IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, 2022

A STUDY ON THE DIGITAL FORENSICS AND CRIMINAL PROFILING IN THE CONTEXT OF CYBERCRIME INVESTIGATIONS

Sakthidevi V[1] (Research Scholar)
Dr. Vishal Khatri[2] (Research Supervisor)
Department of Computer Science
[1,2] Sikkim Professional University, Gangtok, (Sikkim)

ABSTRACT
There is currently a sizable amount of crimes that are committed in online. Along with more recent information- or computer-related transgressions, these crimes also include more conventional ones. Examples of crimes that can be perpetrated online include spam email, cyber terrorism, pedophilia, and various types of child and sexual abuse. Financial fraud is an example of one that has its roots in the physical world. On the other hand, data theft and cyber espionage both totally take place online. In actuality, it represents a serious threat to the civilizations and way of life that prevail in modern times. The fight against cybercrime requires a multifaceted strategy. This study's major objective is to do research on the digital forensics and criminal profiling in the context of cybercrime investigations. A qualitative research methodology was used in this study. This study's findings indicate that it's necessary to take a closer look at cross-data research that makes use of additional data sources. Thus, intelligence agents' internet-based or offline evidence, or other intelligence analysis and source, may help narrow a probe and meet charge breakdown criteria. Various cyber threat monitoring systems, such as the Reliable, require the ability to exchange data in order to be compatible with one other. The recommended procedure can also be expanded to include incident news since it automatically leverages the exchange of indicators details and the built-in risk details expression, both of which are initially critical strategic components of the sharing of data system.
***Keywords**: Digital Forensics; Cyber Profiling; Cyber Crime; Investigations.*

INTRODUCTION
The practice of cybercriminal profiling has the potential to be a significant factor in the degree to which our societies are able to withstand the effects of cyberattacks. This is because it acts as a direct deterrent against the commission of cybercrimes by creating the possibility that the offenders will be discovered and brought to justice (Chang et al., 2020). Additionally, if the data owner is aware of the enemy's profile and what the adversary is aiming for, they can make strategic judgments about what data should be put on the network and how it should be stored. Also, from the perspective of law enforcement, this facilitates the prosecution and punishment of the criminals. Crime scene investigators or forensic specialists gather data on potential offenders so they can create a profile with distinctive traits during normal criminal investigations. This data is employed to create a "profile." Without conducting any additional research, the perpetrator of the crime might be identified if the profile sketch is accurate enough. On the other hand, it might decrease the number of persons who are viewed as suspicious if it matches a small number of already-existing profiles belonging to numerous offenders with verified criminal histories (Han et al., 2019; Spicer, 2019). The image below serves as an illustration of the idea of cyber profiling.

