Analysis of Steganographic on Digital Evidence using General Computer Forensic Investigation Model Framework

Muh. Hajar Akbar[1]
Master Program of Informatics
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Sunardi[2]*
Electrical Engineering Department
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Imam Riadi[3]
Information System Department
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

***Abstract*—Steganography is one of the anti-forensic techniques used by criminals to hide information in other messages which can cause problems in the investigation process and difficulties in obtaining original information evidence on the digital crime. Digital forensic analysts are required ability to find and extract the messages that have been inserted by using proper tools. The purpose of this research is to analyze the hidden digital evidence using steganography techniques. This research uses the static forensics method by applying five stages in the Generic Forensics Investigation Model framework, namely pre-process, acquisition & preservation, analysis, presentation, and post-process as well as extracting files that have been infiltrated based on case scenarios involving digital crime. The tools used are FTK Imager, Autopsy, WinHex, Hiderman, and StegSpy. The results on the steganographic file insertion experiment of 20 files indicate that StegSpy and Hiderman are effective on the steganographic analysis of digital evidence. StegSpy can detect the presence of secret messages with 85% success rate. The extraction process using Hiderman for 18 files with containing steganographic messages had 100% successful.**

***Keywords*—Steganography; anti forensics; general computer forensic investigation model; hiderman**

I. Introduction

Various kinds of crimes and criminal acts currently involve information and communication technology [1] [2]. The widespread of computers and other digital devices usage without security can lead various parties to crimes [3]. Perpetrators of crimes can be subject to punishment based on the evidence [4]. Digital criminals usually use anti-forensic techniques thus causing difficulties to find the digital evidence [5]. One of the anti-forensic techniques is steganography [6]. Steganography is an interesting science to study and research today [7]. Confidentiality, security, or integrity of the information to be conveyed are the main factors in steganography [8] [9]. This technique allows the perpetrator to hide information by inserting the information into other messages in the form of digital media such as text, images, audio or video without arousing suspicion. [10] [11]. Computer crimes related to the misuse of steganographic techniques have been reported through the mass media, including a report from Trend Micro November 2017 with the title “REDBALDKNIGHT’s Daserf Backdoor Now Using Steganography”. It has been reported that the Bronze Butler or Tick type malware was spread by the creator through a steganography technique by inserting it into an image with the extension jpg to spy on Japanese, South Korean, Russian, Singaporean and Chinese companies. Reported by Kompas.com December 9th, 2017 entitled "16 Years of 9/11 Attack: WTC Collapsed not because of a Plane Collision?". At that time, terrorists hide their terror activities in various digital media such as images, audios, and videos. The maps and photos of targets as well as orders for terrorist activity in sport chat rooms, porn bulletin boards, and other websites. The existence of cases reported by the mass media regarding crimes using steganography techniques inserted in electronic storage media. It’s becomes a challenge that must be resolved by investigators and law enforcers in order to reveal the mode, objective, and perpetrators of crimes related to evidence obtained. Therefore, the process of steganography detection is very important for digital forensic investigators [12].

Digital forensics is a applied science to identify, extract, analyze, and present the evidence that has been stored on digital devices [13] [14], or help prevent illegal acts in the process of operating activities carried out [15] use generally accepted methods to make the evidence acceptable in court [16]. Forensic techniques and forensic analysis based on correct methods will have almost 100% success in collecting forensic data [17]. The process of digital forensic investigations on computers or similar devices can be carried out using live forensics or static forensics methods [18]. In this study, static forensic is used. Static forensic is an investigation carried out when the computer is turned off, because of the data can change when the computer is turned on [19]. The forensic framework can implement a framework of several standards that can be used in the forensic process according to international standards including the National Institute of Justice (NIJ), Digital Forensics Research Workshop (DFRWS), Integrated Digital Forensics Investigation Framework (IDFIF), Generic Computer Forensic Investigation Model (GCFIM), Systematic Digital Forensic Investigation Model (SRDFIM) or other forensic process frameworks [20].

The evidence is classified into two forms, namely electronic evidence and digital evidence [21]. Electronic evidence is physical evidence that can be recognized visually, so investigators and forensic analysts need to understand the

*Corresponding Author

evidence when they are searching for evidence at a crime scene. While digital evidence is very vulnerable to changes in the data, therefore we need extra careful handling to keep digital evidence intact [22].

To make easier by investigators for data collecting related to the cases being investigated, forensic software is needed [23]. Forensic software usually multi-purpose, able to perform multiple tasks in the specific application. Computer forensic software complements the hardware available to law enforcement to obtain and analyze digital evidence gathered from suspect devices.

Research with a similar this topic has been conducted by [24] which is the investigation process and finds digital evidence in steganographic files. The process of steganographic analysis uses software, namely WinHex, InvisibleSecrets, and FTK Imager. The methodology or research stages are systematically carried out, namely literature review, observation & data collection, scenario case, preparation system, investigation & analysis case, and report & documentation.

Study with a similar theme was also carried out with the title Steganographic Engineering Analysis and Steganalysis on Multimedia Files Using the Net Tools and Hex Editor [25]. This research discusses use the WinHex application to perform analysis on messages hidden using the Net Tools into the container image. The method used experimental methods, namely identification problem, literature study, testing, and analysis.

The other reference in [26], steganographic file analysis was carried out by applying the Computer Forensic Investigative Process method which is divided into four stages, namely Acquisition, Identification, Evaluation, and Admission.

Further research was carried out by [27]. This research discusses the importance of computer forensic examiners in knowing the types of steganography tools that can be applied to the victim's computer. The tools used are S-tool and OpenStego.

Based on the background described, the objective of this digital forensics research is to find and analyze evidence in the form of files with text, audio, image, and video formats hidden by criminals by using steganography techniques. The static forensics method and GCFIM framework implemented in order to retrieving data on digital evidence, so that the data obtained can be used as legal evidence in court.

II. Research Method

A. Case Scenario

Digital evidence in this research will obtained from the results of case scenario as shown in Fig. 1.

