

Web Forensics Evidence System

Mr. Suchith Narayan¹, Mr. Tarun R², Mr. R Purushotham³, Prof. Hemavathi P⁴

^{1,2,3}B. E Students, Department of Computer Science and Engineering, Bangalore Institute of Technology, Bengaluru, India

⁴Assistant Professor, Department of Computer Science and Engineering, Bangalore Institute of Technology, Bengaluru, India

Abstract - Collection and Storage of confidential digital data and information is a challenging task. In this paper, we propose a System-Web Forensics Evidence System (WEBFES) that collects and secures digital evidence for submission to the court. A target is cloned to get the state of the website and its files. The user specified URL is crawled and the files are cloned. The complete website is downloaded and it can be accessed offline. To maintain integrity a hashing function is used and for confidentiality an encryption mechanism is used.

Key Words: Computer Forensics, Web Forensics Evidence System (WEBFES), Security, Crawl, Clone, Hash, Encrypt, Decrypt

1. INTRODUCTION

In today's fast paced world, organizations have to rely more and more on technology to remain competitive. Cyber Security is a major requirement to these organizations to protect information from online threats. Cybercrime may risk the security of personal data or may even pose threat to the security of a nation and its economy. Hacking, data breaches, copyright infringement, illegal use of data, identity theft etc., have become major threats.

The protection of hardware, software or data in a system is a challenging task with the increased rate of security threats. Therefore, to prevent damage or invasion of a system various security mechanisms can be used. Firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), can detect and prevent network attacks. Antivirus can protect a system from security threats. VPNs can be used to communicate over a secure channel.

Computer Forensics plays an important role when there is a cybercrime. They are responsible for collecting and storing evidence. They are also responsible for investigating where the attack had been originated and how much physical or economical damage the attack has caused to an individual or to a nation. Although computer forensics are majorly involved with the investigation of a cybercrime, they can also be used in court proceedings.

Any digital evidence submitted to the court must be genuine, reliably obtained, and admissible. When there is a security incident on a website, our system collects digital evidence and ensures that it can be securely submitted to the court by the computer forensic organizations.

The web forensic evidence system proposed in this paper provides an approach to crawl, clone, hash, and encrypt evidence. Authenticity of the evidence obtained from this system is ensured by recording the screen during the complete process execution.

2. PROPOSED SYSTEM

The website is cloned, therefore complete access to the website is achieved. Evidence cannot be tampered easily as it is hashed, encrypted and the complete session of evidence collection is recorded.

The Web Forensics Evidence System is initiated by providing an URL as a user input. This URL is stored in a file and it is then used to crawl. The URLs obtained when crawled are stored in the same file. Once the website is crawled, the cloner module downloads the URLs which are stored in the file. The downloaded files are stored in the same file structure that exists in the website. These files are stored as an offline copy of the website.

The offline copy is hashed to maintain integrity. Every file in the offline copy is then encrypted by a user key (E-1). The encrypted files are then zipped into a single file. The zipped file undergoes another layer of encryption by a combination of the user key (E-1) and the hash of encrypted files (HL-1) and the user key (E-2). The encrypted files hence obtained is the secured evidence.

When the evidence is presented in the court, it is decrypted to access the files. The evidence is decrypted by a combination of E-2 key, E-1 Key, Hash (HL-1). The file is then unzipped and undergoes another layer of decryption by user key (E-1) to obtain the digital evidence.

