# Digital Forensic Investigation Report

## 1. Case Information

- **Case ID:** DF-2025-0042
- **Case Title:** Unauthorized Access to Company Email System
- **Date Opened:** April 10, 2025
- **Requesting Party:** IT Security Department, TechNova Solutions Pvt. Ltd.
- **Investigator:** John Smith, Certified Digital Forensic Examiner (GCFE)

---

## 2. Objective

To investigate unauthorized access to the internal email system reported on April 7, 2025, and identify the source and method of intrusion, if any, while preserving the integrity of digital evidence for possible legal proceedings.

---

## 3. Scope of Investigation

- Examination of a company-issued laptop (Asset ID: TN-4578)
- Inspection of the company email server logs
- Recovery and analysis of deleted or suspicious files
- Timeline reconstruction of unauthorized activities

---

## 4. Tools Used

| Tool Name | Version | Purpose |
|---|---|---|
| **FTK Imager** | 4.5 | Forensic imaging |
| **Autopsy** | 4.20.0 | Timeline and file system analysis |
| **Wireshark** | 4.2.1 | Network packet inspection |
| **X-Ways Forensics** | 20.6 | File carving and metadata review |
| **HashCalc** | 1.02 | MD5/SHA1 hash generation |

---

## 5. Chain of Custody

| Date & Time | Evidence Description | Handled By | Action Taken | Signature |
|---|---|---|---|---|
| **10-Apr-2025 10:30** | Laptop (Asset ID: TN-4578) | Jane Doe (IT) | Seized and bagged in evidence kit | Jane Doe [Signed] |

| | | | | |
|---|---|---|---|---|
| **10-Apr-2025 11:00** | Digital image of hard drive created | John Smith | Image acquired using FTK Imager | John Smith [Signed] |
| **10-Apr-2025 11:15** | Original laptop sealed and stored | John Smith | Stored in Evidence Locker #5 | John Smith [Signed] |

All evidence was preserved in a write-protected environment. MD5 and SHA-1 hashes were computed and verified post-copy to ensure forensic integrity.

---

# 6. Evidence Summary

## 6.1 Device Specifications

- **Device Type:** Laptop
- **Manufacturer:** Dell
- **Model:** Latitude 7490
- **OS:** Windows 10 Pro
- **HDD Size:** 512 GB SSD
- **Serial Number:** DLT-7490-000124

## 6.2 Disk Image Hashes

| Hash Type | Hash Value |
|---|---|
| **MD5** | 6f5902ac237024bdd0c176cb93063dc4 |
| **SHA-1** | 9c1185a5c5e9fc54612808977ee8f548b2258d31 |

---

# 7. Findings

## 7.1 Email System Intrusion

- A PowerShell script named `mail_scraper.ps1` was found in the user's `AppData` folder.
- Logs showed remote access via TeamViewer on April 6, 2025, at 02:15 AM without authorization.
- The attacker accessed inboxes of three senior employees and downloaded attachments.

## 7.2 User Account Activity

- The user's account was used to create a scheduled task named `UpdaterTask` running the malicious script.
- Timestamps confirmed execution at irregular hours, outside of working time.

## 7.3 Suspicious Artifacts

| File Name | Path | Status |
|---|---|---|

| | | |
|---|---|---|
| **mail_scraper.ps1** | C:\Users\j.doe\AppData\Roaming | Malicious |
| **updater.log** | C:\ProgramData\Logs | System Log |
| **credentials.txt** | C:\Users\j.doe\Downloads | Plaintext |

---

# 8. Timeline of Events

| Date & Time | Event Description |
|---|---|
| **05-Apr-2025 23:45** | TeamViewer first accessed on suspect laptop |
| **06-Apr-2025 02:15** | Unauthorized session began |
| **06-Apr-2025 02:17** | PowerShell script executed |
| **06-Apr-2025 02:25** | Email attachments downloaded and saved |
| **06-Apr-2025 02:40** | Log file updated by scheduled task |

---

# 9. Conclusion

The digital forensic investigation confirms that the company laptop assigned to Jane Doe was used to conduct unauthorized access to the internal email system. Artifacts and logs indicate remote access and automated scripts were used to extract sensitive information. The evidence collected is consistent, properly preserved, and may be admissible in legal proceedings.

---

# 10. Recommendations

- Revoke access and reset all credentials of affected users.
- Uninstall unauthorized software like TeamViewer from company assets.
- Implement stricter network monitoring during off-hours.
- Conduct employee training on cybersecurity best practices.

---

# 11. Appendices

- **Appendix A:** Hash logs
- **Appendix B:** Screenshots of key evidence
- **Appendix C:** Network logs and event viewer entries
- **Appendix D:** Full forensic disk image hash verification report

---

# 12. Signatures

**Investigator Name:**
John Smith
Digital Forensics Examiner

Signature: _____
Date: April 14, 2025