Graduate School of Science and Technology Master's Thesis Abstract

Laboratory name (Supervisor)	Cyber Resilience (Youki Kadobayashi (Professor))		
Student ID	2411411	Submission date	2026 / 1 / 19
Name	DHITAL NEETI		
Thesis title	Forensic Evidence Loss in Serverless and Ephemeral Cloud Workloads: A Vendor-Neutral Analysis and a Minimal Forensic Readiness Pattern (MFRP)		

Abstract

Cloud computing increasingly relies on ephemeral and event-driven execution models, including short-lived virtual machines, containers, and serverless functions. While these architectures improve scalability and cost efficiency, they fundamentally undermine traditional Digital Forensics and Incident Response (DFIR) assumptions. Volatile forensic artefacts such as process state, memory-resident execution, and transient network associations are irreversibly destroyed upon workload termination, limiting post-incident forensic reconstruction. This thesis empirically investigates forensic evidence loss in Linux-based ephemeral cloud workloads. Experimental analysis demonstrates that cloud-native logging and security monitoring services provide limited visibility into runtime centric and fileless attacks, leaving systematic forensic blind spots under log centric investigation models. To address this limitation, the thesis proposes a **Minimal Forensic Readiness Pattern (MFRP)** a lightweight, vendor-neutral approach for proactively preserving high value volatile forensic artefacts within the execution lifecycle of ephemeral workloads. The pattern targets a minimal set of process, network, kernel, and memory artefacts captured prior to termination.The proposed approach is evaluated using an **Evidence Completeness Model (ECM)**, enabling structured comparison between log-only and volatile aware forensic collection. Results show that the MFRP significantly improves forensic completeness, enabling reliable process attribution, network correlation, and recovery of in-memory execution traces that are otherwise unavailable after workload termination. These findings demonstrate that proactive, minimal forensic readiness is essential for effective DFIR in modern cloud architectures.