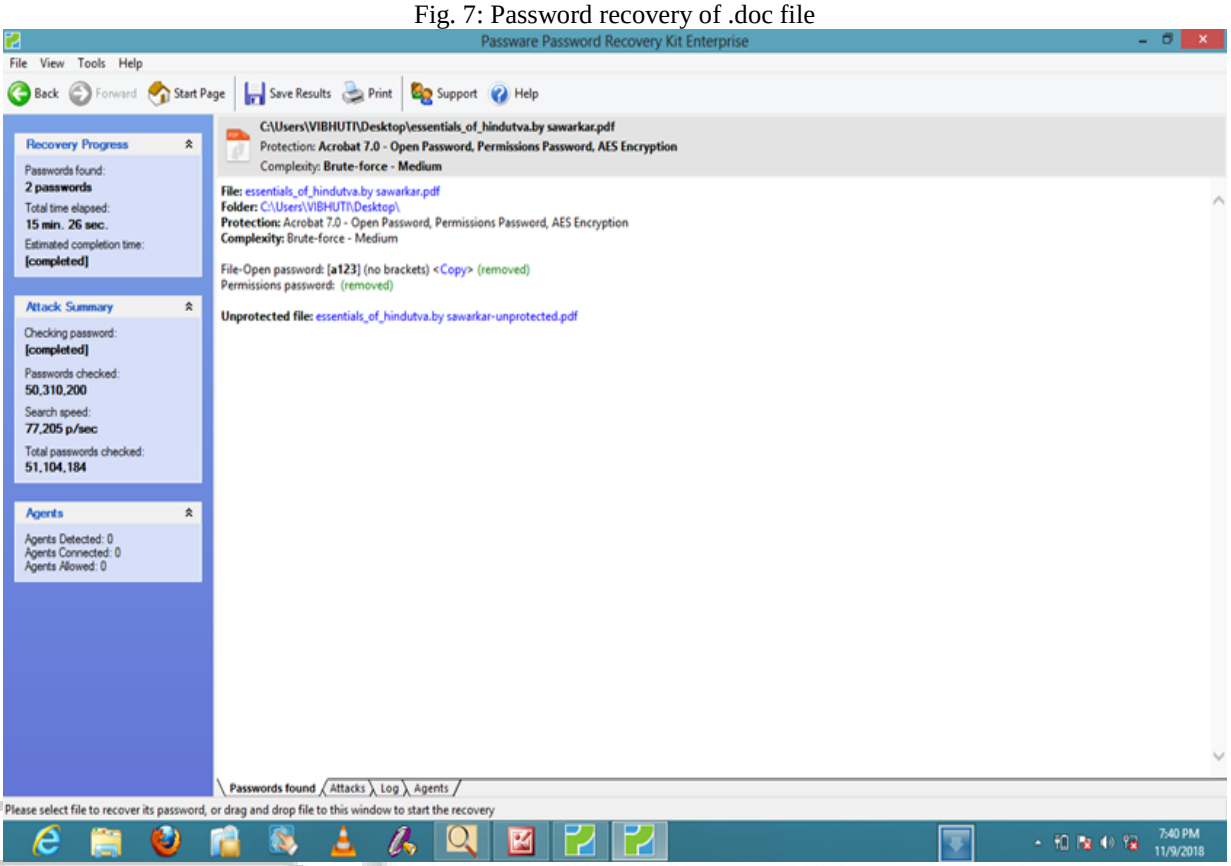

Fig. 8: Password recovery of .pdf file

1) Decryption of True crypt file:

Analyze memory and decrypt hard disk interface of passware password recovery kit forensic provide true crypt file mounting and password extraction facility (Fig 9). On clicking this interface it ask for path of the true crypt file. After giving path run wizard for password extraction. Encrypted true crypt file was successfully decrypted (Fig 10).

