Computational Forensics: The Essential Role of Logs in APT and Advanced Cyberattack Response

Raymond Andre Hagen
Norwegian University of Science and Technology, Gjøvik, Norway

raymohag@stud.ntnu.no

Abstract: Advanced Persistent Threats (APTs) represent one of the most complex challenges in modern cybersecurity, characterized by their stealth, persistence, and sophistication. This study investigates the critical yet underutilized role of log analysis in detecting and responding to APTs, drawing on semi-structured interviews with 12 cybersecurity professionals from diverse sectors. Findings highlight logs as indispensable tools for identifying anomalies, reconstructing attack timelines, and understanding adversary tactics, techniques, and procedures (TTPs). However, barriers such as overwhelming data volumes, lack of standardization, and limited analytical tools hinder their effective utilization. To address these challenges, the study proposes actionable recommendations, including the adoption of standardized log formats, AI-driven real-time analysis, enhanced visibility across systems, and collaboration for threat intelligence sharing. These findings underscore logs' dual role as investigative assets and catalysts for improved cybersecurity resilience, offering a strategic roadmap for leveraging log analysis to counter evolving APT threats.

Keywords: Advanced persistent threats (APT), Computational forensics, Log analysis, Cybersecurity coordination, Threat intelligence, Cybersecurity standardization

1. Introduction

Advanced Persistent Threats (APTs) are among the most formidable challenges in contemporary cybersecurity (Lemay et al. 2018). Characterised by their stealth, sophistication, and persistence, APTs infiltrate networks to steal data, monitor activities, and disrupt operations over extended periods of time (Hutchins et al. 2011). Traditional security measures often fail to detect such threats owing to their ability to evade standard detection mechanisms.

In the field of *Computational Forensics*, which focuses on the application of computational methods to analyse, reconstruct, and interpret digital evidence, log analysis plays a pivotal role. Computational Forensics enhances traditional forensic practices by applying advanced computational methods, which enable more effective processing, analysis, and interpretation of digital evidence (Geradts 2018). Enhancing traditional forensic practices; enabling more effective processing, analysis, and interpretation of digital evidence; and seeking to enhance investigative techniques by leveraging algorithmic and machine-based approaches, making it particularly valuable in detecting and addressing complex cyber threats, such as APTs. By systematically processing and analysing extensive log data, Computational Forensics aids in identifying subtle indicators of compromise that are crucial for responding to APTs.

Logs have emerged as an essential tool in this context. They provide a chronological record of system and network activities, serve as a foundation for detecting anomalies, conduct forensic investigations, and effectively respond to incidents (Chuvakin et al. 2013). Comprehensive log analysis enables organisations to identify early indicators of compromise, understand attackers' tactics, techniques, and procedures (TTPs), and develop strategies to mitigate ongoing threats.

1.1 Problem Statement

The stealthy nature of APTs necessitates the development of advanced detection and response strategies. However, although logs are abundant, they are often underutilized owing to challenges, such as data volume, lack of standardization, and complex analysis requirements, which inhibit timely threat identification and response. Addressing these barriers is critical for strengthening organizational defenses against sophisticated and persistent adversaries. There is a pressing need to understand how logs can be effectively harnessed to enhance cybersecurity defences against APTs (Kim & Choi, 2014).

1.2 Research Objectives

This study addressed the following research questions:

- **RQ1**: What is the critical role of log analysis in identifying and mitigating APT activities, based on insights from cybersecurity experts?
- **RQ2**: How do logs serve as a central forensic tool for responding to incidents involving APTs?

- **RQ3**: What are the challenges and best practices in log management and analysis in combating APTs?
- **RQ4**: What actionable recommendations can enhance log management capabilities, as informed by industry experts' experiences?

