NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 4, Issue – 2, December 2025
E – ISSN – 2583-7559

A Critical Introspective Analysis of Hash Value Calculation Tools

An Investigative Approach

Dr. Rajesh Kumar[1]
[1]Certified Cyber Expert,
Digital Investigation Lab,
Cyber Crime & Security Unit, Bihar, Patna
rajesh.kumar81@nic.in

Ritwik Tripathi[2]
[2]Senior Cybersecurity Engineer,
ZDTA, ZDTE, ZDDC, OpenAI Cyber Deployment certified
Cognizant Technology Solutions, Pvt. Ltd. Noida, UP.
tripathi.ritwik@gmail.com

***Abstract*— Hash values play a vital role in maintaining the integrity of electronic evidence. The New Bhartiya Shakshya Adhiniyam in India mandates the generation of hash values for all electronic evidences. While numerous software, hardware, applications, and online platforms are available for this purpose, concerns remain regarding their accuracy, efficiency, degree of confidentiality and user-friendliness, particularly for non-technical law enforcement personnel at crime scenes. This paper evaluates three widely used hash value generation tools: Software, Offline Applications, and online platform, focusing on their performance on different parameters / criteria with SHA-256 hash value generation. The evaluation criteria include accuracy, as determined through lab testing; user friendliness, assessed through usability analysis; efficiency, tested through time variations while testing; data confidentiality; incorporated through data safety over tool usage; and an empirical study survey analysis, conducted through Google Forms among key stakeholders. The results show that HashCalc is the most balanced and ideal usage tool for law enforcement personnel, maintaining the integrity and evidentiary value of electronic evidence.**

Keywords*— Hash Value, HashCalc, Electronic Evidence, Bhartiya Shakshya Adhiniyam, Data Integrity, Data Confidentiality.

I. INTRODUCTION

Evidence presented before the court of law is a deciding factor in every conviction or acquittal, but their admissibility and appreciation are dependent upon the integrity of evidence presented. The traditional forms of evidences like oral testimonies from witnesses and other physical forms of evidence present at a crime scene are often viewed with uncertainty by the judiciary. The new era of digital age where crimes are evolving rapidly in the cyber space possess a new set of challenges for the judges to make a decision and has made oral or documentary evidence seemingly insufficient to arrive on judgements on critical cases [12]. This has led to the increased reliance on electronic evidence by the Law enforcement agencies and the judicial system. Electronic evidence is highly appreciated by judicial justice system as the integrity of digital evidence can be easily measured by different formats of Hash Values [9]. This concurs with the "Bhartiya Shakshya Adhiniyam" (New Indian Law) as it mandates the collection of Hash Value of every electronic evidence found at a crime scene or encountered during investigation [6,11].

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) certainly defines a new revolutionary shift on how evidence handling should be prioritized and protected by altering the fundamental procedures on device admissibility [11,12]. This new law replaces the Indian Evidence Act of 1872 and recognizes the impact of electronic evidence on the case proceedings which has further helped in modernizing the legal framework with a more streamlined approach while maintaining the core principles of authenticity and integrity [11,12]. The new Adhiniyam aims to simplify the procedure of submitting various forms of digital records, such as, documents, emails, social media posts and multimedia files. [1,12].

A hash value, produced by a hash algorithm acts as a distinctive digital identity of the electronic documents, and serves as a critical data integrity assurance mechanism [2,14]. It is a fixed-length string that goes under immense transformation if the original input is modified with just by one character, a phenomenon referred to as Avalanche Effect. [2] This attribute the hash values to validate the integrity of evidence, allowing for the verification that a document has not been tampered with since its creation [9]. While the concept of a 'hash value certificate' is now standardized, the secure storage of these values, along with associated metadata, serves as proof of the electronic record's genuineness [12].

Section 63(4)C of Bhartiya Shakhya Adhiniyam has provided a standardized hash value certificate [11].

The importance of the hash values has increased rapidly in Indian judicial system, as it is the cornerstone of establishing the authenticity and integrity of electronic. Not only it provides a verifiable digital fingerprint, it also ensures that digital evidence meets the stringent standards of reliability required for court admissibility, particularly under Section 63(4)C of BSA. [3,13].

Section 63 of the BSA has added a new dimension to the admissibility procedure for the electronic evidence by introducing a joint certificate, a part A and part B certificate [1,11]. Part A is completed by the individual filing the evidence and focuses on the basic details such as Serial No., Device name, etc. [1,11] Whereas, part B has to be filed by a qualified professional for the evidence [1,13]. The new method maintains a structured approach by ensuring both

informative and technically validated evidence is presented before the court. Section 63(4)(c) crucially establishes that an expert's statements within Part B of the certificate constitute evidence, thereby solidifying their role in verifying the integrity and authenticity of electronic records [1,13].

II. Hash Functions and SHA256

A hash function is a mathematical formula which takes a variable input like a tiny sentence or this whole manuscript and produces a fixed length string comprising of hexadecimal characters [2,14]. Every file or document stored in electronic storage device such as a laptop, workstation, mobile device, etc. will contain application metadata inside it and would be the variable input for any hash function which will be further transformed into a hash value [12]. As pointed out in earlier section, even a small change to the file or document would result in a catastrophic change to the application metadata and further the hash value (referred to as Avalanche effect). [2] All these things explain how much significance and weight hash values carry and eventually are being utilized as a measure towards one of the rudimentary principles of the CIA (Confidentiality, Integrity, Availability) triad. These play an important role in forensic investigation for proving accuracy of digital data before judiciary as well [4,16].

The SHA-256 hash function processes a 512-bit message block using 32-bit words in the message schedule and employs 64 rounds in the compression function to produce a 256-bit hash value [2,14]. SHA-256 algorithm is widely renowned and utilized for digital signatures (particularly signing digital certificates for TLS protection), authentication, password storage, verification, etc. [2,14].

