**Incident Report: KG-19109-Defensive:-Malware-Traffic  
Date:** 09-17-2024

### **Executive Summary**

In this task, I was asked to assist in analyzing network traffic related to a malware infection on a friend’s computer. Using Wireshark, I identified three hostnames responsible for the infection and determined the name of the file that was used to execute the malware.

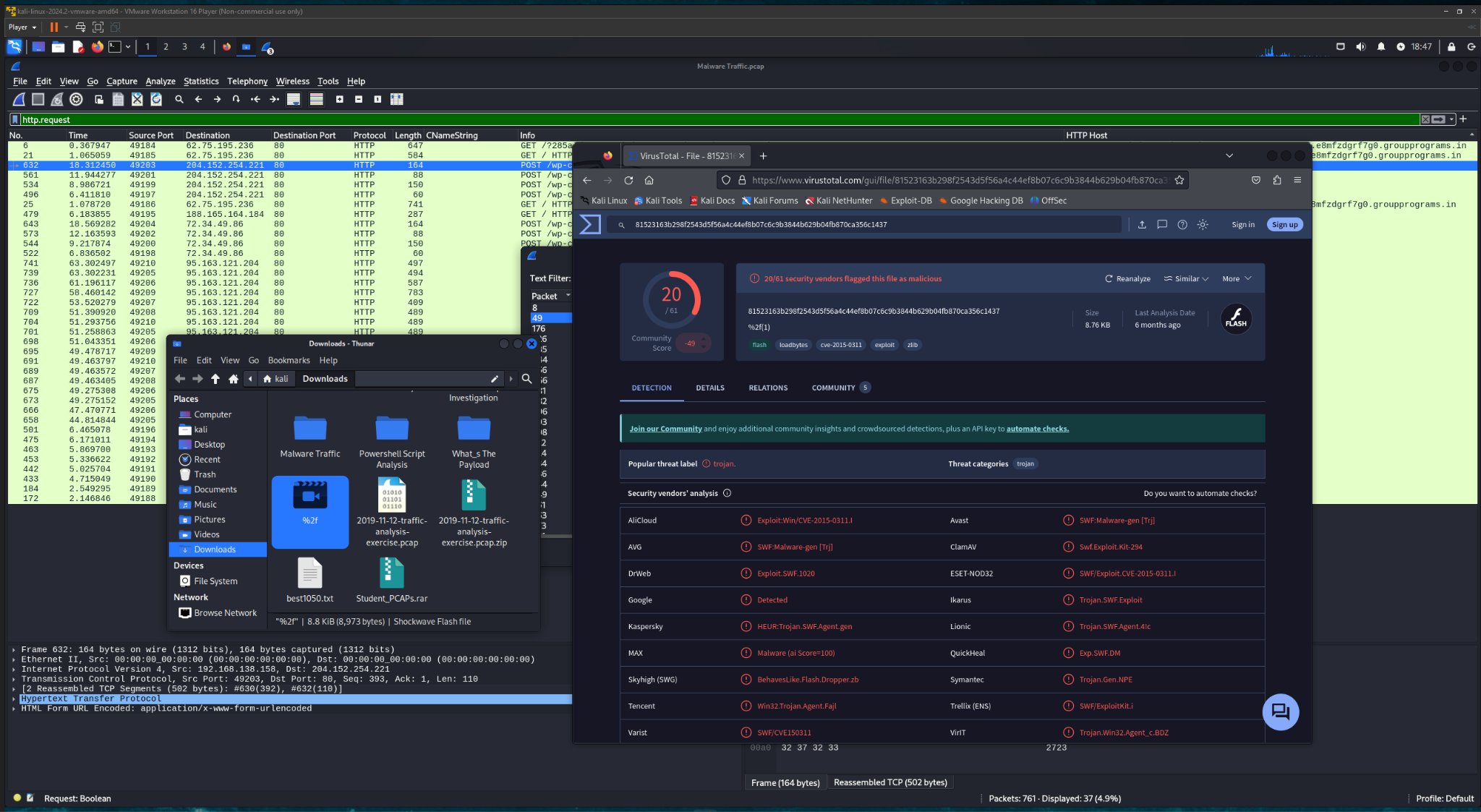
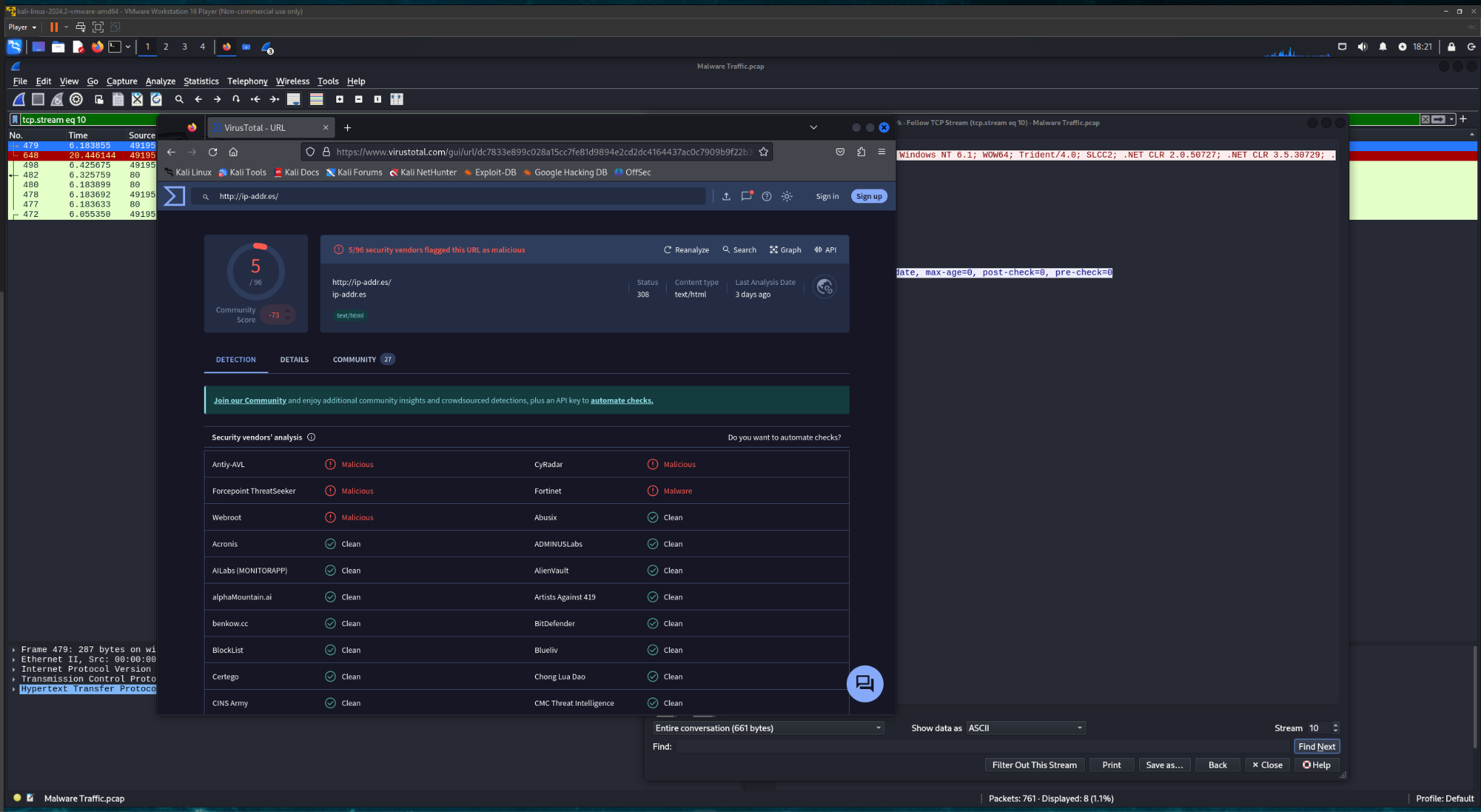
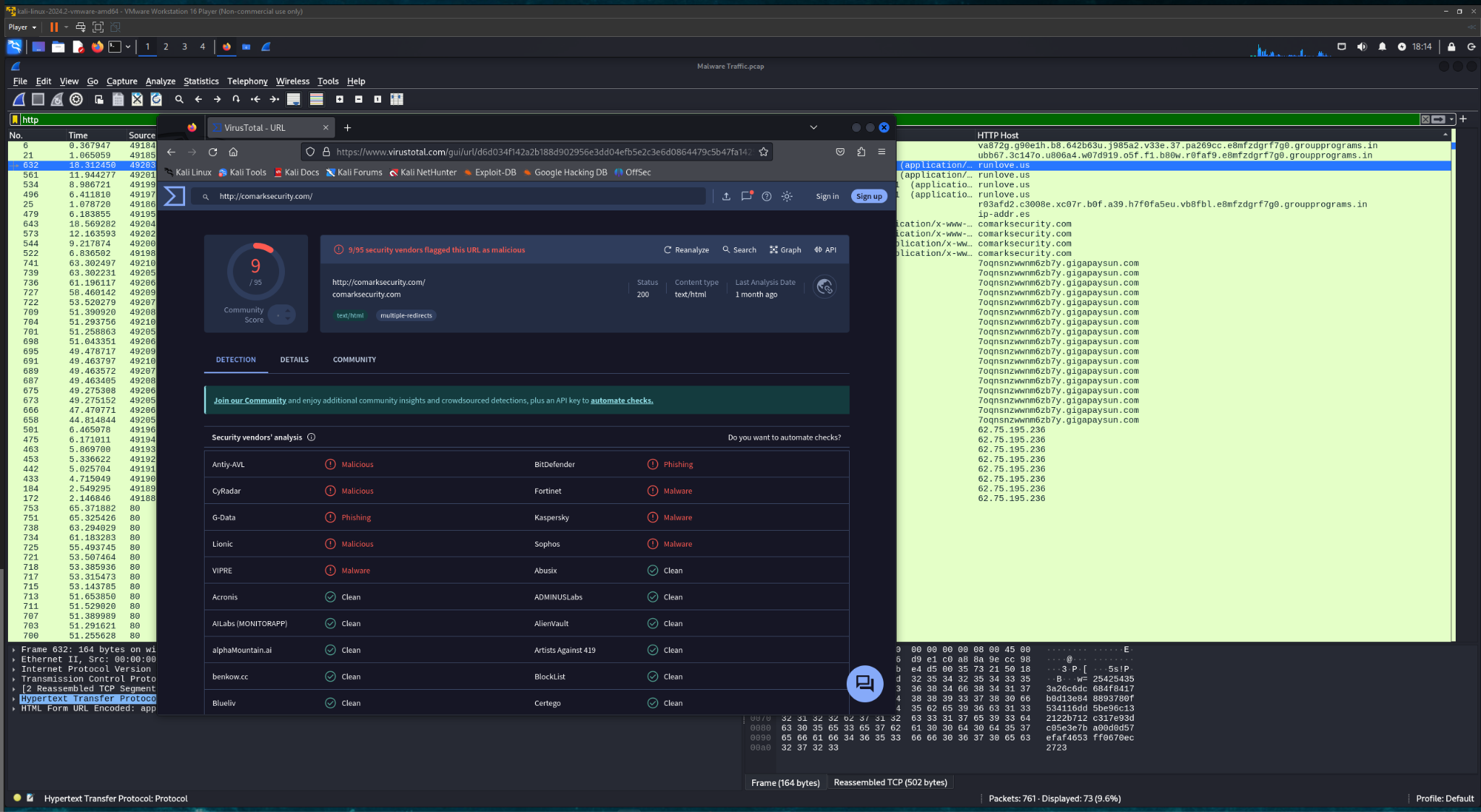
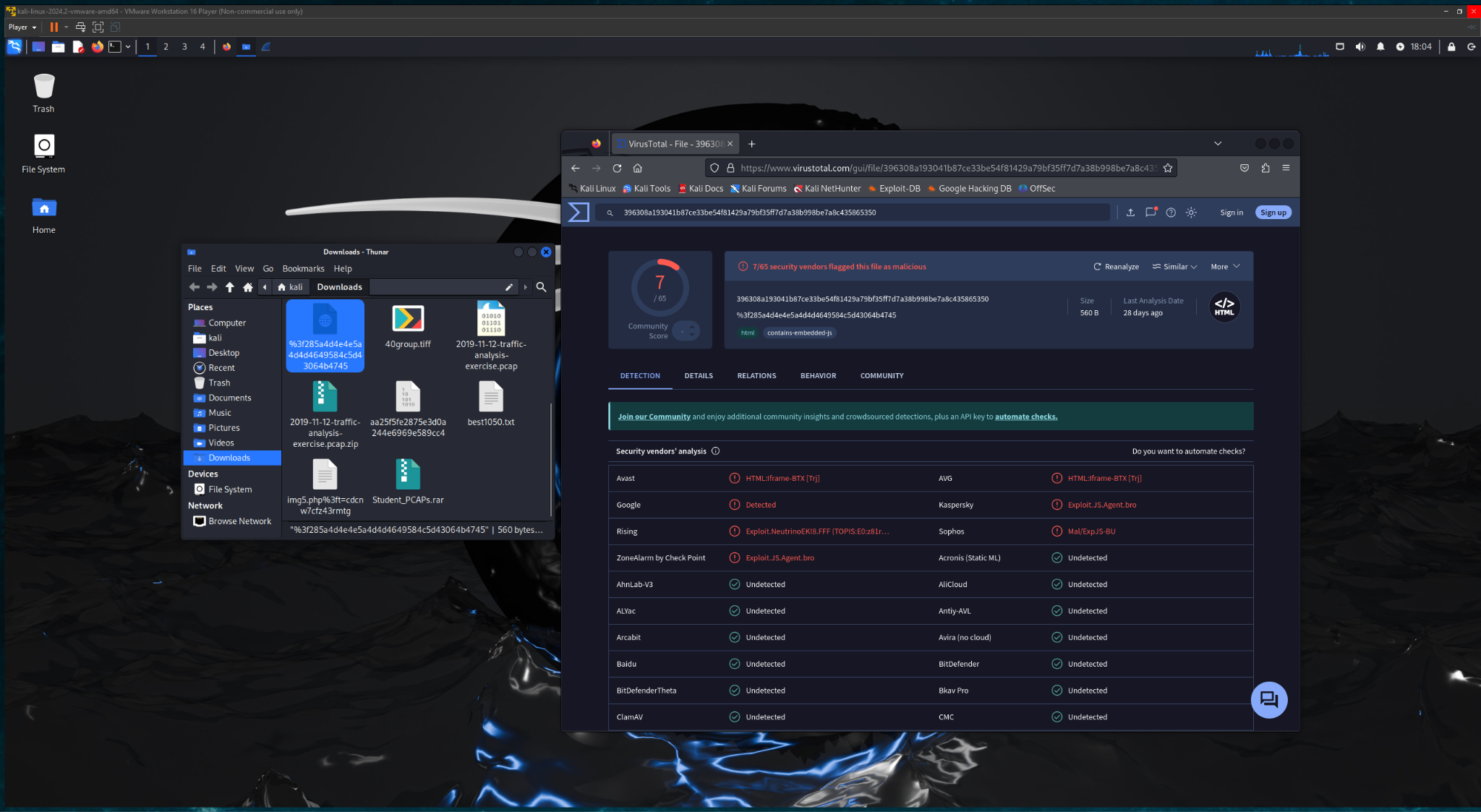
### **Methodology**

