Omsai Dagwar

Pune, Maharashtra

+91 8459749158 dagwarom2112@gmail.com linkedin.com/in/omsai-dagwar

Profile

DFIR Analyst with 2+ years of hands-on experience in digital forensics, incident response, malware analysis, and threat hunting. Proficient in forensic toolkits (FTK, Cellebrite, Autopsy), SIEM platforms (QRadar,Microsoft Defender, Seceon), and forensic acquisition. Trusted by law enforcement and enterprise teams to investigate cybercrimes and secure digital evidence.

Education

Jain University

MCA in Cyber Security — *Bangalore, India*

Bracts Vishwakarma Institute of Information Technology

B.Tech in Electronics and Telecommunication – 7.89 CGPA — *Pune, India*

Experience

Cybermate Forensics and Data Security Solutions Pvt. Ltd. — **Apr 2023 – Present**

Sr.Digital Forensics and Incident Responder — *Pune, India*

- Led 15+ forensic investigations involving mobile, desktop, and cloud environments.
- Performed disk imaging and data recovery using FTK Imager, Guymager, and MacQuisition.
- Utilized **Velociraptor** for endpoint visibility and live memory forensics, accelerating investigations.
- Created and deployed custom **YARA rules** to detect fileless malware and suspicious executables.
- Analyzed malware using static and sandbox techniques to support criminal cases.
- Collaborated with law enforcement agencies and provided digital evidence in legal formats.
- Attended and supported 100+ search and survey operations with the Income Tax Department, assisting in digital evidence identification and seizure.
- Worked on data center forensics, including secure acquisition and backup of servers hosted on cloud pool infrastructure.

RNS Technology MSSP Pvt. Ltd. (Internship) — **Jan 2023 – Apr 2023**

SOC Analyst L1 — *Dubai, UAE (Remote)*

- Supported threat hunting efforts using Seceon, and LogRhythm SIEMs.
- Monitored and triaged 500+ security incidents using QRadar, SentinelOne, and XDR tools.
- Managed incident response processes and maintained SLA compliance throughout investigations.
- Supported malware analysis efforts by employing static analysis and sandbox techniques to examine malicious behavior, aiding in the creation of detection signatures for newly identified threats.

Certifications and Recognition

- Certified Ethical Hacker (CEHv13 ai) – EC - Council
- Digital Forensics Essentials – EC-Council
- Security Analyst Bootcamp (Splunk) – Virtual Testing Foundation
- Blue Team Junior Analyst (BTJA) – Security Blue Team
- Autopsy Forensics (Intro) – Sleuth Kit
- Certified in aiSIEM, aiXDR, aiMSSP – Seceon Inc.
- Awarded “Best Cybersecurity and DF Analyst” by Income Tax and Enforcement Directorate, Mumbai
- SC-200 – Microsoft Security Operations Analyst

Technical Skills

- **Forensics Tools:** FTK Imager, Guymager, Autopsy, Cellebrite UFED, MacQuisition, dtSearch, Velociraptor, OxygenForensics Detective, MobilEdit Forensics Pro, Magnet Axiom, Magnet DVR Examiner, Guymager and CarbonCopy cloner
- **Threat Detection Tools:** YARA Rules, aiSIEM, aiXDR, Microsoft Defender XDR
- **SIEM Platforms:** QRadar, Seceon, Microsoft Defender, Defender for Cloud
- **Skills:** Threat Hunting, Malware Analysis, SOC Operations, Memory Forensics, Incident Response, Disk Imaging
- **Frameworks:** MITRE ATT&CK, Cyber Kill Chain, OSI Model, DFIR Playbooks
- **Hardware Tools:** LogiCube Falcon, Tableau TD-3 Forensic Duplicator

Projects

- **Forensic WhatsApp Database Research** – Successfully implemented Python-based methods for forensic acquisition and decryption of WhatsApp databases on Android devices (up to v12) without requiring root access. Currently extending research to Android v13–15 and developing a custom Python script for secure extraction of WhatsApp encryption keys for investigative purposes.
- **Windows Log Acquisition Automation** – Customized and implemented PowerShell scripts (with research and adaptation from open-source resources) to automate the collection of Windows Event Viewer logs, including Security, Application, and System events. Enhanced the script to export logs into XLSX format for improved analysis and reporting during forensic audits and incident investigations.
- **Mobile Spyware Detection** – **GitHub Repository**. Developed a Python script to identify hidden and spyware applications on Android devices, supporting forensic analysis and mobile threat detection. Published the script on GitHub to contribute to the open-source DFIR community. Explored iOS spyware detection techniques using **iMazing** to analyze configuration profiles, application data, and potential surveillance traces.