Exploring Transboundary Solutions for Forensic Investigations: An Interdisciplinary Approach to Addressing Criminal Behavioral Challenges

Barkha Shree[1,*], Parneeta Dhaliwal[1], and Sanjay Singh[1]

ARTICLE INFO

Article history:
Received: 22 May 2023
Revised: 8 September 2023
Accepted: 24 October 2023

Keywords:
Behavioral evidence analysis
Criminal profile
Digital forensics
Offender behavior
Digital crime

ABSTRACT

In the era of escalating digital crimes, the analysis of existing digital artifacts necessitates enhanced methodologies to unveil offender behavior and investigate criminal activities. In light of the pressing need to address transboundary criminal investigation challenges and promote faster crime resolution, this research article introduces a pioneering approach, Behavioral Evidence Analysis-Standardized (BEA-S), aimed at offering a unified strategy for the comprehensive behavioral analysis of criminals. Our proposed design encompasses a behavior-capturing system specifically tailored for the creation of offender profiles in digital forensic investigations. To validate the practical utility of our model, we present a detailed demonstration of its application in a real-life case study. Through a rigorous comparative analysis with established techniques, we establish the novelty and robustness of our approach, affirming its high effectiveness in addressing forensic challenges with both regional and international perspectives. This research article contributes to the advancement of knowledge by providing a valuable tool for tackling digital crimes and ensuring a secure and sustainable digital environment.

1. INTRODUCTION

Recently, a probe into the offender or victim behaviors, known as Behavioral Evidence Analysis (BEA), has become an essential tool in Digital Forensics (DF) [1]. DF is a specialized discipline encompassing the systematic collection, preservation, and analysis of electronic data stored on various digital devices [1]. It serves as a crucial tool for uncovering digital evidence that can be presented in legal proceedings or used to investigate cybercrimes. On the other hand, BEA involves a meticulous study of behavioral patterns, actions and personality attributes exhibited by individuals engaged in criminal activities [2]. BEA examines evidence from a particular case to derive the behavioral and psychological traits of the likely criminal [2].

The existing techniques deliberate the usefulness of BEA, but there is no homogenous method for its functional integration in criminal forensic investigations as depicted by authors Shree and Dhaliwal in a comprehensive review of existing literature [3]. To bridge the existing knowledge gap, our paper proposes a detailed and homogenous approach to BEA. Our proposed system, Behavioral Evidence Analysis-Standardized (BEA-S), extends the existing BEA process systems [3]. BEA-S is a systematic and lucid method for criminal behavior analysis during investigation of digital crimes. Based on the evidence, the analysis results in fewer potential suspects, thus easing offender identification. Our approach has application across various forensic spheres.

In this paper, Section 2 contains related work. Section 3 covers our proposed approach- BEA-S. Section 4 gives the application of BEA-S on a real-life case study. Section 5 gives a comparative analysis of BEA-S with existing models. Sections 6 and 7 provide the conclusion and future scope, respectively.

2. RELATED WORK

Modern tools and machine learning technologies have guided DF investigations for acquisition of data [4, 5] and analysis of underlying patterns [6]–[9]. However, the incorporation of BEA into DF remains limited.

Previously, researchers have presented different BEA strategies for use during criminal investigations. Authors Almond et al. [10] described an offender's behavioral profile based on his/her environment comprising demographics, socioeconomic upbringing, and social relationships. Authors O'Meara et al. [11] applied extensive research in investigative psychology to analyze the crime scene and create a profile. Some other studies [10, 11] appointed criminal investigative analysis into the elements at crime sites to construct a profile. Johnson and King [14] presented a suspect-based technique built on factors such as race, ethnicity, religion, age, and dress style.

[1]*Department of Computer Science and Technology, Manav Rachna University.*
**Corresponding author:* Barkha Shree; E-mail: barkhashree55@gmail.com.

Hofhansel et al. linked the morphology of the criminal brain to antisocial behavior in offenders [15]. Shenoy et al. depicted the use of video analysis for finding clues of violent objects or suspicious behavior which could lead to crime [16]. Authors Rokven et al. determined the influence of the friends of criminals on the offender's own criminal behavior [17]. Author Shagufta aimed to examine psychopathic traits of offenders as moderators of criminal friends' influence on offender behavior [18]. Authors Willmott et al. emphasized the use of crime-related locations to identify the most probable location from which a serial offender was based [19]. Espuig, Vilar and Sala described criminal cognition, including emotional intelligence, prosocial behavior, and cultural dimensions as a measure of predictive capacity for criminal thinking [20].

Nesse's evolutionary system [21] suggested that criminal behavior was influenced by selective pressure and that mental instincts and behaviors were adaptive. Willmott et al. [22] demonstrated the role of childhood experiences in determining constituents of an offender's adult personality. A study by Walinga [23] described offender behavior as a result of circumstances and external stimuli. Other researchers depicted criminal behavior as an interpretation of: (a) social situations [24], (b) choice, free will, and self-image [25], and (c) biological factors and genetic determinants [26]. Authors Islam et al. argued the lack of distinction between criminal and non-criminal groups and debated that certain delinquent stigma made people start identifying with the appropriate social group and act accordingly [27].

Poltava et al. discussed the social characteristics of juvenile offenders responsible for their criminal behavior [28]. Researchers Kehinde et al. determined group thinking, cohesiveness and personality characteristics for predicting criminal behavior [29]. A study by Woster specified existing killer typologies to differentiate between solo and team killers [30]. Author Galimotu examined cognitive continence and deviant behavior propensities as factors for identifying personality traits as predictors of criminal behavior [31]. Authors Tkazky et al. argued that different crime scenes were left behind by psychopaths and nonpsychopaths revealing distinguishing features of victim choice, violence and other offense variables [32].