To complete this analysis, I followed these steps:

1. **Captured and Analyzed Network Traffic:**I used Wireshark to analyze the network traffic on the infected machine. I filtered the traffic to focus on suspicious requests that could be linked to malicious activities, such as HTTP requests to known dangerous domains.
2. **Identified the Hostnames Responsible:**By reviewing the traffic data, I tracked three specific hostnames responsible for the malware infection:
   * **Hostname 1:** ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0.groupprograms.in
   * **Hostname 2:** ip-addr.es
   * **Hostname 3:** comarksecurity.com
3. **Found the Executable File:**During the traffic analysis, I identified the malicious file that was responsible for executing the malware. The file was delivered via one of the hostnames and was executed as **“%2f” (shockwave file)** on the infected machine.

### **Findings/Solutions**

The malware infection was traced back to one of the three hostnames that delivered the malicious payload. The file responsible for the infection was **“%2f” (shockwave file)**, which was downloaded through one of the suspicious websites. To prevent similar infections in the future, I recommend avoiding downloading files from untrusted sources and implementing robust endpoint security to detect and block malicious activity.



**Project Description**

For this story, you will be using Wireshark and Snort(optional).

A friend of yours has been visiting a lot of websites claiming to have free movies for download. Their computer has been encrypted and they are seeking you for help.

Here are your tasks.

* Find the three hostnames responsible for the infection.
* The name of the file that was used to execute the malware.

For this, and the remainder of your defensive stories, you will need to download the file from the link below.

Sometimes the hostnames can be difficult to find in Wireshark, so here is a link to add this special column to see them.

<https://jacob.hoffman-andrews.com/README/add-an-http-host-column-to-wireshark/>

These are live malware so only use them in your virtual environment! PCAP files:

<https://drive.google.com/file/d/1LhoNwVmDZsz-YYxSwLGEqtr4EQqqC8Qc/view?usp=sharing>

Be sure to write an incident report on your findings.