International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 05 Issue 02 | 2021

Adding Admissibility of Digital Evidence in Court of Law

Anand V[1], Dr. M N Nachappa[2]

[1] Masters in Computer Application Scholar, Department of MCA, School of CS & IT, Jain (Deemed-to-be) University, Bangalore, Karnataka, India

[2] Head of Department, Department of MCA, School of CS & IT, Jain (Deemed-to-be) University, Bangalore, Karnataka, India

ABSTRACT

Almost 80% cases in India fail due to lack of adequate systematic support and non-admissibility of evidence in the court of law. It applies even in the field of Cyber Forensics and Cyber Evidence also. computer forensics has risen to the fore as an increasingly important method of identifying and prosecuting computer criminals. Prior to the development of sound computer forensics procedures and techniques, many cases of computer crime were left unsolved. There are many reasons why an investigation might not lead to a successful prosecution, but the predominant one is a lack of preparation. The organization investigating the suspicious behavior often lacks the tools and skills required to successfully gather evidence. Individuals attempting to investigate such suspicious activity may also lack the financial resources financial resources or tools to conduct such an investigation adequately and ensure that the evidence is undisputable in all circumstances. Moreover, there are instances when all of the above have been adequately put in place by an organization, but, due to a lack of training and correct procedure, the evidence collected can easily be disputed.

Keywords: - Cyber Forensics, Cyber Evidence, Investigation, MD5, Fingerprinting

1. INTRODUCTION

It is a known and disappointing fact that not all the subjects of court of law are not adapting to the fast-changing technology and are still stuck with old/traditional means. The main reason is that their field of expertise is justice and law and not technology, so it's hardly their mistake. But the field of Cyber Forensics is different i.e., it is an integration of both law and technology. A Cyber Forensic Expert will be assigned to any case relating to a Cyber Crime or a Normal Crime where technical experience is necessary in order to go further at the court of law. The Forensic Expert can either be from the Police Force or a recognized individual working under a recognized department [1].

One of the objectives of the Cyber Forensic Expert is to analyze and extract information from a device or computer system as evidence to be presented at the courts and concerned authorities. Extracting evidence from anywhere might not be an issue. The real issue is the risk of not getting it admissible at the court of law or getting rejected due to strong support. There has arose situations in the past where the evidence once accepted got rejected later. Well, in the case of cyber evidence the risk tends to be more, since the data is not physical and has chances to get deleted, changed and manipulated. The cyber security concepts of integrity and non-repudiation are the main factors and objectives of this research.

The cyber forensic analyst should be able to prove that the data/evidence extracted is real and has not been tampered with, and Forensic Expert/Team is presenting it at the court in its original form, i.e., the way it was at the time of collecting the data itself. Suppose if it comes a situation where the suspect or client whose computer was used for extracting information 'denies' that the respective evidence is not from the suspect's computer, the cyber forensic expert must be able to prove so. The objective at that time is to prove that the evidence the expert presented is intact the one which the suspect is alleging to fake.

Once the Cyber forensic team expert proves that their side is true, it will give more support to the case and less chances to rejections in the future. More than anything else, the integrity of the cyber forensic officer is maintained in front of the court of law and the police force and other subjects concerned with that particular case. This will encourage the forces to lend the same team more similar cases to work with. This also motivates others and encourages them 'to go with the tide', i.e., taking advantage of emerging technologies to the maximum benefits rather than sticking to the old and outdated ways.