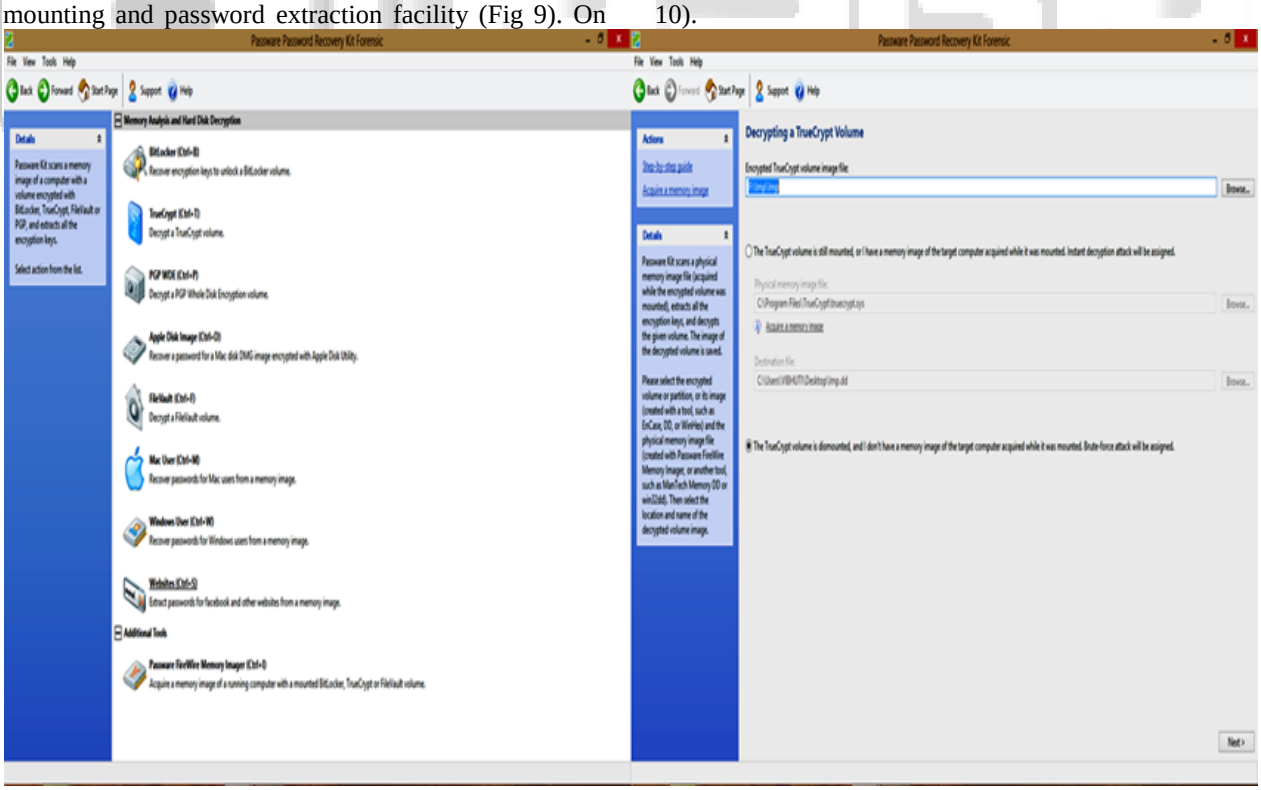

Fig. 9: True Crypt File Password Recovery Interface

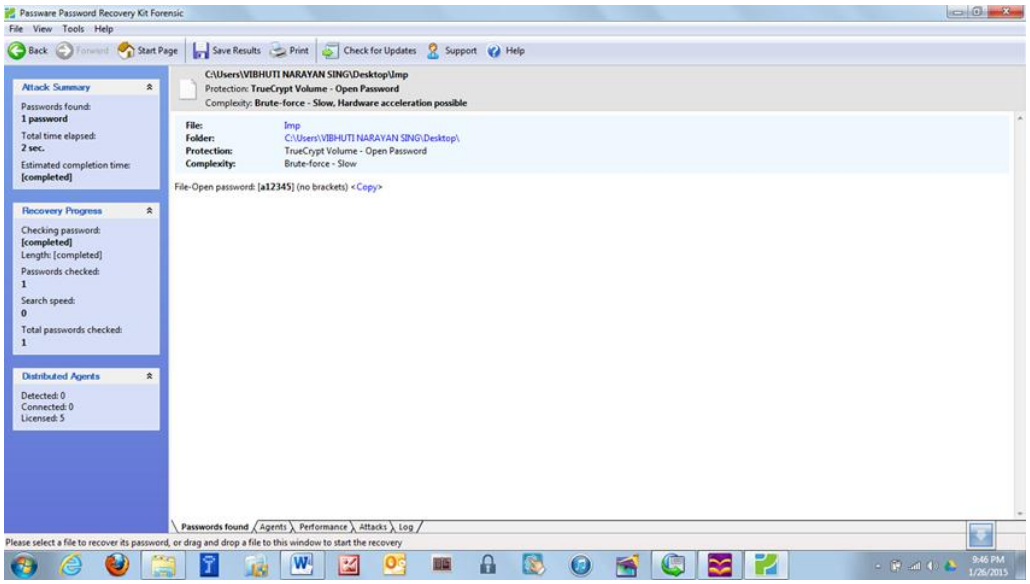

Fig. 10: True Crypt Password Recovery

2) Decryption of True crypt file using Hibernation file:

Sometime hibernation file was present in hard disk. This type of files plays an important role in decryption process. Hibernation file was copied from hard disk image to analysis computer. These files could be used directly or converted to the memory dump depend upon the decryption software requirement.

We mount the Imp true crypt file on passware password recovery kit forensic and provide the hyberfil.sys. Encrypted true crypt volume was successfully decrypted (Fig 11).