2. Related Work

Extensive research has underscored the significance of logs in cybersecurity, particularly for detecting and responding to APTs. Logs offer a granular view of system activities that are essential for identifying anomalies, understanding attack patterns, and performing forensic investigations (Mandia et al. 2003). In recent studies, APTs have been noted for their ability to evade standard detection mechanisms, rendering traditional perimeter defences insufficient (Kim and Choi, 2014). This elusiveness places increased importance on log analysis, where techniques such as correlation and anomaly detection have proven effective in identifying covert indicators of compromise (IOCs) that are typical of APTs. (Li & Chen 2024)

The incorporation of artificial intelligence (AI) and machine learning (ML) into log analysis represents a significant advancement in cybersecurity. These technologies enhance the detection capabilities by processing vast volumes of data to identify patterns that are subtle or otherwise undetectable by human analysts (Almseidin et al. 2017). AI-driven approaches can continuously monitor abnormal activity, effectively adapt to evolving attack vectors, and provide more dynamic defense. Additionally, supervised and unsupervised learning methods within ML frameworks facilitate anomaly detection in real time, further improving responsiveness to potential threats.

Despite these technological advancements, significant log management challenges remain. The volume and complexity of logs generated by modern IT infrastructure can be overwhelming, often exceeding the processing capacity of traditional analytical tools (Chuvakin et al. 2013). Furthermore, a lack of standardization across different systems and applications complicates the integration and correlation of log data, impeding an effective analysis (Kim & Choi, 2014). This fragmentation increases the demand for skilled analysts and necessitates specialized tools capable of aggregating and normalizing disparate log formats to create a cohesive security overview. These persistent challenges highlight the need for continued innovation in automated log analysis and improved industry-wide standards for log-management practices.

Frameworks like "MITRE ATTACK", (Belfadel et al. 2023) commonly used in identifying and categorizing APT techniques, further emphasize the role of log analysis in mapping attacker TTPs to known threat patterns, facilitating a more structured response.

3. Methodology

Qualitative research, using semi-structured interviews with cybersecurity professionals, was conducted to explore the critical role of log analysis in combating APTs.

3.1 Participant Selection

A purpose-sampling method was employed to select 12 cybersecurity professionals from various sectors including government agencies, financial institutions, consulting firms, and technology companies. The participants were selected based on the following criteria.

- **Experience with APTs**: All participants had direct experience dealing with APT incidents.
- **Roles in Incident Response**: The participants held positions that involved incident response and forensic investigations.
- **Diversity of Sectors**: Representation from multiple sectors ensures a comprehensive understanding of issues in different organizational contexts.

Table 1 summarizes the diversity of cybersecurity professionals interviewed, their respective sectors, and their use of log analysis in APT investigations. The data highlights that participants from government agencies and financial institutions frequently engage in log-based forensic analysis, reinforcing the critical role of logs in regulated industries.

Table 1: Participant Overview and Log Utilization in APT Investigations

Respondent	Sector	Interview Date	Uses Logs
R1	Consulting Firm A	August 12, 2024	Yes
R2	Government Agency	August 5, 2024	Yes

Respondent	Sector	Interview Date	Uses Logs
R3	Financial Institution A	August 2, 2024	Yes
R4	Cybersecurity Consulting Firm B	August 20, 2024	Yes
R5	Government Agency B	September 16, 2024	Yes
R6	Consulting Firm C	September 2, 2024	Yes
R7	Financial Institution B	September 5, 2024	Yes
R8	Government Agency C	September 10, 2024	Yes
R9	Cybersecurity Consulting Firm D	August 5, 2024	Yes
R10	Government Agency D	September 10, 2024	Yes
R11	Research Institution	September 15, 2024	Yes
R12	Technology Company	September 20, 2024	Yes

3.2 Data Collection Process

The interviews were conducted between August and September 2024, each lasting between 1.5 and 2 hours. An open-ended question-and-answer interview guide was used to explore participants' experiences with APTs, the role of log analysis in their work, the challenges faced, and the best practices adopted. The sample questions were as follows.

- " Can you describe a situation where log analysis was crucial in detecting an APT?"
- " What challenges have you encountered in managing and analyzing log data?"
- " How do you think log analysis practices can be improved to better combat APTs?"

The interviews were recorded with consent and transcribed for analysis. NVIVO Qualitativate Analysis Software was used for analysis.

To enhance **validity and reliability**, all interviews followed a structured protocol to ensure consistency in questioning. Respondents were selected based on their **direct experience in APT investigations**, ensuring relevant expertise. Additionally, data was cross-checked against **existing literature and industry reports** to strengthen credibility.