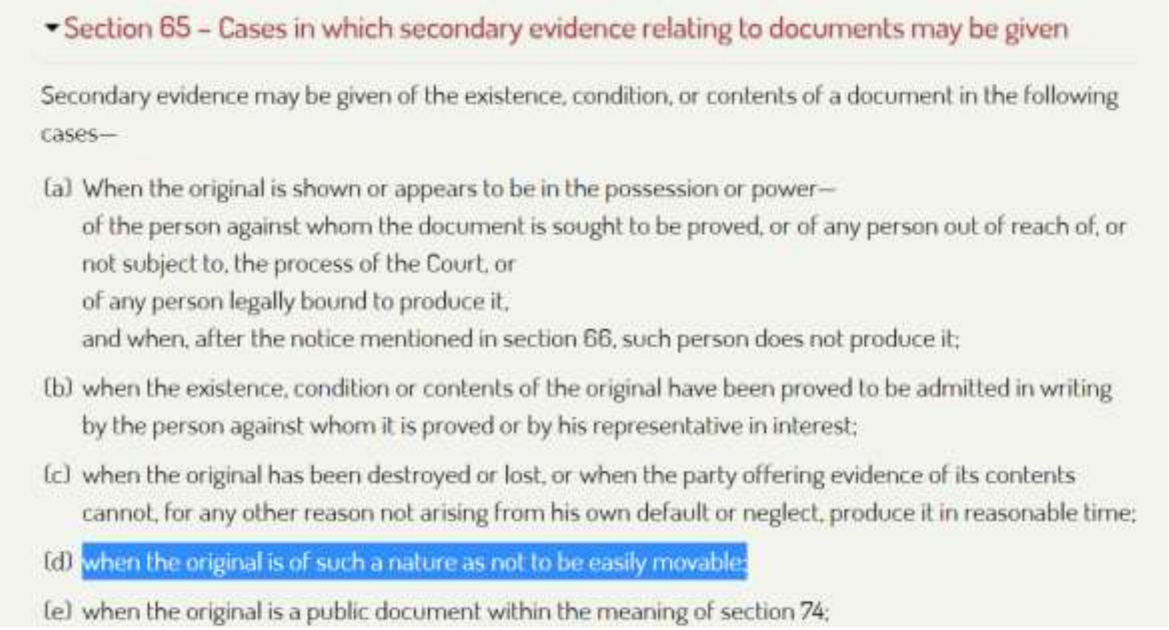
2. LITERATURE REVIEW

The methods of Computer/Digital Forensics have evolved ever since its inception and it has been continuously evolving ever since its inception. The main objective of evidence collection through digital forensics is to make the evidence admissible at the court of law. But due to many reasons, the evidence tends to have lack to admissibility. Due to lack of admissibility, it may get rejected in the court. In this paper a three-phase framework has been used so that the evidence will have admissibility anywhere.

The proposed framework contains three stages. The preparation stage, investigation stage and presentation stage. The preparation stages include terms such as Procedures, Standards and Policies used, Training given to subordinates, Legal advice from legal teams, Checking up with authorities and Planning. The investigation stage includes, Searching and identifying information from computer. Collection after identification. Moving evidence to a safe location and storage. Examining and analyzing the evidence. The final stage which is the presentation stage is presenting the analysis study and proving its originality in the court of law.

2.1 "The Indian Evidence Act, 1872" - https://legislative.gov.in/sites/default/files/A1872-01.pdf

- Sec 64 - Proof of documents by primary evidence. Documents must be proved by primary evidence except in the cases hereinafter mentioned
- Sec 65b - Admissibility of electronic records – Provisions
- In this case a digital signature or proof that the evidence is collected from the client/suspects computer itself and not from any other person, so that the former should not deny it in the court of law



Section 65 – Cases in which secondary evidence relating to documents may be given

Secondary evidence may be given of the existence, condition, or contents of a document in the following cases—

(a) When the original is shown or appears to be in the possession or power—
of the person against whom the document is sought to be proved, or of any person out of reach of, or not subject to, the process of the Court, or
of any person legally bound to produce it,
and when, after the notice mentioned in section 66, such person does not produce it;

(b) when the existence, condition or contents of the original have been proved to be admitted in writing by the person against whom it is proved or by his representative in interest;

(c) when the original has been destroyed or lost, or when the party offering evidence of its contents cannot, for any other reason not arising from his own default or neglect, produce it in reasonable time;

(d) when the original is of such a nature as not to be easily movable;

(e) when the original is a public document within the meaning of section 74;

Figure 1: Section 65b of Indian Evidence Act [9]

Thus, in shorts, according to the 65b of Indian Evidence Act, which deals with the admissibility of electronic evidence, the secondary evidence can be presented at the court of law if the primary evidence is not easily movable or available at ease. A proof is necessary that the evidence extracted is in fact from the primary evidence, in this case, the suspects computer and the it is secondary evidence which can be accepted as document.

