**Cybersecurity Investigation Report: Malicious Traffic Analysis**.

**Objective**

On Day 2 of my cybersecurity training, I analyzed a malicious Packet Capture (PCAP) file using Wireshark to uncover evidence of malware activity. This exercise aimed to enhance my threat detection skills, a critical competency for aspiring SOC Analysts, by identifying infected files, compromised sites, and affected systems within a controlled VMware lab environment.

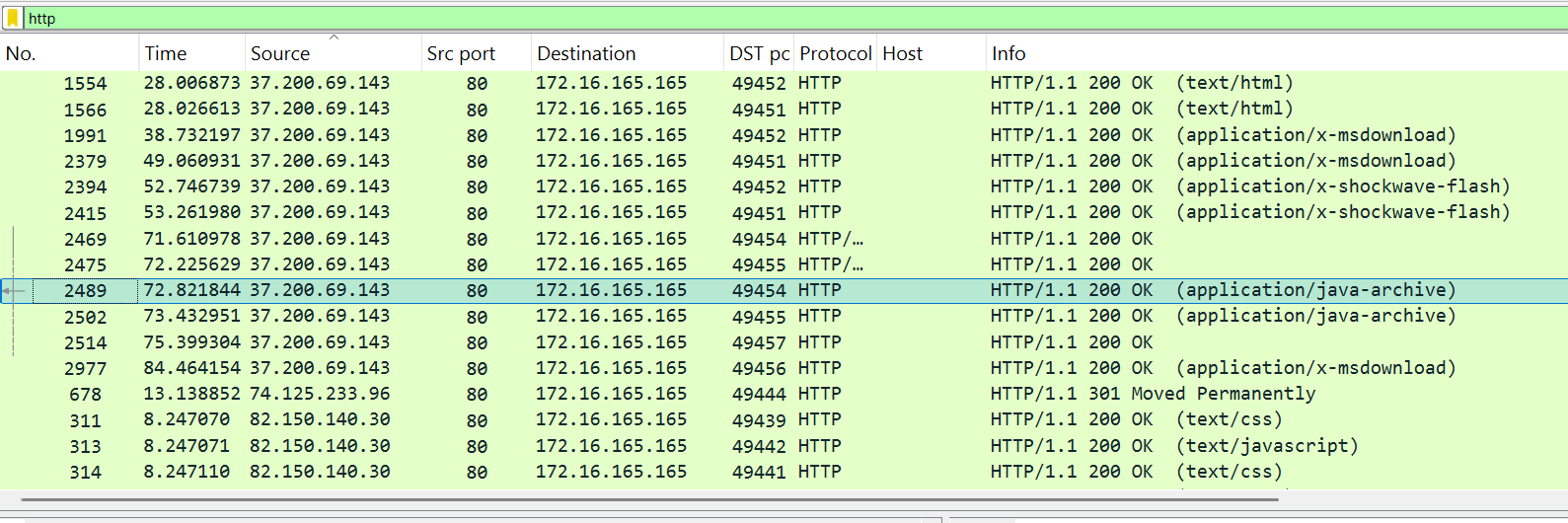
**Lab Environment**

* **Platform**: VMware Workstation Player (free version).
* **Virtual Machines**:
  + Parrot OS Security Edition (IP: 192.168.81.132, 4GB RAM, NAT network).
  + Windows 10 Evaluation (IP: 192.168.81.128, 2GB RAM, NAT network).
* **Tool**: Wireshark (installed on Parrot OS via sudo apt install wireshark -y).
* **PCAP Source**: Malware Traffic Analysis (<https://malware-traffic-analysis.net/>), sample dated 2025-01-22.

**Methodology**

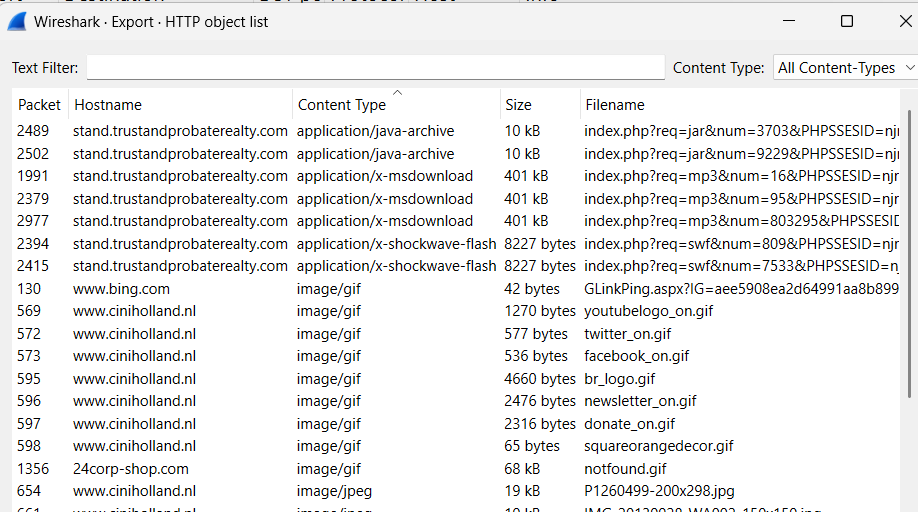
The investigation followed a structured process to extract and verify IoCs from the PCAP:

