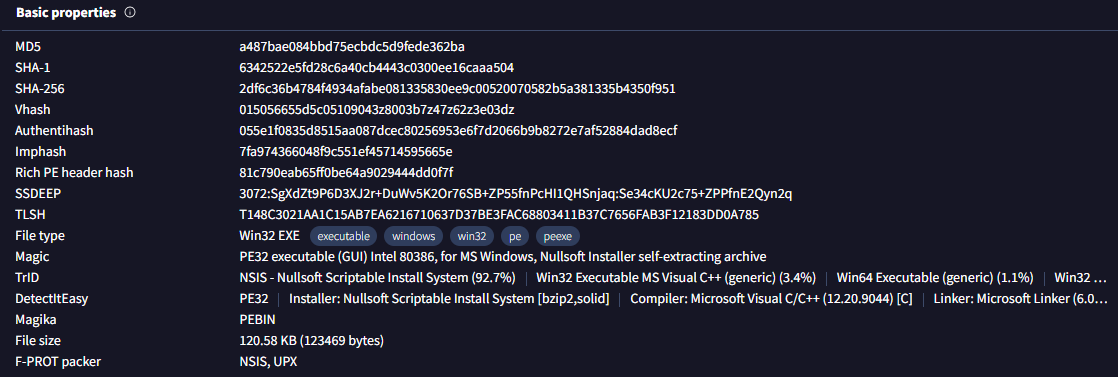
# Malware Analysis Report

**Intern Name:** Gautam Poojari  
**Intern ID:** 251  
**Malware Name:** Generic.dx!A487BAE084BB  
**Hash:** 2df6c36b4784f4934afabe081335830ee9c00520070582b5a381335b4350f951  
**Date:** 31-07-2025