A social media evidence analysis approach by Arshad et al. [33] suggested the examination of metadata including location tags, timestamps, and device details. Sunde and Dror's cognitive bias analysis design [34] focused on the prejudice of the DF practitioner while determining offender behavior. Adeyemi et al. proposed a digital thinking style framework [35] describing criminal behavior based on the different human thinking styles on the internet. A web browser-based model [36] by Al Owainer et al. defined the analysis of the suspect's browser records including URLs, search histories, and cache data dump.

Slide and Angelopoulou [37] proposed a DF model implementing BEA through a cyberstalking profiling methodology. Rogers [38] proposed a behavioral DF model that relied on timeline and frequency analysis to establish the perpetrator of the crime. Mutawa et al. [39] gave a behavioral DF model based on hypothesis testing.

The existing techniques provide different approaches to the analysis of available behavioral clues but none determines a standardized method to investigate the behavioral evidence while probing a criminal case. These current approaches lack standardization and fail to provide systematic investigative directions for BEA. Since no lucid, all-inclusive, and step-by-step approach exists currently, the incorporation of BEA remains limited in the field of digital forensics. Our proposed approach detailed in the next section aims to address these challenges.

3. PROPOSED APPROACH- BEA-S

Our proposed approach, BEA-S, is a novel and homogenous system for behavior analysis in forensic investigations. The design of BEA-S is illustrated in Figure 1. It consists of four fundamental phases of the forensic process, including identification, collection, analysis, and reporting. It merges BEA in stage three, i.e., the analysis phase.

3.1 Stage I: Identification

The Identification stage filters the forensic devices collected from the crime scene to find the "devices of interest." These devices may comprise laptops, tablets, mobile phones, computers, or other electronic gadgets. This stage also includes identifying the locations of the physical evidence relevant to the crime.

3.2 Stage II: Extraction

The second stage of Extraction recovers digital evidence from the devices of interest and physical evidence from the crime scene. It preserves electronically stored data and safeguards the integrity of the crime scene. It involves clicking pictures of the crime site and logging data corresponding to the evidence. It also includes capturing physical evidence like fingerprints, blood samples, etc. The output of the extraction stage comprises all the digital and physical data that could provide valuable pointers during the investigation.

3.3 Stage III: Analysis

The third stage of Analysis is a crucial step in BEA-S. It is an in-depth systematic exploration of the digital and physical evidence related to the case. The Analysis phase is primarily responsible for evaluating the evidence's impact and establishing inferences from evidence analysis.

