



Detection of Unauthorized System Access Using Native Windows Artifacts

Outline

- Research Background
- Problem Statement
- Research Aim and Objectives
- Research Gap
- Proposed Methodology
- Project Planning and Resources
- Project Impact and Limitation
- Reference



Background

In current cybersecurity situations, unauthorized system access is still a major problem, especially for businesses that primarily rely on Windows-based systems for day-to-day operations. Incidents include several unsuccessful login attempts, credential abuse, and illegal privilege escalation have increased in frequency as digital infrastructures grow. Security Event Logs and Registry entries, which document user activity, system modifications, and authentication attempts, are among the useful forensic artifacts that Windows operating systems routinely produce. These artifacts can offer crucial proof for recreating access histories and spotting questionable activity. However, many businesses ignore the investigative potential of built-in Windows programs in favor of concentrating solely on sophisticated monitoring solutions.

Keywords: Unauthorized System Access , Windows Security Event Logs, Repeated Failed Login, Registry Editor



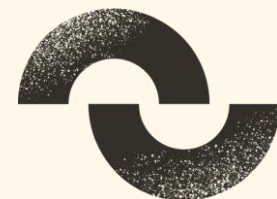
Literature Review

Title and year	Authors	Topic	Research focus	Methodology	Key Finding	Limitations	Relevance to my Research
<i>Sufficiency of Windows Event Log as Evidence in Digital Forensics</i> (2012)	Ibrahim, N.M., Al-Nemrat, A., Jahankhani, H., Bashroush, R.	Windows Event Log as forensic evidence	To evaluate whether Windows Event Logs are sufficient and admissible as legal digital evidence	Simulated cyber-attacks (password guessing, hacking) in a virtual environment; analyzed event logs for evidential value	Event logs can serve as admissible digital evidence if properly preserved and analyzed	Limited to controlled lab environment; focused mainly on evidential admissibility	Affirms the reliability of Event Viewer logs as credible forensic artifacts for identifying fraudulent login attempts.
<i>Windows Event Forensic Process (WinEFP)</i> (2014)	Do, Q., Martini, B., Looi, J., Wang, Y., Choo, K.-K.R.	Event log forensic process	To develop a structured forensic process for analyzing Windows Event Logs	Proposed WinEFP framework covering key Windows event IDs and forensic steps	Provides systematic guidance for event log investigation and improves investigation consistency	Focused primarily on process framework; lacks specific attack scenario correlation	Specifies a methodological framework for systematic log analysis in this research.
<i>Windows Forensic Analysis and Detection of Ransomware Attacks Using Event Logs and Tools</i> (2024)	Prajapati, Y., Gosai, K.	Ransomware detection using Windows logs	To detect ransomware attacks through event log analysis and forensic tools	Analysis of event logs combined with specialized forensic tools for ransomware detection	Event logs reveal identifiable patterns useful for early ransomware detection	Heavy reliance on specialized forensic tools; not focused on native-only analysis	Emphasizes the significance of log-based detection, although distinguishes itself by concentrating on native Windows tools and the identification of login abuse.

Problem

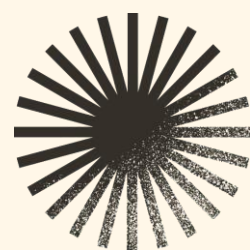


Problem Statement



Unauthorized Login Attempts

Repeated failed logins indicate possible brute-force or password-guessing attacks and can be identified through Windows Security Event Logs **(4)**. Windows Event Logs provide valuable forensic evidence for analysing cyber incidents such as password-guessing attacks and system intrusions **(3)**.



Lack of Native Log Monitoring

Although Windows systems automatically generate detailed security and system logs through Event Viewer, these logs are not always systematically analysed for forensic investigations **(1)**. As a result, valuable digital evidence related to system activities and potential security incidents may remain hidden within Windows event logs without proper forensic analysis **(4)**.



Registry Evidence Ignored

The Windows Registry contains important traces of system configuration and user activities that are valuable for digital forensic investigations and system analysis **(7)**. However, in many security assessments and log-focused investigations, registry artefacts are often overlooked, which may lead to incomplete forensic findings **(5)**.

