Bangladesh Journal of MIS
2025, Vol.11, No.01
https://doi.org/10.61606/BJMIS.V11N1.A1
ISSN:2073-9737 (Print), 2410-7077 (Online)

OPEN ACCESS

Digital Forensics Empowerment of Bangladesh Police: A Comprehensive Analysis of Its Role in Preventing Crimes and Enhancing Investigative Capabilities

Khadija Sharmin[1]
Mohammad Ishtiaque Rahman[2]

ABSTRACT

This research paper examines the significant role of digital forensics in enhancing the Bangladesh Police's ability to combat crime. Researchers identified six key factors by administering questionnaires to 52 members of the Bangladesh Police: the accuracy of collected evidence, the enhancement of evidence collection processes, improved conviction rates, geolocation and criminal mapping capabilities, crime prevention, and the ability to gain fresh perspectives on ongoing investigations. The findings demonstrate that digital forensics plays a pivotal role in strengthening the police's investigative capacity, particularly in improving evidence handling and analysis. Additionally, the study reveals that digital forensics contributes substantially to crime prevention efforts, helping law enforcement agencies stay ahead of evolving criminal tactics. Based on these insights, the paper recommends prioritizing the integration of digital forensics into the police's daily operations and investing in continuous training and technological upgrades to fully harness its potential in crime fighting.

KEYWORDS: Digital Forensics, Bangladesh Police, Evidence Collection, Criminal Mapping, Crime Prevention

1. Introduction

In the modern era of rapid technological advancement, digital devices have become indispensable in daily life. This widespread reliance on technology has transformed society but has also introduced

[1] Department of Management Information Systems, Faculty of Business Studies, Begum Rokeya University, Rangpur, Rangpur-5404, Bangladesh. (CORRESPONDING AUTHOR) khadijasharmin@mis.brur.ac.bd

[2] Department of Computer Information Systems, Thomas More University, Crestview Hills, Kentucky 41017, USA.

ARTICLE HISTORY: *Received:* 08-Nov-2024; *Revised:* 09-Apr-2025; *Accepted:* 30-Jun-2025; *Published:* 18-Dec-2025

new challenges for combating criminal activity. As such, law enforcement agencies worldwide have adopted digital forensics as an essential tool in their crime-fighting efforts. In Bangladesh, a country experiencing rapid digital growth and increasing reliance on technology, digital forensics has become a central component in the fight against crime. The Bangladesh Police has recognized an urgent need to enhance its capacity for managing digital evidence and conducting investigations in the digital realm.

Historically, Bangladesh has already acknowledged the importance of digital evidence in criminal proceedings. This was demonstrated in landmark cases such as Mrs. Khaleda Akter VS State (1985) and Yeasin Khan Palash (2007), where digital evidence like audio and video recordings was deemed admissible (The Daily Sun, 2022). Recognizing the growing importance of digital evidence, Bangladesh amended the Evidence Act of 1872 in 2022, allowing for the admissibility of digital records under Section 65B. This amendment highlights the legal integration of digital forensics into the criminal justice system.

Gary L Parmer (2001) defined digital forensics as, “the use of scientifically derived and proven methods toward the preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations." Quick and Choo (2014) define digital forensics as "the process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is legally admissible." According to BlueVoyant, computer forensics, mobile device forensics, network forensics, forensic data analysis and database forensics are the different branches of digital forensics. Reverse steganography, stochastic forensics, cross-drive analysis, live analysis, and deleted file recovery are techniques of digital forensics.

Despite these advancements, the role of digital forensics in crime investigation remains underexplored, particularly within Bangladesh Police. This study aims to bridge this gap by examining how digital forensics contributes to crime-fighting efforts and improves investigative capabilities within the Bangladesh Police. Specifically, it will assess the adoption of digital forensics, its impact on crime prevention, and the effectiveness of its integration into the police department's routine operations.

By focusing on the Bangladesh Police's current practices and challenges in utilizing digital forensics, this research will offer valuable insights into the role of digital forensics in contemporary crime investigation. It will also provide recommendations on how Bangladesh can enhance its use of digital forensics to keep pace with evolving digital crime trends and improve its overall crime-fighting efforts.

2. Literature Review

According to Data Reportal (2023), at the start of 2023, there were 66.94 million internet users in Bangladesh, and 179.9 million cellular mobile connections were active, a figure equivalent to 104.6 percent of the total population. This statistic regarding the high number of mobile users underscores the necessity of adopting digital forensics solutions as a new approach to solving crimes. Shayna Joubert (2016) stated that technology can prevent crimes by mapping technology, using smartphone apps, and enabling web reporting. Digital forensics has evolved rapidly to keep up with technological advancements, giving investigators access to a vast array of techniques and instruments. This literature review examines the essential factors of digital forensics in the context of investigations.

2.1 Factors of digital forensics

According to a study by Nelson et al. (2010), the analysis of digital evidence requires the identification, extraction, and interpretation of data from various digital sources. Analyzing digital evidence aids in investigating illicit activities including cyberattacks, fraud, and identity theft. Digital forensic investigators analyze data from electronic devices using specialized forensic analysis software tools. Physical devices, such as hard drives and memory cards, may also be examined during the analysis procedure. The examination of digital evidence must comply with jurisdiction-specific regulations and ethical considerations. Nelson et al. (2010) also demonstrated that the final step in the digital forensics' procedure is the presentation of digital evidence. Courts require forensic investigators to present their findings in a plain, concise, and easily understood manner.

Casey (2011) demonstrated in another study that the preservation of digital evidence is crucial to ensuring its admissibility in court. Throughout the investigation process, preservation methods must maintain the integrity and authenticity of the proof. Experts in digital forensics must use techniques such as hashing, imaging, and archiving to ensure the integrity of digital evidence. Preservation must adhere to local regulations and ethical considerations. Failure to properly preserve evidence can result in its exclusion from court proceedings.

According to Pollitt (2013), the accumulation of digital evidence is the first and most important aspect of digital forensics. Collecting digital evidence is a complex procedure that necessitates trained personnel to maintain the evidence's integrity. Different types of digital evidence exist, including E-mail, images, videos, documents, and text messages. The collection procedure must adhere to the norms of evidence, jurisdictional laws, and ethical principles. The process of collection may entail the seizure of electronic devices, the application of imaging techniques, or the duplication of data from servers, computers, and storage devices.

Digital forensics requires collection, preservation, analysis, and presentation of digital evidence. The factors discussed in this literature review, such as the collection, preservation, analysis, and presentation, as well as legal and ethical considerations, are essential for the success of digital forensic investigations. Adhering to these factors can ensure that digital evidence is admissible in court and aid in the investigation of offenses.

2.2 Influence of digital forensics in combating crimes

Realizing the value of technology in combating crimes, many authors have stated the importance of technology in their research. According to Braga, Papachristos, & Hureau (2014), technology advancements have affected the efficiency of police departments in combating crime. It has been determined, for instance, that the use of surveillance cameras and license plate readers reduces crime rates.

Garfinkel (2013) stated in his research that for most Americans, technology has become an integral part of life. So, the collection and use of digital evidence have similarly become a standard of many criminal and civil investigations. Further, Carter (2013) stated digital evidence not only solves e-crime, but also solves all types of crimes, as suspect's E-mail accounts or mobile phone files may contain digital evidence regarding their location, company, and the activities they have performed. According to Casey (2011), digital forensics can play a significant role in crime resolution by providing evidence that helps identify suspects and establish their culpability. Investigators discovered digital evidence in 80% of the 500 cases examined, and they used that evidence to identify the suspect in 74% of these cases. It is possible to use digital evidence to monitor online communications, locate physical devices, and recover deleted files. Digital forensics is essential for the investigation and prosecution of child pornography cases. Investigators use digital evidence to monitor and identify people who possess or distribute child pornography, and they also recover deleted or encrypted evidence. They also use digital forensics. To identify and rescue child pornography victims.