3.3 Usage of AI and Proofreading Tools

To ensure that the ideas in this manuscript were presented with clarity and precision, various AI-based tools were employed, acknowledging challenges such as English not being a native language and dyslexia. Specifically, Grammarly and Writefull within Overleaf was used to enhance grammatical accuracy, stylistic consistency, and coherence during the scientific writing process. Additionally, Paperpal in MS Word was used for further language refinement, ensuring logical flow and comprehensive proofreading. OpenAI's ChatGPT 01-preview was also leveraged to assist with LaTeX coding of tables, citations, and other content. The use of these tools allowed for a more intense focus on the research itself, ensuring that the scientific content was communicated accurately and professionally, thereby enabling readers to concentrate on the presented findings and insights.

3.4 Ethical Considerations

This study was conducted in accordance with the ethical guidelines approved by the Norwegian Agency for Shared Services in Education and Research (SIKT.no, Ref. 530XXX). The participants were informed of the purpose of the study, and confidentiality was ensured. Informed consent was obtained from all participants and confidentiality was maintained by anonymizing participant identifiers in transcripts, securely storing recordings, and using encrypted data files for analysis.

3.5 Data Analysis

Thematic analysis was used to identify key themes related to the research questions (Galletta 2012). Transcripts were coded using deductive and inductive approaches.

- **Deductive Coding**: Based on the research questions and existing literature.
- **Inductive coding**: This allows themes to emerge organically from data.

Data saturation was achieved, indicating that the sample size was sufficient to capture the necessary insights.

3.6 Limitations

While this study provides valuable insights from cybersecurity professionals, it has certain limitations. The sample size of 12 respondents, though diverse in sectors, may not fully capture the broader landscape of APT investigations. Additionally, qualitative interviews, while rich in depth, may introduce subjectivity and potential recall bias, as participants reflect on past experiences rather than live cases. Furthermore, as the study relies on manual thematic analysis, findings may be influenced by researcher interpretation, despite the use of NVIVO software to mitigate bias. Future research could incorporate a mixed-methods approach, integrating quantitative data such as incident response logs or statistical models to validate the trends identified.

4. Findings

Analysis of the interview data revealed several key themes regarding the role of log analysis in detecting and mitigating APTs. Overall, responses from all 12 participants emphasized the critical role of log data in early threat detection, forensic investigation, and response to APT incidents, along with significant challenges and best practices in log management. Among the 12 cybersecurity professionals interviewed, **92% (11 out of 12)** emphasized that log analysis is critical for **early APT detection**, while **75% (9 out of 12)** specifically highlighted its role in tracing lateral movements within networks. Furthermore, **67% (8 out of 12)** reported that anomalies in login attempts and data exfiltration were the most common indicators of compromise found through logs. Figure 1 illustrates the distribution of key findings, highlighting the consensus among respondents on the critical role of log analysis in APT investigations.

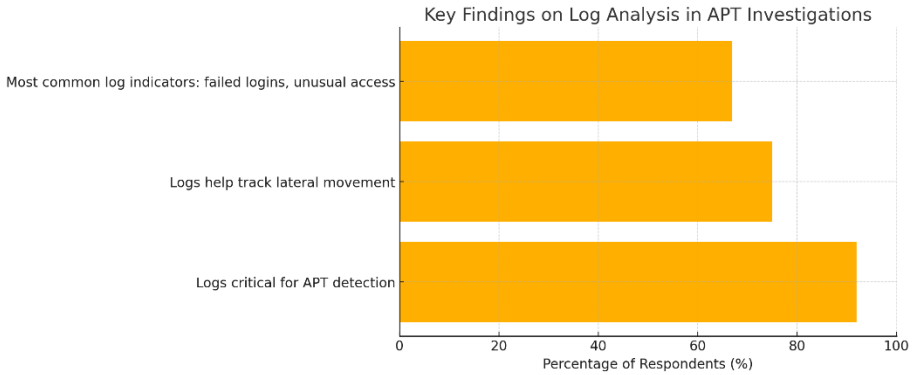

Figure 1: Key findings

Table 2: Summary of Key Findings from Cybersecurity Professionals

Finding	Number of Respondents	Percentage
Logs critical for early APT detection	11/12	92%
Logs help track lateral movement	9/12	75%
Most common log indicators: failed logins, unusual access	8/12	67%

4.1 Critical Role of Log Analysis in APT Detection (RQ1)

Logs are regarded as essential for identifying anomalies and potential breaches associated with APTs. Eleven of the 12 respondents emphasized the primary importance of logs in facilitating early incident detection. For instance, Respondent R1 articulates.