Digital forensics involve a six-stage procedure including the acquisition of digital evidence and analyzing the image of the original evidence created during acquisition [7,15]. While the process of acquiring an image of a file or document takes place, software tools such as FTK Imager, Cellebrite UFED or Magnet Axiom automatically generate a hash value for the captured image [9,16]. This can further be compared against the original value of the source file to confirm integrity [9,10].

The acquisition hash refers to the hash value computed from the original source device at the time of imaging and serves as a baseline reference [9,15]. On the other hand, the verification hash is generated post the acquisition phase to confirm that the digital evidence has remained unaltered during handling and analysis [8,16]. The similarity of these two values confirms that the data has not been tampered, and points to the fact that the integrity of the evidence is maintained. [5,9]

III. Testing Methods and Variables

The researchers have used three different methods to calculate the hash values. The first approach uses the command prompt within a Windows based operating system (MS-DOS). The second method uses a dedicated software application, such as HashCalc, DevToys, HashMyFiles, etc. HashCalc has been selected as the software tool in this paper. The third method uses an online hash value calculator available at md5file.com, though various other online calculators such as md5online.com, Md5calc.com, calculatequick.com, etc. are available as well.

The parameters on which these methods will be evaluated are:

- Accuracy of the hash values generated
- Time efficiency of each method
- Overall user-friendliness of the tools, and
- Degree of data confidentiality

All evaluations conducted during the laboratory testing phase were carried out within a controlled environment. The setup ensured that any kind of external or internal interferences such as stable internet connectivity, proper installation of requisite software applications, physical isolation of the laboratory space, the use of dedicated systems, etc. to ensure the integrity of the results are maintained.

To ensure whether different computer systems would have an effect on any of the listed parameters, two separate computer systems with different hardware and software specifications have been employed as a part of this testing. System details are highlighted in Table I of this paper.

Table 1. System Configuration Comparison.

Configurations	System1	System2
RAM	8.00 GB	16.00 GB
Processor	Intel i5	Intel i7
HDD	2.00 TB	4.00 TB
Graphics Card	128 MB	4.00 GB
System Type	64-bit OS	64-bit OS
OS Spec	Windows 10 Pro	Windows 10 Pro

IV. Process Model Incorporated for Lab Testing.

A. Process Model for MS-DOS (Command Prompt) mode:

The process model which will be followed for MS-DOS mode is explained in the flow chart (Fig 1).

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 4, Issue – 2, December 2025
E – ISSN – 2583-7559

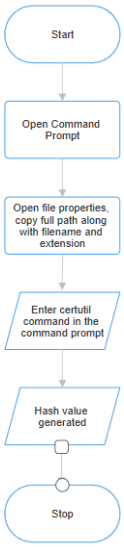


Fig 1. Process Model for hash value calculation using MS-DOS

The command prompt is opened (Fig 2).

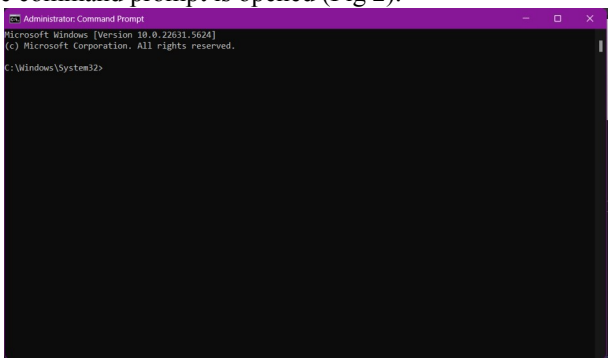


Fig 2. Open Command Prompt

Now, open the properties for the desired file and copy full path along with the file name and extension (Fig 3).

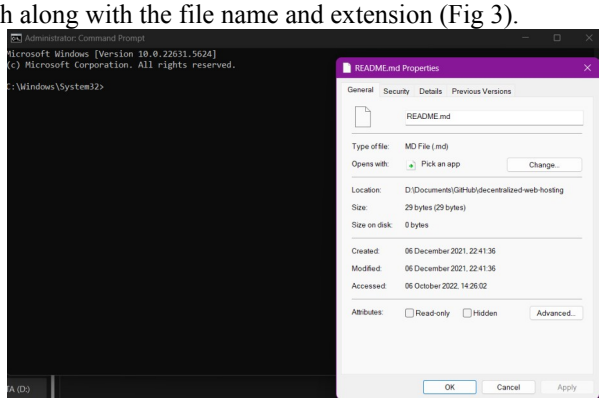


Fig 3. Open properties and copy file path

The certutil command will be used to calculate the hash value of the file. The syntax is shared below (Fig 4).

Syntax: [certtuil -hashfile "File Path\Filename.extension" Hash algorithm]

Command prompt supports various hash algorithm calculations like md5, SHA128, SHA256, SHA384, and SHA512.

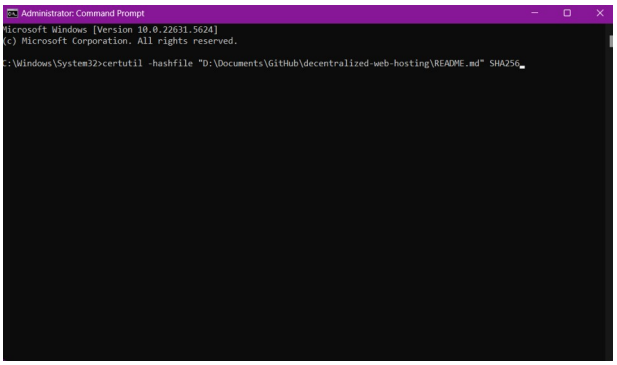


Fig 4. Enter command.