Research Aim

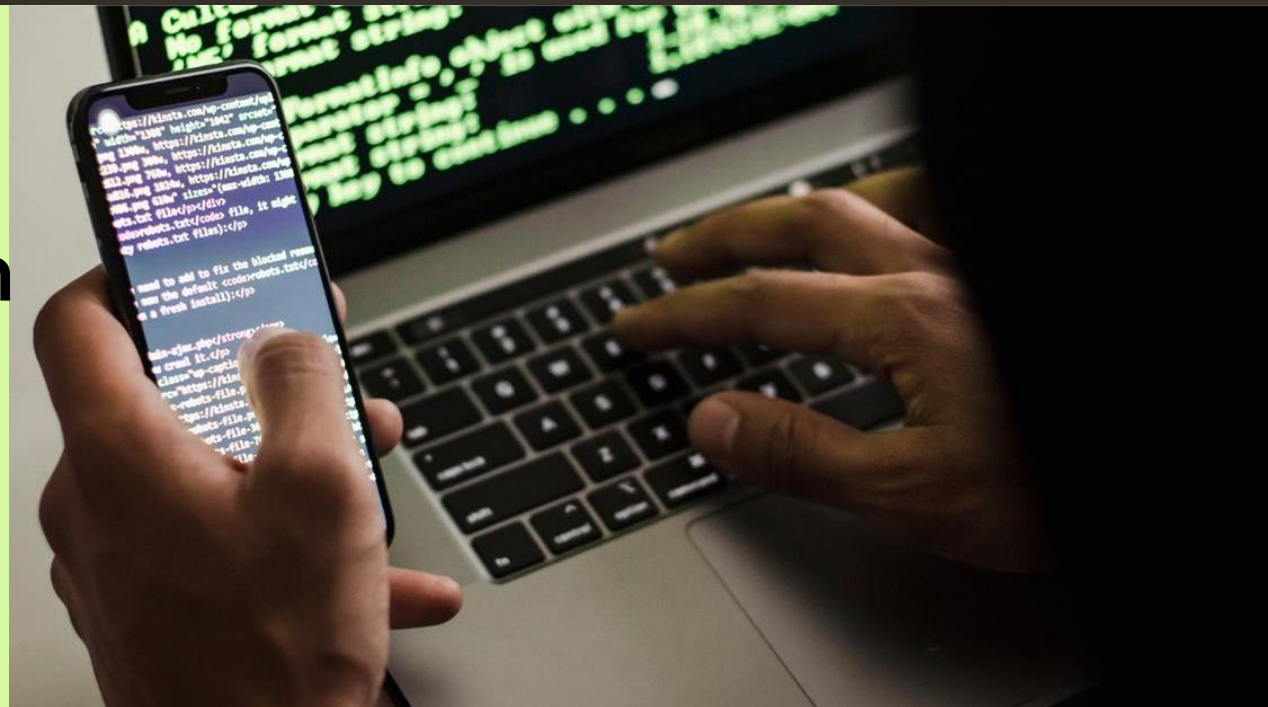


Research Aim and Objective

To detect unauthorized system access using native Windows forensic artifacts such as event logs and registry data.

Log-Based Access Detection

Detect anomalous login activity by analyzing Windows Security Event Logs, including both failed and successful logon attempts.