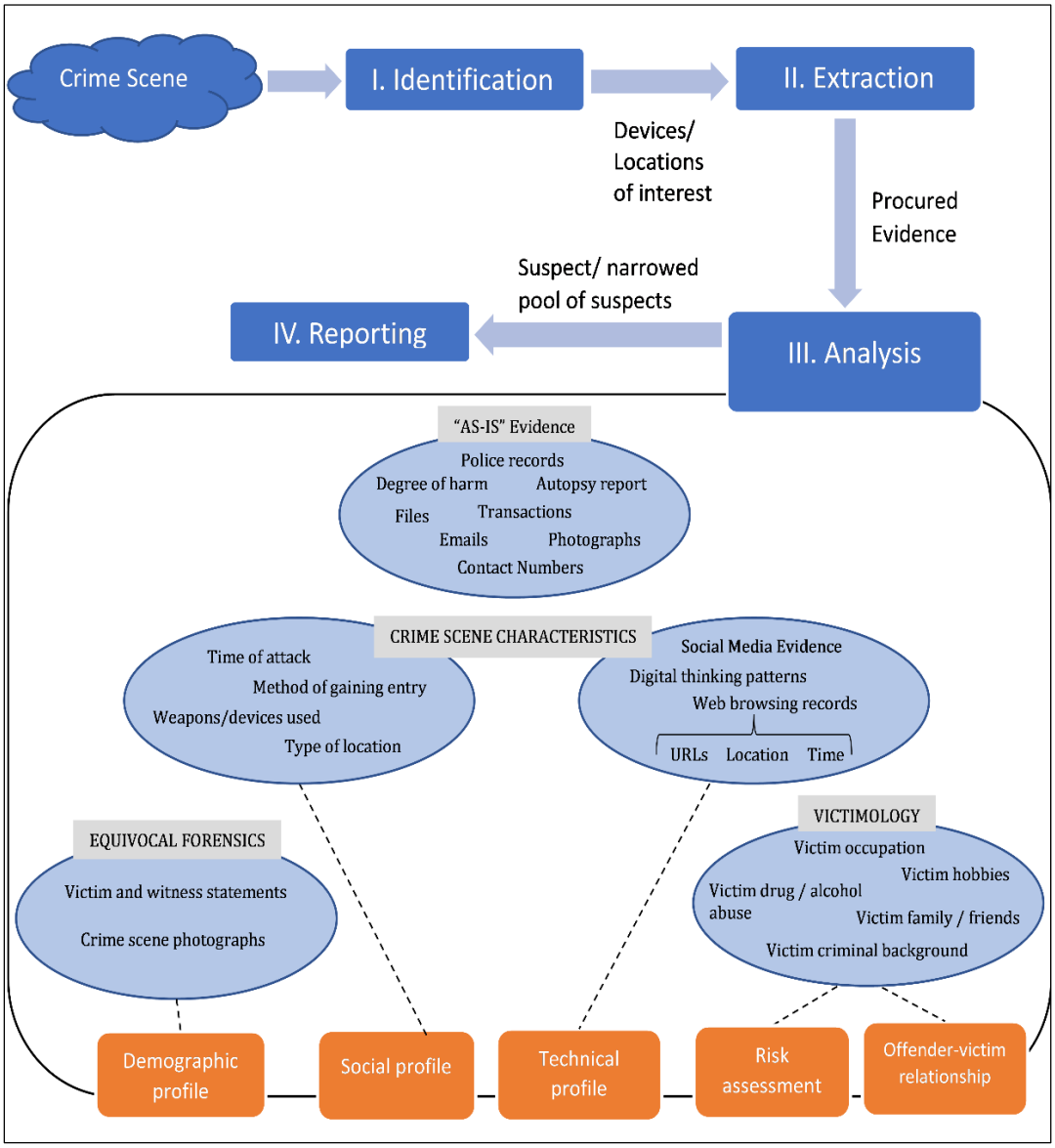

Fig. 1 Behavioral Evidence Analysis- Standardized (BEA-S) model.

To assess the behavior, three types of analyses are applied. These include equivocal forensic analysis, victimology analysis, and crime scene characteristics analysis. Further, the available "as-is" evidence is also analyzed.

3.3.1 Equivocal Forensic Analysis

The Equivocal forensic analysis examines available evidence to interpret the "demographic profile" of the suspect(s). The demographic profile includes age, gender, race/ethnicity, social class, employment, education, marital status, and substance abuse. To infer the demographic profile, the evidence used as parameters are victim statements, witness statements, and crime scene photographs or videos.

The victim statements or testimonial evidence may prove substantial as the victim (of a non-fatal crime) can describe the perpetrator's age group, gender, or race. A witness who saw the offender committing the crime or entering/exiting the location of the crime could give statements to authorities about the offender's demographic traits.

The crime scene photos provide the best chance to discover any neglected or missed pieces of physical evidence. Subject to the type of crime scene, they also provide a window of possibility to explore any environmental elements with demographical value. For example, a cigarette butt or traces of liquor may indicate alcohol/substance abuse and shoe imprints may indicate gender.

Video is a convenient method of detailing the practical details and facilitating a complete description of what

happened at the time of the occurrence of the crime. It is a way to appreciate the unknown demographic traits of the criminal such as age, build, gender, and race, by rendering a sequential account of the crime scene activities. The CCTV videos of the crime scene captured in any on-site camera or covering the route of the entry/escape path of the offender can assist the probe for demographic clues.

3.3.2 Crime Scene characteristics analysis

The Crime Scene characteristics analysis infers the "social profile" and the "technical profile" of the offender.

The social profile determines whether the criminal is a novice, an expert, or a serial offender depending on his skill and planning. The evidence for interpreting the "social profile" includes the means of approach, technique of attack, modus operandi, control mechanism, location type, genre of sexual exploits, preventative deeds, inconsistent actions, verbal activity, distinguishing behavior, and time taken to perpetrate the crime.

The location of the crime that witnessed the salient features of the offender's behavior can determine his/her motive. For example, the crime location may determine if the intention of murder was a robbery or sexual assault. This will further establish the "social profile" of the criminal. The offender's method of gaining entry includes noting access points to the crime scene, including roads, streets, doors, windows, or roofs. The offender's novice hood or expertise in the crime may be explained by his way of approaching the victim. It may take the form of a surprise (waiting for a moment of vulnerability), a con (use of deception), or pre-existing trust (by present or previous relation with the victim). The manner of attack refers to the method of subjugation after approaching the victim. It can be defined in connection with the kind of force utilized or the weapon used. The force may be a verbal command, the verbal threat of lethal action, or a blitz attack. The choice of weapon used to inflict injury or carry out the crime explains much about the perpetrator's mental state. The differentiated injuries caused by different weapons also indicate the social profile of the criminal. For example, neat cuts by knife or clean gunshot wounds indicate a professional or serial offender.

The "technical profile" of the criminal is determined by analyzing digital evidence such as social media evidence, digital thinking patterns, and web-browsing records. Social media evidence like profiles, chats, uploaded photographs, and liked pages can give a clue into the technical knowledge of the criminal. The digital thinking patterns of the offender can be known from the websites visited (pornography, dating sites, chat rooms etc.) and the familiarity of the criminal with such platforms. The visited URLs along with their associated timestamps and location can reveal the user of a device at a particular time in the case of shared systems. Consciously or unconsciously, offenders and victims leave digital footprints on the web. These trails can be retraced to draw pointers into the activities of the involved parties at the time of the crime and associated timeframes. In addition, digital data from the cache, cookies, and archives can provide important investigative leads.

3.3.3 Victimology analysis

Victimology is the comprehensive examination of the victim's circumstances and lifestyle to get additional clues about the case. This analysis is essential as it indicates the risk borne by a victim and determines confident offender choices. It reveals pertinent details about the offender's behavior, like his style, intentions, and proficiency.

Through victimology, we try to infer the "risk assessment" of the victim and the "victim-offender relation." The risk assessment can be categorized into extreme risk, medium risk, and low risk. The victim-offender relation can be of unknown, acquaintance, close contact, or relative. In this stage, the evidence analyzed is the victim's background, occupation, hobbies, criminal record, and drug or alcohol abuse.

The victim's background offers insights into his/her past life that may have influenced potential victimization, degree of harm inflicted, or lasting psychological effects. The victim's occupation and environmental traits determine the risk level based on the exposure to dangerous elements. Victim's risk assessment also involves looking into their criminal background, active investigations, arrests, convictions, protection orders, and warrants. Further, the victim's alcohol and drug abuse habits may greatly influence his or her probability of being selected as a victim.