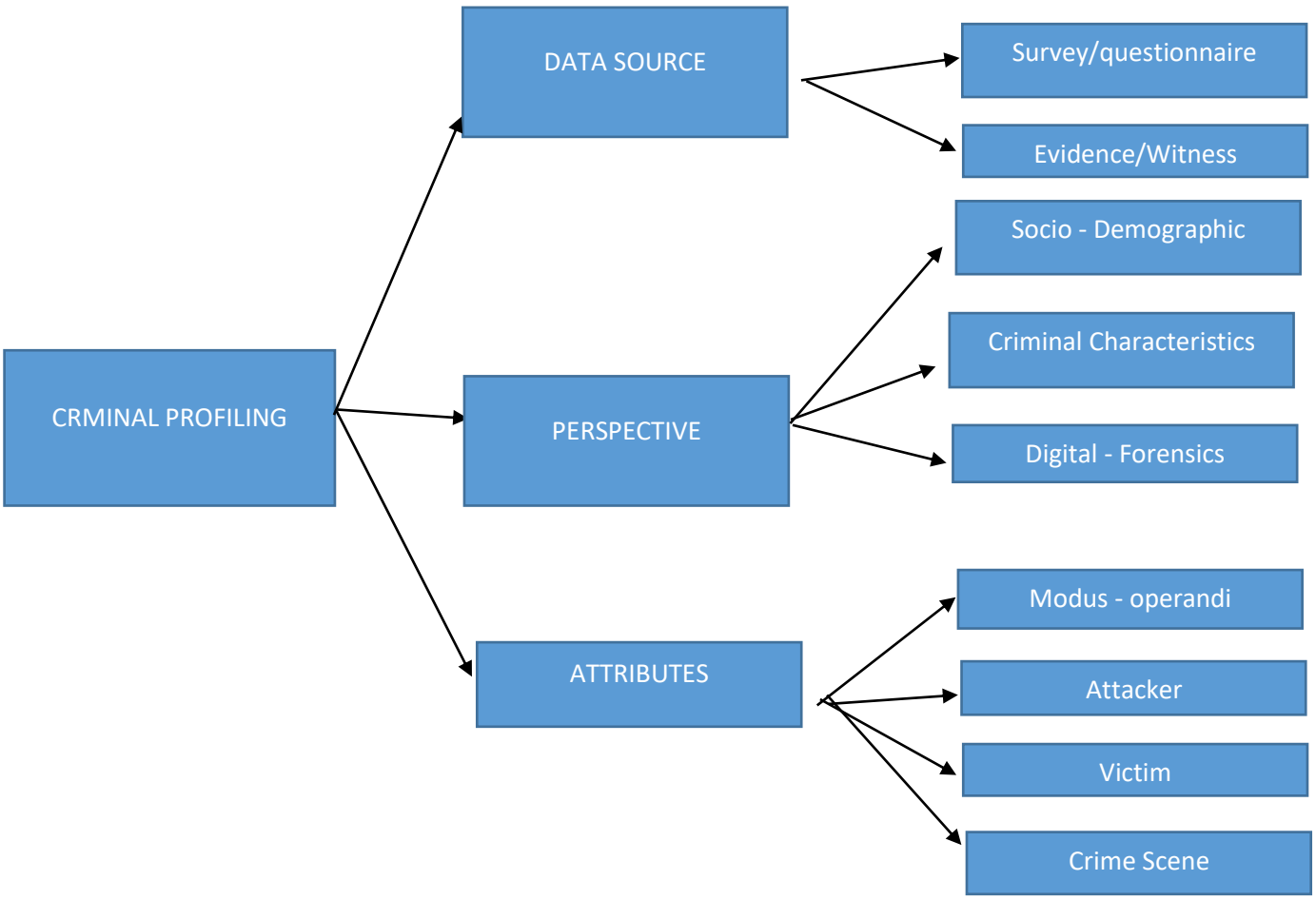

Figure 1: Cyber Criminal Profiling (Kipane, 2019)

The previous literatures that are relevant to this study are elaborated upon in the following sections.

LITERATURE REVIEW

AUTHORS AND YEARS	METHODOLOGY	RESULTS AND FINSINGS
Gadelrab and Ghorbani (2020)	This cited study discussed the issue of criminal profiling online and the reasons why it is different from traditional forms of criminal profiling. It makes an effort to present an overview of the problem as well as the various techniques that are currently being taken, along with a possible solution.	This study covered some significant issues that need to be solved in order to be able to deliver results that can be relied upon, and it concludes by presenting some ideas for the work that was be done in the future.
Sikos (2021)	In computer forensic checks, purpose-designed models allow integrity confirmation using computational reasoning and make it easier to identify anomalies for each link in command. These capabilities are made possible by formally specifying the ideas and properties of digital forensics.	A survey of various ontologies is provided, and an investigation into how their applicability might be utilized in the automation of the processing of traces of digital evidence is carried out.

Martineau et al., (2023)	The main goal of this comprehensive assessment, which was created to look into the state of literature about the use of a human-focused investigations technique (i.e., profiling) to electronic crime, was to publish a kind of qualitative meta-synthesis.	The study's main objective was to further qualitative studies on the practical application of profiles methods and tools related to piracy.

Table 1: Literature Review

This literature evaluation used the CBR approach's similarity measure and clustering processing to compare website defacement incidents. Data parsing and cleaning sanitized raw data from hacked websites. This research's primary objective is to employ a sizable real-world dataset for data-driven hacker profiling. This was accomplished by constructing the case vector and selecting crucial components for case-based reasoning. Cluster analysis is used to create a hacker profile, which is the most important phase in the investigation of a computer crime. Make decisions based on evidence and data to locate pertinent incident occurrences and a lot of information about chosen major events. One must first reduce and then analyze data in order to produce truly valuable intelligence data.