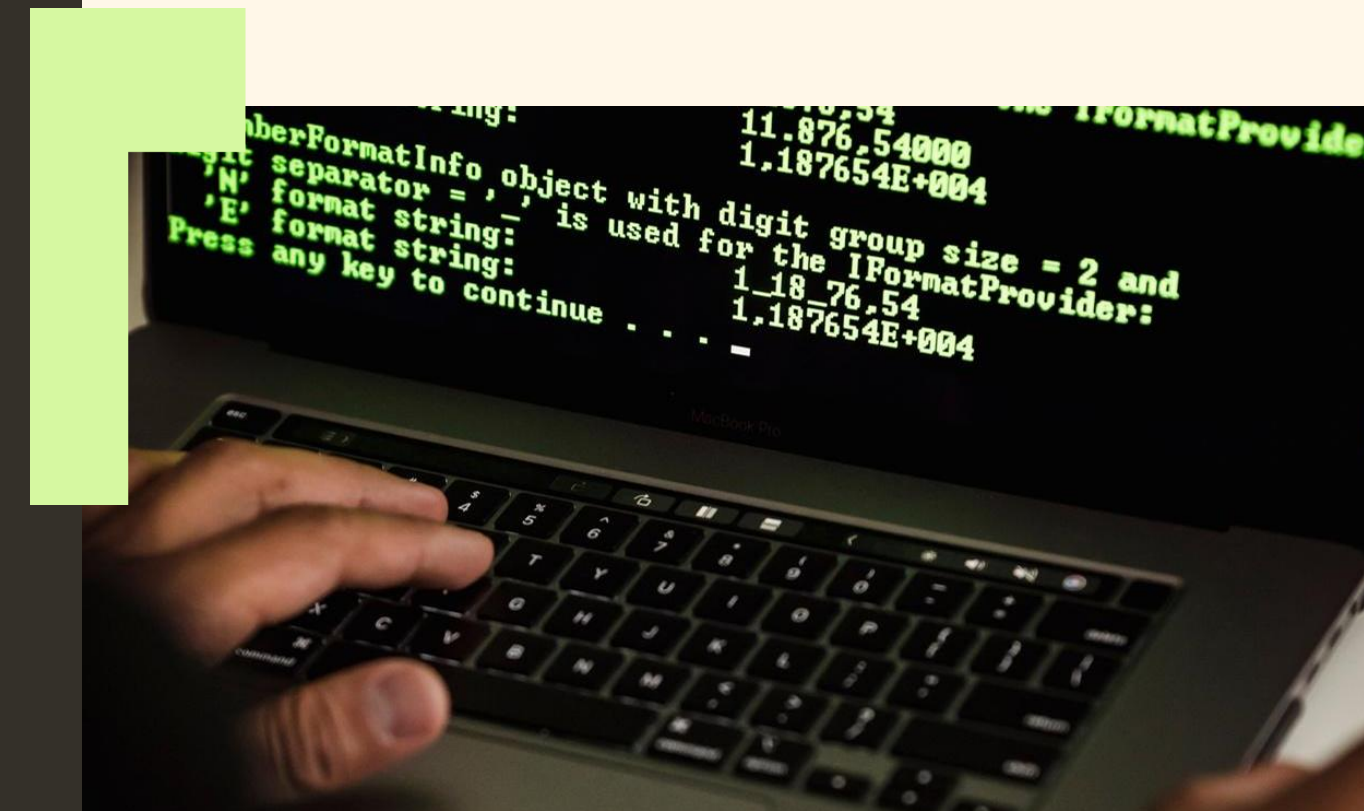


Registry Examination

Evaluate Windows Registry logs to observe user activity, system modifications, and access persistence.