In another research, Kshetri (2014) said digital forensics can also prevent offenses by identifying and interfering with criminal activities before criminals commit them. Law enforcement agencies can use digital forensics to monitor online activities and identify potential threats. This is especially helpful in cases involving cybercrime, terrorism, and other types of organized crime. Digital forensics is crucial in the fight against cybercrime. Cybercrime is a growing hazard that can cause significant monetary losses to individuals and businesses. Digital evidence helps identify and prosecute cybercriminals, recover stolen data, and prevent future attacks. Kshetri (2014) also stated that Digital forensics can also play a crucial role in international criminal investigations through international cooperation. Digital evidence helps authorities to monitor and identify potential transnational criminals. International cooperation is essential for investigators to effectively collect and utilize digital evidence in criminal investigations.

Bocij (2014) stated that authorities can use digital evidence to monitor and identify terrorists, prevent attacks, and disrupt terrorist networks. Digital forensics enables the recovery of data from damaged or obliterated devices, which can be essential following a terrorist attack. Digital evidence helps establish culpability in a range of criminal cases. Investigators can use digital evidence to demonstrate that a suspect was present at the crime site or communicated with other suspects. Digital evidence can also demonstrate a suspect's motive or opportunity to perpetrate a crime. In the research of Kruse & Heiser (2002) it is stated that utilizing digital forensics in criminal

investigations does not come without obstacles. The use of encryption and other security measures can make it challenging to retrieve digital evidence. Moreover, digital forensics requires specialized training and expensive apparatus, which can be prohibitive for law enforcement agencies.

Using telephone surveys of police agencies in the North Texas area, USA, Scott Belshaw (2019) suggested that departments train most examiners first as police officers and digital forensics examiners, digital forensic education. Investigators and prosecutors heavily rely on digital forensics when offenses involve digital evidence. The increasing nefarious use of digital devices and the internet has made digital forensics an indispensable component in the fight against crimes for law enforcement.

2.3 Digital forensics role in Bangladesh

When people discovered that many students had gained admission to Bangladesh's top university, the University of Dhaka, by using unethical methods like getting exam question papers through digital media (messenger, WhatsApp) and using digital hearing aids at the testing center, the education system in Bangladesh faced one of its biggest collapses. In a joint effort by the Bangladesh Police and journalist Abdullah Al Imran (2017), they made the identities of several students public. GPS tracking, mobile forensics, database, and computer forensics all were used to solve this case, and it is still one of the biggest cases of using digital forensics in Bangladesh.

In Bangladesh, digital forensics plays a significant role in criminal investigations. It helps identify and capture digital evidence, such as data from computers, mobile devices, and online platforms. Rahman (2017) and Kabir et al. (2020) have highlighted the efficacy of digital forensics in assisting investigations involving cybercrime, fraud, intellectual property theft, and other criminal activities. By employing sophisticated forensic tools and techniques, law enforcement agencies can extricate valuable information from digital devices, which can serve as crucial courtroom evidence.

According to Islam et al. (2019) the digital landscape in Bangladesh has evolved significantly, with more people relying on digital devices and platforms for various activities. Bangladesh's law enforcement agencies have been gradually adopting and implementing digital forensic practices to combat the rise of cybercrime and effectively handle digital evidence. Research has highlighted the establishment of specialized units within the police force that are endowed with the necessary tools and knowledge to conduct digital investigations. Rahman et al. (2020) stated that cybercrime has emerged as a significant issue in Bangladesh, affecting individuals, corporations, and government agencies. Digital forensics is essential for investigating cybercrimes such as hacking, online deception, and identity theft. The use of digital forensics tools and techniques has facilitated the identification and prosecution of cybercriminals in Bangladesh, according to research. The analysis of digital evidence, such as IP addresses, communication logs, and data recovery, has proved helpful in connecting suspects to cybercrimes.

Mahmud (2020) cited limited funding, infrastructure, and a lack of competent personnel as significant obstacles to the effective use of digital forensics techniques. In addition, the rapid evolution of technology makes it challenging to keep up with emergent digital threats and utilize the most recent forensic tools and techniques. Several recommendations emerge from the research for enhancing the impact of digital forensics in Bangladesh. Hossain et al. (2019) called for the development of a comprehensive digital forensics framework including policies, procedures, and training programs. In addition to facilitating knowledge sharing, research collaborations, and the establishment of digital forensics laboratories, a strengthening of partnerships between law enforcement agencies, academic institutions, and the private sector can facilitate these activities.

2.3.1 Research Gaps

Identified Gaps in Existing Research:

i. **Lack of Focus on Developing Countries**: While there is considerable research on digital forensics in countries with advanced technology infrastructures, studies that specifically address the unique challenges of law enforcement agencies in developing nations, like Bangladesh, are sparse. The limited resources, lack of training, and cultural differences within these countries may hinder the effective adoption of digital forensics practices. This gap in the literature underscores the need for research that evaluates how the Bangladesh Police can implement and benefit from digital forensics.

ii. **Integration of Digital Forensics into Law Enforcement:** Existing research often focuses on individual tools and techniques in isolation, without considering how these tools fit into the broader context of law enforcement practices. A lack of comprehensive studies exists on how digital forensics is integrated into the daily operations of law enforcement agencies, especially in Bangladesh, where traditional methods are still dominant. This research aims to fill that gap by exploring how digital forensics can enhance investigative efficiency and crime-solving capabilities within the Bangladesh Police.

iii. **Challenges of Legal and Institutional Frameworks**: Another significant gap is the legal framework for handling digital evidence. While researchers have studied digital forensics techniques extensively, they have given less attention to how legal systems in developing countries are evolving to accommodate these technologies. Bangladesh's Evidence Act of 2022, which allows for the admissibility of digital evidence, is a critical area of interest that requires further exploration. This study will explore how Bangladesh's legal system and police department can work together to ensure that digital evidence is properly handled, stored, and presented in court.

iv. **Adoption Barriers in Low-Resource Settings**: Many studies have focused on the technical challenges of digital forensics, but few have addressed the institutional barriers to its adoption, such as budget constraints, lack of infrastructure, and insufficient training for officers. Researchers on overcoming these barriers in countries like Bangladesh is limited.

This study aims to contribute to the literature by identifying specific challenges and recommending practical solutions to enhance their use.

This study aims to address the identified gaps by examining the role of digital forensics within the Bangladesh Police. It focuses on both the technical and institutional challenges that hinder its adoption. This study also explores how Bangladesh can implement digital forensics and overcome challenges in training, legal integration, and infrastructure to improve law enforcement in crime prevention and investigation.

The research will also contribute to the academic understanding of digital forensics applications in developing countries, offering a new perspective on how low-resource law enforcement agencies can adapt and benefit from these technologies. This study's findings will be valuable not only for Bangladesh but also for other countries facing similar challenges in integrating digital forensics into their criminal justice systems.

3. Methodology

3.1 Conceptual Framework

Digital forensics provides the Bangladesh Police Department with benefits that help it function better than before. Digital forensics programs strongly correlate with combating crimes more accurately and quickly. Using digital forensics positively impacts the accuracy of collected evidence and reduces the chance of misleading evidence. The enhanced process of evidence collection is directly connected to digital forensics.

Digital forensics enhances the evidence collection process, ensuring less time is spent and a faster collection process. It also increased the probability of gathering proof from erased data. The efficiency of Bangladesh police members has increased with the use of digital forensics.

