Fake Circular Forensic Investigation Using Encase.docx

WORD COUNT 2539
TIME SUBMITTED 10-APR-2023 01:52PM
PAPER ID 98547213

FAKE CIRCULAR FORENSIC INVESTIGATION USING ENCASE

[1] *Dr.K. Suthendran*
Department of Information Technology, Kalasalingam Academy of Research and Institution
Anand Nagar, Krishnankoil, Tamilnadu.
k.suthendran@gamil.com

[1] *Vijaya Kumar G*
Department of Information Technology, Kalasalingam Academy of Research and Institution
Anand Nagar,Krishnankovil,Tamilnadu
vj1403200@gmail.com

[1] *Arichandran K*
Department of Information Technology, Kalasalingam Academy of Research and Institution
Anand Nagar,Krishnankovil,Tamilnadu
arichandran9361@gmail.com

[1] *Tamilelan M*
Department of Information Technology, Kalasalingam Academy of Research and Institution
Anand Nagar, Krishnankovil,Tamilnadu
mtamilelan@gmail.com

[1] *Pappy Anto V*
Department of Information Technology, Kalasalingam Academy of Research and Institution
Anand Nagar, Krishnankovil,Tamilnadu
immrcool113@gmail.com

***Abstract: In** the COVID times, the technologies may have evolved and updated. The COVID-19 pandemic has had a profound impact on the way universities communicate with their students. With the sudden shift to remote and online learning, universities have had to find new ways to reach out to students and keep them informed about important updates and changes. Like E-mails, Online portals, virtual town hall meetings, social media, Text messages. Using these type of communication may lead to some of the wrong spreading of information. Meanwhile, some of them are miss-using this kind of communication. Like, Fake circular spreading, false information spreading on the common groups, and many more are taken places after COVID times. Our Research is based on the Fake Circular Spreading on the University, the spread of false information, especially in the form of circulars, can have serious consequences for universities and their students. It can lead to confusion, misinformation, and even panic among students and other members of the university community, it's important for universities to be proactive in addressing the spread of false information and to work to promote accurate and reliable sources of information within the university community.*

Keywords: Encase, Fake Circular, Spread

1. INTRODUCTION

" The surge in technological advancements and the wide use of cyberspace have facilitated easy dissemination of deceitful data using diverse platforms, including circulars. The exponential rise in faux circular publications poses a grave predicament that could lead to ramifications on individuals, establishments, and society at large [3]. For instance, fictitious job ads can culminate in detrimental economic losses for people while phony investment opportunities can result into fraudulent activities with financial implications. Furthermore, spurious government notices are capable of causing disarray which undermines public trust towards institutions. Consequently,the realm dealing with fake circulatory forensic inquiry has emerged as a countermeasure against false information propagation.Their modus operandi entails employing distinct techniques ranging from digital forensics,content analysis,and linguistic assessment aimed at identifying and dissecting fake bulletins.Furthermore,this probe's objective is two-pronged: prevent harm inflicted on victims;ensure safeguarding integrity surrounding authentic information.However,simultaneously it calls for more research development within this field.This comprises articulating an intricate understanding of various types attainable,detection protocols deployed,magnitude effect imposture data imposes upon implicated parties.As such,it behooves us to undertake literature review survey elucidating current standing regarding pseudo-circulars concerning forensic investigation alongside potential further expansions or exploration areas through future studies envisioned here in above.