> *" Initial detection usually stems from log analysis. Logs reveal unusual patterns that indicate the presence of malicious actors."*

Similarly, Respondent R8 illustrates the role of the log data in revealing suspicious activities.

> *" Analyzing logs unveiled failed login attempts followed by a successful one at an odd hour, leading us to discover an ongoing APT."*

Such accounts illustrate how logs function as the first line of defense, enabling analysts to identify signs of compromise that might otherwise remain unnoticed. Furthermore, eight respondents mentioned that detecting APTs frequently involves identifying anomalies in login attempts, data exfiltration, and access to unusual network segments.

For example, Respondent R12 shares the following characteristics.

> *" Phishing attempts often provide the entry point, but it is the logs that show how attackers establish persistence. Reviewing these logs uncovers the methods they use to maintain access undetected."*

These insights underscore that logs not only support the identification of initial breaches but are also crucial for monitoring ongoing malicious activity by tracking recurrent or unusual access patterns.

4.2 Logs as a Central Forensic Tool (RQ2)

The utility of logs extends beyond detection to become the cornerstone of forensic investigation. All participants agreed on the necessity of logs to reconstruct attack timelines and understand attackers' tactics, techniques, and procedures (TTPs). Respondent R10 emphasized:

> *" Without detailed logs, piecing the attackers' actions together is nearly impossible. Logs are our roadmap during an investigation."*

Similarly, Respondent R4 highlighted the importance of logs in tracing lateral movements in compromised systems.

> *" Logs help us trace how attackers move within the network after initial access, which is vital for assessing the breach's full scope."*

Nine participants also mentioned that logs aid in the identification of attack vectors and potential vulnerabilities within systems. For instance, Respondent R3 discussed the role of logs in understanding the escalation of privileges.

> *" Logs provide us with a trail of privilege escalation efforts that reveal which accounts were exploited and how access was granted, which is crucial for closing security gaps."*

Such statements highlight the critical role that logs play in allowing organisations to conduct thorough forensic analyses, ensuring comprehensive assessments of the attack impact, and guiding incident response efforts effectively.

4.3 Challenges and Best Practices in Log Management (RQ3)

4.3.1 Challenges

The participants identified several significant challenges in managing log data effectively.

- **Volume and Complexity of Data**: All respondents highlighted the overwhelming volume of log data as a considerable challenge. For example, Respondent R9 noted," The sheer volume of log data can be overwhelming, making it difficult to extract meaningful information promptly."

Additionally, seven respondents mentioned that the complexity of logs due to varied system outputs adds to the difficulty of correlating and interpreting data efficiently. Respondent R7 noted:

> *" Logs from different systems come with unique formats and structures, which can turn analysis into a labor-intensive process."*

- **Lack of standardisation**: Eight respondents identified a lack of standardisation across log formats as a barrier to an efficient log analysis. Respondent R11 explained," Logs come in different formats across systems, posing integration challenges."
- **Technical Limitations and Skill Gaps**: Seven participants emphasised the need for advanced tools and experienced personnel to effectively analyse logs. Respondent R5 discussed the skill-related constraints, stating:

> *" Advanced log analysis often requires highly skilled personnel who can interpret complex patterns, which is a resource not all organizations have readily available."*

These challenges reflect the need for better resource allocation and standardisation within organisations to enhance their log-analysis capabilities.

4.3.2 Respondants suggestion for «Best Practice"

To overcome these challenges, the respondents suggested several best log management practices.