B. Research Stages

The research was carried out in accordance with the work steps in the GCFIM framework which were added with one initial stage, namely implementation and case scenario. GCFIM describes the stages of research so that research steps can be known systematically and can be used as an investigative model for any digital investigation as shown in Fig. 2.

GCFIM has a back and forth flow, where it is possible for investigators to return to the previous stage due to the possibility of situations that can change such as the crime scene (both physical and digital), the investigation tools used, the crime tools used, and the investigator's level of expertise. The stages in the GCFIM framework are described as follows:

- Pre-Process. This stage is also called the preparation stage. Investigator doing related work before carrying out an investigation, such as preparing letters and official documents from legal authorities, and preparing tools.
- Acquisition & Preservation. At this stage, all relevant data are retrieved, stored, and prepared.
- Analysis. This stage is the main process in a computer forensic investigation, which is an analysis of the data that has been obtained to identify the source of the crime, the motive for the crime, and ultimately to find the person responsible for the crime.
- Presentation. This stage makes a presentation of the results that have been obtained to the competent authorities. This is important considering that the results of the analysis must not only be presented, but also must be supported by adequate/eligible and acceptable evidence. The results of this stage are to prove and/or deny the alleged criminal act.
- Post-Process. Digital and physical evidence must be returned to the rightful owner and stored in a safe place. The investigator reviews the investigation process that has been carried out so that it can be used to improve the further investigation process.

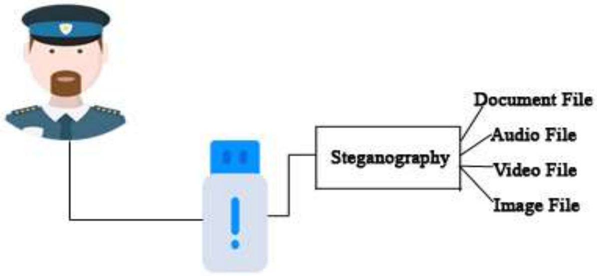


Fig. 1. Case Scenario.

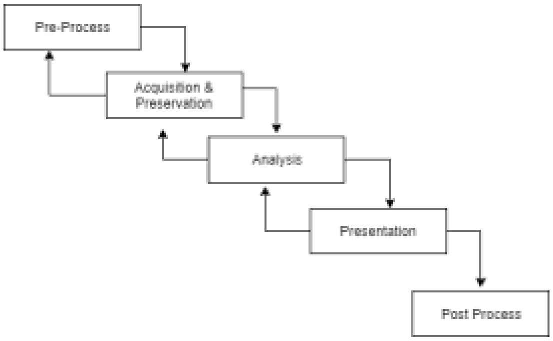


Fig. 2. GCFIM Framework [28].

III. Result and Discussion

A. Implementation Results and Case Scenario

The case scenario is implemented by using the Hiderman application. The hide files process is function to insert steganographic messages into several file formats such as documents, videos, images, and audio which are then stored on flash disk storage media. In this research, the inserted file in the form of stego text. The processing time to hide files is depends on the size of the file inserted. The larger the file size will longer time of insertion process. Fig. 3 is the process of hiding files.

The next step after selecting the container file is to select the files to be hidden or inserted by selecting the Choose the Files You Want to Hide menu as in Fig. 4.

The process in Fig. 4 is to select a secret file that will be inserted into the container file. In this process, the ratio of messages to be hidden can be found. A good ratio when hiding messages is 1 to 10. The hidden files must be 10 times smaller than the container files. After getting the right ratio file, the next step is to select the Hide File (s) menu.

B. Pre-process Results

At this stage, the things that must be prepared by the investigator can be seen in Table I.

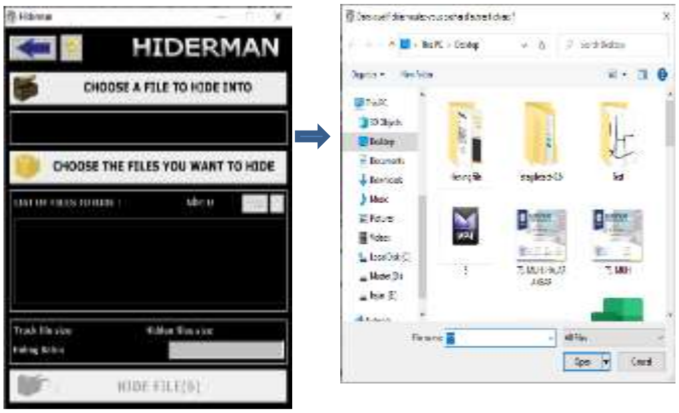
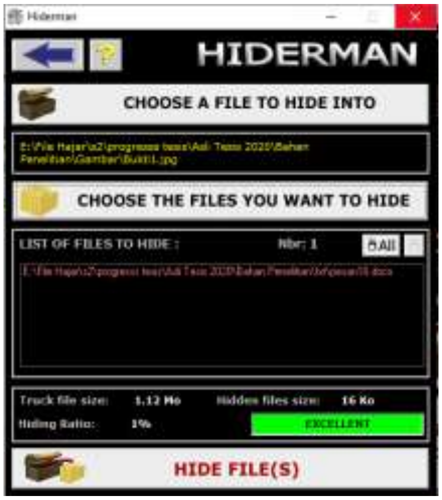


Fig. 3. Choosing the Container File.



E:\File Hajar\s2\progresss tesis\Adi Tesis 2020\Bahan Penelitian\Gambar\Bukti1.jpg

E:\File Hajar\s2\progresss tesis\Adi Tesis 2020\Bahan Penelitian\Infopesan\3.docx

Truck file size: 1.12 Mo Hidden files size: 16 Ko
Hiding Ratio: 1% EXCELLENT

Fig. 4. Secret File Selection.