The framework presented in Figure 1 outlines the relationship between several key independent variables, such as accuracy of evidence collection, conviction rates, crime prevention, and the dependent variable, digital forensics. The accuracy of evidence collection, for example, directly enhances the effectiveness of digital forensics by ensuring that digital evidence is appropriately identified, preserved, and analyzed. This, in turn, improves the overall outcomes of criminal investigations. Similarly, factors like improved conviction rates and crime prevention are mediated by the effectiveness of digital forensics, as accurate and timely evidence contributes to higher conviction rates and the ability to prevent future crimes.

As the accuracy of evidence increases and the evidence collection process improves, the conviction rate for crimes also rises with the use of digital forensics. Most of the time the conviction is convincing towards accuracy. The conviction rate for crimes such as fintech and cybercrimes is high. Most of the cases these days end in jurisdiction, and the judiciary system is becoming more trusted and accurate with the help of digital forensics. However, the police department detects significant national threats, fintech crimes, and terrorist activities earlier and often successfully prevents them. Even if they fail to detect these crimes, they successfully take

immediate action by using digital forensics to combat them. Digital forensics helps the police department prevent crimes. Geolocating and mapping criminals has greatly benefited the department, making it much easier to detect criminals and pinpoint their location accurately.

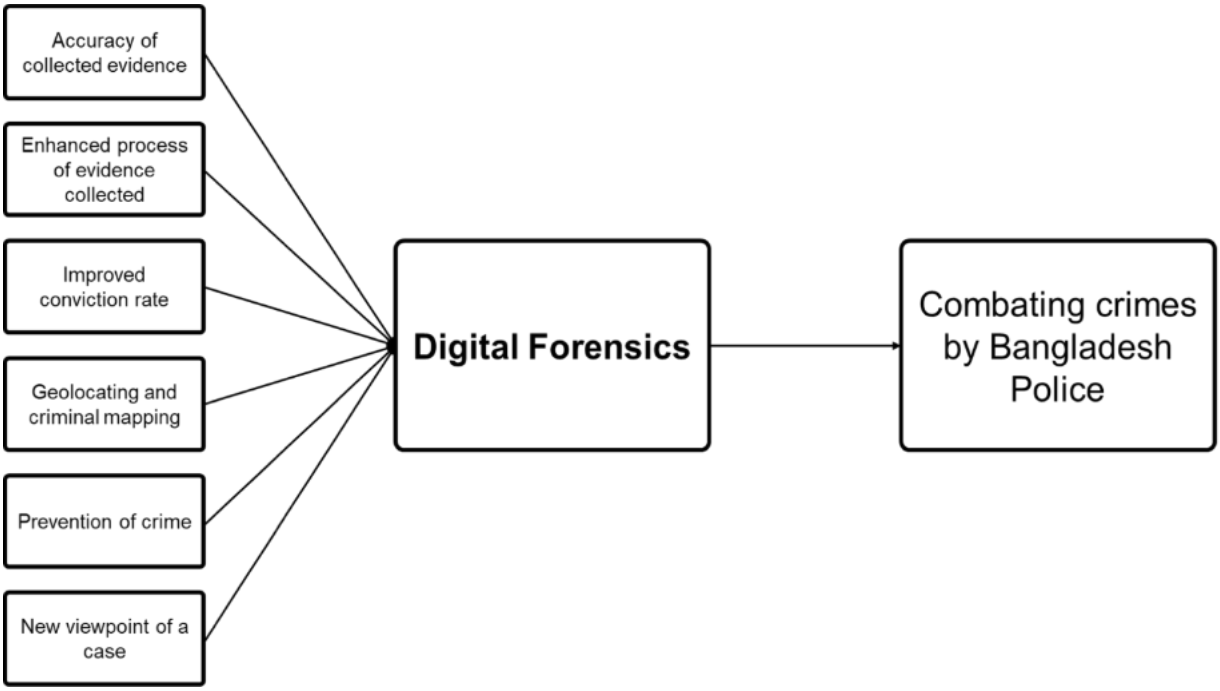

Figure 1: Conceptual Framework (Source: Author's work)

Digital forensics has made fintech and cybercriminals easier to understand. In many cases in Bangladesh, it has helped identify new criminals and provide fresh perspectives on cases. This has improved the accuracy of suspect arrests and increased the reliability of rechecked evidence.

3.2 Theoretical Basis

The conceptual framework of this study is grounded in two well-established theories within criminology and digital forensics: Routine Activity Theory and General Deterrence Theory. These theories provide a robust foundation for understanding how digital forensics contributes to crime prevention, conviction rates, and the accuracy of evidence collection.

i. **Routine Activity Theory - Cohen, L. E., & Felson, M. (1979):** Routine Activity Theory (RAT) posits that crime occurs when three key elements converge: a motivated offender, a suitable target, and the absence of capable guardianship. In the context of digital forensics, capable guardianship refers to the ability of law enforcement agencies to prevent and detect crime through the collection and analysis of digital evidence. Digital forensics serves as a tool for guardianship by enabling police officers to identify, track, and apprehend offenders who might otherwise go undetected. According to RAT, the presence of capable

guardianship — in this case, the use of digital forensics tools — reduces the likelihood of crimes, as offenders are more likely to be caught and prosecuted. The routine activities of individuals in a society are increasingly mediated by technology, creating new opportunities for digital crimes. Digital forensics acts as a preventative mechanism by identifying crimes committed on digital platforms and apprehending offenders, thus reducing overall criminal activity.

This study links crime prevention to the effectiveness of digital forensics in detecting criminal behavior. By improving digital forensics capabilities, law enforcement can better monitor and deter potential offenders, thereby strengthening the principles of Routine Activity Theory.

ii. **General Deterrence Theory - Beccaria, C. (1764):** General Deterrence Theory asserts that individuals are less likely to engage in criminal behavior if they perceive a high likelihood of being caught and punished. The theory suggests that the certainty of punishment, rather than severity, is the most effective deterrent against crime. In the context of digital forensics, the accuracy of evidence collection plays a crucial role in increasing the likelihood of a successful prosecution, which in turn strengthens the deterrent effect. By ensuring that digital evidence is collected and preserved accurately, digital forensics increases the probability of conviction, thus contributing to the deterrence of criminal activity. In cases where digital evidence is crucial, the precision and reliability of forensic tools are essential for securing convictions. The higher conviction rates enabled by digital forensics are expected to send a clear message to potential offenders that their criminal activities will likely lead to detection and punishment, in line with the General Deterrence Theory.

This theory provides a basis for the relationship between the accuracy of evidence collection and conviction rates. By improving the accuracy of digital forensics, law enforcement can not only solve crimes but also enhance the deterrent effect on crime rates, as the perceived likelihood of being caught increases.

iii. **Application to the Study's Conceptual Framework:** This study's framework uses two theories to explain how digital forensics influences crime prevention, conviction rates, and evidence accuracy. It suggests that improving digital forensics through training, technology, and policies enhances crime prevention (Routine Activity Theory) and conviction rates (General Deterrence Theory). Key factors like evidence accuracy and geolocation mapping directly impact digital forensics effectiveness and the resulting outcomes. Thus, the framework aligns with both Routine Activity Theory and General Deterrence Theory, demonstrating that effective digital forensics tools are not only crucial for solving crimes but also play a significant role in preventing crimes and deterring potential offenders.