Activity Timeline

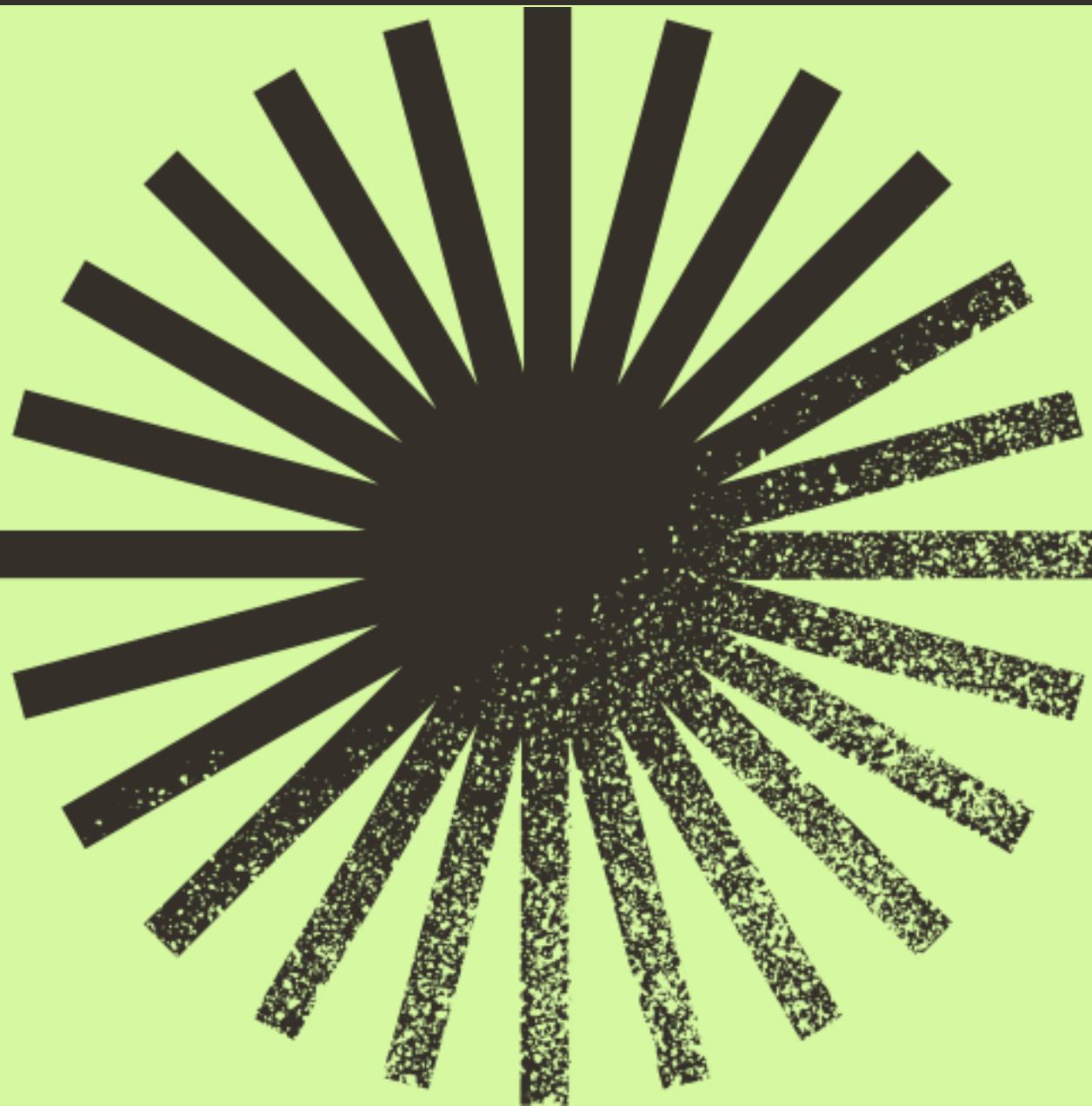
Correlate log and registry evidence to reconstruct a timeline of potential unauthorized access.



Research Gap



Existing tools rely heavily on **commercial forensic software**, which is costly and not always accessible to students or small organizations.



Windows Event Logs are widely studied for forensic investigations, but mainly in post-incident analysis contexts [1]–[3].

Existing research confirms the evidential value of event logs, yet does not establish a structured framework for detecting repeated failed login attempts through artefact correlation [2].

Registry forensic studies focus on hive extraction, large-scale analysis, and data representation systems rather than login misuse detection [4], [6], [9].