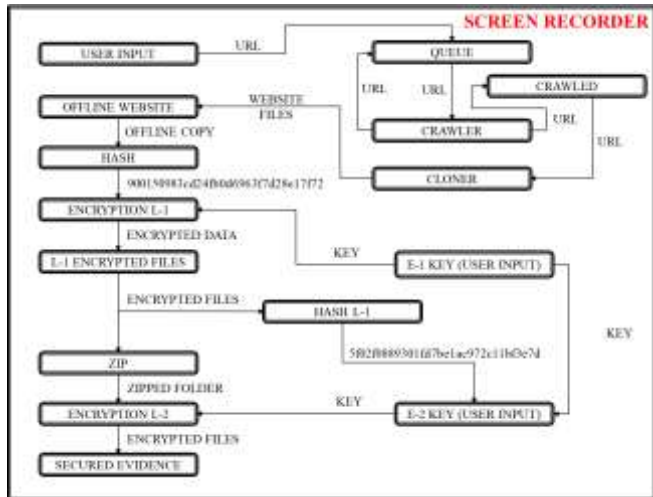


Fig -1: Gathering and Securing Evidence using WEBFES

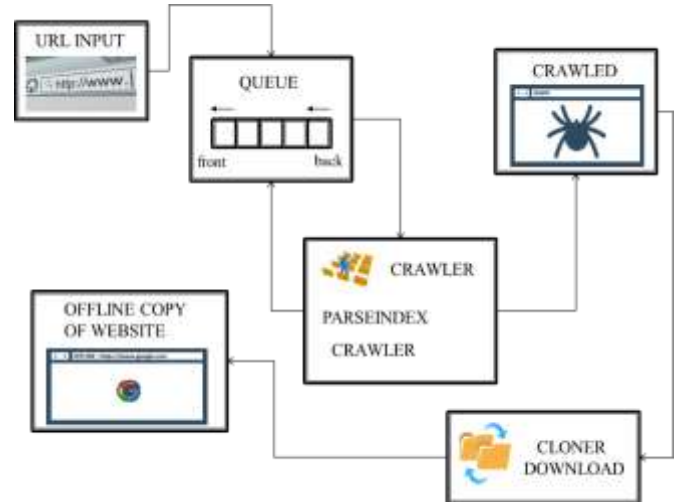


Fig -4: Cloner

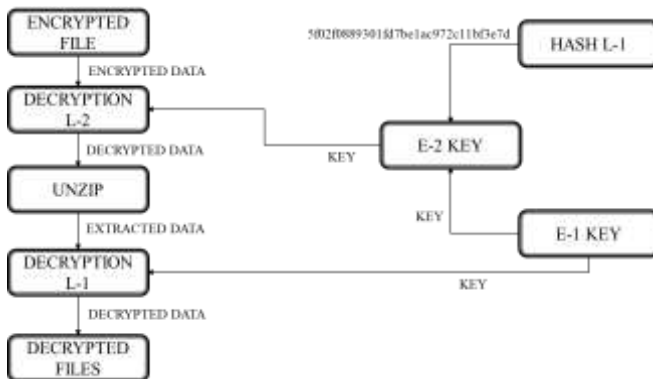


Fig -2: Decrypting the Secured Evidence using WEBFES

3.2 Hash

A hashing algorithm uses files to generate a hash to maintain integrity of the document. It is used to avoid the tampering of evidence. Hashing is implemented in two phases:

Phase 1: Evidence gathered is hashed to get a single hash value.

Phase 2: During verification evidence is again hashed and the hash generated is compared with the hash generated in Phase 1.

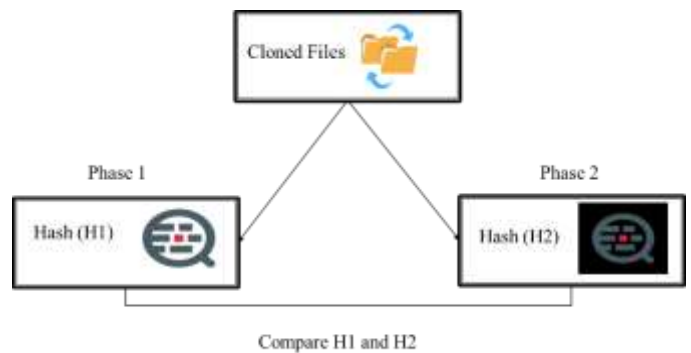


Fig -5: Hash

3. ARCHITECTURE

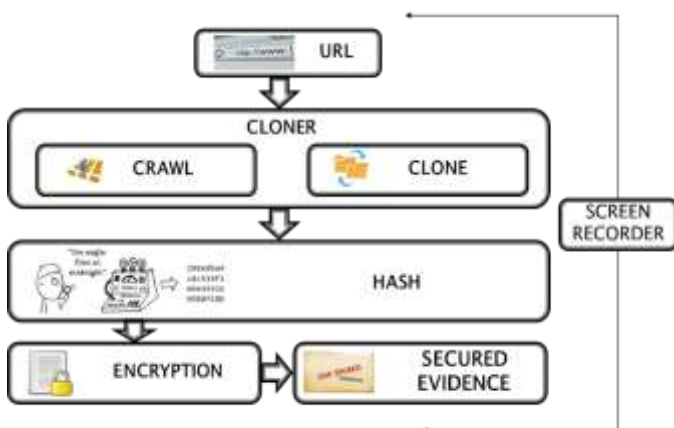


Fig -3: Architecture of WEBFES

3.1 Cloner

Cloner has two sub modules crawl and clone. Crawl is used to parse the given URL to find all possible URLs of the website. Clone is used to copy those crawled files for offline use.