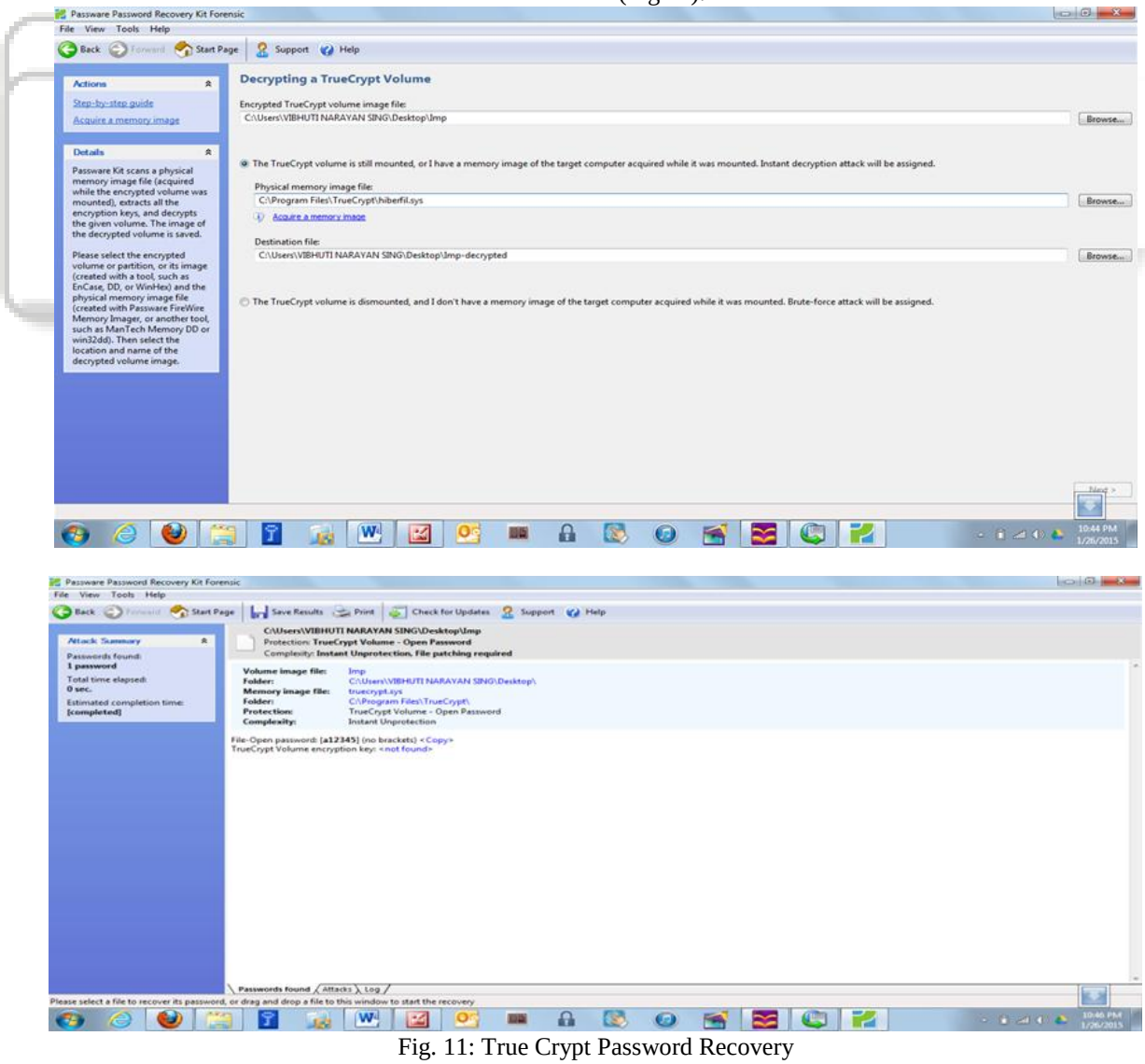

Fig. 11: True Crypt Password Recovery

III. CONCLUSION

If data on hard disks being analysed is encrypted than computer forensic analysis could results as an impossible task or could be difficult one. Tools for software encryption keeps the encryption keys in memory, and sometime the hibernated files might be saved in a disk by hibernation. There are many tools available from which we can decrypt the encrypted files directly or by using hibernation file. This process of decryption of the encryption storage is discussed in our research.

Still further researches should be done towards extraction of encryption key from memory traces in various files on hard disk or hibernation files. In future researches itis also needed to be seen if there is any possibility to prevent extraction of decryption keys from memory from the decrypted files those are available to users.

Hence, it is concluded that extraction of bit by bit information stored in the decrypted hard disk can be done by using appropriate tools under forensically sound conditions and also password recovery can be done using hibernation files. But still there is need to develop more accurate and sensitive forensic tools in the perspective of encryption for forensic investigators.

REFERENCES

[1] Eoghan Casey, "Practical Approaches to Recovering Encrypted Digital Evidence" international Journal of Digital Evidence, Fall 2002, Volume1, Issue 3
[2] Adedayo M. Balogun, Shao Ying Zhu, "Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.5, 2013
[3] Saravanan M, Mukesh Krishnan, "Forensic Recovery of Fully Encrypted Volume" International Journal of Computer Applications (0975 – 8887),Volume 91 – No.7, April 2014
[4] http://en.wikipedia.org/wiki/Encryption
[5] http://en.wikipedia.org/wiki/Encryption
[6] http://www.lostpassword.com/kit-forensic.htm
[7] http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk
[8] http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.2.0