3.3.4 As-is evidence

The "as-is" pieces of evidence are case-based evidence gathered from the crime scene. They either supplement the existing evidence to support the known offender traits or indicate a new behavioral trait of the criminal. Examples of "as-is" evidence include police records, autopsy reports, degree of harm caused, and forensic evidence like residual files, data, emails, photographs, contact numbers, transactions, etc.

The police records including interrogation reports, documentation of evidence, case files, arrest warrants, and decision support systems can help uncover unseen or missed aspects of the investigation. The autopsy reports may reveal any misinterpreted or overlooked patterns occurring in the wounds and injuries of the victim. The degree of harm caused to the victim may indicate the criminal's motive and modus operandi. Other forensic evidence like residual files, data, emails, photographs, contact numbers, and transaction details recovered from the digital devices may suggest the offender's physiognomies. They may also provide insights into the victim's lifestyle and interactions with the offender.

Behavioral clues gathered from the previous analyses (equivocal forensics, crime scene and victimology) combined with the "as-is" evidence narrow the suspect pool and facilitate offender identification.

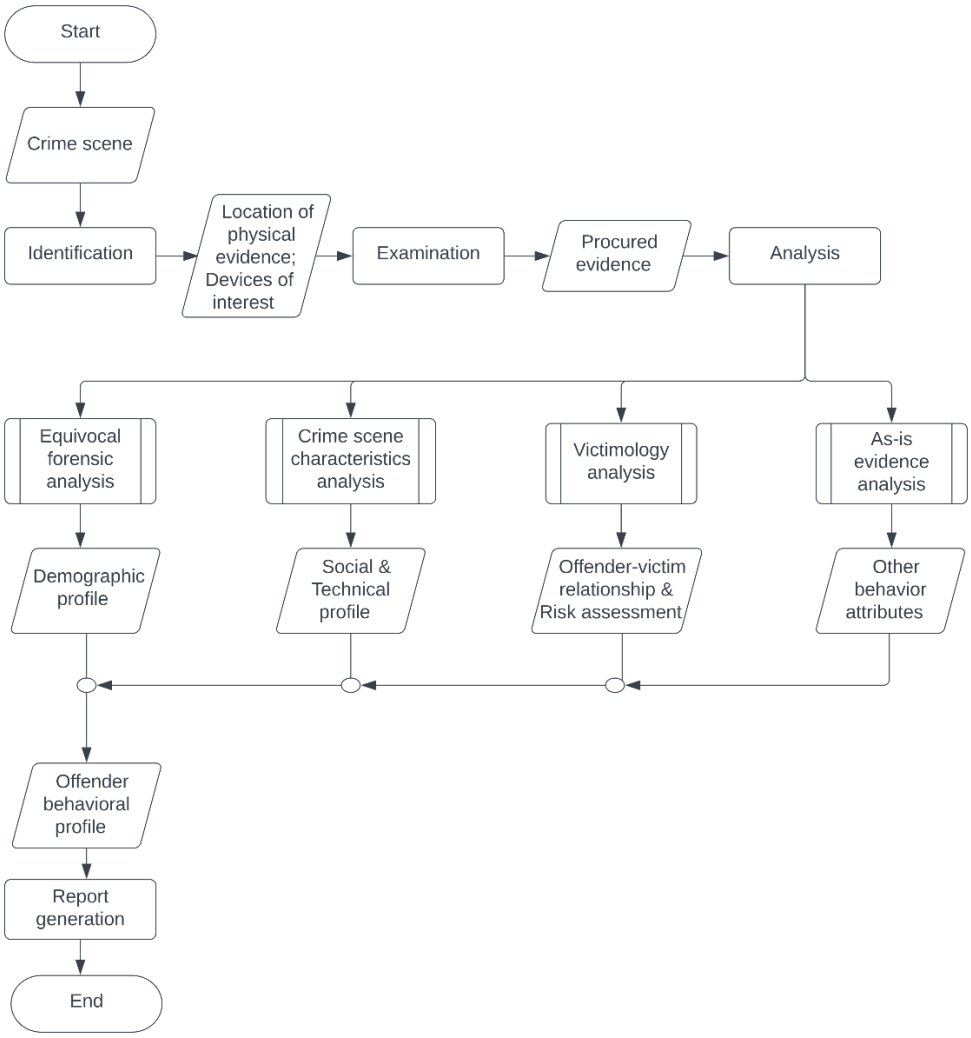

Fig. 2. Detailed BEA-S algorithm.

3.4 Stage IV: Reporting

The final stage of Reporting comprises the decision-making process where outcomes are presented to the information requester. The report generated is a clear and lucid representation of the facts and inferences gathered during the investigation process. This can later be used for filing the final charge sheet in a court of law.

This section of the paper provided an elaborate description of our proposed BEA-S approach. Figure 2 illustrates the detailed BEA-S algorithm. The algorithm of BEA-S is summarized in the following steps:

Algorithm for BEA-S

Step I: Identify "devices of interest" from the crime scene and identify locations of physical evidence (Ref. Section 3.1).

Step II: Extract all relevant evidence from devices of interest and physical evidence from the crime scene (Ref. Section 3.2).

Step III: Analyze extracted evidence to identify the behavioral traits of the offender (Ref. Section 3.3).

i. Do equivocal forensic analysis to identify the demographic profile of the offender (Ref. Section 3.3.1).
ii. Do crime scene characteristics analysis to identify the offender's social and technical profile (Ref. Section 3.3.2).
iii. Do a victimology analysis to evaluate the risk assessment of victim and offender-victim relationship (Ref. Section 3.3.3)?
iv. Use "as-is" evidence to capture offender behaviors that can be used in conjunction with the results of steps i to iii (Ref. Section 3.3.4).

