International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Behavioural Indicators of Emotional States in Digital Forensic Investigations: A Conceptual Framework

Ms. Aswathy Raju

Assistant Professor, Department of Computer Science, Bishop Vayalil Memorial Holy Cross College, Cherpunkal

Abstract

Digital forensic investigations have traditionally focused on the technical recovery and analysis of data from devices, networks, and online accounts. However, a growing body of research argues that technical evidence alone often fails to explain why a suspect or person of interest behaved in a particular way, especially in cases involving threats, violence, fraud, or self-harm. This paper introduces a beginner-friendly conceptual framework for understanding how behavioural indicators of emotional states can be identified and interpreted within digital evidence. Drawing on cyber profiling, behavioural analytics, and digital phenotyping literature, the framework organises emotional indicators into four categories: linguistic and textual cues, temporal and activity-pattern cues, interaction and relational cues, and biometric or sensor-based cues. The paper explains key concepts in simple terms, reviews relevant prior work, and proposes a practical model that students and early-career investigators can use as a starting point. Limitations, ethical considerations, and directions for future research are also discussed.

Keywords: Digital forensics, Behavioural analysis, Emotional indicators, Cyber profiling, Digital phenotyping, Threat assessment, Cyberpsychology

1. Introduction

When a crime or harmful incident has a digital component, investigators usually focus on what happened: which files were accessed, what messages were sent, or which websites were visited. This paper is interested in a different but related question: how did the person feel while they were doing these things? Emotional states such as anger, anxiety, excitement, or distress often leave traces in the way people use technology, even though these traces are not always obvious.

This area of study sits at the intersection of digital forensics, cyberpsychology, and behavioural science. Digital forensics provides the methods for collecting and preserving digital evidence, while cyberpsychology and behavioural science provide theories about how emotion and behaviour are connected. Bringing these fields together can help investigators build a fuller picture of a case, particularly in situations such as threat assessment, cyberbullying, online radicalisation, or workplace misconduct, where understanding intent and emotional state matters as much as understanding the technical facts.

The purpose of this paper is to introduce, at an accessible level, a conceptual framework for recognising behavioural indicators of emotional states in digital evidence. The paper is written for beginners: students,

new analysts, or anyone curious about how psychology and digital forensics can work together. It does not assume prior knowledge of forensic science or psychology.

1.1 Why This Topic Matters

Several recent incidents involving online threats and mass violence have shown that warning signs are sometimes present in a person's digital activity well before an offline event occurs. Researchers studying cyberpsychological indicators of mass violence have argued that integrating behavioural threat assessment with digital intelligence can support earlier identification of risk. At the same time, researchers in digital phenotyping have shown that everyday smartphone and sensor data, such as typing speed, movement patterns, or app usage, can reflect a person's underlying psychological and emotional state. These two strands of research suggest that emotional indicators are not just a theoretical idea; they are measurable and potentially useful in real investigations.

1.2 Aims of This Paper

- To explain, in simple terms, what is meant by a 'behavioural indicator of emotional state' in digital forensics' context.
- To summarise key findings from existing literature on cyber profiling, behavioural analytics, and digital phenotyping.
- To propose a beginner-friendly conceptual framework that organises these indicators into clear categories.
- To discuss how the framework could be applied, and what its limitations and ethical risks are.

2. Background Concepts

2.1 Digital Forensics

Digital forensics is the practice of identifying, collecting, preserving, and analysing electronic evidence so that it can be used in an investigation or legal proceeding. Traditionally, this field has emphasised technical accuracy and the integrity of evidence, such as recovering deleted files or reconstructing a timeline of system events. Recent reviews of the field describe an expanding set of techniques, including cloud forensics, mobile forensics, and the use of machine learning to process large volumes of data more efficiently.

2.2 Cyber Profiling and Behavioural Analysis

Cyber profiling refers to the practice of building a picture of an individual based on their online behaviour, including the language they use, the platforms they visit, and the patterns in their activity. A systematic review of cyber profiling literature has proposed organising this field into a structured framework, highlighting that behavioural analysis can support investigators in understanding motive, intent, and psychological state, not just technical actions. Related work on behavioural analytics in cybersecurity similarly argues that combining behavioural data with technical forensic data produces richer investigative insight than either approach alone.