The calculated hash value will be displayed at the bottom.

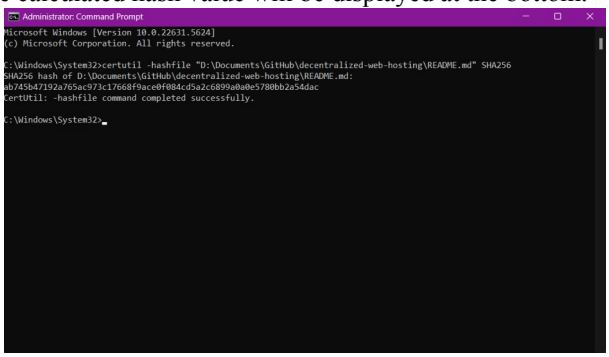


Fig 5. Hash Value generated

B. Process Model for HashCalc:

The process model which will be followed for HashCalc mode is explained in the flow chart (Fig 6).

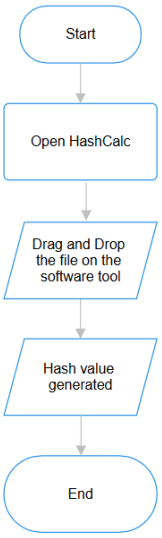


Fig 6. Process Model for hash value calculation using HashCalc

Launch the HashCalc application (Fig 7).

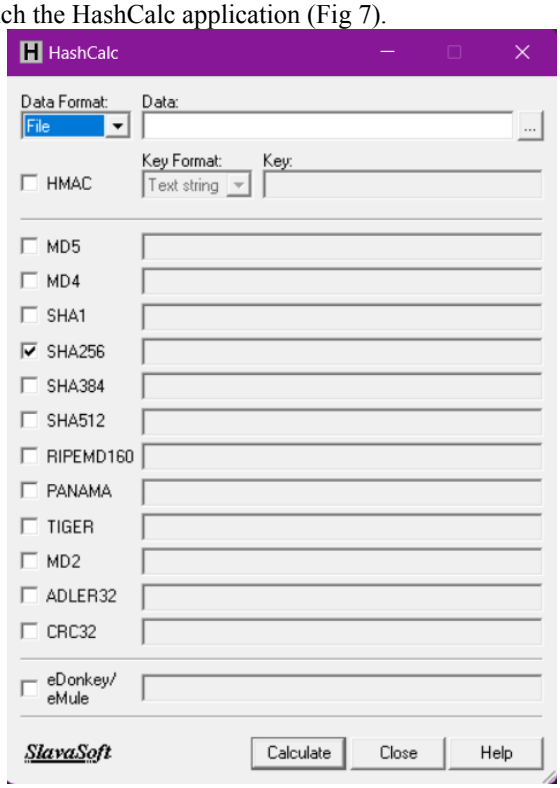


Fig 7. Open HashCalc

Now, drag and drop the file onto the application window (Fig 8).

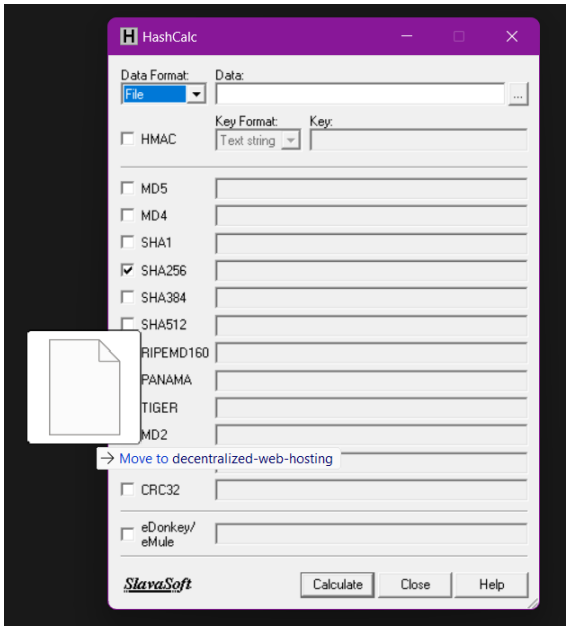


Fig 8. Drag and drop the file onto the application window

The hash value is calculated automatically, and result is displayed beside the selected hash algorithm (Fig 9).

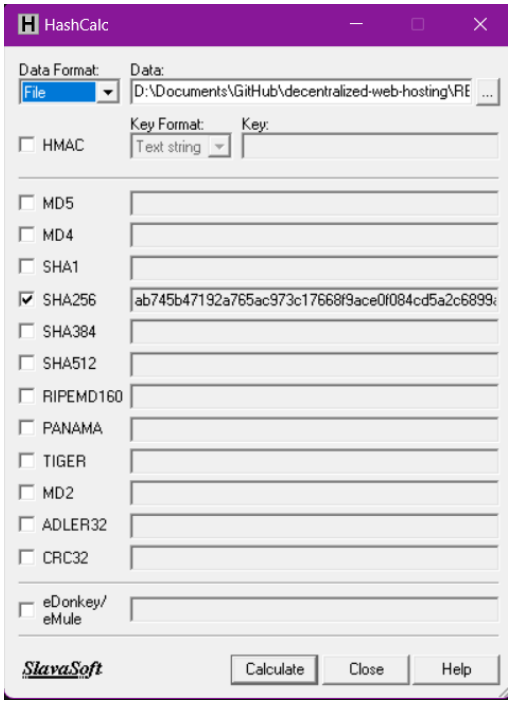


Fig 9. Hash value is calculated and displayed beside the selected algorithm

C. Process Model for Online md5file.com UI:

The process model which will be followed for Online UI mode is explained in the flow chart (Fig 10).