LITERATURE REVIEW

Digital forensics is used in a wide range of investigations, including cybercrime, intellectual property theft, and fraud. It can be used to retrieve and analyze data from digital devices [1]. The Fake circular can be spread in the form of many ways like text format, video, audio, that are shared in the social medias like WhatsApp, Facebook, Telegram, Gmail and etc…. [2] Social networks and social media in general supply a medium in which the news production and sharing is available to the general public, not only to established news agencies. [3] It's not always guarantee to get the recovered or deleted files from the RAM is not possible [4]. There are many ways to change the original documents, and rest of all getting the fake documents from just one file of original copy [5]. The Digital data is easily get copied from the original source, therefore the data can be modified into wrong portrays, information's or delete the info's and added the fake information etc and the change of data also can happen sometimes [6]. The digital evidence that extract from the crime scene that then evidence that are based on the law no11 2008 act they may considered as an Electronic Information and Electronic Documents that type of evidences may be divided as a Logical Evidence, Audio files, Video files, E-mails, Documents, SMS, MMS, Steganography and Call Logs [7]. The lack of file system on the Logical Method, the data will not be indexing means the data files cannot be retrieved or acquired, through physical acquisition method can extract all the data from the flash memory card after it is connected by a USB cable or using wireless, thus including normal boot mode and recovery boot mode, compare to logical method, physical method can have the maximum possibilities to recover the data which are confidential evidences in the criminal investigation [8]. The metadata of a file is not corrupted we can maximum chance to recover the information that are deleted such as authorship, creation/modification date or when the file is created, the version of the software the pdf file is created is also shown. So, it takes less amount of time to spent for the analyzing the evidences and they avoid needlessly depend the investigation into meaningless such as craving the false information about the evidence may consume our time which provides no metadata about the in formation of the evidence. On the other side, where the file is deleted or hidden the investigators are used to search all possible ways for the evidences claims [9]. The data may be encrypted as known as encrypted file, it would encrypt the file with the stored data. Encryption can be applied to every individual file that we create such as database, email, or entire hard disks using several algorithms [10]. However, they have advantages at the same time also they also have drawbacks, they criminals who having the high intelligence in the morphing documents or image processing and audio and video footage mixing they create them without leaving any hints to the forensic examiners, in order the spreading of fake information getting more and more common now days. There are many software's spreads in the internet to do this type of criminal activities, where they can be easily download from the internet now days. For examples some tools like deep fake, voice changer, Photoshop, pixlr etc [11]. Since we are now a days using USB drives mostly, Write blocker used to prevent the data in the USB drives without modifies and we cannot write the USB drive only we can read the USB drive only write blockers were used to preserve the Integrity of data that are present in the USB drive accquirng the information without creating the possibility of damaging the drive contents [12].

EnCase

EnCase is a forensic investigation tool to investigate the devices that are seized from the crime scenes. They can be used to produce the report and required the acquired data from devices. There are certain ways involved in acquiring the data in the EnCase [12],

1. While opening the EnCase application, the investigator hould conncet the EnCase Dongle provided by the GUIDANCE SOFTWARE.
2. After opening the application, the investigator has to create the new case file and set the outpath for the case file to be stored, if we need backup we can give the backup option if we don't need we can turn off the Backup option.
3. And now the investigator need to insert the device foe the examine that device for acqurring evidence.
4. After adding the device for examine, the investigator needs to acquire and process the case file for obtain the Ex1 in the Encase image format.
5. Now the software starts to acquire and the process the devices for evidences.
6. After the acquiring and processing is completed, the output will be saved in the outpath given by the examiner.
7. Now we can see the collected evidences from the devices.

The primary webpage for the Encase digital forensics programme is the homepage. The program, its characteristics, and the advantages of using it for digital investigations are all described on the homepage. The various Encase versions, such as Encase Forensic, Encase Endpoint Investigator, and Encase eDiscovery, are described on the homepage. Every version is created to address the particular requirements of various kinds of investigations, from criminal investigations to internal company investigations. The site also gives access to tools like white papers, case studies, and webinars as well as details on the most recent software changes and releases. Users can also access forums, technological help, and documentation in the

support area. embedding procedure to embed message into the encrypted pixels

EnCase INTERFACE

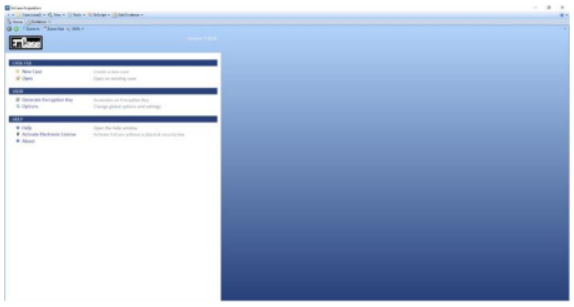


Fig. 1. Home Page for Encase Software

First we have to the insert codemeter in our device and run the EnCase software on the system. And then we have to add the vidences

ADDING EVIDENCES

Fig. 2. Evidence Adding

To add a new case in EnCase software, you can follow these steps:

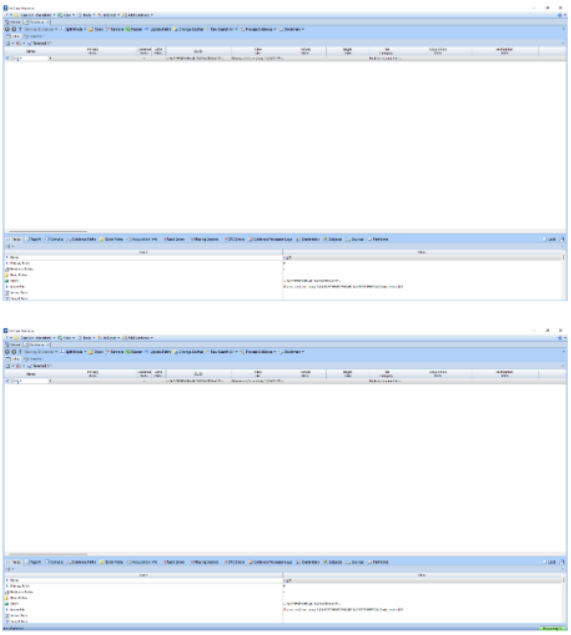
Open EnCase software and click on "New Case" from the "Case" menu. In the "New Case" window, enter a name for your case in the "Case Name" field. Enter a description for your case in the "Description" field. This can include information such as the purpose of the case, the date range of the investigation, and any relevant details. Choose a location for your case files by clicking on the "Browse" button next to the "Case Location" field. This will open a window where you can navigate to the folder where you want to store your case files.

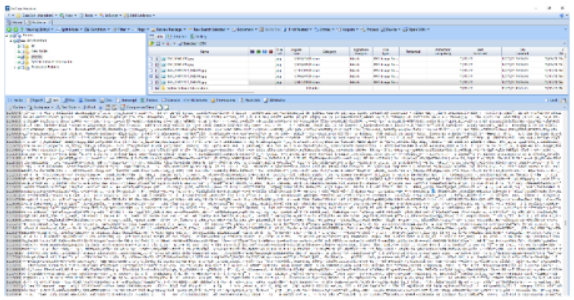
Choose a case type from the "Case Type" drop-down menu. This will determine the default settings for your case and the types of evidence you can process. Select the "Evidence Processor" you want to use from the drop-down menu. This will determine the type of evidence you can process in your case. Choose the "Data Source" you want to use from the drop-down menu. This will determine the type of data you can collect from your evidence. Click on the "Create" button to create your new case. Once the case is created, you can add evidence to it by clicking on the "Add Evidence" button from the "Evidence" menu. This will open a window where you can select the type of evidence you want to add and the location of the evidence files. Follow the on-screen instructions to process the evidence and add it to your case. You can then begin analyzing the evidence and creating reports using the various tools available in EnCase software.

Note: These steps may vary slightly depending on the version of EnCase software you are using.

ACCQUIRING AND PROCESSING

Fig. 3. Selecting the drive for Processing and Accquiring





Select the drive which we want to examine that seized devices from crime scene. After selecting the drive, we gave to acquiring and processing that device to obtain the missing evidences that are deleted, modified, and writing date of the device. The Accquiring process takes much to complete the task it takes about 20-30 minutes to completed the acquiring process. After completing the Accquiring the drive needs to process to complete the examination. The processing may take upto 30 minutes approx. to complete it. All these have done only with the help of Codemeter, without that we can't get the detailed information of the devices. And then we can examine the device to see the modifications in the drives.

COLLECTED EVIDENCES FROM THE DEVICE:

Fig. 4. COLLECTED EVIDENCES

We analyse the evidences using hex code in Diffchecker, while we analyse the hex codes through diff checker we found the culprit who spread the fake circular, we found that the original pdf is shared in the time of 5.30 AM at the date of 12.12.22. Later it can be modified in the time of 6.00 PM at the date of 13.12.22. The original pdf was created in the Microsoft Word 2016 version. And the fake circular was edited in the Adobe Acrobat. The both of the PDF were using UTF – 7 – Byte Order mark for text. The Length of the Original Pdf is 284. Later, we found that the Fake circular pdf length is 304. The Flat Decode length of the Original Pdf is 183875 and the Fake Circular Decode Length was 183904. The Width of the Original Pdf is 17 and the width of the Fake Pdf is same as the original pdf shared by the Culprit. The first Character length of the Pdf is 32 and the Fake circular first character length is also 32 only. The last Character of the original Pdf is 150 and the Last character of the Fake pdf is 130. With all of these we can found the major differences between the original and Fake Pdf. At last we can examine thoroughly we can find the name and gmail of the culprit who spread the fake circular.