Other researchers have proposed integrating behavioural analysis directly into the standard digital forensic investigation process, rather than treating it as a separate, optional step. This suggests that behavioural and emotional indicators are increasingly seen as a core part of forensic practice rather than an afterthought.

2.3 Digital Phenotyping and Emotional Cues

Digital phenotyping is the idea that ordinary interactions with digital devices, such as typing, scrolling, or moving between locations, can be used to measure a person's psychological state, sometimes called a 'digital phenotype'. Reviews of this field describe both the opportunities it presents, such as continuous

and unobtrusive measurement of mood and behaviour, and the challenges, including data privacy, consent, and the risk of misinterpreting patterns. Separately, research into eye gaze and emotional state detection has shown that even consumer-grade devices can pick up signals related to a person's emotional or attentional state, suggesting that the boundary between 'forensic data' and 'emotional data' is increasingly blurred.

3. Literature Review

This section summarises the main strands of literature that inform the proposed framework. The studies have been grouped into three broad themes for clarity.

3.1 Cyber Profiling and Investigative Frameworks

Martineau, Spiridon, and Aiken (2023) carried out a systematic review of 72 studies on cyber profiling and used the findings to build a comprehensive cyber behavioural analysis (CBA) framework. Their starting point was that combating cybercrime has historically been treated as a purely technical problem, even though cybercrime is ultimately the result of human decisions and motives, meaning that understanding the person behind the keyboard matters as much as understanding the technical evidence. Earlier work by Steel (2014) took a different but complementary approach: rather than studying the aggregate behaviour of cybercriminals as a group (a nomothetic approach), Steel proposed idiographic digital profiling (IDP), which analyses one individual's specific digital footprint to support an active investigation, including case planning, identifying a suspect, and generating leads. This idiographic, case-by-case approach is well suited to identifying emotional indicators, since emotional expression varies considerably between individuals and a one-size-fits-all profile is unlikely to capture it accurately.

3.2 Behavioural Analysis Within Digital Forensics

Al-Mutawa (2018) conducted a structured research programme on incorporating behavioural analysis (BA) into the digital forensic investigation process. The research found that, although most practitioners agreed BA had potential value across many parts of an investigation, it was in practice used only to a limited extent in day-to-day casework. Based on this, a digital forensics investigation model was proposed that explicitly incorporates behavioural analysis to support a more structured, multidisciplinary examination of digital evidence relating to interpersonal crimes. More recently, Pawani and colleagues (2025) demonstrated a machine learning approach to criminal behaviour analysis, using Long Short-Term Memory (LSTM) networks and autoencoders to detect subtle anomalies and suspicious patterns in browser activity data. Their goal was to make it easier to flag deviations in browsing behaviour that might otherwise be missed using traditional, manual forensic methods, illustrating how automated tools can support, but not replace, human judgement when assessing behavioural and emotional signals in digital evidence.

Ceballos-Espinoza (2024) proposed reconstructive psychological assessment (RPA) as a method for analysing digital behavioural residues, the traces of psychological state left behind in a person's digital activity, within forensic contexts. This work is particularly relevant to the present framework, as it explicitly connects psychological assessment methods to the forensic interpretation of digital traces.

3.3 Threat Assessment and Applied Contexts

Malin (2021) introduced the discipline of Digital Behavioural Criminalistics and the related concept of the Cyber Pathway to Intended Violence (CPIV), arguing that digital behavioural artifacts, the evidence 'breadcrumbs' an offender leaves on social media, messaging apps, and personal devices, allow investigators to reconstruct an offender's escalating thoughts and actions leading up to a planned violent act in much finer detail than was previously possible. Shawe and Clark (2026) build on this broader threat