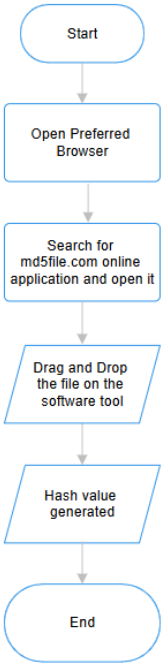


Fig 10. Process model for hash value calculation using md5file.com UI

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 4, Issue – 2, December 2025
E – ISSN – 2583-7559

Launch the preferred web browser application (Google Chrome in this scenario) followed by searching for md5file.com online application (Fig 11).

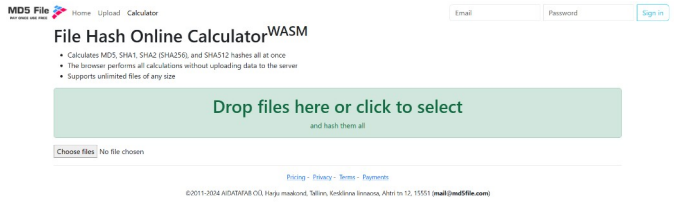


Fig 11. Open desired browser and further navigate to md5file.com UI.

Now, drag and drop the file onto the browser window (Fig 12).

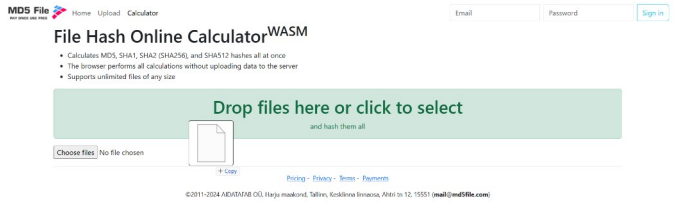


Fig 12. Drag and drop the file on the UI interface

The hash values are calculated and displayed.

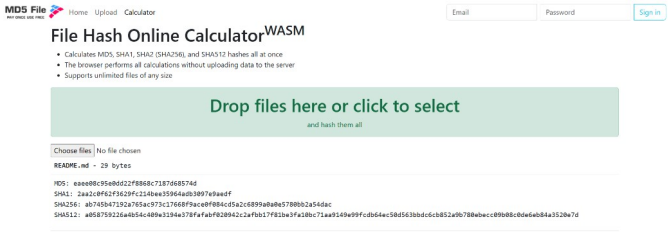


Fig 13. Hash Value results will be generated and displayed on the bottom

V. Findings and Observations of Lab Testing

Seven file formats to simulate real-world scenarios were incorporated in this research. These included a video file (.mp4), a document file (.pdf), an image file (.jpg), a word processing file (.docx), a compressed archive (.zip), a presentation file (.pptx), and a spreadsheet file (.xlsx). Each file format represented a unique test case, in a total of seven scenarios for examination All the selected file formats and the corresponding methods employed to generate the comparative outcomes across the two test systems have been systematically evaluated against the four key parameters, namely, time consumption, accuracy, user-friendliness, and confidentiality of data associated with each method. The consolidated findings for every file type examined are presented in individually structured tables, as shown below.

Table 2. Observation table for .docx file (Word Document).

Method	File Type	File Size	Hash Algorithm	Calculated Hash Value	Time Consumption		Accuracy		User Friendliness		Confidentiality of Data
					System1	System2	System1	System2	System1	System2	
S-DOS	.docx	≈2.1 MB	SHA256	58ce11327b0fca92f042c96450775d058bd4c918211259175d3bd7b8df348ff8	< 1s	< 1s	Yes	Yes	No	No	Yes
HashCalc				58ce11327b0fca92f042c96450775d058bd4c918211259175d3bd7b8df348ff8	< 1s	< 1s	Yes	Yes	Yes	Yes	Yes
Online (md5file)				58ce11327b0fca92f042c96450775d058bd4c918211259175d3bd7b8df348ff8	< 1s	< 1s	Yes	Yes	Yes	Yes	No

Table 3. Observation table for .zip file (Zipped /Archived).

Method	File Type	File Size	Hash Algorithm	Calculated Hash Value	Time Consumption		Accuracy		User Friendliness		Confidentiality of Data
					System1	System2	System1	System2	System1	System2	
MS-DOS	.zip	≈9.21 MB	SHA256	0c1cdbbf2a72bf8e5297d3ae9c416fcaf11ad31b75d6e39a0edcd3740ebf6fcf	56.08s	11.02s	Yes	Yes	No	No	Yes
HashCalc				0c1cdbbf2a72bf8e5297d3ae9c416fcaf11ad31b75d6e39a0edcd3740ebf6fcf	01:01.08 min	33s	Yes	Yes	Yes	Yes	Yes
Online (md5file)				0c1cdbbf2a72bf8e5297d3ae9c416fcaf11ad31b75d6e39a0edcd3740ebf6fcf	03:40.59min	02:05.02min	Yes	Yes	Yes	Yes	No

Table 4. Observation table for .pptx file (PowerPoint Presentation).

Method	File Type	File Size	Hash Algorithm	Calculated Hash Value	Time Consumption		Accuracy		User Friendliness		Confidentiality of Data
					System1	System2	System1	System2	System1	System2	
MS-DOS	.ppt	≈0.65 MB	SHA256	c3463d9ff03479e69bf9362d5e502e72298ea516dd413e65e639b95eb1ebed67	< 1s	< 1s	Yes	Yes	No	No	Yes
HashCalc				c3463d9ff03479e69bf9362d5e502e72298ea516dd413e65e639b95eb1ebed67	< 1s	< 1s	Yes	Yes	Yes	Yes	Yes
Online (md5file)				c3463d9ff03479e69bf9362d5e502e72298ea516dd413e65e639b95eb1ebed67	< 1s	< 1s	Yes	Yes	Yes	Yes	No

Table 5. Observation table for .xlsx file (Excel Spreadsheet).