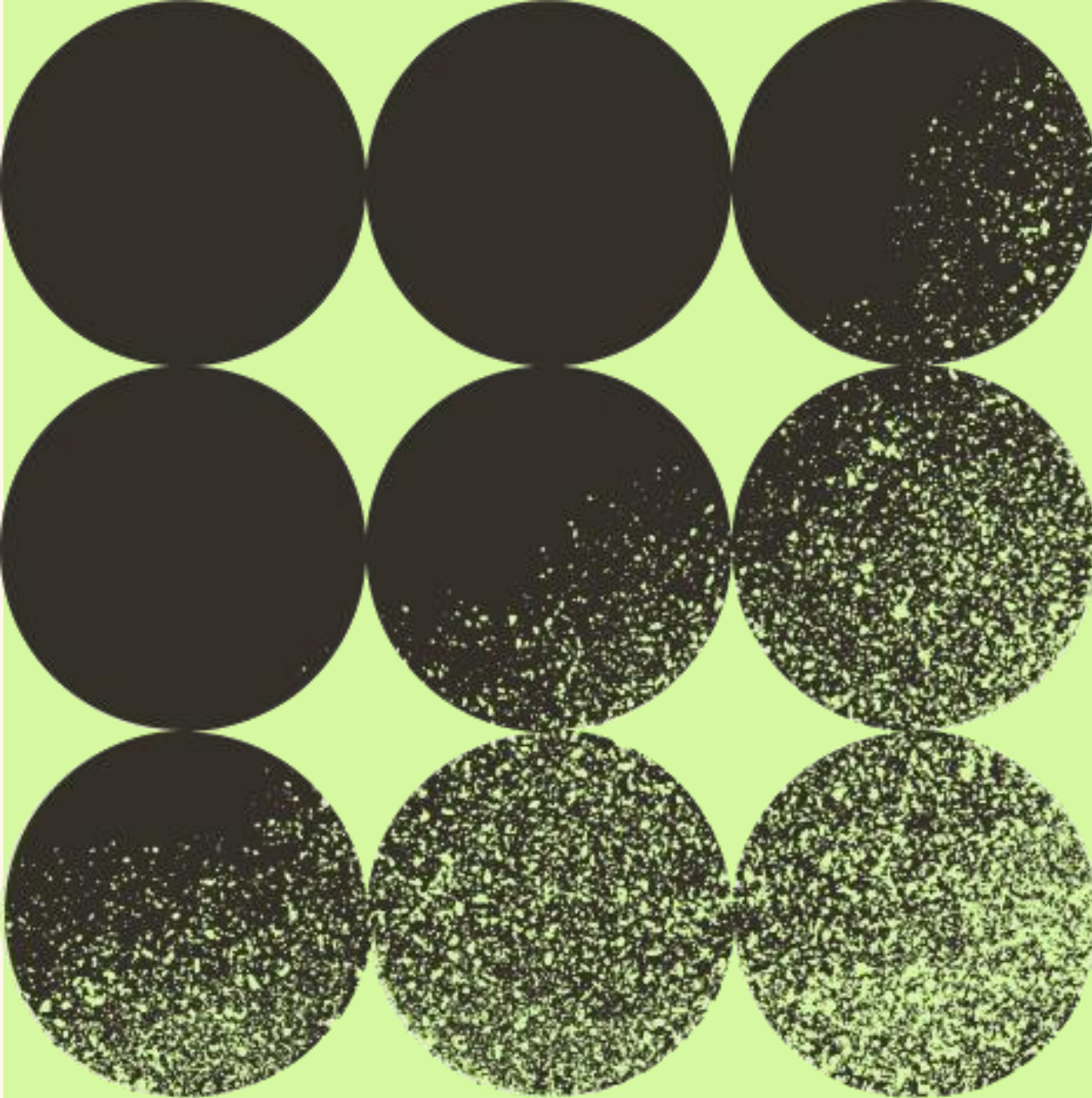
Most digital forensic research focuses on large-scale cyberattacks or network-based investigations.

Many forensic models rely on commercial tools or enterprise-scale investigation methods, leaving low-cost, host-based detection approaches underexplored [5], [7].

Limited academic validation exists for integrating Security Event Logs and Registry artefacts in Windows 10/11 environments to detect repeated wrong password attempts.

Existing studies demonstrate structured log extraction and XML-based forensic storage models, but they focus primarily on general malicious activity detection rather than targeted failed login analysis [1].