3.3 Hypotheses of the study

The study tested the following hypotheses to examine the relationship between digital forensics and crime-fighting effectiveness in the Bangladesh Police Department:

- **Hypothesis 1:** The Accuracy of evidence collected through digital forensics positively influences the ability of digital forensics to combat crime.
- **Hypothesis 2:** An enhanced process of evidence collection positively contributes to the ability of digital forensics in combating crime.
- **Hypothesis 3**: Improved conviction rates are positively associated with the importance of digital forensics in combating crimes.
- **Hypothesis 4**: The prevention of crime is positively related to the importance of digital forensics.
- **Hypothesis 5**: Enhanced geolocation and criminal mapping positively influence the ability of digital forensics to combat crime.
- **Hypothesis 6**: New viewpoints of a case positively influence the ability of digital forensics to combat crime.

3.4 Materials

This research adopts positivism as its research philosophy. The study uses a quantitative measurement approach, which provides greater accuracy and reliability. The research gathered primary data from the members of the Bangladesh Police Department and conducted a survey-based analysis. The study used analyses like descriptive statistics, regression analysis, and correlation for the following reasons:

- This research paper has six hypotheses. Researchers tested these hypotheses because they chose a deductive research approach.
- Using descriptive statistics, the basic characteristics of the dataset have been described and quantified.
- Moreover, descriptive statistics serve as a starting point for accurate data analysis, helping to organize, simplify, and summarize the primary dataset.
- Through regression analysis, all kinds of patterns have been able to understand what took place in those primary datasets. Again, the researchers developed new insights that provide valuable understanding of which variables had a significant impact.
- While analyzing the regression, the researchers used Analysis of Variance (ANOVA) to test for differences in the means across groups. Finally, they applied correlation to study the statistical relationship between two variables.

3.4 Relationship Between the Research Terms

This study employs a quantitative research approach, suitable for analyzing numerical data and identifying patterns or trends. The researcher used survey-based research as the primary method

for data collection, administering structured questionnaires to a sample of 52 Bangladesh Police officers. This approach enabled the collection of quantifiable data on the role of digital forensics in combating crime.

3.5 Sampling

The role of digital forensics in combating crimes within the Bangladesh Police is analyzed based on the information collected from the questionnaire. Researchers used the random sampling method, selecting a sample size of 52 from individuals working in the Bangladesh Police who use digital forensics.

Researchers calculated the sample size using the following:

a) **Confidence Level (CL):** This represents the degree of certainty that the actual value falls within the confidence interval.

b) **Confidence Interval (CI):** This margin of error represents the range within which the actual value falls, expressed as a percentage. For example, if you have a 5% confidence interval, the true value is expected to be within 5% of the sample estimate.

c) **Population Proportion (PP):** This is an estimate of the percentage of the population with a certain characteristic. If the proportion is unknown, a value of 50% is often used because it provides the most conservative sample size estimate.

d) **Sample size calculation:** Confidence Level (CL): Approximately 80% (Z-score is approximately 1.14) Confidence Interval (CI): 10% (0.1 as a decimal) Population Proportion (PP): 50% (0.5 as a decimal) Using the formula: n = (Z^2 * p * (1-p)) / E^2

   Where Z: The Z-score corresponding to the desired confidence level (1.14 for approximately an 80% confidence level) p: The estimated population proportion (0.5) E: The margin of error (0.1 for a 10% confidence interval). Plugging these values into the formula:

   n = (1.14^2 * 0.5 * (1-0.5)) / 0.1^2 n ≈ 41. In this case, a sample size of approximately 41 would be needed to achieve an approximately 80% confidence level with a 10% confidence interval, assuming a population proportion of 50%.

e) **Description:** When conducting a survey or study, it is crucial to select an appropriate sample size to ensure reliable results. In this case, the goal is to achieve a confidence level of approximately 80%, indicating that there is an 80% probability that the actual population value falls within the specified confidence interval. The confidence interval is set at 10%, which represents the margin of error or the range within which the true value is expected to fall. By assuming a population proportion of 50%, the required sample size to meet these criteria is approximately 41. By surveying this number of participants, the study will have an approximately 80% chance of capturing the actual population value within a 10% margin of error.

f) **Justification of the sample size:** The sample size calculation for this study uses a confidence level of 80%, which is often acceptable for exploratory research where precision is not the primary goal. An 80% confidence level is commonly employed in cases where time, resources, and access to the population are limited, but the findings still provide valuable insights. In contrast, a 95% confidence level is more common for studies with larger sample sizes or when the precision of the results is critical. Given the context of this study, with a sample of 52 respondents from a specialized group (Bangladesh Police), an 80% confidence level is deemed sufficient for understanding trends and drawing actionable conclusions.

4. Result

4.1 Demographic Characteristics

The study observed the following demographic table from the 52 respondents.

Table 1: Demographic profile of the respondents

Demographic Profile		
Age	25-35	22
	36-45	17
	46-55	13
	Total	52
Designation	Deputy Inspector General	1
	Additional Deputy Inspector General	1
	Superintendent of Police	7
	Additional Superintendent of Police	4
	Assistant Superintendent of Police	17
	Inspector of Police	2
	Sub Inspector	9
	Assistant Sub Inspector	4
	Sergeant of Police	1
	Cadet Sub Sergeant	1
	Total	47

Source: Author's work

Overall, the demographic profile consists of 52 respondents. Most respondents fall within the 25–35 age group. The 36–45 age group includes 17 respondents, and the 46–55 age group includes 13 respondents. The largest number of respondents hold the position of Assistant Superintendent of Police (ASP), with 17 individuals. The Superintendent of Police (SP) position has seven respondents. Additional SP has four respondents, while Inspector has two, Sub-

Inspector has three, and Assistant Sub-Inspector has four. There is also one DIG and one Additional DIG. However, five respondents did not share their designation with the researcher.

4.2 Descriptive Analysis

The following results were found after the descriptive analysis of the dependent and independent variables of this paper.

Table 2: Descriptive Statistics Results

Variable	Mean	Median	Mode	Standard Deviation	Range	Skewness	Kurtosis
ACE	3.8	3.75	3.75	0.61	3.25	-0.73	2.34
ICR	4.28	4.5	4.5	0.5	1.75	-0.31	-0.80
GCM	3.96	4.0	4.0	0.53	2.5	-0.27	0.38
EPEC	4.28	4.5	5.0	0.67	2.5	-0.90	0.12
PCFH	3.86	4.0	3.25	0.63	2.5	-0.20	-0.80
NVC	4.3	4.25	4.25	0.55	2.0	-0.55	0.04
IDF	4.56	5	5	0.67	3	-1.78	4.02

Source: Author's work

Here, ACE refers to the Accuracy of Collected Evidence, ICR to the Improved Conviction Rate, GCM to Geolocation and Criminal Mapping, EPEC to the Enhanced Process of Evidence Collection, PCFH to the Prevention of Crime, NVC to the New Viewpoint of a Case, and IDF to the Importance of Digital Forensics. From the tables, it is observed that,

a) The New Viewpoint of a Case, Enhanced Process of Evidence Collection, and Improved Conviction Rate are the most crucial roles played by digital forensics, as shown by the mean and median of each independent variable. Their mean and median values are the highest, at 4.2987 and 4.25, 4.2804 and 4.5, and 4.2805 and 4.5, respectively.

b) The Enhanced Process of Evidence Collection (EPEC) shows more variability than the other independent variables, as its standard deviation and variance are higher than those of all other variables. Additionally, the range of EPEC is also higher than most of the independent variables.

c) The Enhanced Process of Evidence Collection shows a high degree of negative skew, with a skewness close to -1. The New Viewpoint of a Case has a slight negative skew, with a skewness of -0.5.

d) The distribution of the Accuracy of Collected Evidence is highly peaked, as its kurtosis value is greater than +1.