Method	File Type	File Size	Hash Algorithm	Calculated Hash Value	Time Consumption		Accuracy		User Friendliness		Confidentiality of Data
					System1	System2	System1	System2	System1	System2	
MS-DOS	.xlsx	≈3.11 MB	SHA256	a4ccd2940adbbae269cc29346d76cee50074094a8a1c4b8e0ccd3a54f8200bed	< 1s	< 1s	Yes	Yes	No	No	Yes
HashCalc				a4ccd2940adbbae269cc29346d76cee50074094a8a1c4b8e0ccd3a54f8200bed	< 1s	< 1s	Yes	Yes	Yes	Yes	Yes
Online (md5file)				a4ccd2940adbbae269cc29346d76cee50074094a8a1c4b8e0ccd3a54f8200bed	< 1s	< 1s	Yes	Yes	Yes	Yes	No

Table 6. Observation table for .jpg file (Image).

Method	File Type	File Size	Hash Algorithm	Calculated Hash Value	Time Consumption		Accuracy		User Friendliness		Confidentiality of Data
					System1	System2	System1	System2	System1	System2	
MS-DOS	.jpg	≈5.0 MB	SHA256	ca97497b626da0065573e266e3607e51a4f391aae088afeb6b78a1ff2e6af239	< 1s	< 1s	Yes	Yes	No	No	Yes
HashCalc				ca97497b626da0065573e266e3607e51a4f391aae088afeb6b78a1ff2e6af239	< 1s	< 1s	Yes	Yes	Yes	Yes	Yes
Online (md5file)				ca97497b626da0065573e266e3607e51a4f391aae088afeb6b78a1ff2e6af239	< 1s	< 1s	Yes	Yes	Yes	Yes	No

Table 7. Observation Table for .pdf file (PDF).

Method	File Type	File Size	Hash Algorithm	Calculated Hash Value	Time Consumption		Accuracy		User Friendliness		Confidentiality of Data
					System1	System2	System1	System2	System1	System2	
MS-DOS	.pdf	≈3.5 MB	SHA256	d1bf2b16c2f2f7e74666f3d9943f9b763c1455498bf7397f6958a27f4973c456	< 1s	< 1s	Yes	Yes	No	No	Yes
HashCalc				d1bf2b16c2f2f7e74666f3d9943f9b763c1455498bf7397f6958a27f4973c456	< 1s	< 1s	Yes	Yes	Yes	Yes	Yes
Online (md5file)				d1bf2b16c2f2f7e74666f3d9943f9b763c1455498bf7397f6958a27f4973c456	< 1s	< 1s	Yes	Yes	Yes	Yes	No

Table 8. Observation table for .mp4 file (Video).

Method	File Type	File Size	Hash Algorithm	Calculated Hash Value	Time Consumption		Accuracy		User Friendliness		Confidentiality of Data
					System1	System2	System1	System2	System1	System2	
MS-DOS	.mp4	≈9.21 GB	SHA256	2d0ab2525ec4cc3231361029fcbb8271ed0962de14b6fa220ff33687692c58db	02:45.08 min	25 s	Yes	Yes	No	No	Yes

HashCalc				2d0ab2525ec4cc3231361029fcbb8271ed0962de14b6fa220ff33687692c58db	02:47.08 min	01:11.94 min	Yes	Yes	Yes	Yes	Yes
Online (md5file)				2d0ab2525ec4cc3231361029fcbb8271ed0962de14b6fa220ff33687692c58db	08:36.78 min	04:53.78 min	Yes	Yes	Yes	Yes	No

VI. Lab Testing Data Interpretation

The testing carried out in this paper has produced a clear and significant result confirming the robustness of the methods and parameters employed. More importantly, these findings match closely to the researcher's original hypothesis, which has served as the cornerstone of this entire paper.

The video file chosen for this evaluation measured approximately 10 GB in size. All three hashing methods have generated an identical hash value, which hereby confirming the accuracy of each method. However, the computational efficiency varied across the employed methods and the differences are clear when we closely look at the Table VIII.

The document files, in essence, .pdf, .docx, .ppt, and .xlsx measured within 4 MB in size each. All three hashing methods have generated an identical hash value, which hereby confirming the accuracy of each method, while the time difference between them is non-existential to discuss upon. The image file (jpg) was measured 5 MB in size produced a similar result when compared to the document files.

Finally, the zipped file (zip) measuring 10 GB in size reflected analogous results to those produced by a video file.

This testing has also demonstrated a key aspect when we discuss the importance of systems on which the hash values were calculated. System2 has exhibited a greater performance advantage over System1 with respect to computational speed of the hash values. When we talk about accuracy, both systems have resulted in identical outcomes and the user-friendliness of the tools.