I. CONCLUSION

To conclude, the forensic analysis of the fraudulent circular has exposed that this document was not genuine and constructed to deceive its recipient. Innovative approaches such as digital forensics, manuscript scrutiny, and handwriting examination have played a fundamental part in disclosing reality. The implications of these findings are crucial for those implicated and can be used as evidence in legal matters if necessary. It is worth noting that bogus documents carry severe repercussions; thus it's wise always to authenticate any paperwork before acting on their contentions. All-in-all, this inquiry provided insightful knowledge into creating counterfeit circulars while underlining how vital precise investigations were essential when searching for truthfulness.

REFERENCES

- [1] Vimal shetty, Ramesh Vardhan, "Digital Forensics using Data Mining", International Journal of Computer Trends and Technology (IJCTT) volume 22 Number 3rd April 2015

- [2] Detecting Fake News in Social Media using voting classifiers, Eman Elaseed, Osama Ouda, Mohammed M. Elmogy, Ahemd Atwan, Eman El Daydamony, December 1 2021.

- [3] How to Fight Fake News Spreading in Online Social Networks (Alina campan, Alfredo Cuzzocrea, Traian Marius Truta published on December 2017)

- [4] Asynchronous Forensic Investigative Approach to Recover Deleted Data from Instant Messaging Applications (Fahad E Salamh, Umit Karabiyik, Marcus K Rogers published on 25 December 2022)

- [5] Image Processing based forensic investigation of morphed documents (Shruti Ranjan; Prayati Garhwal; Monika Arora; Anu Mehra) published on 29-31 March 2018.
- [6] A Forensic Investigation for Suspects' digital evidences using Image Categorization (Youngsoo Kim; Dowon Hong; Dongho Won) INSPEC A No. 10425724 published on 13-15 December 2008

- [7] Development of Digital Evidence Collection Methods in Case of Digital Forensic Using Two Step Inject Methods (Nana Rachmana Syambas; Naufal El Farisi) published on 23-24 October 2014.

- [8] Digital forensics and analysis for Android devices (Zhi Li; Bin Xi; Shunxiang Wu) was published on 23-25 August 2016, INSPEC Accession Number: 16358250.

- [9] Model of hierarchical disk investigation (Umit Karabiyik; Sudhir Aggarwal) was published on 25-27 April 2016.

- [10] Overview of Digital Forensics and Anti-Forensics Techniques (Hussein Majed; Hassan N. Noura; Ali Chehab) was published on 01-02 June 2020.

- [11] An Overview on Digital Forensics Tools used in Crime Investigation for Forgery Detection (Gangannagari Upender Reddy; Myneni Madhu Bala; B Padmaja) was published on 13-14 March 2020.

- [12] Forensic investigation on electronic evidences using encase and autopsy *Sustainable Development in Engineering and Technology* 2022, ISBN 978-84-124943-4-1

Fake Circular Forensic Investigation Using Encase.docx

ORIGINALITY REPORT

7%
SIMILARITY INDEX

PRIMARY SOURCES

1	"Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2018)", Springer Science and Business Media LLC, 2020 Crossref	72 words — 3%
2	Zhi Li, Bin Xi, Shunxiang Wu. "Digital forensics and analysis for Android devices", 2016 11th International Conference on Computer Science & Education (ICCSE), 2016 Crossref	32 words — 1%
3	advservices.nku.edu Internet	20 words — 1%
4	Yang Gao, Yuan Yao, Yunliang Jiang. "Multi-target 3D Reconstruction from RGB-D Data", Proceedings of the 2nd International Conference on Computer Science and Software Engineering, 2019 Crossref	18 words — 1%
5	Umit Karabiyik, Sudhir Aggarwal. "Model of hierarchical disk investigation", 2016 4th International Symposium on Digital Forensic and Security (ISDFS), 2016 Crossref	10 words — < 1%
6	Foundation Flash MX Applications, 2003. Crossref	6 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE SOURCES	OFF
EXCLUDE BIBLIOGRAPHY	ON	EXCLUDE MATCHES	OFF