3.3 Encryption

An encryption algorithm is used to maintain the confidentiality of the documents.

A dual layer encryption is implemented:

Layer 1: Every individual file is encrypted.

Layer 2: The complete folder is encrypted into a single file.

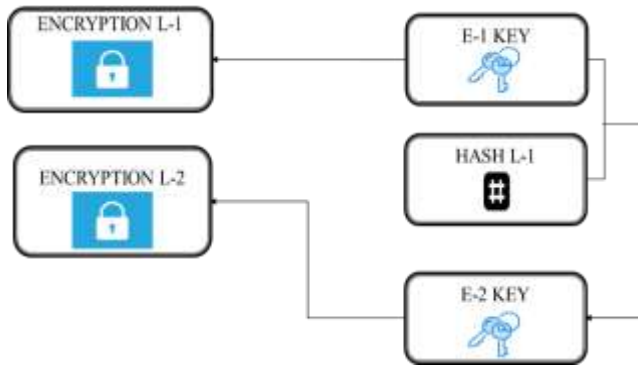


Fig -6: Encryption

3.4 Decryption

E-1 key is entered by User 1 to decrypt layer 1.

E-2 key is entered by User 2. E-1 key and hash is used to decrypt layer 2.

The folder with all the contents is obtained after decryption.

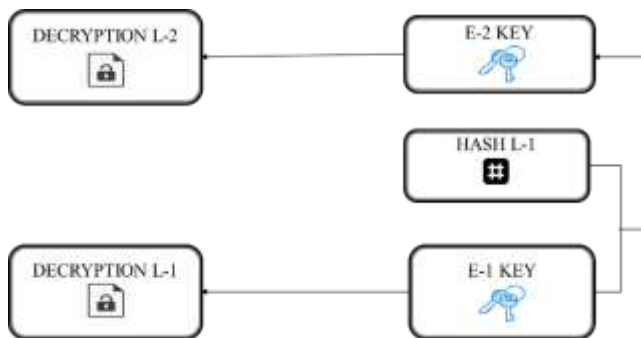


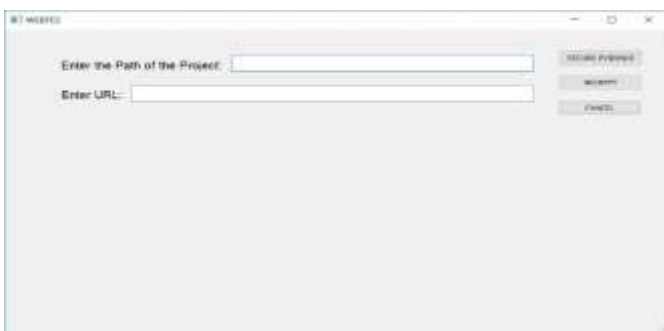
Fig -7: Decryption

3.5 Screen Recorder

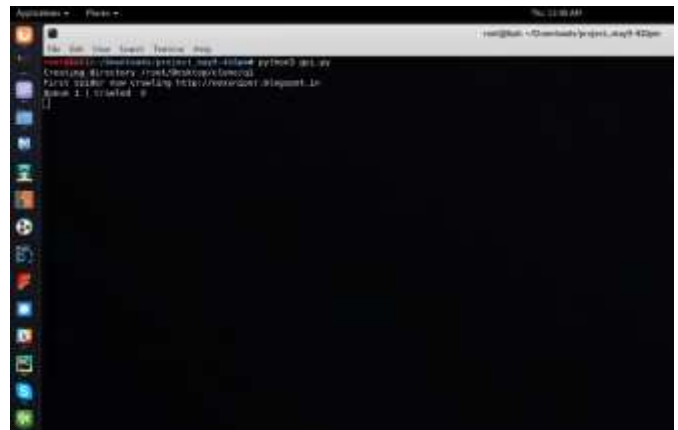
The recording begins when the application is started. The complete session is captured in .avi format. All the phases of this tool is recorded to ensure integrity of the process. The recording stops when the application terminates.