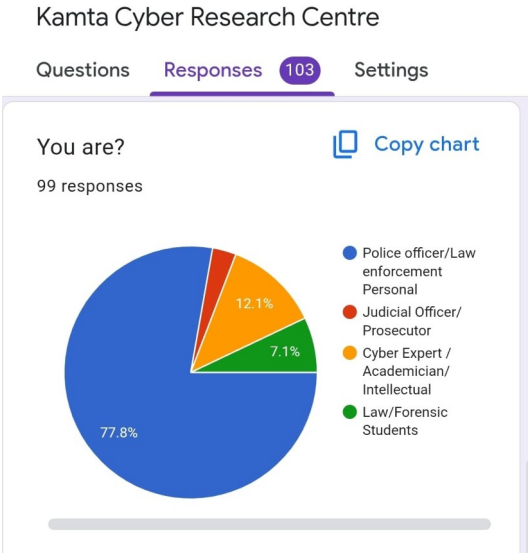
To conclude, the following key interpretations can be derived based on the testing results:

- Accuracy: All three methods produced a consistent and identical hash value across all the file formats that were chosen for this task and this confirms that all three methods are reliable when we talk about accuracy alone.
- User-Friendliness: If we consider a naïve user who has to perform the task of calculating hash values for a file, HashCalc and md5online.com will always prevail over MS-DOS due to the complexity of the method.
- Efficiency: MS-DOS is the most efficient when we compare the computation speed and beats the other two methods by an enormous margin.
- Confidentiality: Hash Calc and the MS-DOS method operate locally and this ensure that all data remains on the system. On the other hand, md5online.com involves uploading files on a third-party server and thus doesn't hold the confidentiality just to the user or the local system.

VII. Empirical Study and Analysis

An empirical survey was conducted to assess the application of tools and techniques used for generating Hash Values among key domain stakeholders. The primary objective was to determine the level of understanding of Hash Values, including their role, characteristics, function, and importance, among participants. The survey was executed in an online mode using a Google form questionnaire to achieve maximum reach across the country, with approximately 103 respondents participating. The researcher specifically focused on Police Officers, Judicial Officers/ Prosecutors, Intellectuals /Academicians/ Cyber Experts and Students of Law/ Forensics to ensure the collection of realistic and relevant data.

The survey was targeted towards specific groups including Police Officials, Judges, Advocates, Academicians, Students and many more such professionals. The total participation across various groups is illustrated in Fig 14. The participant breakdown shows that Police/Law enforcement Officers constituted the largest segment at 77.8%. Other groups included Cyber Experts/Academicians/Intellectuals at 12.1%, Law/Forensic Students at 7.1%, and Judicial/Prosecution Officers at 3.0%.



NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 4, Issue – 2, December 2025
E – ISSN – 2583-7559

Fig 14. Total Participation in Empirical Survey

The empirical survey presented four questions to measure awareness, understanding, and application skills related to Hash Values. The first question, "What is Hash Value?", was aimed to understand the level of familiarity amongst the participants about the core concept of data integrity as illustrated by the pie chart below (Fig 15).

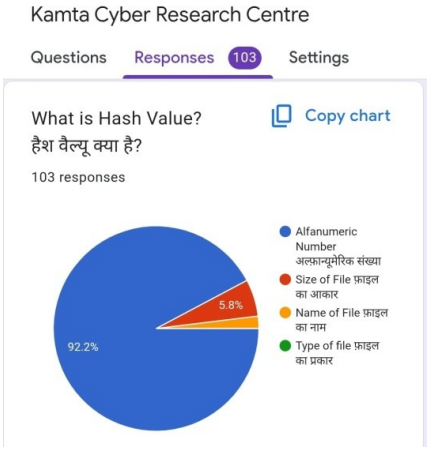


Fig 15. Responses to Question 1.

92.2% of the respondents were aware that a Hash Value is an Alphanumeric Number and an approximate 8.0% of the participants were not aware of this.

The next question, "Why are Hash Values used in digital forensics?", was aimed at identifying the level of understanding regarding the role of Hash values in police investigation. The responses are illustrated in Fig 16.

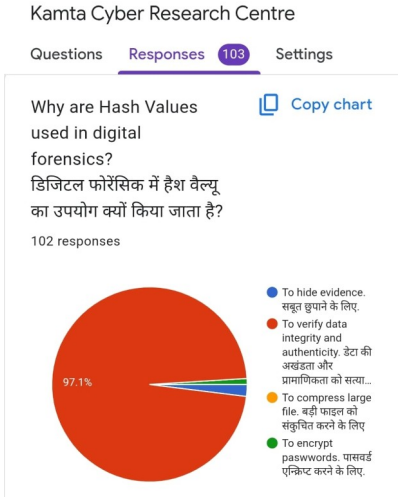


Fig 16. Responses to Question 2.

97.1% of responders stated that Hash Values are used "To verify data integrity and authenticity" of digital evidence. This unanimous response clearly states that the survey group understands the criticality of hash values and its usage.

The third question, "Do you know 'How the Hash Value calculated'?" was aimed to uncover the practical challenges in the application of Hash Value calculation and the responses did reveal a gap between knowledge and practical skill, as shown in Fig 17.



Fig 17. Responses to Question 3.

78.6% responded to yes, indicating that they possess practical knowledge to calculate hash values. However, 21.4% of the survey group did not know the method of calculation. This indicates a practical application challenge gap.

The last question aimed at recognizing the preferred method for calculating hash values with the question, "Which do you think is the easiest way to calculate the hash value?". The results, presented in figure No. 18, showcase a preference for user-friendly tools over native operating system functions.

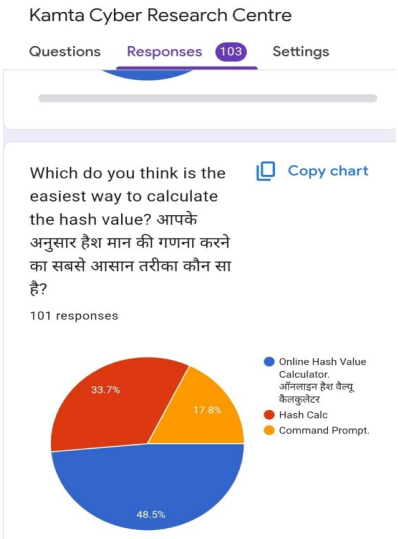


Fig 18. Responses to Question 4.