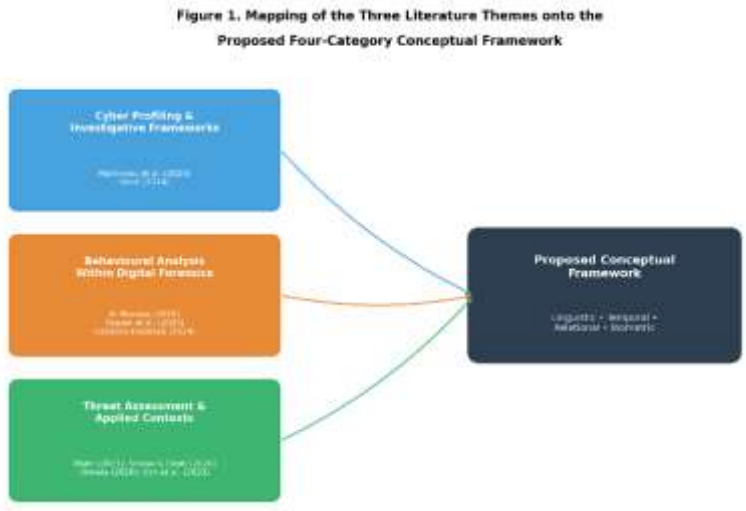
assessment tradition by proposing the integration of cyberpsychological indicators with law enforcement intelligence for mass violence threat assessment. Bwangah (2023) reviewed behavioural analytics applications in cybersecurity more broadly, while Sharma and Khan (2025) and Mcalaney, Hills, and Cole (2024) provided wider context on emerging trends in digital forensics and cybercrime, respectively, situating behavioural and emotional analysis within the broader forensic discipline.

Finally, work on digital phenotyping by Onnela (2020) explains how the widespread use of smartphones has created new opportunities to passively capture social, behavioural, and cognitive data in everyday settings, while also highlighting major challenges in how such data should be collected and analysed responsibly. Separately, research on emotional state detection using consumer devices by Kim, Lee, Kim, and Oakley (2023) points toward the technical feasibility of detecting emotional signals, such as through eye gaze, using off-the-shelf hardware. Together, these two strands of research support the idea that emotional signals captured through ordinary digital interactions could, in principle, also be recoverable and relevant in a forensic context.

3.4 Summary of the Literature

Taken together, the literature suggests three consistent messages: first, behavioural analysis is increasingly recognised as a legitimate and useful part of digital forensic practice in daily crime investigation; secondly, individual-level (idiographic) approaches are better suited to capturing emotional nuance than population-level comparisons; and third, emotional and psychological signals can, in principle, be detected through ordinary digital activity, even though doing so reliably and ethically remains a significant challenge.

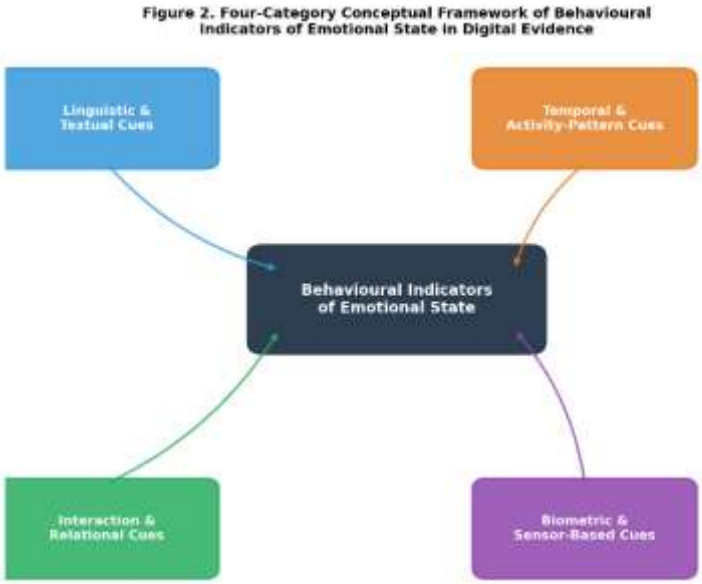
Figure 1: Three Key Themes Emerging from the Literature Review



4. Proposed Conceptual Framework

Based on the literature reviewed above, this paper proposes a simple framework consisting of four categories of behavioural indicators that may reflect a person's emotional state within digital evidence. The framework is intended as a starting point for beginners and would need to be tested and refined through further empirical research.