TABLE I. Pre-Process Stage

No	Tool's name	Uses
1	Investigative administration	Search warrant and confiscation warrant
2	Digital camera	To photograph crime scenes and evidence by forensic photography
3	Stationery	To record technical specifications regarding electronic evidence and witness statements
4	Number, measuring scale, Institution label, blank label sticker	To mark each electronic evidence found at the crime scene
5	Chain of Custody Form	Report of the investigation of evidence

C. Acquisition and Preservation Results

This stage is the starting stage for the identification of evidence at the scene of the crime which is continued with the process of acquisition and maintenance of the originality of the evidence. The aim is to secure the evidence from changes in physical form or changes in data by storing it in a safe place. The data acquisition process on physical evidence (flash disk) is carried out using the FTK Imager tool. Choose the create disk image option and the physical drive option is selected for the full acquisition process. The source drive selection option is made with the name "Kingston Data Traveler 2.0". Choose the destination of the storage drive. Then select the image type with the Raw (dd) format. Fig. 5 and 6 is the process of create an image of evidence.

The acquisition results in two hash values, namely Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm 1 (SHA1) which are used to verify the authenticity of the duplicated image files. The hash value obtained by the recipient then compared with the hash value sent by the sender of the message to check the suitability and authenticity of the message. Fig. 7 is the log result and acquisition hash value on flash disk evidence using the FTK Imager tool.

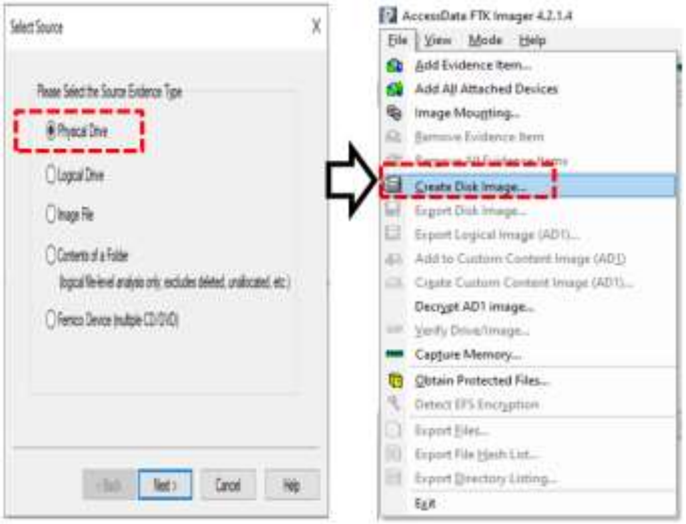


Fig. 5. Create Disk Image Process.

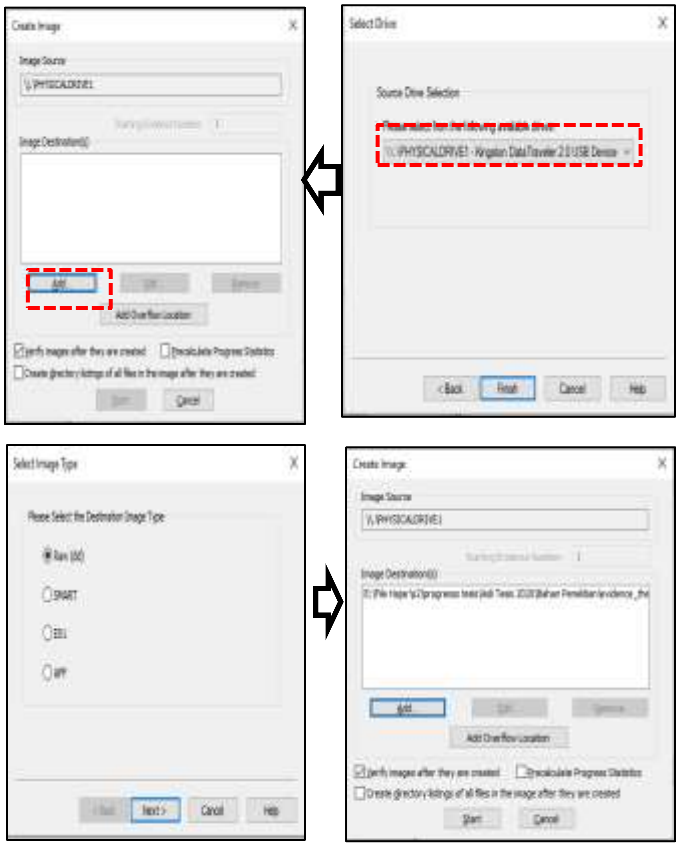
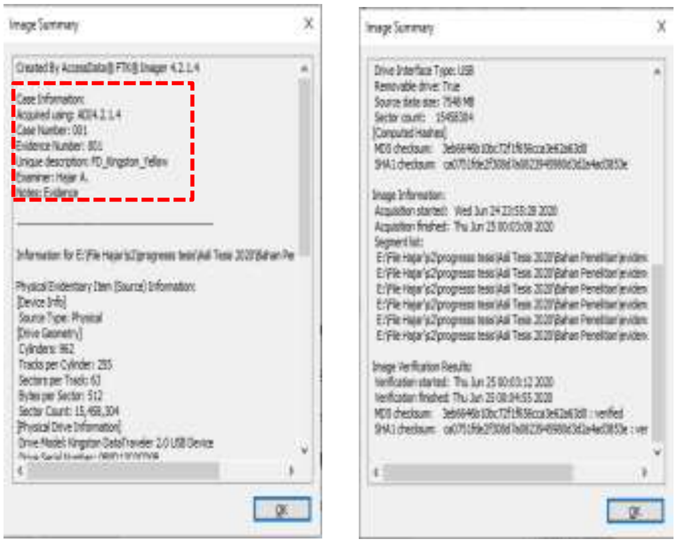

Create Image
Image Source
\\.\PHYSICALDRIVE1
Starting Evidence Number
Image Destination(s)
Add
Edit
Remove
Add Overflow Location
☑ Verify images after they are created
□ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created
Start
Cancel
Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE1 - Kingston DataTraveler 2.0 USB Device
< Back
Finish
Cancel
Help
Select Image Type
Please Select the Destination Image Type
● Raw (dd)
○ SMART
○ E01
○ AFF
< Back
Next >
Cancel
Help
Create Image
Image Source
\\.\PHYSICALDRIVE1
Starting Evidence Number
Image Destination(s)
E:\File Hajar's\2\progress tesis\Adi Tesis 2020\Bahan Penelitian\evidence_fhd
Add
Edit
Remove
Add Overflow Location
☑ Verify images after they are created
□ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created
Start
Cancel