- **Real-time Monitoring**: Continuous log analysis was highlighted by eight respondents as essential for promptly detecting anomalies. Respondent R5, for instance, emphasized," Real-time monitoring of logs is necessary to catch unusual activity as it occurs, especially in environments vulnerable to frequent attacks."
- **Leveraging AI and Automation**: Six respondents advocated AI-driven analytics to handle large volumes of logs more efficiently. Respondent R12 noted:

"AI can help sift through massive amounts of log data to surface patterns humans might miss, which is invaluable in an age of big data."

- **Standardisation of Log Formats**: Six participants suggested that implementing standardised log formats would simplify integration and analysis across different systems. Respondent R6 stated:

" Standardized logging formats across systems would make it easier to correlate data points, creating a more cohesive view of security events."

- **Cross-Team Collaboration**: Three respondents recommended stronger collaboration between IT and security teams as a practice to improve log analysis efforts. As Respondent R10 pointed out:

" Effective incident response requires IT and security teams to work closely, ensuring that log data is comprehensive and that response strategies are based on all available insights."

These suggestions on "best practices" underscore the importance of technological investment, organizational cooperation, and standardised procedures in improving the efficacy of log management in APT detection and response.

4.4 Emerging Threats and Patterns in APT Activity

Six participants observed notable trends and shifts in APT activity, particularly with increased sophistication in persistence mechanisms and data exfiltration tactics. Respondent R2 described:

" Advanced actors have become highly adept at evading detection by maintaining persistence through methods like registry modification or encoded scripts that are challenging to catch."

Similarly, four respondents observed a trend of APT actors using credential stuffing and password spraying in their access systems. Respondent R9 emphasised the significance of these trends:

" Credential stuffing is one of the simpler tactics that can lead to deep compromise if it goes unchecked, making user authentication a prime focus."

5. Discussion

These findings highlight the indispensable role of log analysis in combating APTs. Logs provide the necessary visibility for network activities, enabling organisations to promptly detect and respond to threats. The identified challenges align with the existing literature, which emphasises the difficulties in managing and analysing large amounts of log data (Chuvakin et al. 2013).

5.1 Integration of Advanced Technologies

The use of AI and machine learning in logarithmic analysis has emerged as a critical advancement, improving the ability to detect subtle indicators of compromise (Sommer and Paxson, 2010). These technologies can process and analyse data at a scale and speed unattainable by human analysts alone. However, their effectiveness depends on the quality and consistency of log data, reinforcing the need for standardized log formats (Gholamian & Ward, 2021). It also adds to the risk of over-reliance on automation and bias in the training of AI models; therefore, it is important to understand the limitations of such technologies. (Nguyen 2024)

5.2 Standardization and Collaboration

The lack of standardisation in log formats was a significant challenge for participants. Standardising log data facilitates easier analysis within organisations and enhances the ability to share threat intelligence across organisations. Collaboration and sharing of log-derived intelligence can significantly enhance collective cybersecurity efforts, as noted by Respondent R11:

" Sharing insights from our log analyses with other organizations and CERTs helps everyone improve their defences against APTs."

5.3 Implications for Cybersecurity Practices

The findings of this study have practical implications for how organisations approach cybersecurity.

- **Resource Allocation**: Investing in advanced log management tools and skilled personnel are essential.
- **Policy Development**: Establishing policies for log retention, analysis, and sharing can enhance preparedness.
- Cybersecurity teams require comprehensive training to develop competencies in log management practices, including understanding the importance of logs, methods for their collection, and analysis for investigation of APTs.

6. Conclusion

Logs play a fundamental role in the investigation and management of Advanced Persistent Threats (APTs), serving as indispensable tools for detecting, understanding, and mitigating sophisticated cyberattacks. This study has demonstrated the dual importance of logs as both an investigative asset and a foundation for developing robust cybersecurity strategies.

Through interviews with cybersecurity professionals, this research revealed the essential capabilities logs provide in detecting anomalies, reconstructing attack timelines, and understanding attacker behaviors. The study also highlighted significant barriers, including data volume, lack of standardization, and analytical complexities, which hinder the effective utilization of logs. Addressing these challenges is crucial for improving log management practices and enhancing organizational resilience against APTs.