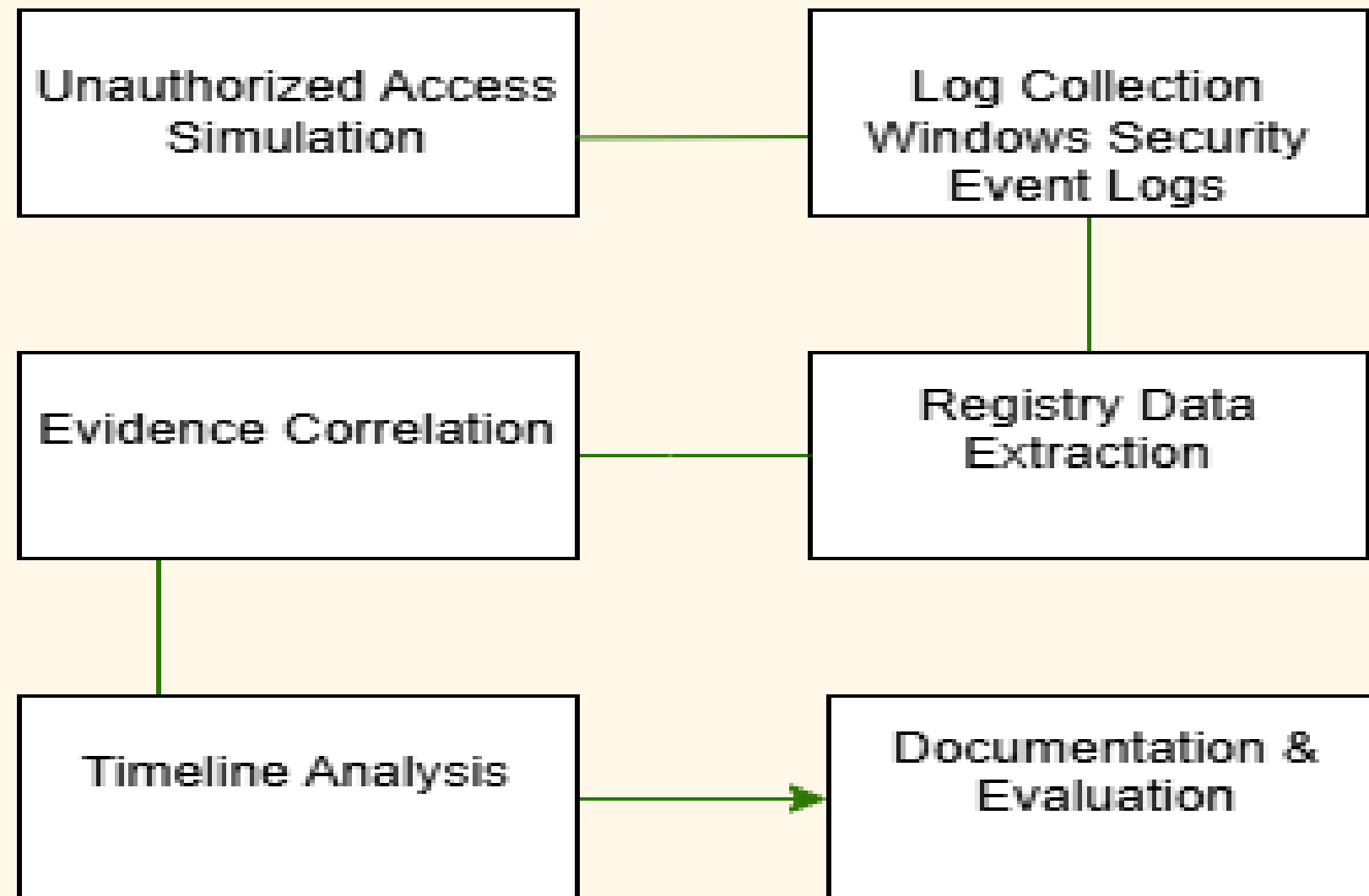
Many forensic models are designed for law-enforcement environments, not for academic or small-scale investigations.

Need low-cost practical investigation methods.

Real-world simulation studies are limited.

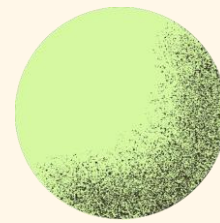
Built-in evidence sources are overlooked.

Research Methodology



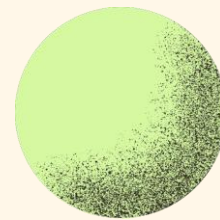
Proposed Methodology

Windows **Event Viewer** logs will be analyzed to identify security events such as failed logins, account usage, and suspicious activity.



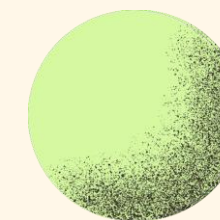
Log Analysis

Investigate Windows Security Event Logs for evidence of unreliable logins, authorized access, and unusual activity.



Registry Examination

Examine Windows Registry artifacts to trace user activity and system access patterns.