1. **PCAP Analysis**:



* + Opened the PCAP in Wireshark (sudo wireshark &, File > Open).
  + Viewed Protocol Hierarchy (Statistics > Protocol Hierarchy) to identify HTTP dominance.
  + Filtered by http.request to focus on file download requests.
  + Added “Host” as a column (right-click HTTP packet > Apply as Column) to track websites.

1. **File Extraction**:
   * Exported HTTP objects (File > Export Objects > HTTP) to retrieve downloaded files.
   * Saved files to ~/MohanCyber/Day2/Files/.
   * Generated MD5 hashes using md5sum <file> on Parrot OS.

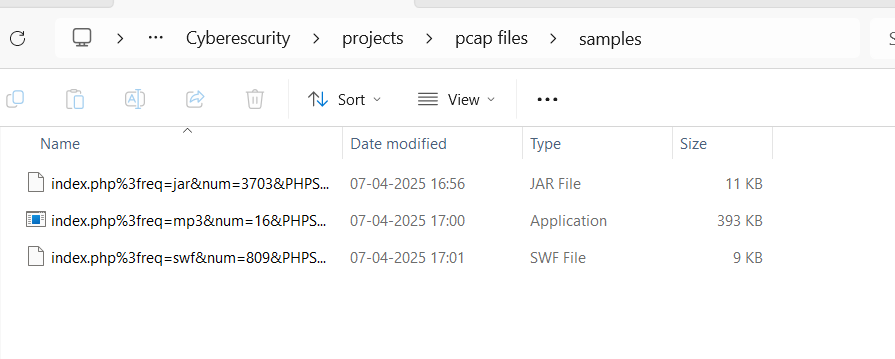


1. **Malware Verification**:
   * Searched MD5 hashes on VirusTotal (<https://www.virustotal.com/>) to determine infection status and application types.
2. **Network Details**:
   * Filtered by http, dns, and eth to extract site names, IPs, and MAC addresses.