Step IV: Compile the results and generate a report for authorities (Ref. Section 3.4).

As no design is perfect, similarly our proposed system BEA-S has some limitations. The lack of available evidence will cause one or more offender traits to remain unidentified. It will lead to the creation of a wider suspect pool. To ensure systematic application of BEA-S, the forensic practitioner investigating the case must have considerable knowledge and training in BEA investigations.

4. APPLICATION OF BEA-S- A CASE STUDY

Consider a real-life case study [40] of the murder of a 39-year-old woman in the United States, who lived with her 40-year-old husband. For ease of representation, let us call the slain woman X and the husband Y. Victim X was killed using a .357 Magnum gun at the home where she lived with her husband. The husband, Y, stated that a masked intruder who broke into their home tied him up, shot his wife, and committed the crime. Police found Y with one arm and a leg tied to a folding chair and sprawled on the kitchen floor.

4.1 Stage I- Identification

While using the proposed model to investigate the above case, the first stage included the "identification" of the digital devices of interest. Here, the devices of interest consisted of the cell phones of X and Y, Y's Microsoft Surface Pro laptop, house alarm logs, and X's Fitbit. Figure 3 summarizes the Identification phase.

Fig. 3. Stage I of BEA-S- Identification.

4.2 Stage II- Extraction

In the second stage of "extraction," all the digital evidence was extracted from these devices. It included cell phone records, emails, text messages, social media activity, web browsing records, and alarm company records. It also comprised the data from the digital pedometer of the Fitbit and CCTV surveillance footage of the fitness center that X visited on the day of her murder. Figure 4 gives an overview of the Extraction stage.

Fig. 4. Stage II of BEA-S- Extraction.

4.3 Stage III- Analysis

The input to the "analysis" stage is the evidence extracted in the previous step and the physical evidence associated with the case. Figure 5 illustrates the Analysis stage.

4.3.1 Equivocal Forensic Analysis

The evidence analyzed in the "equivocal forensics" included the witness statements. In his statements to the police, Y stated that "*a masked intruder, 6'2", stocky/obese, wearing a camouflage dress, mask and gloves broke into the house and shot his wife X when she got home from her fitness center*." He "*could not tell whether the intruder was black or white*."

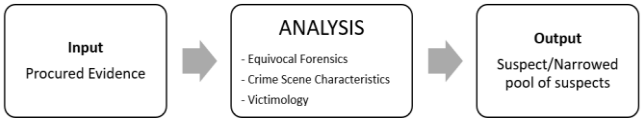

Fig. 5. Stage III of BEA-S- Analysis.

Further, Y claimed that the attacker "*had a knife and demanded his wallet and belongings*" and "*had a Vin Diesel voice*." He mentioned that "*after leaving home in the morning between 0820 hours and 0830 hours, he drove back home between 0845 hours and 0900 hours*" on realizing he had left his laptop. Y stated that on arriving home at 0900 hours, he found an unknown intruder who disabled him using "pressure point" techniques. As per Y, the intruder chased him into the basement, shot, and killed X (with Y's handgun). Then tied him to a chair (one arm and one leg with Y's zip-ties) and assaulted him (with Y's utility knife) before leaving.

The CCTV surveillance footage recovered from the fitness center that victim X visited on the day of the murder showed her arriving at 0853 hours and leaving at 0908 hrs. In the absence of cameras at the crime scene (X's home), no view of the intruder could be seen. For the "demographic profile" of the alleged intruder, we had Y's statement that the suspect was a 6'2" male with a stocky build and wearing a camouflage dress with a mask. However, a corroborative probe of the closet where the intruder hid (as per Y) revealed that it was too small for a person of size and build as the intruder. Figure 6 illustrates the Equivocal Forensics analysis.

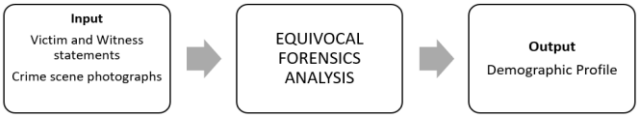

Fig. 6. Sub-Stage of Analysis- Equivocal forensics.

4.3.2 Crime Scene characteristics analysis

The "crime scene" analysis examined the social media evidence, web browsing records, house alarm logs, cell phone records, and data from X's Fitbit. A Fitbit is a wearable fastened to the body that tracks physical activity, heartbeats, sleep schedules, locations, and distances. According to Y's statement to the police, the assaulter attacked X after chasing her to the basement when she came home from the fitness center. In contrast, X's Fitbit recorded

her entrance to the home around 0918 hours and continued registering movement until 1010 hours (almost an hour after her husband said that an intruder in their basement murdered her). Moreover, the distance calculated by the Fitbit device during this time was around 1217 ft., although the total distance X would walk from her vehicle to her final rest in the basement would be no more than 125 ft. As per X's Facebook account data, she uploaded three videos at 0946 hours. However, Y claimed that she was gunned down around 0905 hrs. In addition, an analysis of web browsing records of Y showed that he had searched for "group exercise schedules" of the fitness center of X on the day of the crime. Y had stated in a recorded statement that when he left for the office and forgot to take his laptop, he sent an email to his supervisor from his car, saying that he had to go home to check on an alarm activation. This email was sent by logging in to his outlook email account **********@outlook.com at 0905 hrs. However, web browser analysis revealed that this access to the mail was done using the IP address of his residence.