Fig. 6. Create an Image of Evidence.



```
Created By AccessData® FTK® Imager 4.2.1.4

Case Information:
Acquired using: ADI4.2.1.4
Case Number: 001
Evidence Number: 001
Unique description: FD_Kingston_Yellow
Examiner: Hajar A.
Notes: Evidence

Information for E:\File Hajar's\2\progress tesis\Adi Tesis 2020\Bahan Pe

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 962
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15,458,304
[Physical Drive Information]
 Drive Model: Kingston DataTraveler 2.0 USB Device
```

```
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7548 MB
 Sector count:    15458304
[Computed Hashes]
 MD5 checksum:    3eb6646b10bc72f1f656cca3e62a63d0
 SHA1 checksum:   ca0751fde2f308d7a0823945980d3d2a4ad3853e

Image Information:
 Acquisition started:  Wed Jun 24 23:58:28 2020
 Acquisition finished: Thu Jun 25 00:03:08 2020
 Segment list:
  E:\File Hajar's\2\progress tesis\Adi Tesis 2020\Bahan Penelitian\eviden
  E:\File Hajar's\2\progress tesis\Adi Tesis 2020\Bahan Penelitian\eviden
  E:\File Hajar's\2\progress tesis\Adi Tesis 2020\Bahan Penelitian\eviden
  E:\File Hajar's\2\progress tesis\Adi Tesis 2020\Bahan Penelitian\eviden
  E:\File Hajar's\2\progress tesis\Adi Tesis 2020\Bahan Penelitian\eviden
  E:\File Hajar's\2\progress tesis\Adi Tesis 2020\Bahan Penelitian\eviden

Image Verification Results:
 Verification started:  Thu Jun 25 00:03:12 2020
 Verification finished: Thu Jun 25 00:04:55 2020
 MD5 checksum:    3eb6646b10bc72f1f656cca3e62a63d0 : verified
 SHA1 checksum:   ca0751fde2f308d7a0823945980d3d2a4ad3853e : ver
```

Fig. 7. Case Information and Hash Image.

Based on Fig. 6, the information regarding the MD5 hash value in the image file is “1Hw91XA9c1CuLKp9PhAt1ujZ963ZsagEBf”, while the SHA1 hash value is “ca0751fde2f308d7a0823945980d3d2a4ad3853e”. Furthermore, the preservation stage is carried out to prove the integrity of the acquired image file is identical to the file on the original evidence.

D. Preservation Results

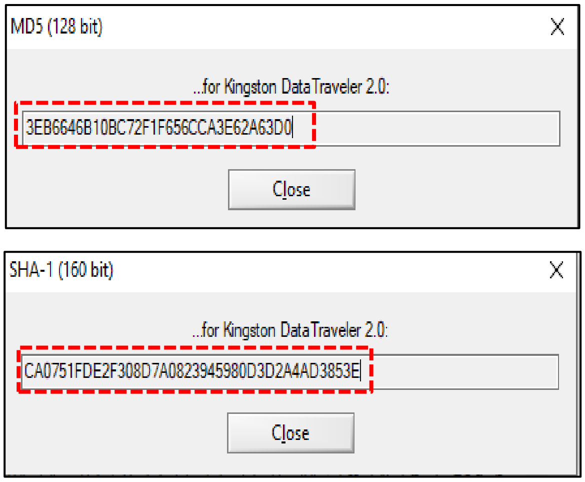
This stage is retested by matching the MD5 and SHA1 hash values between the hash values of the original evidence and the evidence files of the acquisition or imaging results. Checking the hash value of original evidence is done using the Winhex tool. The MD5 and SHA1 hash values of the original evidence files can be seen as in Fig. 8.

After obtaining the hash value of the original evidence file, the next step is to match the hash value between the imaging evidence and the hash value of the original evidence which can be seen in Table II. The hash value of the acquisition/imaging evidence has the same value as the original evidence. Therefore, it can be concluded that the cloned evidence file is identical to the original evidence.

E. Results of Analysis

The analysis stage is divided into three stages, namely the identification stage, the steganalysis stage, and the extraction stage.

1) Identification stage: Analysis of the "image" file resulted from the acquisition & preservation process is carried out in this stage. The initial analysis process uses the Autopsy tool. Autopsy has several advantages for conducting content analysis and identification, data recovery, and metadata analysis. The process of input cases (case) on the Autopsy tool as shown in Fig. 9 as the initial stage of starting the "image" analysis phase.



...for Kingston DataTraveler 2.0:

3EB6646B10BC72F1F656CCA3E62A63D0

...for Kingston DataTraveler 2.0:

CA0751FDE2F308D7A0823945980D3D2A4AD3853E

Fig. 8. Testing MD5 and SHA1 Hash Values.

TABLE II. HASH VALUE MATCHING

Original Evidence	
MD5	***SHA1***
3EB6646B10BC72F1F656CCA3E62A63D0	ca0751fde2f308d7a0823945980d3d2a4ad3853e
Image File	
3eb6646b10bc72f1f656cca3e62a63d0	ca0751fde2f308d7a0823945980d3d2a4ad3853e

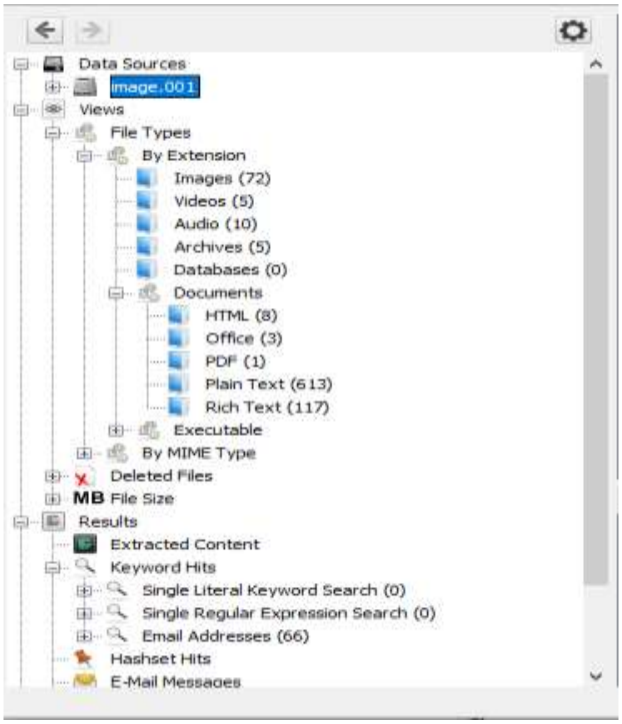


Fig. 9. Image Identification Stage.