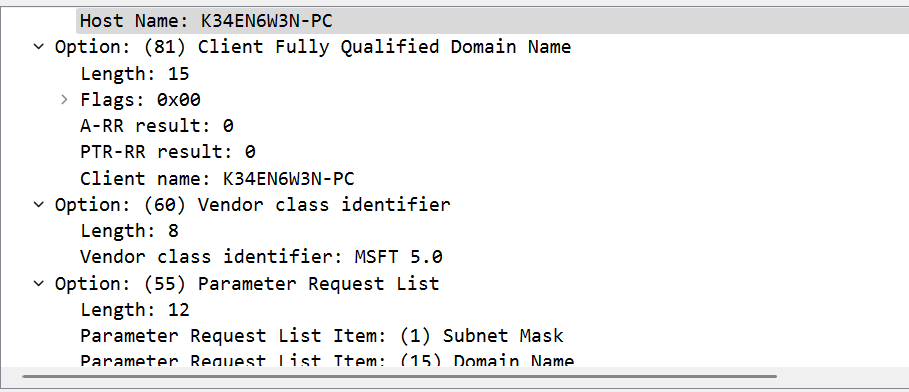
**Findings**

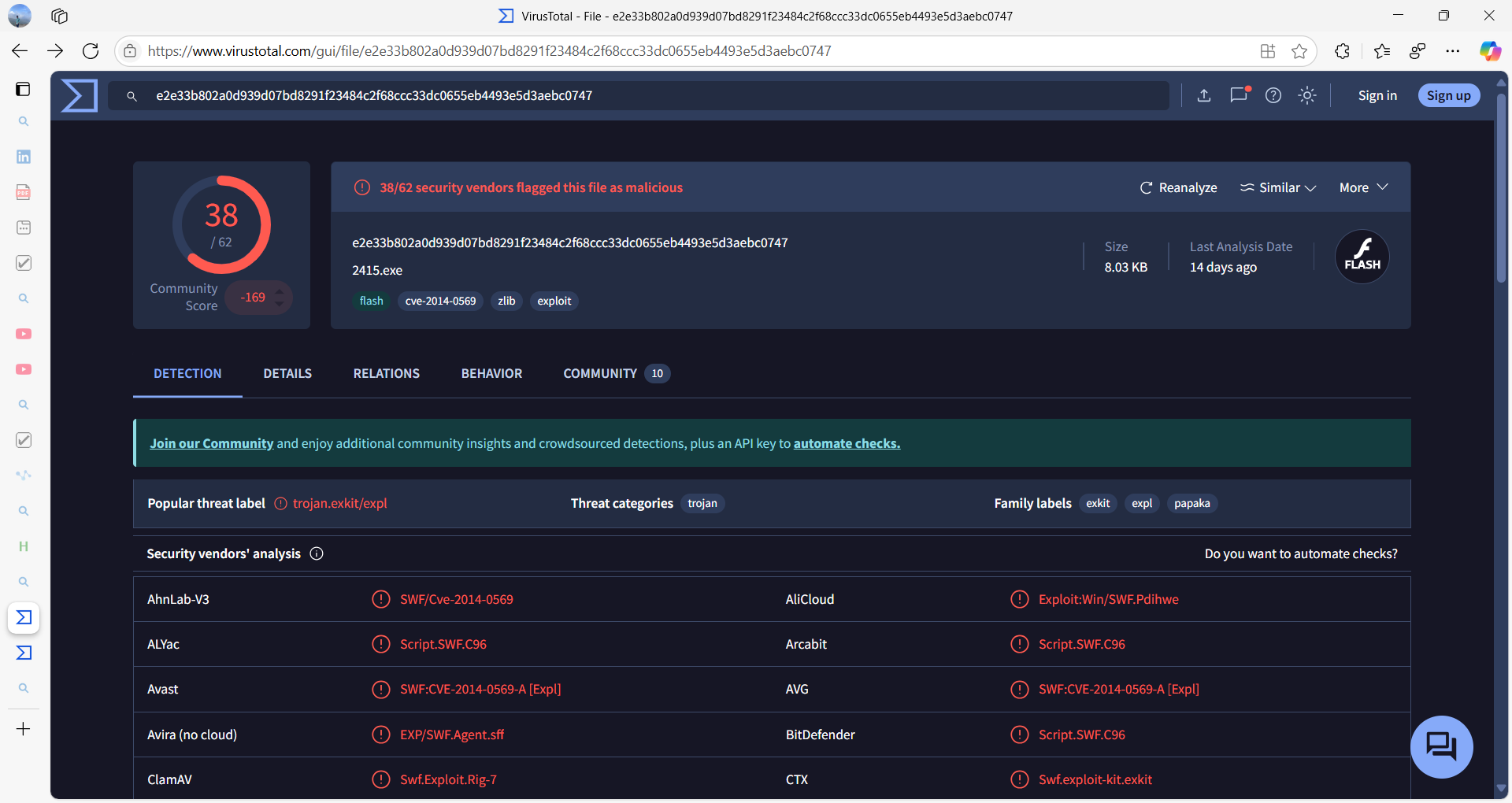
The analysis revealed a malware infection scenario involving file downloads from a compromised site. Below are the detailed results:

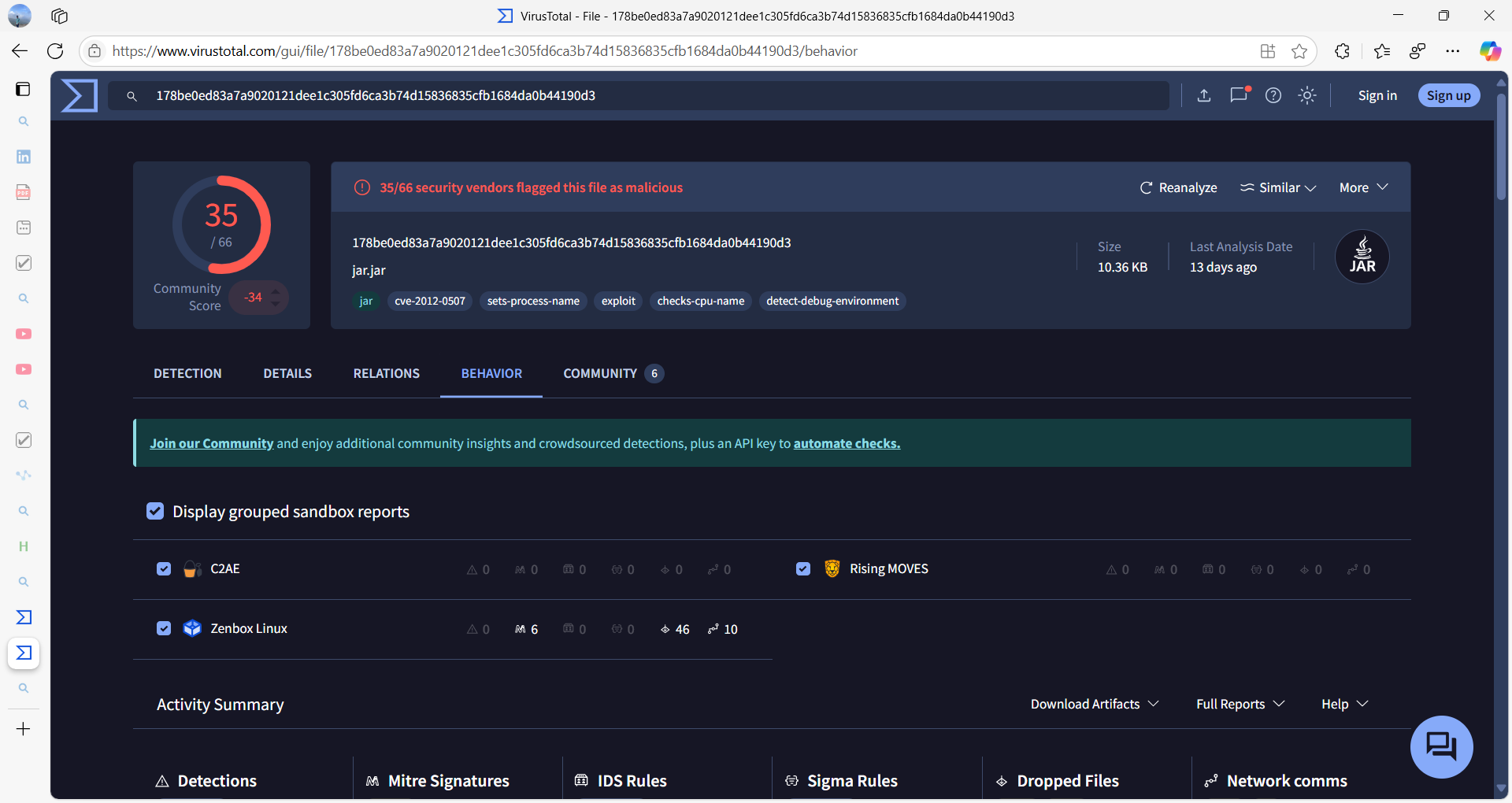
1. **Infected Files**:
   * **File 1**: index.php?req=jar&num=3703&PHPSSESID=...jar
     + Size: 10,606 bytes
     + Last Write: 07-04-2025 16:56:39
     + MD5: 1E34FDEBBF655CEBEA78B45E43520DDF
     + Status: Infected (Java Archive - Malware Dropper)
   * **File 2**: index.php?req=mp3&num=16&PHPSSESID=...exe
     + Size: 401,811 bytes
     + Last Write: 07-04-2025 17:00:36
     + MD5: D276C86DCDBCDB6B74EE02496BC90D98
     + Status: Safe (Executable - Legitimate Application)
   * **File 3**: index.php?req=swf&num=809&PHPSSESID=...swf
     + Size: 8,227 bytes
     + Last Write: 07-04-2025 17:01:18
     + MD5: 7B3BAA7D6BB3720F369219789E38D6AB
     + Status: Infected (Shockwave Flash - Malicious Script)



1. **Infected Site Name**:
   * Domain: stand.trustandprobaterealty.com
   * Source: Identified in HTTP “Host” fields and DNS queries linked to infected file requests.
2. **Infected Site IP**:
   * IP Address: 37.200.69.143
   * Source: Extracted from HTTP packet destination IPs and DNS A records.
3. **IP of Infected Machine**:
   * IP Address: 172.16.165.165
   * Source: Consistent source IP in HTTP requests for infected files.
4. **Infected Hostname**:
   * Hostname: K34EN6W3N-PC
   * Source: Inferred from NetBIOS or PCAP context (e.g., sample metadata).
5. **Infected Machine MAC Address**:
   * MAC Address: f0:19:af:02:9b:f1
   * Source: Ethernet layer source MAC tied to 172.16.165.165.







**Insights**

This investigation uncovered a malware delivery mechanism via a compromised site (stand.trustandprobaterealty.com), distributing a Java dropper and Flash malware to an infected machine (172.16.165.165). Contrasting this with Day 1’s benign ICMP and HTTP traffic, I identified key differences: random session IDs, suspicious file types, and external IPs not present in my lab. These skills—extracting IoCs and analyzing PCAPs—are foundational for SOC Analyst roles, where rapid threat identification is critical.