48.5% of respondents found Online Hash Calculation tools to be the easiest mode compared to 33.7% considered HashCalc Software the easiest way. Surprisingly, only 17.8% were comfortable using Command Prompt. The results suggest that

stakeholders are aware of the Hash Value's importance but there is a strong inclination toward simplified software or online solutions for its actual calculation.

RESEARCH FINDINGS

The admissibility of electronic evidence in a court of law hinges critically on the integrity of the electronic data. The general practice applied to maintain and ensure this integrity is the creation of a Hash Value. This research paper aimed to explore the easiest tool or technique to create a Hash Value at the scene of the crime using a combination of doctrinal study, empirical survey, and lab testing (experimental) methods.

The empirical survey question number 4 (four) gave three main options for Hash Value generation. Firstly, online application (the most common practice), software and hardware tools (frequently used), and the Command Prompt over DOS Mode (suggested by some agencies and technically-abled individuals).

The researcher's lab testing process utilized four key parameters or testing variables to compare these methods: Accuracy, User friendliness, Confidentiality, and Time consumption. The findings from this controlled testing environment are summarized below:

Table 9. Comparative analysis and conclusion for incorporated methods against enforced parameters

Parameter / Methods	Online Application	HashCalc Software	Command Prompt
Accuracy	Same as others	Same as others	Same as others
User Friendliness	Much user friendly	Much user friendly	No user friendly
Confidentiality	High exposure risk of confidential data	No risk	No risk
Time Consumption	Depends on system config/ Internet speed	Depends on system config	Depends on system config

LIMITATIONS

While this study has provided useful insights into identifying the most prominent method for hash value computation, it's important to admit the limitations that would affect the results when these methods are applied. These limitations draw the line of the computational method being employed and provides a clear boundary of key considerations along with when there is a need for caution.

- Md5file.com (Online Application)

This method is simple and very user friendly but its reliability is put under question when internet conditions are not suitable. This affects the upload and download speeds and further would make this process extremely slow. Additionally, uploading the investigative data to the open internet or third-part domain is an invitation to breaches of confidentiality and integrity, as such exposures would risk the original evidence being tampered and even false assertion of the authenticity of the tampered version, undermining the credibility of the data and compromising the investigative process.

- HashCalc:

The accuracy and user-friendliness of this method is undeniable as it offers a really comfortable experience for the user along with the added advantage of data being handled locally on the local system, thus providing relaxation over data confidentiality concerns. However, the dependency on a dedicated software installation for hash value computation is a challenge as such tools might not be readily available on demand and in some cases might not be permitted to use as well.

- DOS-Mode:

The computational efficiency, the accuracy and the degree of confidentiality outshines this method beyond the other two. However, the only challenge it presents is being less user friendly compared to the other two. MS-DOS mode requires the technical command knowledge and this method limits the users coming in from a non-technical background. As a result, the adaptation of this method remains challenging for users who serve at the frontline of the crime scene investigations.

- Configuration of Computer Systems.

The experiment has revealed a key factor when computing hash values. For all the test cases employed, the system with the stronger hardware configuration has surpassed the system with lenient hardware configuration. A direct relation between system performance and computational speed can be derived from the results that are generated as a part of this research.

CHALLENGES

The research has provided a lot of insights to act on and challenges that are hard to overlook. A crime scene is far more complex than what is immediately visible. The reality of the situation extends beyond what is documented in official paperwork and charge sheets. There could be certain situations where the accused might be armed. A victim at the crime scene requiring immediate protection or medical assistance by the personnels. The accuse attempting to destroy or tamper critical evidence while the crime scene is being secured. The above examples clearly exhibit that calculated responses are required to preserve the integrity of all types of evidence while ensuring the safety of all parties involved unless they become hostile. Every second at a crime scene is a challenge for the investigating team while following standard response

protocols including capture of hash values while simultaneously managing the unforeseen events.

While calculating the hash value for a document is straightforward for individuals with a strong technical background, it does possess a real challenge for others. Engineering graduates or IT professionals can usually handle this task with much ease using the methods outlined in this study compared people without technical expertise often struggle. This highlights the need for user-friendly tools in digital evidence handling.

MS-DOS (Command Prompt) is still widely recognized and even referenced in police orders [6], it certainly produce difficulties for personnels unfamiliar with basic command-line operations. This technical skills gap can undermine the crucial goal of preserving the integrity of digital evidence collected at crime scenes where accuracy and reliability are important.

While most users rely on easily available and accessible options like online hash generators for example, md5file.com, these platforms could be really dangerous as these require uploading sensitive evidence to public servers compromising the confidentiality and can even cause reputational harm to victims. Over time, reliance on such tools for convenience and due to the lack of awareness of safer methods, the best practices in digital forensics put an adverse effect on the outcome of investigations.

Offline applications like HashCalc do offer a safer alternative as they are easier to use than command line tools and keep all data on the local system promoting data confidentiality. But their use in formal investigations has been limited due to certain factors, such as licensing and authorization requirements from judicial and law enforcement authorities.

Despite this advantage software tools like HashCalc are yet to gain widespread formal recognition as a clear regulatory endorsement and standardized procedures, ensuring the secure and effective use remains a challenge.

RECOMMENDATION

Accuracy and Time:

The researcher concluded that accuracy remains the same across all tools and techniques. Furthermore, the time consumed for Hash Value creation is dependent only on the system configuration, where higher-version systems yield faster results. These two parameters do not distinguish the best method.

User Friendliness vs. Confidentiality Trade-off:

The core trade-off lies between user experience and security.

- User Friendliness: Both the Online application (platform) and HashCalc software are much more user-friendly compared to Command Prompt. This aligns with the empirical survey result showing high preference for these simplified methods (48.5% for Online, 33.7% for HashCalc).
- Confidentiality: The risk of exposure of confidential data is much higher with the online platform as the data potentially enters the public domain. In contrast, Command Prompt and HashCalc (being local software) carry a significantly lower risk.