Autopsy identify all the details of the data contained in the storage of evidence (flash disk) which has been neatly arranged and has become a data source in Autopsy. It is divided into several components including file types, deleted files, and file size. The file listing that is suspected of having confidential content is a file with the name of the audio, document, image, video folder, and one file in the .txt format which can be seen in Fig. 10.

Furthermore, the file extraction process is carried out in the suspected folder based on Fig. 10. The extraction process aims to obtain files so that re-analysis of the suspected file contents is carried out. The file extraction process can be seen in Fig. 11.

The file extraction process is carried out in order to export the image file based on the suspected folder. Files obtained after the extract process which consists of 4 folders and 1 file with the .txt format as listed in Fig. 11.

2) Steganalysis stage: The steganalysis process is carried out on the extracted files from the initial analysis to identify the files with secret messages that have been inserted. The second stage of the analysis process is shown as in Fig. 12 using the StegSpy tool in each extracted file.

The results of the analysis of the existence of secret files are shown in Table III. Based on the test results on 21 files, it was found that 18 files were identified to contain steganographic messages,

Based on Table III, StegSpy has successfully detected 18 steganographic files that have been inserted in various file formats and provided information about the detected marker values while three files were not detected.

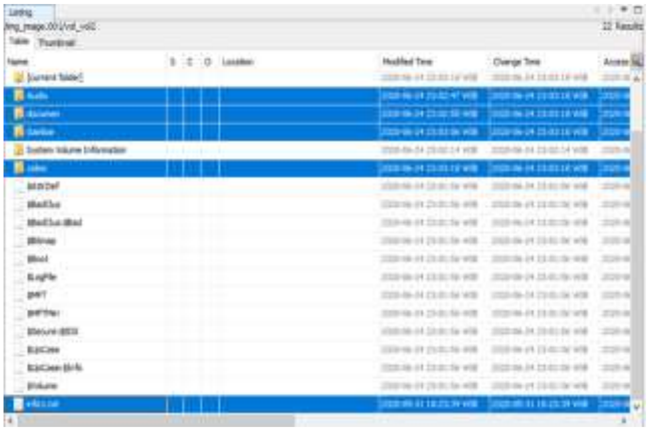


Fig. 10. Confidential Content.

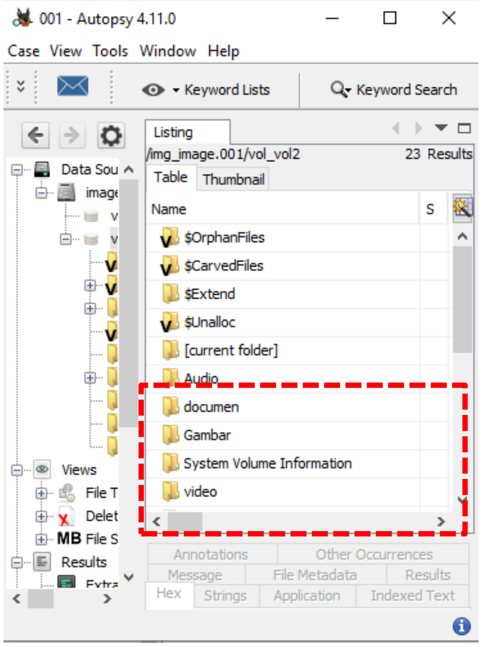
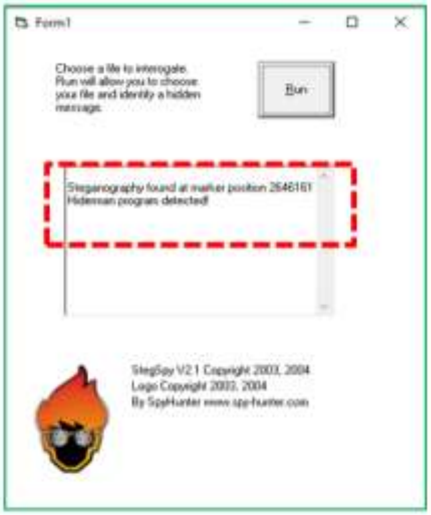


Fig. 11. The Extraction Stage.



Choose a file to interrogate.
Run will allow you to choose your file and identify a hidden message.

```
Steganography found at marker position 2646161
Hiderman program detected!
```

StegSpy V2.1 Copyright 2003, 2004
Logo Copyright 2003, 2004
By SpyHunter www.spy-hunter.com

Fig. 12. Steganalysis Stage.