At the time Y claimed that the intruder had fled after tying him to a chair, there were records of internet browsing history on his Microsoft Surface Pro tracing back to his home IP address. It included visiting Facebook, reading an article on *Star Wars* movie reviews, and surfing through the website of X's Fitness center. This digital evidence revealed that Y had not left home on the day of his wife's murder. Y had a reasonably good "technical knowledge", as was evident from his emails and ease of internet usage. The technical evidence also exposed his false statements given to the police earlier. According to the call records, Y called 911 at 1019 hours (a gap of 1 hour and 14 minutes from when Y stated that he had called 911). As seen from the crime scene, there were no signs of anyone entering or exiting the couple's home on foot, and sniffer dogs found no scent of any intruder. The murder was done in a secured home during morning hours using a gun Y had bought a few months earlier. It indicated the "social profile" of the offender that the murder required considerable skill and planning. The digital evidence in this case indicated that the perpetrator of the murder could be Y himself. Figure 7 gives an overview of the Crime Scene characteristics analysis.

Fig. 7. Sub-Stage of Analysis- Crime Scene characteristics.

4.3.3 Victimology analysis

In the “victimology” stage, the details corresponding to the victim X were recovered. X worked as a pharmaceutical sales representative in an international company. She completed college in 1999 after finishing high school in 1995 and was a former member and vice president of Ambulance Corporation. The friends and family of X told that she was tense about her husband's undue expenditures but never mentioned getting a divorce. From one of Y's friends, it was learned that Y had a girlfriend whom he had impregnated, and her delivery was due in the month following X's murder. No pointer indicated X’s knowledge of her husband’s affair. Some friends said that X disliked guns and Y owned three guns that he kept in the house. From the victim's details, it was inferred that X was at a "low-risk level" and an unknown offender would not kill her without a strong motive. The victim's details, corroborated with other evidence examined, indicated that victim X and the suspect knew each other. This further re-instantiated that Y could be the culprit. The girlfriend's pregnancy could be evaluated as one of the motives of the crime. The sub-stage of Victimology is illustrated in Figure 8.

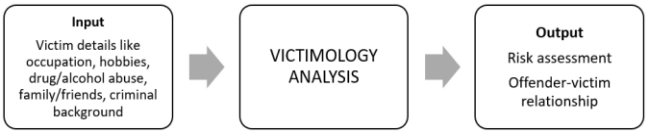

Fig. 8. Sub-Stage of Analysis- Victimology.

4.3.4 As-is evidence

The "as-is" evidence included police records with interrogation reports of Y, which on corroboration showed that he had been giving false statements. The degree of harm caused by the attack on X was fatal. There were, not one, but two fatal gunshot wounds showing that it was a deliberate attempt. The medical reports proved that the cuts made by the alleged intruder on Y’s neck and thighs were superficial, and one could very well make such lacerations on their own.

The text messages between Y and his girlfriend showed that he was trying to hide an extramarital affair from X. One day before the murder, Y messaged his girlfriend saying, "*I'll see you tomorrow, my little love nugget*." In another message, Y said that he would be getting a divorce from X. On X's cell phone, in the "notes" folder, was a list titled "*Why I want a divorce*" – that included arguments on why she wanted to dissolve her marriage with Y. The list mentioned various reasons including Y's undue expenditure, uncaring attitude, and neglectful parenting.

Now, the behavior traits given by previous analyses were integrated with the clues from as-is evidence. The results indicated that the statements made by Y were false, and clearly, there was no intruder. All evidence and derived behavior pointed towards Y being the perpetrator of the crime. Figure 9 portrays the as-is evidence analysis sub-phase of the framework.

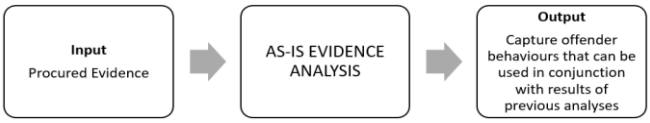

Fig. 9. Sub-Stage of Analysis- As is evidence.

4.4 Reporting

The Reporting stage involved drafting a detailed assessment of the case for submission to authorities. Figure 10 gives an overview of the Reporting stage.

Fig. 10. Stage IV of BEA-S- Reporting.

In the given case study, our proposed model generates a rough behavioral sketch of the perpetrator. Our model not only produces the social, demographic, and technical profiles of the offender, but also provides risk assessment and victim-offender relationship. Digital forensics, coupled with a flavor of BEA, allows for targeted searches on the offender so that he can be identified and prosecuted. The digital forensics process alone was not sufficient to achieve this. Our framework, BEA-S, is not limited to one forensic domain. Instead, it integrates many evidence types including psychological traits, victim habits, social media footprints, web records, physical evidence from crime scenes, police records, and more. The extensive scope of our approach makes it consistent with almost all criminal situations. In this sense, BEA-S is a step towards standardizing the BEA process and integrating it into traditional digital forensics.

5. COMPARATIVE ANALYSIS

This section establishes the novelty of our proposed approach by comparing it with existing behavioral digital forensic models. Table 1 provides a comparative analysis of BEA-S with (a) Slide and Angelopoulou's DF profiling methodology [37], (b) Roger's psychological profiling [38], and (c) Mutawa's Behavioral DF model [39].

