**🛡️ Internship Project Report: Incident Response and Malware Investigation (Simulated)**

**Student Name:** Vaibhav Ratan  
**Intern ID:** 441  
**Organization:** DigiSuraksha Parhari Foundation  
**Branch & Year:** B.Tech 1st Year – Computer Science  
**Date Of Submission:** July 25, 2025

**📘 1. Incident Response Field Interview Questions (Filled Example)**

| **No.** | **Interview Question** | **Field Notes / Data to Capture** | **Purpose** |
| --- | --- | --- | --- |
| 1 | Who discovered/reported the incident? | Riya Mehta (HR Staff), riya@organization.org, 21/07/25 10:38 AM | Contact for more info |
| 2 | What suspicious activity or alert triggered the response? | Antivirus alert after opening an Excel file named payroll\_data.xlsm | Identify how it started |
| 3 | What were the first actions taken after the incident/alert? | Laptop disconnected from Wi-Fi, user informed IT team | Stop spread & begin response |
| 4 | What systems/hosts appeared affected? | HR-LAPTOP01, IP: 192.168.5.44, User: Riya Malhotra | Locate infected system |
| 5 | Has this issue been reported before? | No, first time from this user/system | Check if it’s repeating |
| 6 | Are there business processes/data at risk? | HR employee data and salary records | Understand risk level |
| 7 | What logs or devices generated alerts? | Windows Defender, System Event Logs | Find source of truth |
| 8 | Any unauthorized account activity or privilege escalation? | Login from unknown device ID at 2:45 AM | Check for attacker behavior |
| 9 | Were there unusual network connections? | Outbound traffic to unknown server IP 85.200.91.77 | Could be data exfiltration |
| 10 | Did anyone download/open suspicious files, links, emails? | Yes, user opened email with subject “Urgent Salary Slip Request” | Infection method |
| 11 | Have any remediation steps been performed? | File deleted, antivirus scan completed, admin password changed | Limit damage |
| 12 | Any other notable user/system actions noted? | Registry entry found for xlsm\_launcher.exe | May indicate persistence |

**🧾 2. Field Notes Table (Simplified)**

| **Field** | **Captured Data** |
| --- | --- |
| Incident Reporter | Riya Mehta (HR), riya@digisuraksha.org |
| Date/Time | 21 July 2025, 10:38 AM |
| Affected System | HR-LAPTOP01, IP: 192.168.5.44 |
| Nature of Incident | Malware infection from Excel macro |
| Alert Source | Windows Defender: Trojan Detected |
| Immediate Action | System disconnected from Wi-Fi, IT informed |
| Log Sources | Windows Defender, Event Viewer |
| Open Questions | Was any data uploaded? Is the malware still running in background? |
| Analyst Name | Vaibhav Ratan |
| Status | Closed and resolved |

**📊 3. Alert & Log Analysis (Simple Workflow)**

**Tools/Methods Used:**

* 🖥️ **Windows Defender Alert**: Showed Trojan detected
* 🧾 **Event Viewer**: Showed unknown .exe added to startup
* 🔗 **Wireshark (simulated)**: Outbound DNS query to paydata.ru
* 🧪 **VirusTotal**: Macro file hash flagged by 55 vendors

**🧪 4. Malware Analysis (Basic)**

| **Area Checked** | **Finding** |
| --- | --- |
| **Downloads Folder** | File: payroll\_data.xlsm |
| **Registry Run Key** | Entry for xlsm\_launcher.exe |
| **Browser History** | Visited paydata.ru/slip before infection |
| **Antivirus Logs** | Signature: Trojan:Win32/Fuerboos.C!cl |

**⚙️ 5. Tools Used by Me**

| **Tool** | **Purpose** |
| --- | --- |
| VirusTotal.com | Check malware signature of file |
| Wireshark *(simulated)* | Identify DNS to suspicious IP |
| md5sum | Generate file hash in Kali |
| Windows Event Viewer | Check system logs and app launches |

**Sample Hash Command:**

bash

CopyEdit

md5sum payroll\_data.xlsm

**6. Investigation Planning Checklist**

* Collected user & system details
* Noted alert & initial response
* Verified malware via VirusTotal
* Found registry persistence
* Identified suspicious DNS activity
* Wrote this report

**🧠 7. Key Learnings**

* Phishing emails can carry dangerous macros
* Checking logs and alerts is critical to investigate
* Tools like **VirusTotal** and **Event Viewer** are very helpful
* Immediate action (disconnect, report) is very important
* Even as a beginner, I could understand and simulate real-world cybersecurity steps

**📘 8. Final Notes**

* **Status:** Resolved
* **Date Closed:** 23rd of July, 2025
* **Handled by:** Vaibhav Ratan

**🛠️ Tools Used & Simulation Disclaimer**

**🔍 Overview of Tools Used**

As part of this **simulated cybersecurity incident response project**, I used a set of basic but powerful tools to learn how malware incidents are investigated and responded to:

**1. VirusTotal**

An online malware analysis tool used to check if a suspicious file (in this case, payroll\_data.xlsm) was flagged by global antivirus engines.

* 🔗 https://www.virustotal.com

**2. Windows Event Viewer *(Simulated)***

Used to review basic system activity logs, identify odd login times, and track registry or executable changes linked to the malware.

**3. Wireshark *(Simulated Use)***

Simulated to learn how to analyze network traffic and detect unusual DNS queries or connections to external IPs.

**4. md5sum on Kali Linux**

Used to generate the MD5 hash of the file for further checking with VirusTotal.

bash

CopyEdit

md5sum payroll\_data.xlsm

**📌 Simulation Disclaimer**

This project was completed as a **simulation** for **educational purposes only**.  
No real-world systems, networks, users, or organizations were affected. All names, events, systems, and IP addresses used are **fictional but based on realistic scenarios** commonly taught during beginner-level cybersecurity training.

The entire analysis process was carried out manually and independently by **Vaibhav Ratan (Intern ID: 441)** as part of his internship at **DigiSuraksha Parhari Foundation**.

**🤖 Use of Kali GPT**

To support formatting, structure, and guidance, **Kali GPT**—an AI assistant trained in Kali Linux and cybersecurity—was used during the creation of this report.

❗ However, all **content writing, tool research, simulated log analysis, and final answers were done by the intern himself**.

Kali GPT only helped in **organizing the report**, suggesting correct formats, and explaining technical tools in beginner-friendly ways.

**📚 Reference Sources**

* Incident Response Interview & Analysis Workbook (File 1.pdf)
* Kali Linux Knowledge Files (2024 & 2025 editions)
* Official documentation from:
  + VirusTotal
  + Wireshark
  + Microsoft Event Viewer
  + Basic Linux utilities