TABLE III. STEGANOGRAPHY FILE ANALYSIS RESULTS

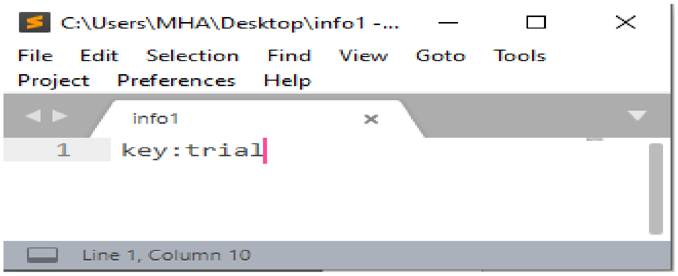
No	File Type	File Name	Format	Information	Marker
1	Audio	evidence6	.wav	Found	2646161
		evidence7	.wav	Found	1073335
		evidence8	.wav	Found	2146284
		evidence9	.wav	Found	5226880
		evidence10	.wav	Found	10406854
2	Image	evidence1	.jpg	Found	1128234
		evidence2	.jpg	Found	5463476
		evidence3	.jpg	Found	785400
		evidence4	.jpg	Found	2546084
		evidence5	.jpg	Not found	-
3	Document	evidence16	.xls	Found	39655
		evidence17	.pdf	Found	941323
		evidence18	.ppt	Found	11093743
		evidence19	.doc	Found	93794
		evidence20	.txt	Found	374135
4	Video	evidence11	.mp4	Found	7832077
		evidence12	.mp4	Found	3517633
		evidence13	.mp4	Found	874744
		evidence14	.mp4	Not found	-
		evidence15	.mp4	Found	2769824
5	document	Info1	.txt	not found.	-

3) *Extraction stage:* The extraction stage is the analysis process carried out to reveal the presence of steganographic messages that have been detected in the steganalysis process. Based on the extraction results in the previous stage, after observation, there is a file with the file name info1.txt which contains information as in Fig. 13.

Based on Fig. 12, the file with the name info1 in the .txt format is suspected to be the key used to open the secret message contained in the detected file. Furthermore, at this stage an analysis is carried out using the Hiderman forensic tool to decrypt the steganography file using the "trial" key. The process of encrypting steganography files can be seen in Fig. 14.

After selecting a file that is infiltrated with steganographic messages, the next step as shown in Fig. 15, is to select the extract data menu and determine the place where the extracted file is stored.

After the key input process is done, the hidden secret files can be discovered automatically. The secret file obtained is in the form of a .txt text message as shown in Fig. 16.



```
1  key:trial
```

Line 1, Column 10

Fig. 13. Info1.txt.

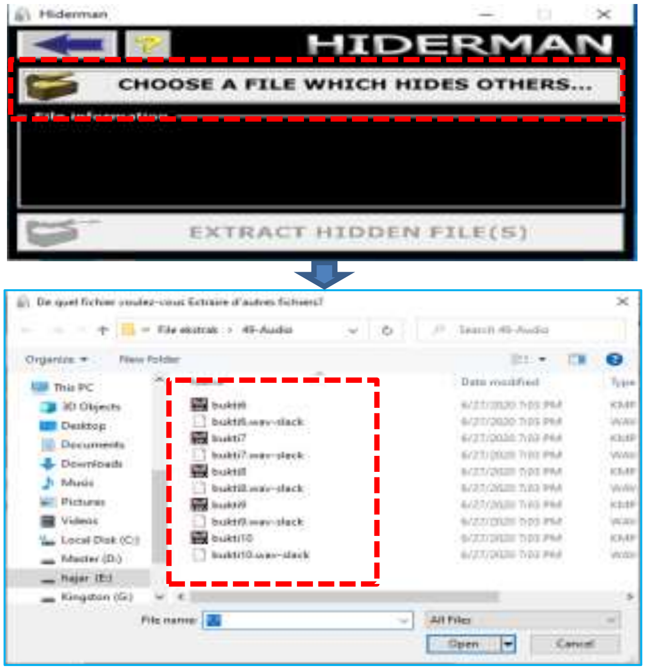
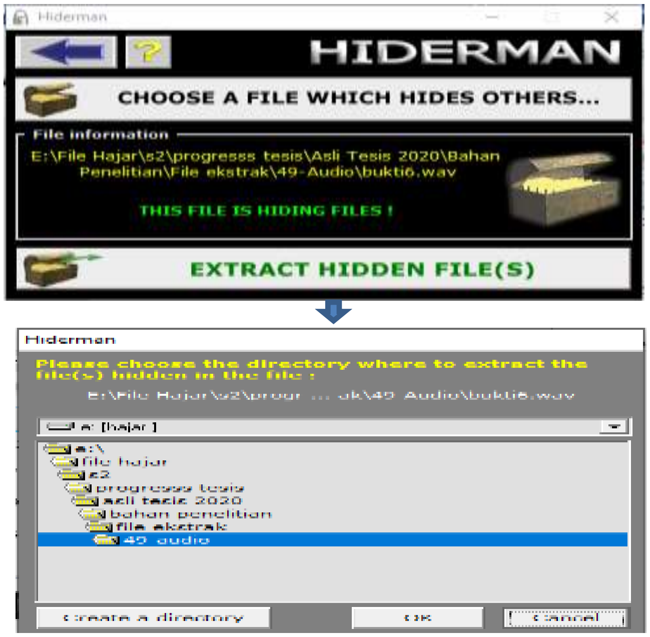


Fig. 14. Selection of the Inserted File.



E:\File Hajar\s2\progresss tesis\Asli Tesis 2020\Bahan Penelitian\File ekstrak\49-Audio\bukti6.wav

THIS FILE IS HIDING FILES !

Please choose the directory where to extract the file(s) hidden in the file :

E:\File Hajar\s2\progr ... ak\49 Audio\bukti6.wav

Fig. 15. Extraction Process.

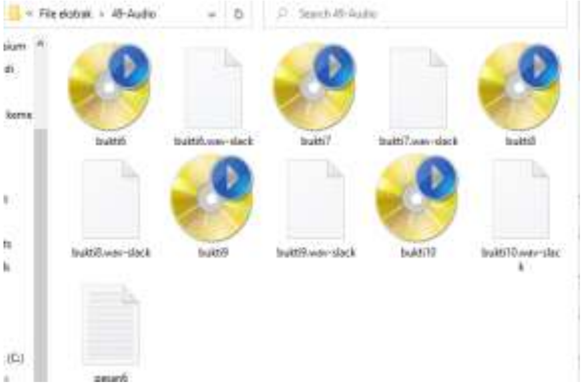
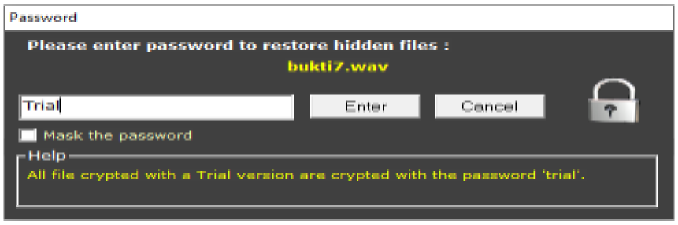


Fig. 16. Extraction Process and Directory Selection.