4.3 Regression Analysis Results

Regression analysis is a statistical method used to understand the relationship between one dependent variable and one or more independent variables. This study uses regression analysis to examine how different factors, such as the accuracy of evidence collection and enhanced processes of evidence collection, influence the effectiveness of digital forensics in combating crime. The results showed the strength and significance of these relationships, with some variables showing more substantial impacts than others. This figure illustrates the regression analysis conducted to examine the relationship between the variables of digital forensics and crime fighting. The model shows a significant positive relationship between the accuracy of evidence collection and the ability of digital forensics to combat crime. Analyzing all the variables, the following results were found:

Table 3: Regression Statistics

Regression Statistics	
Multiple R	0.745
R Square	0.555
Adjusted R Square	0.476
Standard Error	0.4865
Observations	52

Table 4: ANOVA Results

ANOVA					
	df	*SS*	*MS*	*F*	*Significance F*
Regression	6	10.049	1.675	7.075	5.99954E-05
Residual	34	8.048	0.237		
Total	40	18.097			

Source: Author's work

Table 5: Regression Results

	Coefficients	Std. Error	t Stat	P-value	Lower 95%	Upper 95%
Intercept	2.928	0.860	3.404	0.002	1.180	4.676
ACE	0.120	0.178	0.673	0.505	-0.242	0.481
EPEC	0.483	0.172	2.801	0.008	0.133	0.834
ICR	-0.356	0.203	-1.757	0.088	-0.767	0.056
PCFH	-0.328	0.131	-2.501	0.017	-0.594	-0.061
GCM	-0.077	0.157	-0.491	0.627	-0.396	0.242
NVC	0.513	0.196	2.616	0.013	0.114	0.911

From Table-3, it can be observed that,

a) In the regression analysis, the Multiple R was 0.7451. Multiple R shows the relationship between independent variables and dependent variables. It shows how much the independent variables depend on the dependent variable. The higher the multiple R, the better the model. Here, the Multiple R is approximately 74%, indicating a strong relationship between the independent and dependent variables.

b) The R-squared value was 0.5552, while the adjusted R-squared value was 0.4767. R square is called the coefficient of determination. R-squared measures how strongly the independent variables define the dependent variable. In the given model, independent variables are 55% able to explain digital forensics. Adjusted R-squared is the interrelationship between the independent variables. The regression statistics show that the independent variables are correlated to each other by 47%.

c) However, it also affects R. R-squared is always greater than the adjusted R-squared, and these regression analyses follow the same pattern. R squared is greater than adjusted R squared.

d) A very insignificant 48% standard error is also present in the model. How much error the model contains in several processes is shown by the standard error.

4.3.1 ANOVA

In the ANOVA (table 4),

a) Degrees of freedom (df) represent the maximum number of independent values that can vary in a data sample. Here, the degrees of freedom (df) are six, which is equal to the number of independent variables.

b) SS is of regression is 10.0490, MS 1.6748, which refers to the sum of squares (SS) for each source of variation and mean sum (MS) of variation.

c) The F in the ANOVA table is the variation between sample means or variation within the sample. The higher the F value, the lower the p-value. Here, the F value is high at 7.0752, which results in a lower p-value in the next section.

d) Significance F in the ANOVA table is 5.99954E-05. It can be written as 0.00005. This is the measurement of the significance level of the model. As the significance F is lower than 0.05, this model is acceptable.

e) In the next table, the intercept coefficient is 2.9277, which means that when all independent variables (ACE, EPEC, ICR, PCFH, GCM, and NVC) equal zero, the expected value of Y is still 2.9277, or Y = 2.9277.

f) The coefficients of ACE are 0.1196, EPEC is 0.4831, ICR is -0.3558, PCFH is -0.3277, GCM is -0.0770, and NVC is 0.5125. The coefficient shows how much the dependent variable will

change if one independent variable change by 1 unit. For example, if ACE is altered by 1 unit, then the Impact of Digital Forensics will be changed by 0.1196.

4.5 Hypothesis Testing

Hypothesis 1: Accuracy of evidence collected through digital forensics positively influences the ability of digital forensics to combat crime (Accepted)

The analysis aimed to test Hypothesis 1, asserting that the accuracy of evidence collected through digital forensics positively influences its effectiveness in combating crime. The combined likelihood ratio test yielded a highly significant relationship (p-value: 3.49e-05), supported by a robust combined correlation coefficient of 0.8615. Subsequent assessments of predictor variables revealed that the variables "Correctness of Digital Forensics," "Positive Impact on Evidence," and "High Accuracy" exhibited statistically significant positive influences (coefficients: 0.1862, 0.4153, and 0.3223, respectively; p-values: 0.123, 0.000, and 0.000). As a result, we accept Hypothesis 1 for these variables, indicating their substantial impact on the perceived importance of digital forensics in crime combat. However, the variable "Misleading" did not demonstrate a significant influence (coefficient: -0.0728, p-value: 0.291), leading to the non-acceptance of the hypothesis for this variable.

Table 6: Combined Likelihood Test Result (*Accuracy of Evidence Collected)*

Combined p-value	Combined Correlation Coefficient	Dep. Variable	Log-Likelihood	Deviance	Pearson chi2	Intercept Coef	Predictor Coef	P-value
3.49E-05	0.8615	Digital forensics correctness	-47.81	19.148	19.1	3.939	0.186	0.123
		Positive impact on evidence	-37.56	12.91	12.9	2.838	0.415	0
		High accuracy	-41.688	15.131	15.1	3.2898	0.322	0
		misleading	-48.442	19.619	19.6	4.8376	-0.073	0.29

Hypothesis 2: An enhanced process of evidence collection positively contributes to the ability of digital forensic in combating crime (Accepted)

The investigation aimed to evaluate Hypothesis 2, proposing that specific factors related to digital forensics significantly contribute to the perceived importance of digital forensics in crime prevention. The combined likelihood ratio test revealed a highly significant relationship (p-value: 2.53e-08) with a robust combined correlation coefficient of 0.9653, indicating a substantial association. Upon examining four predictor variables—time efficiency, fostering growth of evidence collection, data discovery from erased evidence, and increased efficiency of police—their impacts on the dependent variable importance of digital forensics were assessed. Notably, time efficiency exhibited a coefficient of 0.2965 with a highly significant p-value of 0.001, signifying a positive and statistically significant influence. Similarly, fostering the growth of evidence collection displayed a

noteworthy coefficient of 0.5606, coupled with a highly significant p-value of 0.000, indicating a substantial positive impact. Conversely, data discovery from erased evidence yielded a coefficient of 0.0846 with a non-significant p-value of 0.378, suggesting no discernible influence. Lastly, increased police efficiency demonstrated a significant positive impact, with a coefficient of 0.3966 and a p-value of 0.000.

Table 7: Combined Likelihood Test Result (*Enhanced Process of Evidence Collection)*

Combined p-value	Combined Correlation Coefficient	Dep. Variable	Log-Likelihood	Deviance	Pearson chi2	Intercept Coef	Predictor Coef	P-value
2.53e-08	0.9653	Time efficiency	-43.412	16.169	16.2	3.3687	0.2965	0.001
		Fostering growth of evidence collection	-30.234	9.7399	9.74	2.1441	0.5606	0.000
		Data discovery from erased evidence	-48.615	19.750	19.8	4.2980	0.0846	0.378
		Increased efficiency of police	-42.310	15.497	15.5	2.8501	0.3966	0.000

Hypothesis 3: Improved conviction rate is positively associated with the importance of digital forensics (Rejected)

Hypothesis 3 aimed to explore the relationship between improved conviction rates and the perceived importance of digital forensics. However, the combined likelihood ratio test resulted in a non-significant p-value of 0.2603, indicating a weak association. The combined correlation coefficient was relatively low at 0.0632. The study examined how four predictor variables—accurate conviction, higher cybercrime conviction, enhanced judiciary accuracy, and increased conviction rates—affect the importance of digital forensics. However, none of the variables demonstrated a statistically significant influence. For accurate conviction, the coefficient was -0.1046 with a non-significant p-value of 0.350. Higher cybercrime conviction exhibited a coefficient of 0.1392 with a non-significant p-value of 0.324. Enhancing judicial accuracy showed a coefficient of 0.0587 with a non-significant p-value of 0.620. Lastly, for boosting conviction rates, the coefficient was -0.0115 with a non-significant p-value of 0.921.