SUGGESTION: LEVERAGING HASHCALC / OFFLINE APPLICATIONS FOR STANDARDIZED HASH VALUE CALCULATION

The empirical study and lab testing results clearly indicate that stakeholders have a strong preference for simplified, graphical user interface (GUI) tools over highly technical & complex native command-line methods like Command Prompt or Online Hash Calculation Platform, where high risk exposure of confidential data in public domain is absolutely concerning, HashCalc or other offline applications (such as HashMyFiles, HashFarm, Tom's Hash Calculator, DevToys, etc.) presents an ideal starting point for standardizing the practical application of Hash Value calculation across police and law enforcement agencies.

CONCLUSION

The research established a critical trade-off where the highly preferred Online Application (Platform) carries a severe security risk. Since **HashCalc Software** is also highly user-friendly and maintains a high level of confidentiality due to its local operation, the researcher concluded that HashCalc represents the most balanced and ideal option. The researcher's full study combining user preference (empirical finding) with high security (lab testing finding) leads to the conclusion that **HashCalc** is the superior, easiest and safest option for police and law enforcement officers to maintain the integrity of digital evidence at the crime scene. It addresses the practical skill gap by being easy to use (33.7% already prefer it) while protecting the integrity and confidentiality of the electronic evidence which is paramount for admissibility in court.

FUTURE WORK

- Future studies could compare different hash calculation tools to determine the best alternative to HashCalc.
- Developing automation scripts may help improve tools like HashCalc by speeding up hash calculations, boosting efficiency, and reducing repetitive manual work.
- Another area for future work is addressing the confidentiality issues of online platforms by creating secure, ethically managed environments where users can safely store and handle data.

REFERENCES

[1] V. Rana and N. Nagpal, "Tech Savvy Evidence System: Step by Step Guide to Extract Hash Function Value from Electronic Evidence," Bar & Bench, 2024. [Online]. Available: https://www.barandbench.com/

[2] S. Sharma, "A Comprehensive Study of Cryptographic Hash Functions," presented at the Defence Materials and Stores Research and Development Establishment Conference, Kanpur, 2024.

[3] Supreme Today AI, "What Is the Importance of Hash Value Certificate," Mar. 16, 2025. [Online]. Available: https://supremetoday.ai/issue/what-is-the-importance-of-hash-value-certificate

[4] K. Kumar, S. Sofat, S. K. Jain, and N. Aggarwal, "Significance of Hash Value Generation in Digital Forensic: A Case Study," Int. J. Eng. Res. Dev., vol. 2, no. 5, pp. 64–70, Jul. 2012. [Online]. Available: https://www.ijerd.com/

[5] A. Varol and Y. Ü. Sönmez, "Review of Evidence Collection and Protection Phases in Digital Forensics Process," Int. J. Inf. Secur. Sci., vol. 6, no. 4, 2017.

[6] Bihar Police, "Bihar Police Order No. 330-25," Nov. 07, 2025. [Online]. Available: https://police.bihar.gov.in/Police_Order.aspx

[7] F. Casino, T. Dasaklis, G. Spathoulas, et al., "Research trends, challenges, and emerging topics of digital forensics: A review of reviews," arXiv, 2021. [Online]. Available: https://doi.org/10.48550/arxiv.2108.04634

[8] R. Zahid, A. T. Maolood, and A. Al-Adhami, "A review of digital forensics using artificial intelligent," AIP Conference Proceedings, vol. 3224, p. 030022, 2025. [Online]. Available: https://doi.org/10.1063/5.0254375

[9] M. S. M. B. Shah, S. Saleem, and R. Zulqarnain, "Protecting Digital Evidence Integrity and Preserving Chain of Custody," *J. Digit. Forensics, Secur. Law*, vol. 12, no. 2, Art. no. 12, Jun. 2017. [Online]. Available: https://doi.org/10.15394/jdfsl.2017.1478

[10] M. AlKhanafseh and O. Surakhi, "Evidence preservation in digital forensics: An approach using blockchain and LSTM-based steganography," Electronics, vol. 13, no. 18, p. 3729, 2024. [Online]. Available: https://doi.org/10.3390/electronics13183729

[11] Government of India, *The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023)*, Ministry of Law and Justice, The Gazette of India, New Delhi, Dec. 25, 2023. [Online]. Available: https://www.indiacode.nic.in/

[12] T. Dubey and K. Sharma, "Digital Evidence and Electronic Record Management and Criminal Trials," *Int. J. Creat. Res. Thoughts (IJCRT)*, vol. 14, no. 8, Sep. 2026. [Online]. Available: https://ijcrt.org/viewpaperforall.php?paper=IJCRT2608468

[13] R. Nick S., "The Examiner, the Algorithm, and the Accused: Assessing the Adequacy of the Bharatiya Sakshya Adhiniyam, 2023," *Indian J. Integr. Res. Law (IJIRL)*, vol. 6, no. 2, pp. 1962–1975, Mar. 2026. [Online]. Available: https://ijirl.com/

[14] National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, FIPS PUB 180-4, U.S. Dept. of Commerce, Gaithersburg, MD, USA, Aug. 2015. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.180-4

[15] Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence, ISO/IEC 27037:2012, International Organization for Standardization, Geneva, Switzerland, 2012.

[16] K. R. Dodiya, K. Kumar, K. Joshi, M. A. Rajesh, B. Doshi, and P. Sharma, "A Non-Destructive Technique for Extraction of Digital Data in Forensic Analysis," *Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET)*, vol. 13, no. 3, pp. 510–516, Mar. 2025. [Online]. Available: https://doi.org/10.22214/ijraset.2025.67302