Table 1 Comparative analysis of BEA-S with existing approaches

Parameter	**Approach (a)** [37]	**Approach (b)** [38]	**Approach (c)** [39]	**Proposed approach BEA-S**
Design of model	3 stages	6 stages	4 stages	4 stages
Standardization	Not applicable	Not applicable	Not applicable	Provided by homogenous design applicable across all digital crimes
Behavioral parameters covered	Only cyberstalking behaviors	Only online behaviors	Only online behaviors	Social, demographical, technical, environmental, and situational behaviors
Guidelines for implementation	No explicit guidelines for BEA	No explicit guidelines for BEA	Guidelines on model stages but not on finding offender behavior	Well-defined guidelines for both BEA and finding offender behavior
Focus area	Only technical stage that guides search/ recovery of evidence	Only frequency and timeline analysis	Only analysis of multiple users of same device	All available forms of digital evidence
Practical utility	Not known on real cases	Known on cases of known suspects only	Known on two case studies – online impersonation and online fraud	Our real-life case study creates a profile that can be mapped to both known and unknown suspects
Output	Evidence locations on victim's or suspect's device, ***no behavioral details***	***Only online behavior profile*** of the suspect	Hypothesis on what may have happened during crime but ***no profile of likely offender***	***Complete behavioral profile*** of suspect (social, technical, demographical)

6. CONCLUSION

Our work aims to introduce much-needed standardization and homogeneity for implementing BEA in criminal

forensic investigations. Our proposed solution, BEA-S, clearly outlines the incorporation of behavioral analysis in digital forensics. BEA-S also proves its utility in practical, real-world applications. It enhances forensic investigations by utilizing evidence from multiple and diverse sources. It accounts for all aspects of the offender and victim behavioral cues, thus readily adapting it for use across various forensic disciplines. Due to its ability to handle varied evidence, BEA-S shows potential to addresses not only the current digital crimes but also new crimes in the future.

7. FUTURE SCOPE

Our proposed framework can be enhanced by using machine learning and deep learning techniques to accelerate and automate the model's processes.

This will further drive the model's utility in multiple applications of trending digital domains, including hate speech analysis, Internet of Things (IoT) forensics, and cloud forensics.

REFERENCES

[1] A. A. Khan, A. A. Shaikh, A. A. Laghari, M. A. Dootio, M. M. Rind, and S. A. Awan, "Digital forensics and cyber forensics investigation: security challenges, limitations, open issues, and future direction," *Int. J. Electron. Secur. Digit. Forensics*, vol. 14, no. 2, pp. 124–150, 2022.

[2] B. E. Turvey and M. A. Esparza, *Behavioral Evidence Analysis: International Forensic Practice and Protocols*. 2016.

[3] B. Shree and P. Dhaliwal, "Behavioural Evidence Analysis," *Int. J. Digit. Crime Forensics*, vol. 13, no. 5, pp. 20–42, Sep. 2021.

[4] P. Sharma and B. Nagpal, "Regex: an experimental approach for searching in cyber forensic," *Int. J. Inf. Technol. 2019 122*, vol. 12, no. 2, pp. 339–343, Nov. 2019.

[5] G. Surange and P. Khatri, "Integrated intelligent IOT forensic framework for data acquisition through open-source tools," *Int. J. Inf. Technol. 2022 146*, vol. 14, no. 6, pp. 3011–3018, Jul. 2022.

[6] A. Bihari *et al.*, "Identification of Hate Speech on Social Media using LSTM," *GMSARN Int. J.*, vol. 17, no. 4, pp. 468–474, 2023.

[7] S. Fahad, P. Bhushan, S. Agrawal, P. Tripathi, P. Mishra, and A. Deepak, "A Self-Attention Based Hybrid CNN-LSTM for Speaker-Independent Speech Emotion Recognition," *GMSARN Int. J.*, vol. 17, no. 4, pp. 429–435, 2023.

[8] P. Kapoor and P. K. Singh, "Robbery pattern analysis (RPA) using the concept of multipolarity and examining the influencing factors," *Int. J. Inf. Technol. 2021 143*, vol. 14, no. 3, pp. 1425–1432, Jan. 2021.

[9] R. Kumar and B. Nagpal, "Analysis and prediction of crime patterns using big data," *Int. J. Inf. Technol. 2018 114*, vol. 11, no. 4, pp. 799–805, Dec. 2018.

[10] L. Almond, M. McManus, and G. Curtis, "Can the offence behaviours of stranger rapists discriminate between UK and non-UK nationals," *J. Aggress. Confl. Peace Res.*, vol. 11, no. 1, pp. 67–76, 2019.

[11] P. O'Meara, A. Coyne, and M. Brassil, "An appraisal of investigative psychology and the applications to suspicious approaches to children in the Irish criminal justice system," *J. Investig. Psychol. Offender Profiling*, vol. 16, no. 3, pp. 213–221, Oct. 2019.

[12] L. Almond, M. A. McManus, S. Giles, and E. Houston, "Female Sex Offenders: An Analysis of Crime Scene Behaviors," *J. Interpers. Violence*, vol. 32, no. 24, pp. 3839–3860, Dec. 2017.

[13] R. J. B. Lehmann, A. M. Goodwill, R. K. Hanson, and K.-P. Dahle, "Acquaintance Rape: Applying Crime Scene Analysis to the Prediction of Sexual Recidivism.," *Sex. Abuse*, vol. 28, no. 7, pp. 679–702, Oct. 2016.

[14] B. D. Johnson and R. D. King, "FACIAL PROFILING: RACE, PHYSICAL APPEARANCE, AND PUNISHMENT*," *Criminology*, vol. 55, no. 3, pp. 520–547, Aug. 2017.

[15] L. Hofhansel, C. Weidler, M. Votinov, B. Clemens, A. Raine, and U. Habel, "Morphology of the criminal brain: gray matter reductions are linked to antisocial behavior in offenders," *Brain Struct. Funct.*, vol. 225, no. 7, pp. 2017–2028, Sep. 2020.

[16] R. Shenoy, D. Yadav, H. Lakhotiya, and J. Sisodia, "An Intelligent Framework for Crime Prediction Using Behavioural Tracking and Motion Analysis," *2022 Int. Conf. Emerg. Smart Comput. Informatics, ESCI 2022*, pp. 1–6, 2022.

