Cracking passwords

Technology

Introduction

A password is made of characters that are meant for user identification to gain access to a resource. It is used to prove the identity of a person that distinguishes one from others. The evidence is the accessible group of facts that show a belief is valid. Recovery is the act of trying to save data that cannot typically be accessed. Some procedures are used for evidence recovery by using forensic tools and hexadecimal editors.

Methods of evidence retrieval with forensic tools include verification. Verification is the step whereby the determination of the occurrence is done, and the best method for evidence identification and collection is done. Secondly, is system description that involves system operating outline, its configuration and where the evidence is located. The next step is the acquisition of proof whereby both volatile and non-volatile data from the drive is collected. Then investigations showing the time when the files were improved opened and created in the system are done (Moore, 2010).

Media analysis provides information about all the files and the programs that have been created and accessed in the period of interest. Byte search is the next step, which is used to look into the specific information, by providing signatures to the relevant information being looked at. Finally, analysis of the actions performed and the recommendations of the action to be taken after that are put down.

The hexadecimal editor is a program that is used to retrieve low-level evidence. The first step is observing raw data. Raw data is that that is not written in text form. The editor is widely used in looking at what type of data

is being represented in a file in a system. Secondly, is editing the raw and real contents that are in a file. During editing, the program changes the way the raw data appears in the system for easier and clearer observation and analysis. Finally, the hex editor is then used in correcting the raw data. Adjusting of corrupt data by a system changes the way a file or program has been stored in the system thereby retrieving the accurate and true data.

File headers identification is made through some ways. The file header is identified by a unique value that is used to represent it; this is done by a file identifier. Then, determination of the version value of the image in the file is done with the help of file format. The file header identification also is made by describing the number of lines that a picture has, hence representing the size of the picture (Amirani, Toorani, and Mihadoost, 2013). This is made possible through the use of the field version application. For the format support, encoding is done by the compression type field. Then the coordinates of the image are shown by the use of the x and y coordinates. Lastly, there is the identification of the unused space that contains no data and is undocumented (Moore, 2010).

The file headers extensions are deliberately mismatched to conceal the content in a file. The unique value used for its identification is changed hence not easily noticed. Determination of the image value is, and the description of the number of lines per image is not correctly done hence does not reveal the exact information being held in the header. In the case of the format support file encoding of the data that is represented is emitted or is wrongly entered. This is in an attempt to hide any information that is contained in a program or file (Casey, 2011).

Tools used to recover passwords from protected files are quite a number. They include password Fox, a tool used to recover passwords and user names in Firefox while Chrome pass recovers passwords and usernames in Chrome internet browser (Casey, 2011). Messen Pass is a tool that recovers passwords from instant messengers. Mail Pass View recovered stored passwords Gmail, Group Mail Free among others. Free word also excels a password is a tool that is used to crack word passwords and also excel passwords (Casey, 2011).

Conclusion

In conclusion, retrieving evidence and passwords can be utilized for some reasons though mainly it is used to recover information that has been stored in corrupt files and programs. Forensic tools and hexadecimal editors are some of the ways used to recover evidence. Identification of file headers is made through some forms that help identify the content in a file; however, their extensions can be mismatched in an attempt to conceal the information being stored in a file. Protected files can be accessed through tools and techniques that involve cracking of their passwords hence their information can be accessed.

References

Amirani, M. C., Toorani, M., & Mihandoost, S. (2013). Feature-based Type Identification of File Fragments. Security and Communication Networks, 6(1), 115-128.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.

Moore, R. (2010). Cybercrime: Investigating high-technology computer crime. Routledge.