2.2 Hash Function

Hash function is a mathematic function that maps and converts any data into a fixed size alphanumeric value also known as checksum. The alphanumeric value will be unique to that data or piece of information and to that information only. Even a single bit of information is changed, it will change the whole hash value. Mostly Hashing is used for storing the passwords in online databases and for checking data integrity. Examples of hash functions are MD5 (Message Digest 5), SHA (Secure Hash Algorithm). MD5 is a 128-bit hash function and fastest but provide less integrity when compared to SHA. The SHA has different standards such as SHA-0, SHA-1, SHA-2, SHA-3.

3. METHODOLOGY

Adequate knowledge in command prompt and software signatures of the computer is enough. Using Python programming language is recommended. But experts are free to choose any programming language as the end result is given importance not the language used.

- Ensure the presence of a recognized person assigned by the law and enforcement, while working on the suspect's computer, that person can give statement for the expert at the court if the former is being questioned regarding their work of collecting evidence.
- Take photos of the Desktop computer, model numbers, serial numbers printed on back side of laptops etc. Take Screenshots of your works also. This is to make sure that the suspect should not change/misplace the target device if it is demanded to present the system, physically at the court.
- While working on the suspect's/client's system, note down the unique ids, elements of the system such MAC address and product ids. For this command prompt can be used, terminal in the case of Linux operating systems. Note that these ids are unique to that systems and that system only, something which cannot be changed that easily or hidden
- The choice to choose which function is up to the cyber forensic analyst according to the size of the evidence extracted and importance of integrity in the evidence.

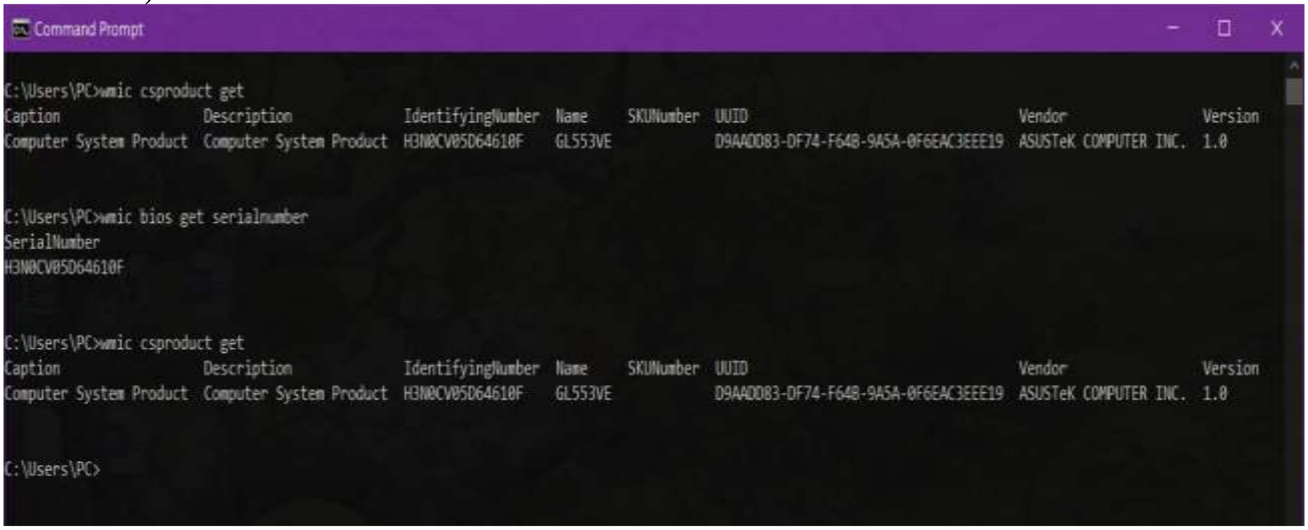
Command to get MAC address – `getmac`

Even though there is risk of mac address spoofing, noting it down is recommended

Command to get Unique product id's – `wmic csproduct get`

One example of this practices which can be followed as below

- Identifying the information which is to be extracted and has potential chance of admissibility at the court of law.
- Combining the digital evidence archive and the unique id values and run a Cryptographic hash function. (MD5 or SHA).



```
C:\Users\PC>wmic csproduct get
Caption                  Description              IdentifyingNumber  Name     SKUNumber  UUID                                  Vendor                 Version
Computer System Product  Computer System Product  H3N0CV05D64610F    GL553VE             D9AADD83-DF74-F64B-9A5A-0F6EAC3EEE19  ASUSTeK COMPUTER INC.  1.0


C:\Users\PC>wmic bios get serialnumber
SerialNumber
H3N0CV05D64610F


C:\Users\PC>wmic csproduct get
Caption                  Description              IdentifyingNumber  Name     SKUNumber  UUID                                  Vendor                 Version
Computer System Product  Computer System Product  H3N0CV05D64610F    GL553VE             D9AADD83-DF74-F64B-9A5A-0F6EAC3EEE19  ASUSTeK COMPUTER INC.  1.0


C:\Users\PC>
```