The final step in the extraction process is to enter the key or password found based on the contents of the info1 file, as shown in Fig. 17.


Password

Please enter password to restore hidden files :
bukti7.wav

Trial

□ Mask the password

Help

All file crypted with a Trial version are crypted with the password 'trial'.

Fig. 17. Confidential Password Files were Found.

Information regarding the confidential files that have been found is shown in Table IV.

F. Presentation Results

After the analysis process on digital evidence was carried out using Stegspy and Hiderman, digital evidence was obtained on the flash disk image file as in Table V. Based on the process of detecting and extracting digital evidence, secret messages regarding delivery schedules are found.

TABLE IV. CONFIDENTIAL FILE INFORMATION FOUND

Message Name	**Format**	**Size**	**Hash (MD5)**
Message1	.txt	1 kb	AADCCD6FD16370F7DDB14DFAEE213BB0
Message2	.txt	1 kb	72C2E79FBA5225F3C5BE3F734795EADF
Message3	.txt	1 kb	A86BB86287E005045AF4C4AD32650732
Message4	.txt	1 kb	94305EEE69C737D258A5B81646F328A9
Message5	.txt	1 kb	A4871E4D6B386E29AF2FCD2025189753
Message6	.txt	1 kb	F500126EE1EB22DD402B8100556EBE95
Message7	.txt	1 kb	2C35E96B69903883A6731F838699309A
Message8	.txt	1 kb	BD41F794F04DEA470F1ACD38FD05877D
Message9	.txt	1 kb	FA1ABD78B1A8D5FD06E7EC36EE18AF6A
Message10	.txt	1 kb	A5C0B0FE889FC53B4CC4AEB7E97831AF
Message11	.txt	1 kb	FF73BBFDBBCB24B59A01FABF2C15ADBD
Message12	.txt	1 kb	D4E4D9DD9B2F1561C3B0D1C02DC34A85
Message13	.txt	1 kb	2D537F93BBB4D61857378E7403D9BA4A
Message14	.txt	1 kb	1Hw91XA9c1CuLKp9PhAt1ujZ963ZsagEBf
Message15	.txt	1 kb	C4ABF8E5D2A505B6A5F6CB2AD98E3795
Message16	.txt	1 kb	1Hw91XA9c1CuLKp9PhAt1ujZ963ZsagEBf
Message17	.ppt	553 kb	5A9A559EE1C31B8A1E0B60BB9164B053
Message18	.doc	16.2 kb	954D8897DE0774600DBD9356229575CA
Message19	.pdf	46.4 kb	25C6796DE638FB818825384BED0D539B
Message20	.pdf	365 kb	D6BF7444584D42C78E5477599188E071

TABLE V. PASTED MESSAGE

Container	**Secret file**	**Size**	**Message**
Evidence1.jpg	Message1.txt	1.07 mb	Monday, January 6, 2020. at 02.30.
Evidence2.jpg	Message2.txt	5.20 mb	Sunday, January 12 2020. Delivery at 04.30.
Evidence3.jpg	Message3.txt	766 KB	Thursday, January 30, 2020. Delivery at 23.30.
Evidence4.jpg	Message4.txt	2.42 MB	Saturday, March 14, 2020. Delivery at 19.30.
evidence6.wav	Message6.txt	2.5 MB	Thursday, April 16, 2020. Delivery at 20.30.
evidence7.wav	Message7.txt	1.02 MB	Saturday, April 18 2020. Delivery at 22.30.
evidence8.wav	Message8.txt	2.04 MB	Tuesday, April 28, 2020. Delivery at 17.30.
evidence9.wav	Message9.txt	4.98 MB	Friday, May 1, 2020. Delivery at 15.30.
evidence10.wav	Message10.txt	9.92 MB	Friday, 15 May 2020. Delivery at 15.30.
Evidence11.mp4	Message11.txt	7.46 MB	Monday, 25 May 2020. Delivery at 12.30.
Evidence12.mp4	Message12.txt	3.35 MB	Monday, 25 May 2020. Delivery at 12.30.
Evidence13.mp4	Message13.txt	854 KB	Sunday, 31 May 2020. Delivery at 13.30.
Evidence15.mp4	Message15.txt	2.64 MB	Wednesday, 3 June 2020. Delivery at 19.30.
Evidence11.mp4	Message11.txt	7.46 MB	Monday, 25 May 2020. Delivery at 12.30.

IV. CONCLUSION

The analysis process uses the static forensics method with the Generic Computer Forensic Investigation Model framework successfully implemented. The secret message that has been inserted using steganography technique was found steganographic messages in the form of stegotext. The success rate of the StegSpy forensic tool based on the detection process of digital evidence containing an average of 85% steganography and 15% unknown files. The accuracy of the Hiderman tool based on digital evidence that has been successfully extracted is 100%.

ACKNOWLEDGMENT

This research is supported by Directorat Riset dan Pengabdian Masyarakat, Direktorat Jenderal Penguatan Riset dan Pengembangan Kementerian Riset, Teknologi dan Pendidikan Tinggi Republik Indonesia. Surat Kontrak Pelaksanaan Penelitian Kementerian Riset dan Teknologi/Badan Riset dan Inovasi Nasional (KEMENRISTEK/BRIN) Tahun Tunggal Tahun Anggaran 2020 Nomor: PTM-027/SKPP.TT/LPPM UAD/VI/2020.

REFERENCES

[1] B. K. Payne and L. Hadzhidimova, "Disciplinary and interdisciplinary trends in cybercrime research: An examination," Int. J. Cyber Criminol., vol. 14, no. 1, pp. 81–105, 2020, doi: 10.5281/zenodo.3741131.

[2] A. Kurniawan, I. Riadi, and A. Luthfi, "Forensic analysis and prevent of cross site scripting in single victim attack using open web application security project (OWASP) framework," J. Theor. Appl. Inf. Technol., vol. 95, no. 6, pp. 1363–1371, 2017.