Table 8: Combined Likelihood Test Result (*Improved Conviction Rate)*

Combined p-value	Combined Correlation Coefficient	Dependent Variable	Independent Variable	Log-Likelihood	Deviance	Pearson chi2	Intercept Coef	Predictor Coef	P-value
0.2603	0.0632	Importance of digital forensics	Accurate conviction	-49.011	20.054	20.1	4.6829	-0.0115	0.921

Combined p-value	Combined Correlation Coefficient	Dependent Variable	Independent Variable	Log-Likelihood	Deviance	Pearson chi2	Intercept Coef	Predictor Coef	P-value
0.2603	0.0632	Importance of digital forensics	Higher cybercrime conviction	-48.889	19.960	20.0	4.3763	0.0587	0.620
0.2603	0.0632	Importance of digital forensics	Enhancing judiciary accuracy	-48.567	19.714	19.7	5.0349	-0.1046	0.350
0.2603	0.0632	Importance of digital forensics	Boosting conviction rates	-48.515	19.675	19.7	4.0428	0.1392	0.324

Hypothesis 4: Prevention of crime is related to the importance of digital forensics (Rejected)

Hypothesis 4 sought to explore the relationship between various crime prevention factors and the perceived importance of digital forensics. The combined likelihood ratio test did not yield a significant p-value (0.4670), indicating no strong association. The combined correlation coefficient was notably negative at -0.5727, suggesting an inverse relationship. The analysis focused on four predictor variables: preventing major crimes, preventing general crimes, rapid response after missed prevention, and insufficient technology for preventing significant crimes. Their impacts on the dependent variable, the importance of digital forensics, were examined. For preventing major crimes, the coefficient was -0.1299 with a non-significant p-value of 0.199. Preventing general crimes exhibited a coefficient of -0.1173 with a non-significant p-value of 0.297. Rapid response after missed prevention showed a coefficient of -0.1069 with a non-significant p-value of 0.281. Lastly, for insufficient technology preventing significant crimes, the coefficient was -0.0858 with a non-significant p-value of 0.222.

Table 9: Combined Likelihood Test Result (*Prevention of Crime*)

Combined p-value	Combined Correlation Coefficient	Dependent Variable	Independent Variable	Log-Likelihood	Deviance	Pearson chi2	Intercept Coef	Predictor Coef	P-value
0.4670	-0.5727	Importance of digital forensics	Preventing major crimes	-48.171	19.416	19.4	5.1066	-0.1299	0.199
		Importance of digital forensics	Preventing general crimes	-48.458	19.631	19.6	5.1061	-0.1173	0.297
		Importance of digital forensics	Rapid response after missed prevention	-48.418	19.601	19.6	5.0665	-0.1069	0.281
		Importance of digital forensics	Insufficient technology for preventing big crimes	-48.253	19.477	19.5	4.9381	-0.0858	0.222

Hypothesis 5: Enhanced geo location and criminal mapping positively influence the ability of digital forensics to combat crime (Accepted)

Hypothesis 5 explored the relationship between geolocation factors and high accuracy in digital forensics. The combined likelihood ratio test produced a p-value of 0.0794, with a combined correlation coefficient of 0.0172. The study examined three predictor variables: 'Accurate Criminal Location,' 'Effective Geolocation in Cyber FinTech Crimes,' and 'Criminals Manipulating Location.' For the variable 'Accurate Criminal Location' the coefficient was -0.1496, indicating a negative but non-significant impact (p-value: 0.383). Conversely, 'Effective Geolocation in Cyber FinTech Crimes' exhibited a positive and significant influence (coefficient: 0.3477, p-value: 0.041). The variable 'Criminals Manipulating Location' had a negative impact (coefficient: -0.1070) with a non-significant p-value of 0.303. While the overall p-value suggests a trend, the mixed results for individual predictors require caution in interpretation.

Table 10: Combined Likelihood Test Result (*Enhanced Geo Location and Criminal Mapping)*

Combined p-value	Combined Correlation Coefficient	Dependent Variable	Independent variable	Log-Likelihood	Deviance	Pearson chi2	Intercept Coef	Predictor Coef	P-value
0.0794	0.0172	High accuracy	Accurate criminal location	-71.007	46.732	46.7	4.7341	-0.1496	0.383
		High accuracy	Effective geolocation cyber finTech crimes	-69.310	43.778	43.8	2.6485	0.3477	0.041
		High accuracy	Criminals manipulating location	-70.854	46.456	46.5	4.5086	-0.1070	0.303

Hypothesis 6: New viewpoints of a case positively influence the ability of digital forensics to combat crime (Accepted)

Hypothesis 6 investigated the impact of various factors on high accuracy in digital forensics. The combined likelihood ratio test yielded a p-value of 0.0006, and the combined correlation coefficient was exceptionally high at 0.9551. The study examined four independent variables: 'Offering Fresh Case Perspectives,' 'Uncovering Hidden Criminals,' 'Getting a New Viewpoint,' and 'Increased Digital Evidence Rechecking.' For 'Offering Fresh Case Perspectives,' the coefficient was 0.5346, indicating a positive and significant impact (p-value: 0.001). 'Uncovering Hidden Criminals' exhibited a positive and significant influence (coefficient: 0.7529, p-value: 0.000). 'Getting a New Viewpoint' showed a positive and significant effect (coefficient: 0.5720, p-value: 0.001). Lastly, 'Increased Digital Evidence Rechecking' had a positive and significant impact (coefficient: 0.6040, p-value: 0.002). The results suggest that these factors contribute significantly to achieving high accuracy in digital forensics.

Table 11: Combined Likelihood Test Result (*Enhanced Geo Location and Criminal Mapping)*

Combined p-value	Combined Correlation Coefficient	Dependent Variable	Independent Variable	Log-Likelihood	Deviance	Pearson chi2	Intercept Coef	Predictor Coef	P-value
0.0006	0.9551	High accuracy	Offering fresh case perspectives	-66.058	38.631	38.6	2.0037	0.5346	0.001
		High accuracy	Uncovering hidden criminals	-64.393	36.235	36.2	0.9008	0.7529	0
		High accuracy	Getting a new viewpoint	-65.872	38.356	38.4	1.687	0.572	0.001
		High accuracy	Increased digital evidence rechecking	-66.825	39.787	39.8	1.4665	0.604	0.002

5. Discussion

It is clear from the results section that the analysis supports hypotheses 1, 2, 5, and 6, but not hypotheses 3 and 4. The regression analysis shows that an improved conviction rate does not positively relate to the importance of digital forensics, so the study rejects hypothesis 3. The p-value for the relationship between improved conviction rates and digital forensics was non-significant (0.2603), suggesting that there is insufficient evidence to support this hypothesis. This indicates that other factors, such as judicial processes or case complexity, may be influencing conviction rates, rather than digital forensics alone.