4. RESULTS

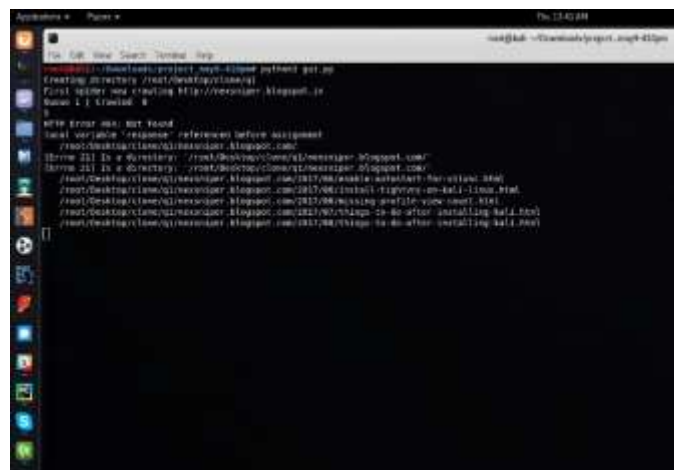
4.1 User interface



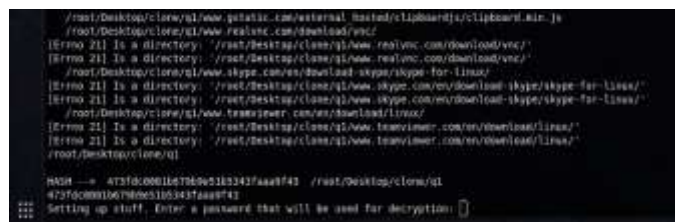
4.2 Crawler



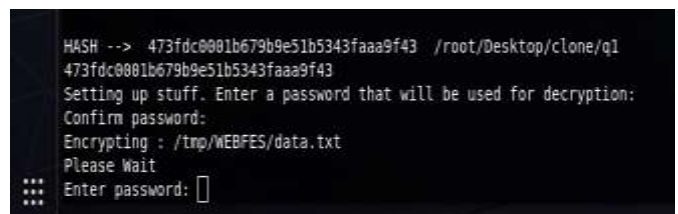
4.3 Cloner



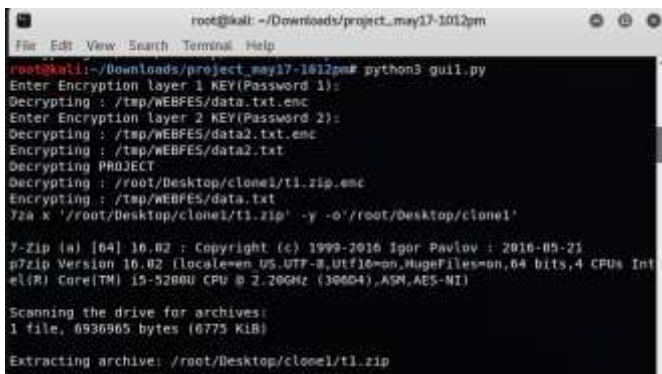
4.4 Hash



4.5 Encryption



4.6 Decryption



```
root@kali: ~/Downloads/project_may17-1012pm
File Edit View Search Terminal Help
root@kali:~/Downloads/project_may17-1012pm# python3 gui1.py
Enter Encryption layer 1 KEY(Password 1):
Decrypting : /tmp/WEBFES/data.txt.emc
Enter Encryption layer 2 KEY(Password 2):
Decrypting : /tmp/WEBFES/data2.txt.emc
Encrypting : /tmp/WEBFES/data2.txt
Decrypting PROJECT
Decrypting : /root/Desktop/clone1/t1.zip.emc
Encrypting : /tmp/WEBFES/data.txt
7za x '/root/Desktop/clone1/t1.zip' -y -o'/root/Desktop/clone1'

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,utf16=on,hugefiles=on,64 bits,4 CPUs Intel(R) Core(TM) i5-5200U CPU @ 2.20GHz (39864),ASM,AES-NI)

Scanning the drive for archives:
1 file, 6936965 bytes (6773 KiB)

Extracting archive: /root/Desktop/clone1/t1.zip
```

5. CONCLUSIONS

Preventing security threats and data breaches is important for forensic organizations which manage digital evidence.

The proposed tool collects and stores digital evidence securely by hashing and encrypting the files, and also by recording the complete usage of this tool to prevent evidence tampering.

The security of the digital data obtained from this tool is ensured and submitted to the court as evidence.

REFERENCES

- [1] Taher Ahmed Ghaleb, "Website Fingerprinting as a Cybercrime Investigation Model: Role and Challenges", IEEE, 2015.
- [2] Asaf Varol, Yessim Uleen Sonmez, "Review of Evidence Analysis and Reporting Phases in Digital Forensics Process", IEEE, 2017.
- [3] Parameshwaran Nampoorthiri V, N.Sugitha. "Digital Image Forgery-A threaten to digital forensics", IEEE, 2016.
- [4] Cornell Walker, "Computer Forensics: Bringing the Evidence to Court", IEEE, 2016.