[3] L. L. Alaydrus and D. Nusraningrum, "Impact of Computer Misuse in the Workplace," KnE Soc. Sci., vol. 2020, pp. 1–7, 2020, doi: 10.18502/kss.v4i7.6838.

[4] A. Yudhana, I. Riadi, and F. Ridho, "DDoS classification using neural network and naïve bayes methods for network forensics," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 11, pp. 177–183, 2018, doi: 10.14569/ijacsa.2018.091125.

[5] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. J. Cano, "Digital forensic analysis of cybercrimes: Best practices and methodologies," Int. J. Inf. Secur. Priv., vol. 11, no. 2, pp. 25–37, 2017, doi: 10.4018/IJISP.2017040103.

[6] A. Jain and G. S. Chhabra, "Anti-forensics techniques: An analytical review," 2014 7th Int. Conf. Contemp. Comput. IC3 2014, no. August 2014, pp. 412–418, 2014, doi: 10.1109/IC3.2014.6897209.

[7] L. Widyawati, I. Riadi, and Y. Prayudi, "Comparative Analysis of Image Steganography using SLT, DCT and SLT-DCT Algorithm," MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput., vol. 20, no. 1, pp. 169–182, 2020, doi: 10.30812/matrik.v20i1.701.

[8] M. Khalid, K. Arora, and N. Pal, "A Crypto-Steganography: A Survey," Int. J. Adv. Comput. Sci. Appl., vol. 5, no. 7, pp. 149–155, 2014, doi: 10.14569/ijacsa.2014.050722.

[9] I. Riadi, A. W. Muhammad, and Sunardi, "Neural network-based ddos detection regarding hidden layer variation," J. Theor. Appl. Inf. Technol., vol. 95, no. 15, pp. 3684–3691, 2017.

[10] M. Dalal and M. Juneja, "Video steganalysis to obstruct criminal activities for digital forensics : a survey," vol. 10, no. 4, pp. 338–355, 2018.

[11] T. Sloan and J. Hernandez-Castro, "Forensic analysis of video steganography tools," PeerJ Comput. Sci., 2015, doi: 10.7717/peerj-cs.7.

[12] S. Rathore, "Steganography: Basics and Digital Forensics," Int. J. Sci. Eng. Technol. Res., vol. 4, no. 7, pp. 2589–2593, 2015.

[13] K. K. Sindhu and B. B. Meshram, "Digital Forensics and Cyber Crime Datamining," J. Inf. Secur., 2012, doi: 10.4236/jis.2012.33024.

[14] A. Iswardani and I. Riadi, "Denial of service log analysis using density K-means method," J. Theor. Appl. Inf. Technol., vol. 83, no. 2, pp. 299–302, 2016.

[15] Sunardi, I. Riadi, and A. Sugandi, "Forensic analysis of Docker Swarm cluster using GRR Rapid Response framework," Int. J. Adv. Comput. Sci. Appl., 2019, doi: 10.14569/ijacsa.2019.0100260.

[16] K. K. Sindhu and B. B. Meshram, "Digital Forensic Investigation Tools and Procedures," Int. J. Comput. Netw. Inf. Secur., vol. 4, no. 4, pp. 39–48, 2012, doi: 10.5815/ijcnis.2012.04.05.

[17] I. Riadi, R. Umar, and I. M. Nasrulloh, "Digital Forensic Analysis On Frozen Solid State Drive Using National Institute of Justice (NIJ) METHOD," Elinvo (Electronics, Informatics, Vocat. Educ., 2018, doi: 10.21831/elinvo.v3i1.19308.

[18] M. Rafique and M. N. A. Khan, "Exploring Static and Live Digital Forensics: Methods, Practices and Tools," Int. J. Sci. Eng. Res., 2013.

[19] Sunardi, I. Riadi, and M. H. Akbar, "Application of Static Forensics Method for Extracting Steganographic Files on Digital Evidence Using the DFRWS Framework," Rekayasa Sist. dan Teknol. Inf. (RESTI), vol. 4, no. 3, pp. 576–583, 2020.

[20] A. Yudhana, I. Riadi, and I. Anshori, “Facebook Messenger Digital Evidence Analysis Using Nist Method,” IT J. Res. Dev., 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[21] D. Mugisha, “DIGITAL FORENSICS : Digital Evidence in judicial System,” no. April, 2019.

[22] S. H. Belshaw, “Next Generation of Evidence Collecting: The Need for Digital Forensics in Criminal Justice Education,” J. Cybersecurity Educ. Res. Pract., vol. 1, no. 3, 2019.

[23] E. K. J. Melanie, M. V. Naseri, and N. A. B. Sabri, “Image forensics tool with steganography detection,” J. Crit. Rev., vol. 7, no. 3, pp. 130–134, 2020, doi: 10.31838/jcr.07.03.24.

[24] A. P. Saputra and N. Widiyasono, “Forensic Digital Analysis of Steganographic Files (Case study: Drug Trafficking),” J. Tek. Inform. dan Sist. Inf., 2017, doi: 10.28932/jutisi.v3i1.594.

[25] Y. B. Utomo and D. Erwanto, “Analisa Teknik Steganografi dan Steganalysis Pada File Multimedia Menggunakan Net Tools dan Hex Editor,” Gener. J., vol. 3, no. 1, pp. 16–22, 2019, doi: 10.29407/gj.v3i1.12698.

[26] V. A. Silalahi and I. Sembiring, “Digital Forensics Investigation Analysis on Digital Steganographic Evidence,” Artik. Ilm., 2017.

[27] I. A. Yari and S. Zargari, “An Overview and Computer Forensic Challenges in Image Steganography,” in Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017, 2018, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.60.

[28] Y. Yusoff, R. Ismail, and Z. Hassan, “Common Phases of Computer Forensics Investigation Models,” Int. J. Comput. Sci. Inf. Technol., vol. 3, no. 3, pp. 17–31, 2011, doi: 10.5121/ijcsit.2011.3302.