Similarly, Hypothesis 4, which suggested that the prevention of crime is related to the importance of digital forensics, was also rejected. The combined likelihood ratio test yielded a non-significant p-value (0.4670), and the correlation coefficient was negative (-0.5727). This result indicates that digital forensics, while crucial in identifying and solving crimes, does not have a direct influence on crime prevention as initially hypothesized. The lack of a significant relationship reflects limitations in the scope of data or other factors, such as the strategic use of digital evidence by law enforcement agencies.

According to the first hypothesis, the Accuracy of evidence collected through digital forensics positively influences the ability of digital forensics to combat crime. According to CBS News (2017), as part of an insurance fraud, Ross Compton set fire to his own home in Middletown, Ohio. Compton initially told authorities that he witnessed the fire when he woke up. Still, later Compton's pacemaker's data revealed beyond a reasonable doubt that he was the one who started the fire in his home. The USA police had previously validated the theory that we found to be true for the Bangladeshi police.

The second hypothesis claims that an enhanced process of evidence collection positively contributes to the ability of digital forensics to combat crime. Bevan Harley (2023) wrote, Dennis Rader, the infamous BTK murderer who killed ten people in Wichita, Kansas, between 1974 and 1991, was not taken into custody until authorities obtained a disc with evidence against him. This was among the first cases that digital forensics was able to solve. Digital forensics resolved cases by extracting data from the evidence that had previously remained unsolved.

After the news on Channel 24 (2022), everyone was in shock following the horrific heist at the former ambassador's residence in Dhaka, Bangladesh. The thieves went unpunished and carried on robbing several locations in Dhaka. However, the Dhaka Detective Branch used geo-location to track down the robbers and discovered that they frequently visited the victim's home in the capacity of a plumber, food delivery person, etc. According to hypothesis 5, enhanced geo-location and criminal mapping positively influence the ability of digital forensics to combat crime, and Bangladeshi police are already putting it into practice.

Most people in Bangladesh are aware of Abrar Fahad's case, a student at the Bangladesh University of Engineering and Technology. Investigators initially used social media forensics on several homicides, which led them to discover a few additional implicated students. According to Prothom Alo (2019), their masterminding role in Abrar Fahad's murder appeared in a leaked Messenger conversation. In this instance, Bangladeshi police have validated our hypothesis 6 —that new viewpoints of a case positively influence the ability of digital forensics to combat crime.

Our four hypotheses become clearer when looking at the national and international instances. These real-world instances all support our findings. Additionally, our results make sense in practical applications. The other findings, apart from the hypothesis testing, are:

i. The researcher wanted to identify the variables of combating crimes in the Bangladesh police department. From the result section, it is found that six independent variables, like the accuracy of collected evidence, enhanced process of evidence collection, improved conviction rate, geolocating, and criminal mapping, prevention of crime, new viewpoint of a case and the dependent variable were digital forensics. Most of the respondents strongly agreed or agreed on observing those six independent variables as a role of the dependent variable.

ii. In the second objective, the researcher aimed to evaluate the influence of digital forensics on combating crime within the Bangladesh Police. Descriptive statistics show that a new viewpoint on a case, an enhanced evidence collection process, and an increased conviction rate have the greatest influence in combating crime as roles of digital forensics, based on the mean and median values of the independent variables. Their mean and median values, which are 4.2987 and 4.25, 4.2804 and 4.5, and 4.2805 and 4.5, respectively, are the highest.

iii. In the third objective, the researcher wanted to investigate the relationship between the variables to explain the acceptance of digital forensics. From the multicollinearity, it is shown that VIF is less than 3 between all independent variables. Multicollinearity refers to the

situation where independent variables in a regression model are highly correlated with each other.

This can cause issues in interpreting the results because it becomes difficult to determine the individual effect of each independent variable on the dependent variable. In this study, the analysis revealed that multicollinearity was not a problem, as the variance inflation factor (VIF) values were below 3, which is considered acceptable. This implies that multicollinearity is nonexistent. Researchers can predict the values of all independent variables independently. Total VIF from the regression analysis is below 3, which proves the acceptance of the whole model of this research paper.

Apart from this, regression analysis showed a 74% relationship between independent and dependent variables. The ANOVA table demonstrates how changes in the independent variables affect the dependent variable.

6. Conclusion

The findings of this research highlight the crucial impact of digital forensics in Bangladesh's police force's efforts to combat crime. Researchers identified key factors essential to the success of digital forensics, including the accuracy of evidence collection, improved evidence handling procedures, and enhanced ability to map criminals and prevent crimes. The study emphasizes the need for the Bangladesh Police to fully integrate digital forensics into their investigative practices, as this has been shown to increase conviction rates and offer valuable new insights into criminal cases.

Furthermore, the research advocates for the continued development of specialized training programs for police officers, ensuring that they have the necessary skills to use digital forensics tools effectively. Finally, it stresses the importance of updating policies and investing in state-of-the-art technology to ensure the Bangladesh Police can keep pace with the rapidly changing landscape of digital crime. This research lays out a foundation for future advancements in digital forensics within the police department, providing actionable recommendations for improving crime-fighting strategies.

6.1 Recommendations

To strengthen the Bangladesh Police's digital forensics capabilities, it is helpful to draw from the experiences of other nations that have successfully implemented digital forensics policies. For instance, the United States has significantly enhanced its digital forensics capabilities through the National Integrated Ballistic Information Network (NIBIN), which helps track digital evidence related to firearms. Additionally, the United Kingdom has successfully integrated digital forensics into its criminal investigations through its Forensic Computing Service (FCS), which is part of the National Crime Agency (NCA). These agencies have adopted advanced forensic tools and built strong partnerships between law enforcement and tech experts, which has resulted in more efficient evidence collection and improved conviction rates.

Similarly, Singapore's government has successfully implemented digital forensics strategies through its Cybersecurity Agency. The agency's comprehensive approach includes investing in the

latest forensic tools and training law enforcement personnel, allowing them to tackle cybercrime more effectively. Bangladesh could benefit from adopting a similar integrated approach, focusing on improving both the technology and the skills of its law enforcement officers. By observing all the findings above, the following recommendations can be made:

- According to the study, digital forensics can significantly enhance the Bangladesh police department's capacity to combat crime. Therefore, the government and police departments should invest more in digital forensics technology to improve the efficiency of criminal investigations and resolutions.
- Since the study found that accurate digital forensics evidence positively impacts the ability to combat crime, the study recommends developing specialized training programs for police officers to acquire the necessary skills and knowledge in digital forensics tools and techniques. This will ensure that police officers have the proper training and tools to conduct effective investigations.
- The study emphasizes the significance of a more efficient evidence collection procedure and a higher conviction rate in the fight against crime using digital forensics. Therefore, the Bangladeshi police should collaborate with digital forensics experts, such as forensic analysts, to strengthen their evidence collection process and improve conviction rates.
- Given the significance of digital forensics in fighting crime, the Bangladesh Police Department should establish units specializing in digital forensics investigations. Thus, investigators can conduct digital forensic investigations more efficiently and effectively.
- As technology continues to advance, it is crucial that digital forensics policies are reviewed and updated on a regular basis to keep up with the most recent trends and techniques.