Figure 2: The Four Categories of Behavioural Indicators of Emotional State



4.1 Linguistic and Textual Cues

This category includes the words, tone, punctuation, and structure of written communication, such as emails, messages, and social media posts. Sudden changes in writing style, increased use of negative or aggressive language, or shifts in sentence length and complexity may indicate changes in emotional state such as stress, anger, or anxiety.

4.2 Temporal and Activity-Pattern Cues

This category includes when and how often a person engages in digital activity, such as posting at unusual hours, a sudden increase or decrease in activity, or repetitive checking behaviour. Disruptions to a person's normal digital routine can be a useful, if indirect, indicator of emotional disturbance.

4.3 Interaction and Relational Cues

This category includes changes in who a person communicates with, how often, and in what manner, such as withdrawing from established contacts, escalating conflict in conversations, or forming new connections with concerning content or individuals. These patterns draw directly on cyber profiling and threat assessment research discussed in section 3.3.

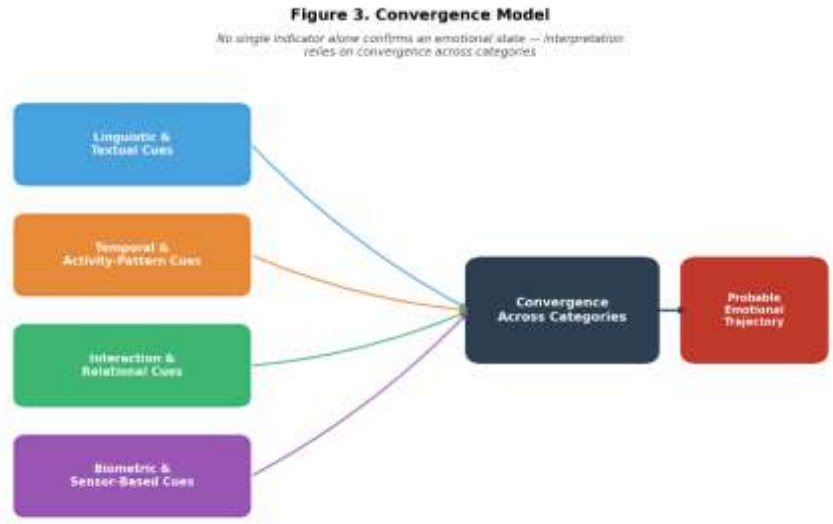
4.4 Biometric and Sensor-Based Cues

Where available and legally obtained, this category includes data such as typing speed and pressure, mouse or touchscreen movement, eye gaze, or device sensor data. This category is the most technically demanding and ethically sensitive, drawing on digital phenotyping and emotion-detection research discussed in section 2.3.

4.5 How the Categories Work Together

No single indicator from these four categories should be treated as proof of a particular emotional state on its own. The framework is designed to encourage investigators to look for convergence, that is, multiple indicators across different categories pointing in the same direction, before drawing conclusions. This mirrors the idiographic, case-by-case approach recommended by Steel (2014) and the integrated investigative process described by Mutawa and Khurshid (2018).

Figure 3: Convergence of Indicators Across Categories



5. Discussion

5.1 Practical Applications

For a beginner analyst, this framework could be used as a checklist when reviewing digital evidence: noting any linguistic changes, unusual activity patterns, relational shifts, or available sensor data, and then considering whether these indicators converge to suggest a particular emotional path or track, such as escalating distress or anger. This would not replace formal psychological assessment but could support investigators, much as Ceballos-Espinoza's (2024) reconstructive psychological assessment approach suggests.

Figure 4: Practical Application Workflow for Beginner Analysts

5.2 Limitations

This framework has several limitations. First, it is conceptual and has not been practically tested; future research would need to validate whether these categories reliably predict emotional states. Second, individual and cultural differences in communication style mean that the same indicator could reflect different emotional states in different people. Third, automated tools such as those described by Pawani and colleagues (2025) can introduce their own errors or biases if used without careful human oversight.