Timeline Reconstruction

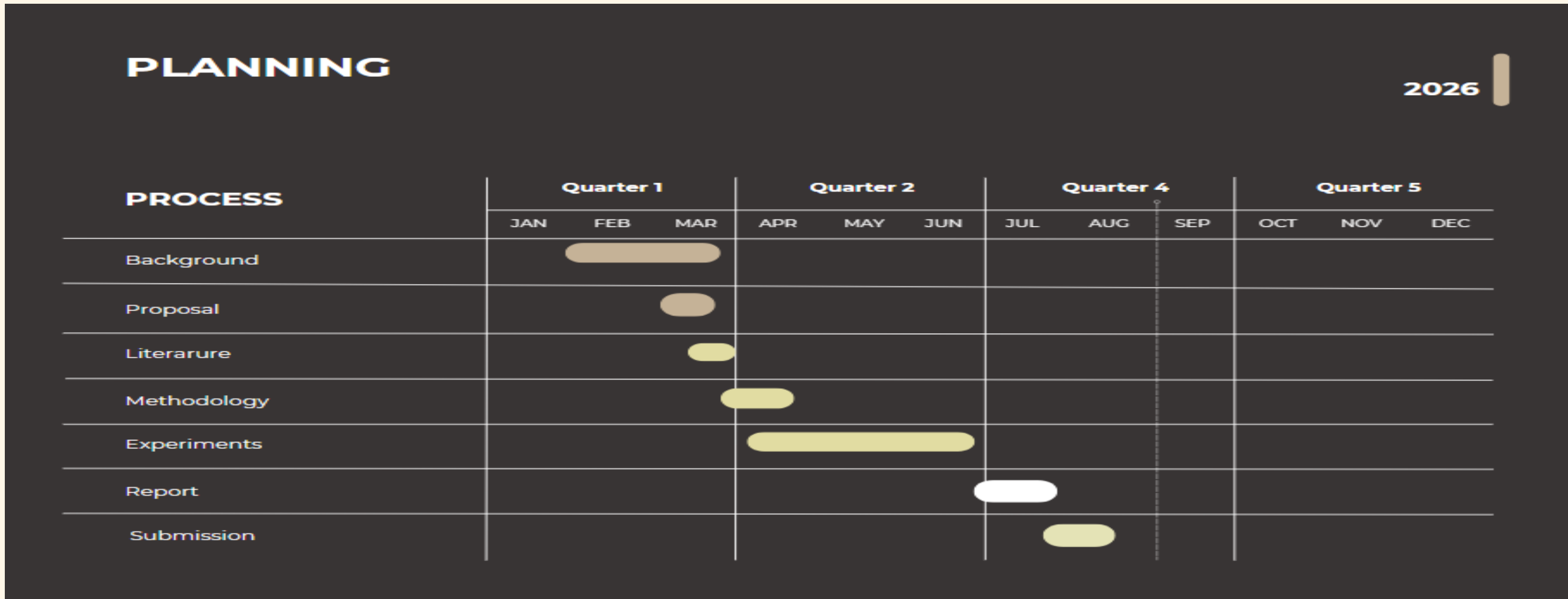
Compare Event Viewer timestamps with registry artefacts to build an activity timeline. Identify patterns of repeated logon attempts to detect suspicious behavior.



Forensic Investigation Process

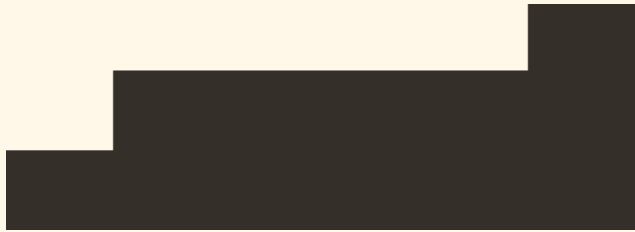
Follow structured digital forensic procedures to preserve and analyze system evidence.

Project Planning



Resource

- Windows operating system for generating and analysing system artefacts
- Windows Event Viewer for analysing security logs
- Windows Registry tools for examining registry entries
- Academic research papers and digital forensic guidelines
- A personal computer for data collection and analysis