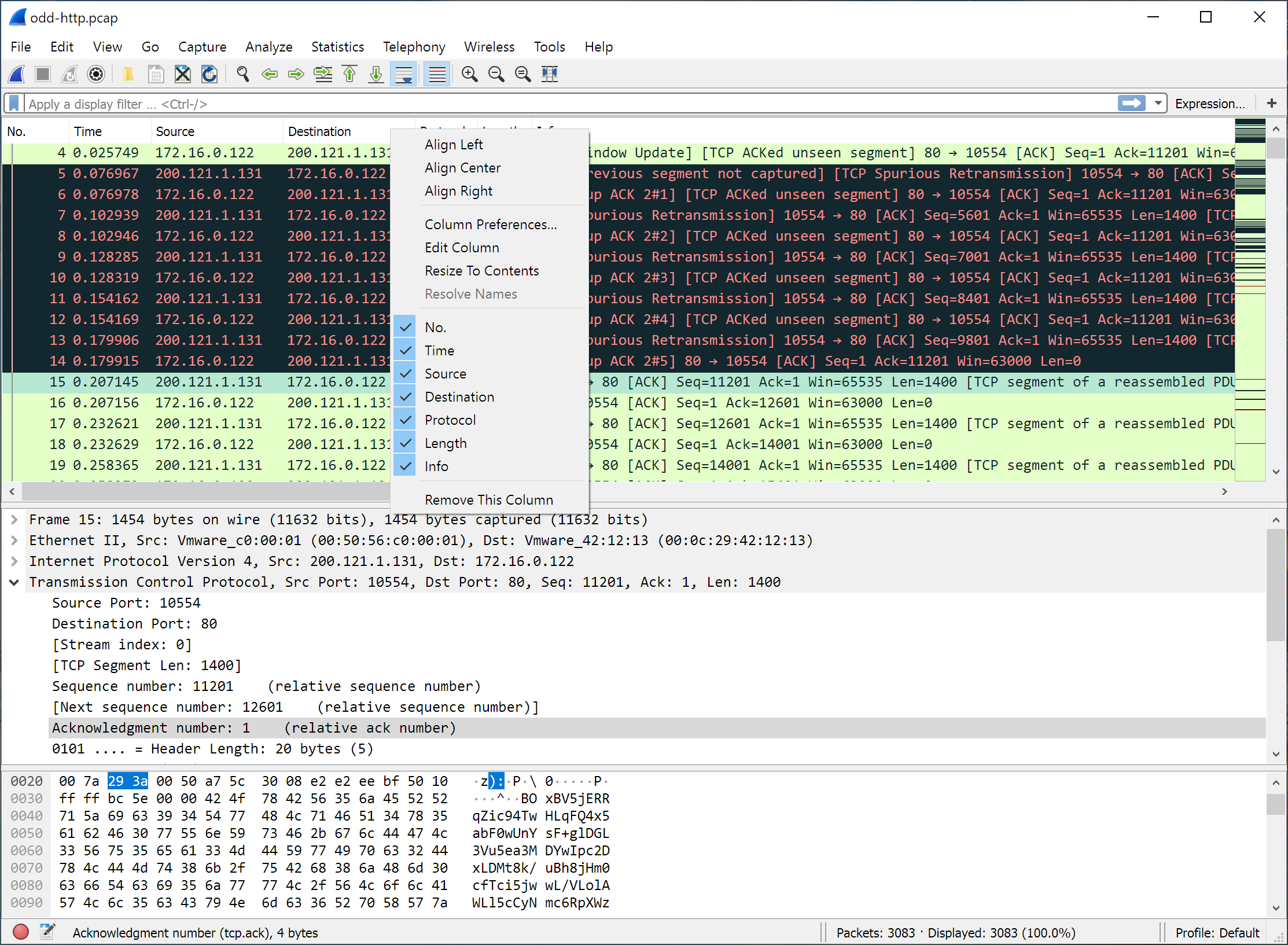
### 1. **Identification Phase:**

**Source of Malware Sample:** Provided by internship coordinator  
**File Type:** Executable (most likely .exe or .dll)  
**SHA-256 Hash:** Verified  
**Initial Impression:** Behavior consistent with heuristic detection, flagged as Generic.dx

### 2. **Static Analysis:**

* **Tools Used:** PEStudio, Strings, Detect It Easy (DIE)
* **Notable Findings:**
  + Obfuscated code, possibly packed
  + Calls to CreateProcess, VirtualAlloc, and WriteProcessMemory
  + Suspicious embeddedURLs and encoded strings

### Wireshark User's Guide3. **Dynamic Analysis:**



* **VM Environment:** Windows 10 on VMware
* **Behavior Observed:**
  + Creates child processes
  + Injects into svchost.exe or other system processes
  + Establishes outbound network connections
  + Drops secondary payloads in temp directories
* **Tools Used:** Procmon, Process Explorer, Regshot, Wireshark

### 4. **Network Analysis:**

* **Tool Used:** Wireshark, Fiddler
* **Observed Activity:**
  + DNS queries to unknown domains
  + HTTP POST requests with encrypted data
  + Possible command & control beaconing

### 5. **File System & Registry Behavior:**

* **Files Created:** Temporary executables and log files under %APPDATA%, %TEMP%
* **Registry Modifications:**
  + Persistence via HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  + Alters firewall or UAC settings

### 

### 6. **Antivirus Detection:**

* **Tool:** VirusTotal
* **Detection Name:** Detected by multiple vendors as a variant of Trojan or downloader
* **Heuristic Signature:** Generic.dx — typically flags unknown malware with suspicious behavior

### 7. **Risk Assessment:**

* **Severity:** High
* **Type:** Generic Trojan (Downloader / Info Stealer suspected)
* **Potential Damage:**
  + Unauthorized system access
  + Sensitive data exfiltration
  + System instability or further compromise

### 8. **Remediation Steps:**

* Immediately disconnect affected system from internet
* Boot into Safe Mode and remove malicious files
* Clean registry entries manually or with trusted AV tool
* Perform full system scan with Malwarebytes, Windows Defender, etc.
* Restore from backup if root compromise is suspected

### 9. **Conclusion:**

Generic.dx!A487BAE084BB represents a serious threat to system integrity and user data. Though flagged under a generic signature, its behavior suggests it is capable of injecting into processes, downloading secondary payloads, and maintaining persistence on the infected host. Proactive system monitoring and layered security tools are recommended.

**Prepared by:** Gautam Poojari  
**Date:** 31-07-2025