Figure 2: Finding the Unique id of the system

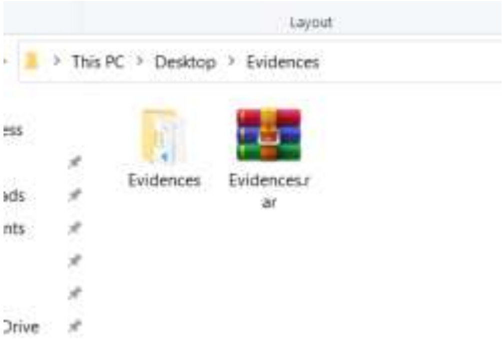
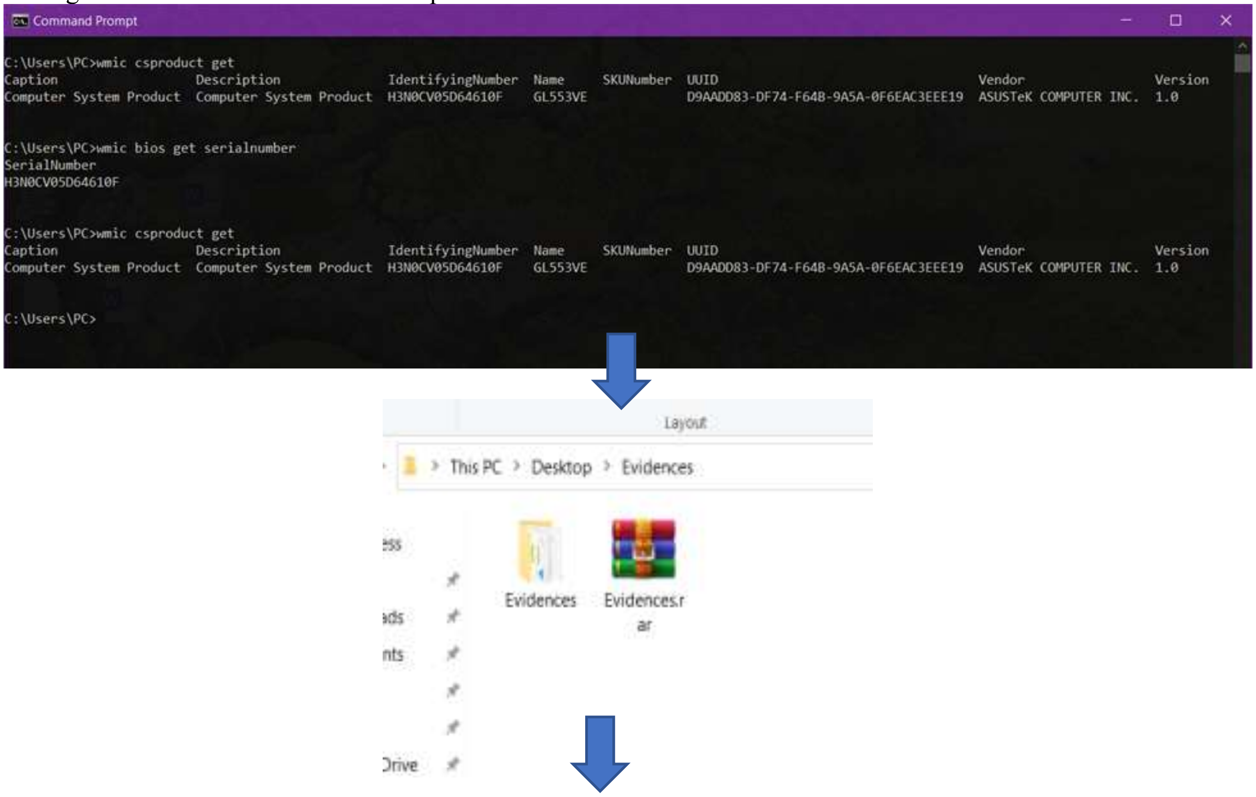