5.3 Ethical Considerations

Because this framework deals with inferring a person's internal emotional state from their digital activity, it raises important investigation ethical questions around privacy, consent, and the risk of misinterpretation. Digital phenotyping research has highlighted similar concerns, noting that the same data that can support wellbeing research could also be misused for surveillance. Any application of this framework in real investigations should be guided by appropriate legal authority, professional ethical standards, and an awareness that behavioural indicators are uncertain, not definitive.

6. Conclusion

This paper has introduced a beginner-friendly conceptual framework for identifying behavioural indicators of emotional states of a human being within digital forensic investigations. By organising indicators into linguistic, temporal, relational, and biometric categories, the framework offers a structured starting point for thinking about how human emotions and digital behaviour intersect. The framework is grounded in, and consistent with, existing research on cyber profiling, behavioural analytics, and digital phenotyping. Future work should focus on empirically testing this framework, refining its categories, and developing clear ethical guidelines for its responsible use in real-world investigations.

References

1. Bwangah, M.L., Behavioural Analytics in Cyber Security for Digital Forensics Application, International Journal of Computer Science and Information Technology, 2023, 15 (1). https://doi.org/10.5121/ijcsit.2023.15106
2. Ceballos-Espinoza, F., Reconstructive Psychological Assessment (RPA) Applied to the Analysis of Digital Behavioral Residues in Forensic Contexts, Journal of Criminal Psychology, 2024. https://doi.org/10.1108/jcp-04-2024-0030
3. Hussain, M., An Approach for Digital Forensics Using Behavior Analysis, 2015.
4. Kim, J., Lee, D., Kim, J., Oakley, I., Can Eye Gaze Improve Emotional State Detection on Off-the-Shelf Smart Devices, Proceedings of BigComp 2023, 2023. https://doi.org/10.1109/BigComp57234.2023.00090
5. Malin, C.H., Digital Behavioral Criminalistics to Elucidate the Cyber Pathway to Intended Violence, 2021. https://doi.org/10.1093/MED-PSYCH/9780190940164.003.0032
6. Martineau, M., Spiridon, E., Aiken, M., A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature, Forensic Sciences, 2023, 3 (3), 32. https://doi.org/10.3390/forensicsci3030032
7. Mcalaney, J., Hills, P., Cole, T., Forensic Perspectives on Cybercrime, 2024. https://doi.org/10.4324/9781003300359
8. Mutawa, A., Khurshid, N., Integrating Behavioural Analysis Within the Digital Forensics Investigation Process, 2018.
9. Onnela, J., Opportunities and Challenges in the Collection and Analysis of Digital Phenotyping Data, Neuropsychopharmacology, 2020. https://doi.org/10.1038/s41386-020-0771-3
10. Pawani, W., Sewwandi, J., Samesha, D.G., Gonawala, N., Gethmi, R.K., Rathnayaka, H., Senarathne, A., Deemantha, S.M., Siriwardena, N., Machine Learning-Based Criminal Behavior Analysis for Enhanced Digital Forensics, PLOS ONE, 2025. https://doi.org/10.1371/journal.pone.0332802

11. Shawe, R., Clark, R.W., Cyberpsychological Indicators of Mass Violence: Integrating Behavioral Threat Assessment with Law Enforcement Intelligence, International Journal of Academic and Applied Research, 2026, 11 (2). https://doi.org/10.51505/ijaemr.2026.11214
12. Sharma, P., Khan, M.W., A Review of Digital Forensics Techniques and Emerging Trends, Proceedings of IC3ECSBHI 2025, 2025. https://doi.org/10.1109/IC3ECSBHI63591.2025.10990354
13. Steel, C.M.S., Idiographic Digital Profiling: Behavioral Analysis Based on Digital Footprints, Journal of Digital Forensics, Security and Law, 2014, 9 (2). https://doi.org/10.15394/JDFSL.2014.1160