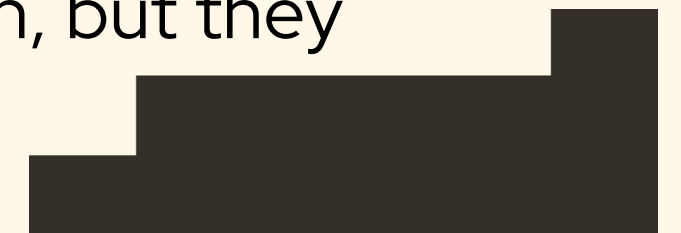


Project Impact

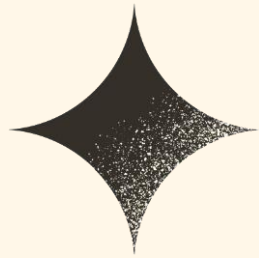
- Demonstrates that repeated unauthorized login attempts can be detected using native Windows 11 artefacts.
- Shows practical use of built-in tools (Event Viewer and Registry utilities) without relying on expensive commercial forensic software.
- Strengthens forensic analysis by correlating Security Event Logs with registry artefacts for improved timeline reconstruction.
- Promotes low-cost, accessible digital forensic investigation methods in modern Windows environments.

Project Limitations

- Limited to host-based unauthorized login attempts in a Windows 11 system under management.
- excludes malware assaults, network-based intrusions, and sophisticated privilege escalation methods.
- Security Event Logs are vital for detection; if logs have been eliminated or stopped, analysis may be affected.
- Registry artifacts are restricted in their ability to monitor direct authentication, but they do offer supporting evidence.



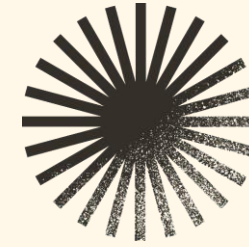
Conclusion



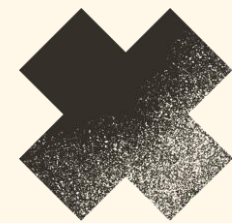
Registry analysis provides
hidden evidence



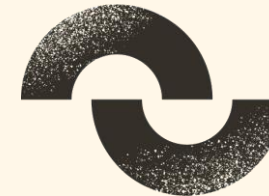
Always report
suspicious activity



Ensure each password
is unique



Identified unauthorized
access patterns



Events and registry data
help recreate attack
scenarios.

Reference

- [1] P. Patel, P. M. Bhatt, U. Parmar, and K. Bhavsar, "A forensic perspective on the use of Event Viewer for detecting malicious activities and ensuring system integrity," *ShodhKosh: Journal of Visual and Performing Arts*, vol. 5, no. 1, 2024.
- [2] Ibrahim, N.M., Ameer Al-Nemrat, Hamid Jahankhani and Rabih Bashroush (2012). Sufficiency of Windows Event Log as Evidence in Digital Forensics. *Lecture Notes in Computer Science*, pp.253–262. doi:https://doi.org/10.1007/978-3-642-33448-1_34.
- [3] Q. Do, B. Martini, J. Looi, Y. Wang, and K.-K. R. Choo, "Windows Event Forensic Process," in *Advances in Digital Forensics X*, 2014.
- [4] M. K. Singh and B. B. Meshram, "Cybercrimes and Digital Evidence Objects in Windows OS," *Journal of Criminology and Forensic Studies*, 2024.
- [5] Studiawan, H., Sohel, F. and Payne, C. (2019). A survey on forensic investigation of operating system logs. *Digital Investigation*, 29, pp.1–20. doi:<https://doi.org/10.1016/j.diin.2019.02.005>.
- [6] J.-H. Lee and H.-Y. Kwon, "Large-scale digital forensic investigation for Windows registry," *PLOS ONE*, 2022.
- [7] "Prajapati, Y. and Gosai, K. (2024). Windows Forensic Analysis and Detection of Ransomware Attacks Using Event Logs and Tools. *2023 4th International Conference on Intelligent Technologies (CONIT)*, [online] pp.1–6. doi:<https://doi.org/10.1109/conit61985.2024.10626973>.
- [8] Chang, K., Kim, G., Kim, K. and Kim, W. (2007). Initial Case Analysis Using Windows Registry in Computer Forensics. *Future Generation Communication and Networking (FGCN 2007)*. doi:<https://doi.org/10.1109/fgcn.2007.151>.
- [9] Chirath, W.D.A. and Rupasinghe, L. (2019). Comprehensive Forensic Data Extraction and Representation System for Windows Registry. *2019 International Conference on Advancements in Computing (ICAC)*. doi:<https://doi.org/10.1109/icac49085.2019.9103417>.