



**Case ID:** 2025-ALPHA

**Case Name:** Law Firm Malware Incident – Case 2025-Alpha

**Requesting Organization:** CyArt

**Requesting Contact:** CyArt-Manager

**Examiner Name:** Adithya Baragi S

**Examiner Role:** Junior Digital Forensics Examiner (Intern)

**Organization:** BMS Institute of Technology and Management (BMSIT), Bengaluru

**Phone / Email:** +91-9591256101 / adithyabaragis@gmail.com

## Description of Evidence

### 1. Alpha-Workstation.E01 (1.2 GB)

- Description: Forensic disk image of employee laptop (Windows workstation).
- Source: Seized from “Alpha Workstation – Employee Laptop” at Law Firm Office, Bengaluru, India.

### 2. Alpha-Memory.mem (600 MB)

- Description: Physical memory (RAM) capture of the same workstation.

### 3. Alpha-Traffic.pcap (80 MB)

- Description: Network packet capture associated with the workstation during the incident window.

### 4. Alpha-EventLogs.evtx (12 MB)

- Description: Exported Windows Event Logs from the workstation.

## Acquisition Details

**Date & Time of Acquisition (UTC):** 2025-03-10 16:00

**Acquired By:** Rahul Mehta, IT Administrator

**Acquisition Method:** Forensically sound imaging using FTK Imager with write blockers where applicable.



### Storage Location

**Primary Storage:** External HDD CYART-EVIDENCE-01, DFIR Evidence Locker, Bengaluru

**Working Copy:** D:\DFIR\Case-2025-Alpha (examiner's analysis workstation)

### Chain of Custody Log

Date/Time (UTC)	From (Name / Role)	To (Name / Role)	Action	Initials
2025-11-19 16:00	Rahul Mehta / IT Admin	Adithya Baragi S / DF Examiner (Intern)	Evidence received	AB
2025-11-19 16:15	Adithya Baragi S	Adithya Baragi S	Working copies created	AB
2025-11-19 10:00	Adithya Baragi S	Supervisor / Mentor (Digital Forensics)	Report submitted/reviewed	AB

### Certification

I, **Adithya Baragi S**, certify that the evidence listed above was received, stored, and analyzed in a forensically sound manner. To the best of my knowledge, the integrity of the evidence has been maintained throughout the examination.

Signature: Adithya

Date: 19/11/2025