6.1.1 Potential Challenges in Implementing the Recommendations:

While the recommendations outlined above provide a roadmap for enhancing digital forensics within the Bangladesh Police, there are several challenges to consider when implementing them:

- **Budgetary Constraints:** Implementing a robust digital forensics program requires significant investment in both technology and human resources. The procurement of advanced forensic tools and systems, as well as the establishment of dedicated digital forensics units, can be costly. To mitigate this challenge, the government may need to prioritize funding and seek financial support through international cooperation or partnerships with tech companies specializing in digital forensics.
- **Training and Skill Development:** One of the biggest hurdles is ensuring that police officers have the necessary skills to use sophisticated digital forensic tools effectively. While technical training is essential, it can be resource-intensive and time-consuming. To address this, Bangladesh could implement a phased training program that initially targets officers in critical roles, followed by expanded training for the broader police force. Additionally, partnerships

with international organizations and universities could be leveraged to provide affordable training programs.

- **Cybersecurity and Data Privacy:** With the increasing reliance on digital evidence comes the challenge of ensuring that the evidence collected is secure and handled in compliance with privacy laws. There must be a clear policy for data protection and evidence handling to prevent misuse or unauthorized access. The Bangladesh Police could draw on the experience of countries like Estonia, which has implemented strict data privacy laws alongside its digital forensics policies.

6.2 Limitations

While this study provides valuable insights, researchers should consider several limitations. First, the sample size of 52 respondents is relatively small and may not fully represent the views of all law enforcement officers involved in digital forensics. Second, the study relied solely on responses from police officers, which may introduce response bias, as officers might have provided answers that reflect institutional biases or positive views of digital forensics practices.

Future studies could expand the sample to include a broader range of stakeholders, such as prosecutors, defense attorneys, and judges, to obtain a more comprehensive understanding of the impact of digital forensics.

6.3 Implications

- **Practical Implications**: This study has important practical implications for law enforcement agencies in Bangladesh and similar developing countries. It suggests that prioritizing investment in digital forensics, along with comprehensive officer training, can significantly improve evidence collection practices, leading to higher conviction rates and better crime prevention strategies. Additionally, strengthening the use of digital forensics could also reduce the reliance on traditional investigative methods, which may be more prone to human error.

- **Theoretical Implications**: The study contributes to the growing body of research on digital forensics by connecting General Deterrence Theory and Routine Activity Theory to the use of digital forensic tools in criminal investigations. By applying these theories to the context of Bangladesh, this research extends the understanding of how digital forensics can enhance crime prevention and law enforcement practices.

6.4 Future Research

Future research could explore the impact of digital forensics training programs on the effectiveness of evidence collection and criminal investigations. Given the limitations of this study sample, additional research should also focus on a more diverse set of respondents, including non-police professionals involved in criminal investigations, such as prosecutors and digital forensic experts. Furthermore, studies could investigate the economic implications of implementing advanced digital

forensics technologies in low-budget law enforcement agencies, particularly in developing countries like Bangladesh.

Acknowledgment

This study was made possible by the support of 52 members of the Bangladesh Police Department who have used or engaged with using Digital Forensics. Their valuable insights and cooperation have significantly contributed to the success of this study.

Funding

No funding was received for this study.

Conflict of Interest

The authors declare no conflict of interest.

Citation

Sharmin, K. & Rahman, I. M. (2025). Digital Forensics Empowerment of Bangladesh Police: A Comprehensive Analysis of Its Role in Preventing Crimes and Enhancing Investigative Capabilities. *Bangladesh Journal of MIS, 11*(1), 01-26. https://doi.org/10.61606/BJMIS.V11N1.A1

References

Al Imran, A. (2017, December 8). Searchlight: Admission is fraudulent. Channel 24. https://youtu.be/VnQO3yunDGM?si=p63LjlxnD561zwZp

Al Imran, A. (2022, June 4). Robbery at the ambassador's house. Channel 24. https://tinyurl.com/bdffbvrx

American Statistical Association. (2019). Ethical guidelines for statistical practice.

Bangladesh Legal Information Institute. (2022). The evidence acts 1872 65B. http://bdlaws.minlaw.gov.bd/act-24/section-51389.html

Beccaria, C. (1764). On crimes and punishments (M. J. B. C. & H. P. D. R. D. L. R. Trans.). Hackett Publishing Company. (Original work published 1764)

Belshaw, S. H. (2019). Next generation of evidence collecting: The need for digital forensics in criminal justice education. Journal of Cybersecurity Education, Research and Practice, 2019(1), Article 3.

Bocij, P. (2014). Cybercrime and cybersecurity: An introduction. Pearson Education Limited.

BlueVoyant. (n.d.). Understanding digital forensics: Process, techniques, and tools. https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools

Braga, A. A., Papachristos, A. V., & Hureau, D. M. (2014). The effects of hot spots policing on crime: An updated systematic review and meta-analysis. Justice Quarterly, 31(4), 633-663.

Carter, D. L. (2013). Homicide process mapping: Best practices for increasing homicide clearances. Institute for Intergovernmental Research.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

CBC News. (2017, February 7). Man's pacemaker data used against him in arson case. CBS News. https://www.cbsnews.com/news/mans-cardiac-pacemaker-data-led-to-arson-charges/

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589

Fatema, H. (2022, October 27). Admissibility of digital evidence: Opening of a legal new era. Daily Sun. https://www.daily-sun.com/post/652585/Admissibility-of-Digital-Evidence:-Opening-of-a-Legal-New-Era

Garfinkel, S. (2013). Digital forensics. American Scientist, 101(5), 370.

Hossain, M. A., Hasan, M. R., & Islam, M. S. (2019). A comprehensive framework for digital forensics implementation in Bangladesh. International Journal of Cyber Criminology, 13(1), 94-110.

Hurley, B. (2023, August 24). The BTK killer's need for notoriety led to his capture a decade ago. Independent News. https://www.the-independent.com/news/world/americas/crime/btk-killer-dennis-rader-suspect-b2399051.html

Islam, M. S., Hossain, M. A., & Hasan, M. R. (2019). Adoption and implementation of digital forensics in Bangladesh: A study on police personnel. International Journal of Cyber Criminology, 13(2), 353-369.

Kabir, M. H., Hasan, M. R., & Sattar, M. A. (2020). Digital forensics in Bangladesh: A review of current trends and future directions. Journal of Digital Forensics, Security and Law, 15(3), 73-86.

Kemp, S. (2023, February 13). Digital 2023: Bangladesh. https://datareportal.com/reports/digital-2023-bangladesh

Kruse, W. G., & Heiser, J. G. (2002). Computer forensics: Incident response essentials. Addison-Wesley Professional.

Kshetri, N. (2014). The global cybercrime industry: Economic, institutional and strategic perspectives. CRC Press.

Mahmud, M. (2020). Challenges of digital forensics implementation in Bangladesh: A qualitative study. International Journal of Digital Crime and Forensics (IJDCF), 12(2), 44-62.

Nelson, B., Phillips, A., & Steuart, C. (2010). Guide to computer forensics and investigations. Cengage Learning.

Palmer, G. L. (2001). A road map for digital forensic research (Technical Report DTR-T0010-01). Digital Forensic Research Workshop (DFRWS).

Pollitt, M. M. (2013). Digital forensics: Challenges and future research directions. Journal of Information Security, 4(02), 47-53.

Prothom Alo. (2019, October 10). Messenger conversation before killing Abrar Fahad. Prothom Alo. https://tinyurl.com/285mc822

Rahman, M. A. (2017). Digital forensic investigation in Bangladesh: A review of current practice and future directions. International Journal of Cyber-Security and Digital Forensics, 6(3), 130-142.

Rahman, M. A., Islam, M. S., & Hasan, M. R. (2020). Role of digital forensics in cybercrime investigations in Bangladesh. International Journal of Cyber Criminology, 14(2), 173-189.

Shayna, J. (2016, July 22). 3 ways to prevent crime with technology. https://graduate.northeastern.edu/resources/3-ways-to-prevent-crime-with-technology/