RESEARCH METHODOLOGY

The tactics, procedures, or tactics used in the act of gathering facts or proof for investigation in order to uncover new information or produce greater comprehension of a topic are referred to as methodology in research. Case-based deduction, or CBR for a nutshell is a method of problem-solving that makes use of prior knowledge or instances. Even when the new challenges are not precisely same as the ones from the past, CBR may nevertheless provide a recommendation for an interim response. The following is a rundown of the primary methodologies utilized in this investigation:

- A decision support technique for cybercrime investigation based on CBR was proposed in this work. The suggested cybercrime investigation approach aids security analysts in identifying past attack instances that are most comparable to a particular attack and gaining knowledge that can be applied to detect website defacement cybercrime networks. High-value intelligence is generated using a data-driven analytic system in this situation.
- The study demonstrated the clustering technique and visualization. Clustering helps researchers analyze large data sets and understand their findings. Additionally, the representation helps investigators instantly spot criminal behavior trends.
- This research suggested turning disorganized data, like web defacement occurrences, into ordered data for similarity evaluation and ranking.

RESULTS AND DISCUSSIONS

As terrorists don't always use similar or distinctive attack strategies, the parallelism approach may be hard to evaluate. Attackers' programming improves over time. Situations may affect the assault strategy, argument purpose, and target audiences. Instead of testing the analogous process in this research, the percentage of successfully found hackers was employed to evaluate the suggested technique's success. The next four operations, outlined in Figure 2, were used to test the created methods: where "K" represents all database hackers.

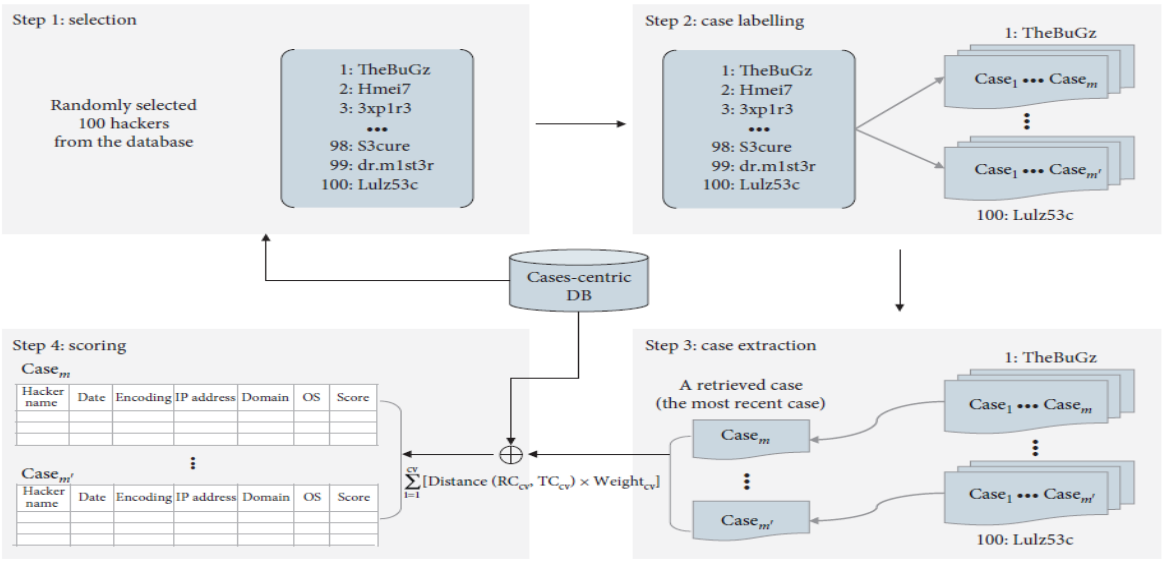

Figure 2: The developed testing processes, beginning with step 1 and continuing until step 4. (Han et al., 2019)

N_{Scope} = (Count ($Case_K^{Scope}$) / ($Case_K^{all}$)) * 100 ----------(2)

R_K = Count ($Case_k^m$) / Count ($Case_K^{all}$ ..... (3)

where "m" refers to the previous examples that fall inside the given scope and involve a hacker who was chosen at random and denoted by "k."