Key Contributions:

- **Operational Insights**: Logs enable early detection of anomalies, support detailed forensic investigations, and provide a critical resource for understanding and countering APTs.
- **Challenges Identified**: Common issues include overwhelming log data volumes, insufficient standardization, and gaps in technical and analytical expertise.
- **Actionable Recommendations**: The study underscores the need for real-time monitoring, AI-driven analytics, standardized log formats, and cross-team collaboration to address these challenges effectively.

Implications:

The findings advocate for holistic improvements in log management, encompassing technological advancements, process enhancements, and strategic investments in tools and expertise. Organizations must prioritize comprehensive logging strategies and foster a culture of collaboration and intelligence-sharing to counteract sophisticated adversaries.

Future Work:

Building on these insights, future research should explore:

- Developing and testing standardized logging frameworks across diverse systems.
- Leveraging advanced AI techniques for real-time anomaly detection.
- Investigating the interplay between organizational policies and log analysis practices to identify areas for improvement.

By addressing these gaps and implementing the recommended practices, organizations can transform logs from passive data repositories into active enablers of cybersecurity resilience. This proactive approach is essential for mitigating the evolving threats posed by APTs and ensuring a secure digital ecosystem.

Acknowledgements

Gratitude was extended to all cybersecurity professionals who participated in this study for their invaluable insights and contributions.

References

Almseidin, M., Alzubi, S., Kovacs, S. & Alkasassbeh, M. (2017), Evaluation of machine learning algorithms for intrusion detection system, *in* '2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)', pp. 1–6.

Belfadel, A., Boyer, M., Letailleur, J., Petiot, Y., Yaich, R., Abie, H., Pallas, F., Katsikas, S., Mylopoulos, J., Cuppens, , Pohle, J., Kalloniatis, C., Sasse, M. A., Ranise, S., Verderame, L., Maestre Vidal, J., Pirbhulal, S., Katt, B., Pallas, F., Sasse, M. A., Verderame, L., Albanese, M., Pohle, J., Sotelo Monge, M. A., Katsikas, S., Cuppens, F., Kalloniatis, C., Abie, H., Ranise, S., Cambiaso, E., Shukla, A. & Mylopoulos, J. (2023), Towards a security impact analysis framework: A risk-based and mitre attack approach, *in* 'Computer Security. ESORICS 2022 International Workshops', Vol. 13785 of *Lecture Notes in Computer Science*, Springer International Publishing AG, Switzerland, pp. 212–227.

Chuvakin, A., Schmidt, K. J. & Phillips, C. (2013), *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*, Syngress, Waltham, MA.

Galletta, A. (2012), 'Mastering the semi-structured interview and beyond : from research design to analysis and publication'.

Geradts, Z. (2018), 'Digital, big data and computational forensics', *Forensic sciences research* **3**(3), 179–182.

Gholamian, S. & Ward, P. A. S. (2021), 'A comprehensive survey of logging in software: From logging statements automation to log mining and analysis'.

Hutchins, E. M., Cloppert, M. J. & Amin, R. M. (2011), 'Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains', *Leading Issues in Information Warfare & Security Research* **1**, 80–106.

Kim, H. & Choi, J. (2014), Log-based detection of advanced persistent threats, *in* '2014 International Conference on Information and Communication Technology Convergence (ICTC)', pp. 79–83.

Lemay, A., Calvet, J., Menet, F. & Fernandez, J. M. (2018), 'Survey of publicly available reports on advanced persistent threat actors', *Computers Security* **72**, 26–59. **URL:** *https://www.sciencedirect.com/science/article/pii/S0167404817301608*

Li, L. & Chen, W. (2024), 'Congraph: Advanced persistent threat detection method based on provenance graph combined with process context in cyber-physical system environment', *Electronics (Basel)* **13**(5), 945.

Mandia, K., Prosise, C. & Pepe, M. (2003), *Incident Response: Investigating Computer Crime*, 2nd edn, McGraw-Hill Osborne Media, Berkeley, CA.

Nguyen, J. K. (2024), 'Human bias in ai models? anchoring effects and mitigation strategies in large language models', *Journal of behavioral and experimental finance* **43**, 100971.

Sommer, R. & Paxson, V. (2010), 'Outside the closed world: On using machine learning for network intrusion detection', *IEEE Symposium on Security and Privacy* pp. 305–316.