Figure 3: Archived Evidence

4. RESULTS AND DISCUSSION

After combining both and running an MD5 algorithm written in any programming language, an MD5 hash can be created. That hash value can be generated only be generating by using both evidence and the unique values, thus linking the evidence to the device's unique ids.



```
C:\Users\PC>wmic csproduct get
Caption                  Description              IdentifyingNumber  Name     SKUNumber  UUID                                  Vendor                Version
Computer System Product  Computer System Product  H3N0CV05D64610F    GL553VE             D9AADD83-DF74-F64B-9A5A-0F6EAC3EEE19  ASUSTeK COMPUTER INC.  1.0

C:\Users\PC>wmic bios get serialnumber
SerialNumber
H3N0CV05D64610F

C:\Users\PC>wmic csproduct get
Caption                  Description              IdentifyingNumber  Name     SKUNumber  UUID                                  Vendor                Version
Computer System Product  Computer System Product  H3N0CV05D64610F    GL553VE             D9AADD83-DF74-F64B-9A5A-0F6EAC3EEE19  ASUSTeK COMPUTER INC.  1.0

C:\Users\PC>
```

Sample hash checksum - 6219b1bc3542949e012616059409f1cc

- Suppose if it comes a situation where the suspect denies that the particular piece of information is not from the suspect's system and says that the Forensic expert tampered/altered the evidence or is giving a false evidence to trap the suspect.
- Then the algorithm can be re-executed on the same system with the same evidence archive file.
- The hash value noted down at the time of extraction can be compared and it will produce the same result, as hash value can never be mimicked and also the unique values of the pc cannot be altered.
- Even a slight change in content would've changed the whole hash value.
- Thus, the forensic expert can establish that the data presented at the court is in fact from the suspect's PC.
- The forensic expert can present the photos/screenshots mentioned earlier and a statement from the recognized individual from the police force assigned to the forensic expert to add more integrity to their claim.

5. CONCLUSION

As the number of users of digital resources are increasing day-by-day, cybercrimes are also increasing. Now-a-days a large chunk of evidence can be found on the digital devices itself. As this research was from the point of view of a cyber forensic expert, the objectives are considered and studied. One of the main objectives of the expert is to present the evidence in the court in such a way that it will not get rejected even if it has matter to it. Through a simple and small way, the admissibility of evidence was increased to a little extend. Even though it may not be hundred perfects, something is better than nothing. Integrating aspects from different fields is always recommended and encouraged. This will motivate others to gain more knowledge on the technical aspects and using it to combat cybercrime. As the cyber criminals gain more knowledge on how to perform new malicious activities and getting away with scot-free, we must also try to gain more knowledge and use some unexpected tricks up our sleeves to prevent them.

6. REFERENCES

[1] Ananthanarayanan, G., Blagsvedt, S., & Toyama, K. (n.d.). OWeB: A Framework for Offline Web Browsing.

[2] Certified Forensic Computer Examiner. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Certified_Forensic_Computer_Examiner

[3] Department, I. L. (n.d.). The Indian Evidence Act,1872. Retrieved from https://legislative.gov.in/sites/default/files/A1872-01.pdf.

[4] Evidence, S. W. (n.d.). Best Practices for Computer Forensics.

[5] Kohn, M., Eloff, J., & Olivier, M. (n.d.). Framework for a Digital Forensic Investigation. Information and Computer Security Architectures Research Group (ICSA).

[6] Mehta, D. S. (2012). Cyber Forensics and Admissibility of Digital Evidence. The Practical Lawyer.

[7] Redhat. (n.d.). Retrieved from Generating a New Unique MAC Address: access.redhat.com

[8] Rivest, R. (1992, April). The MD5 Message-Digest Algorithm. MIT Laboratory for Computer Science.

[9] Unique Device Identification. (n.d.). Retrieved from WikiPedia: https://en.wikipedia.org/wiki/Unique_Device_Identification

[10] Yasinsac, A., Erbacher, R., Marks, D., Pollitt, M., & Sommer, P. (2003, July-Aug). Computer forensics education. IEEE Security & Privacy.