After randomly selecting 100 hackers, all earlier attack instances of each hacker were retrieved and abstracted from the collection. The hacker's name was written next to each archive case. The number of website defacement attacks each hacker has committed is shown in Figure 3. The third and fourth phases compared a freshly retrieved instance to all website defacement cases.

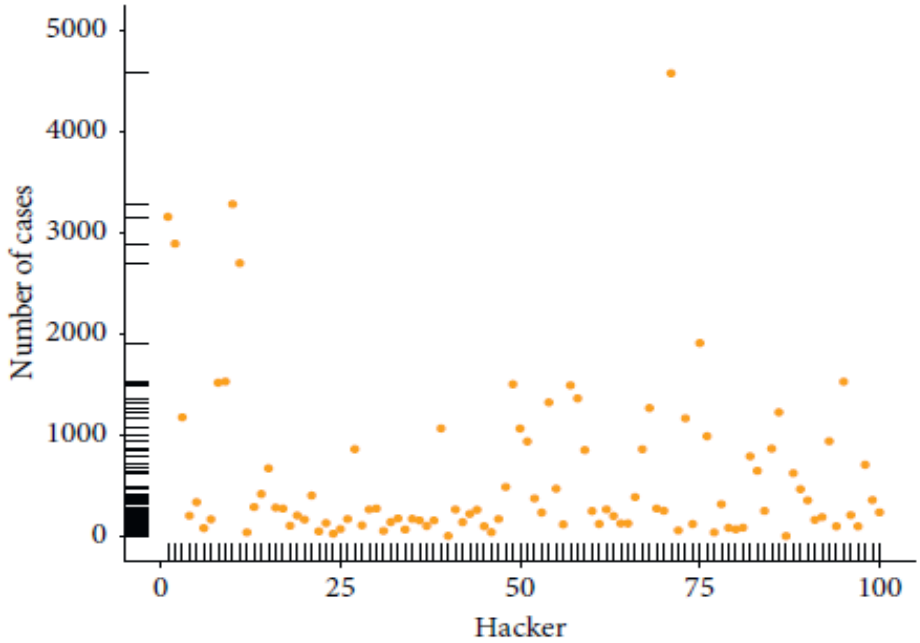

Figure 3: The total number of websites that each thief has defaced in the previous (Han et al., 2019)

CONCLUSION

The study suggested cross-data research using additional data sources. Thus, further internet-based or offline evidence acquired by intelligence officers or other intelligence analyses and sources may help narrow an inquiry and meet charge breakdown standards. The described procedure can be modified to include event news so that it is compatible and transferable among cyber threat surveillance systems like the Reliable automatically makes use of the expression of the built-in danger details and the exchange of indicators details, both of which are initially strategic components of the data sharing system.

REFERENCES

1. Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees. *Technological forecasting and social change*, *158*, 120166.
2. Han, M. L., Kwak, B. I., & Kim, H. K. (2019). Cbr-based decision support methodology for cybercrime investigation: Focused on the data-driven website defacement analysis. *Security and Communication Networks*, *2019*, 1-21.
3. Kipane, A. (2019). Meaning of profiling of cybercriminals in the security context. In *SHS Web of Conferences* (Vol. 68, p. 01009). EDP Sciences.
4. Spicer, J. (2019). Cybercriminal profiling. *EDPACS*, *60*(3), 1-17.
5. Gadelrab, M. S., & Ghorbani, A. A. (2020). Cyber Criminal Profiling. In *Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice* (pp. 144-163). IGI Global.
6. Sikos, L. F. (2021). AI in digital forensics: Ontology engineering for cybercrime investigations. *Wiley Interdisciplinary Reviews: Forensic Science*, *3*(3), e1394.
7. Martineau, M., Spiridon, E., & Aiken, M. (2023). A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. *Forensic Sciences*, *3*(3), 452-477.