[17] J. J. Rokven, G. De Boer, J. Tolsma, S. Ruiter, and J. Rokven, "How friends' involvement in crime affects the risk of offending and victimization," *Eur. J. Criminol.*, vol. 14, no. 6, pp. 697–719, 2017.

[18] S. Shagufta, "Criminal Friends' Influence on Criminal Behavior of Adult Offenders Moderated by Psychopathic Traits," *FWU J. Soc. Sci.*, vol. 14, no. 2, pp. 108–116, 2020.

[19] D. Willmott, D. Hunt, and D. Mojtahedi, "Criminal Geography and Geographical Profiling within Police Investigations-A Brief Introduction," *Internet J. Criminol.*, pp. 1–24, 2021.

[20] J. M. Escrig-Espuig, M. Martí-Vilar, and F. González-Sala, "Criminal Thinking: Exploring its Relationship with Prosocial Behavior, Emotional Intelligence, and Cultural Dimensions," *https://journals.copmadrid.org/apj*, vol. 33, no. 1, pp. 9–15, Feb. 2023.

[21] R. M. Nesse, "Evolutionary Psychology and Mental Health," in *The Handbook of Evolutionary Psychology*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2015, pp. 1–20.

[22] D. Willmott, D. Boduszek, and R. Robinson, "A psychodynamic-behaviourist investigation of Russian sexual serial killer Andrei Chikatilo," *J. Forensic Psychiatry Psychol.*, vol. 29, no. 3, pp. 498–507, May 2018.

[23] J. Walinga, "2.3 Behaviourist Psychology." University of Saskatchewan Open Press, 28-Jun-2019.

[24] B. Robinson-Riegler and G. Robinson-Riegler, "Cognitive psychology : applying the science of the mind," *Fac. Bookshelf*, Jan. 2016.

[25] A. M. Bland and E. M. DeRobertis, "Humanistic Perspective," *Encycl. Personal. Individ. Differ.*, pp. 2061–2079, 2020.

[26] K. Veroude, Y. Zhang-James, N. Fernàndez-Castillo, M. J. Bakker, B. Cormand, and S. V. Faraone, "Genetics of aggressive behavior: An overview," *Am. J. Med. Genet. Part*

B Neuropsychiatr. Genet., vol. 171, no. 1, pp. 3–43, Jan. 2016.

[27] S. Islam, S. S. Y. Khan, K. Gul, and Y. Khan, "Criminal Behaviour in the Context of Various Criminal Theories," *Rev. Educ. Adm. Law*, vol. 5, no. 4, pp. 643–655, Dec. 2022.

[28] K. O. Poltava, O. V Dubovych, A. V Serebrennikova, T. I. Sozanskyy, and I. V Krasnytskyi, "Juvenile Offenders: Reasons and Characteristics of Criminal Behavior," *Int. J. Criminol. Sociol.*, vol. 9, pp. 1573–1578, 2020.

[29] C. Kehinde, B. Emmanuel Temitope, A. Olubukola, and F. Bruno Costa Cepp, "Personality, Group Thinking and Cohesiveness as Predictor of Criminal Behavior among Adolescents," *South Asian J. Soc. Stud. Econ.*, vol. 12, no. 4, pp. 119–130, 2021.

[30] M. Woster, "Differences in Characteristics of Criminal Behavior Between Solo and Team Serial Killers," *Dissertations*, Jun. 2020.

[31] N. Chopra Galimotu, "Personality Predictors of Criminal Behaviour Among College Students Gap Indian Journal of Forensics and Behavioural Sciences Personality Predictors of Criminal Behavior Among College Students," 2021.

[32] S. Tkazky, D. Youngs, and D. Rowlands, "Psychopathy, offending style and crime scene behavior," *Psychopathy Crim. Behav.*, pp. 273–294, Jan. 2022.

[33] H. Arshad, A. Jantan, and E. Omolara, "Evidence collection and forensics on social networks: Research challenges and directions," *Digit. Investig.*, vol. 28, pp. 126–138, 2019.

[34] N. Sunde and I. E. Dror, "Cognitive and human factors in digital forensics: Problems, challenges, and the way forward," *Digit. Investig.*, vol. 29, no. March, pp. 101–108, 2019.

[35] I. R. Adeyemi, S. A. Razak, M. Salleh, and H. S. Venter, "Leveraging human thinking style for user attribution in digital forensic process," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 7, no. 1, pp. 198–206, 2017.

[36] B. H. AlOwaimer and S. Mishra, "Analysis of web browser for digital forensics investigation," *Int. J. Comput. Appl. Technol.*, vol. 65, no. 2, pp. 160–172, 2021.

[37] A. Silde and O. Angelopoulou, "A digital forensics profiling methodology for the cyberstalker," in *Proceedings - 2014 International Conference on Intelligent Networking and Collaborative Systems, IEEE INCoS 2014*, 2014, pp. 445–450.

[38] M. K. Rogers, "Psychological profiling as an investigative tool for digital forensics," in *Digital Forensics: Threatscape and Best Practices*, Elsevier Inc., 2016, pp. 45–58.

[39] N. Al Mutawa, J. Bryce, V. N. L. Franqueira, A. Marrington, and J. C. Read, "Behavioural Digital Forensics Model: Embedding Behavioural Evidence Analysis into the Investigation of Digital Crimes," *Digit. Investig.*, vol. 28, pp. 70–82, 2019.

[40] "Dabate Arrest Warrant," *DocumentCloud*, 2017. [Online]. Available: https://www.documentcloud.org/documents/3671492-Dabate-Arrest-Warrant. [Accessed: 13-May-2022].