**LAB 1: Public AV Scanner and Sandbox**

**Course Name**: Malware Analysis and Reverse Engineering (IAM302)

**Student Name**: Nguyễn Trần Vinh – SE160258

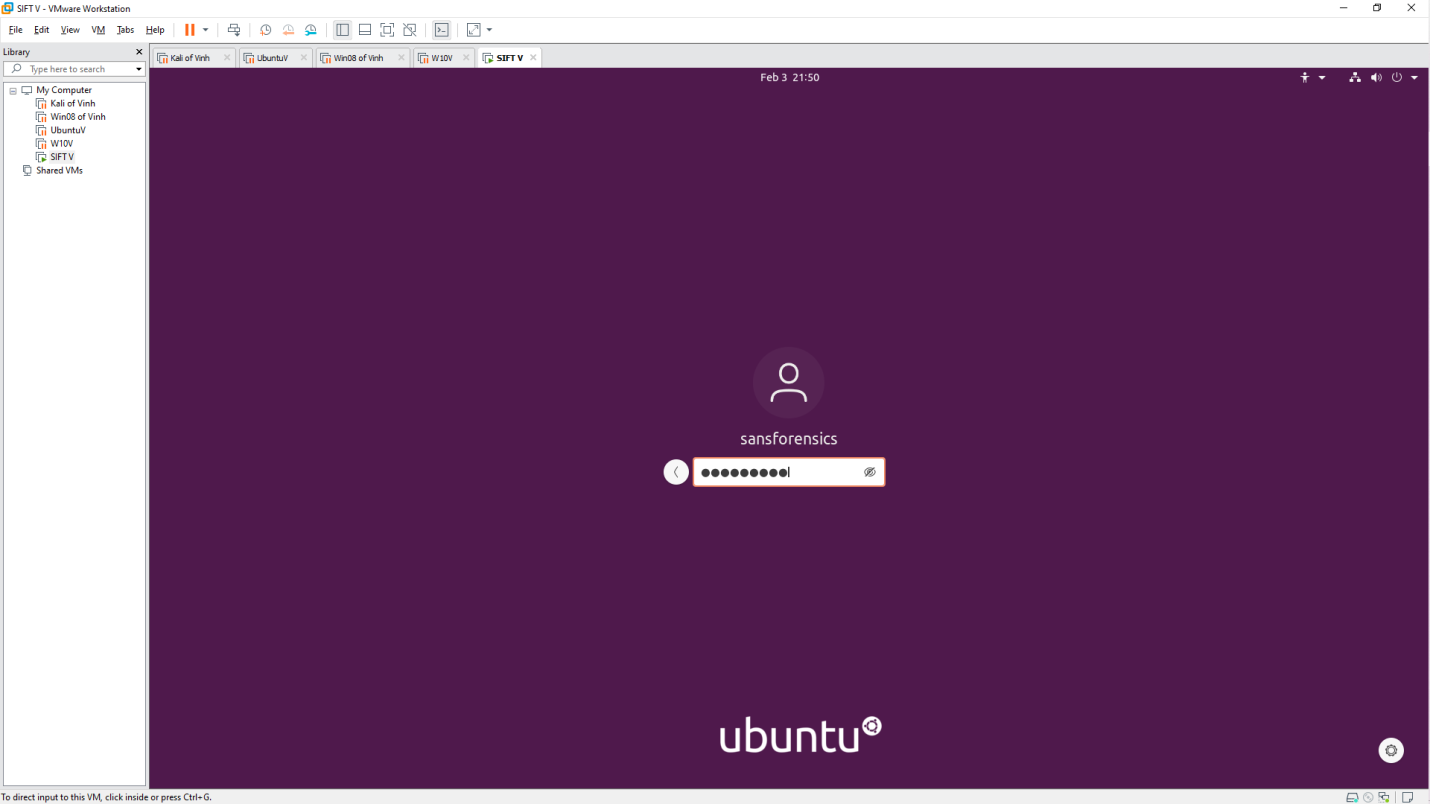
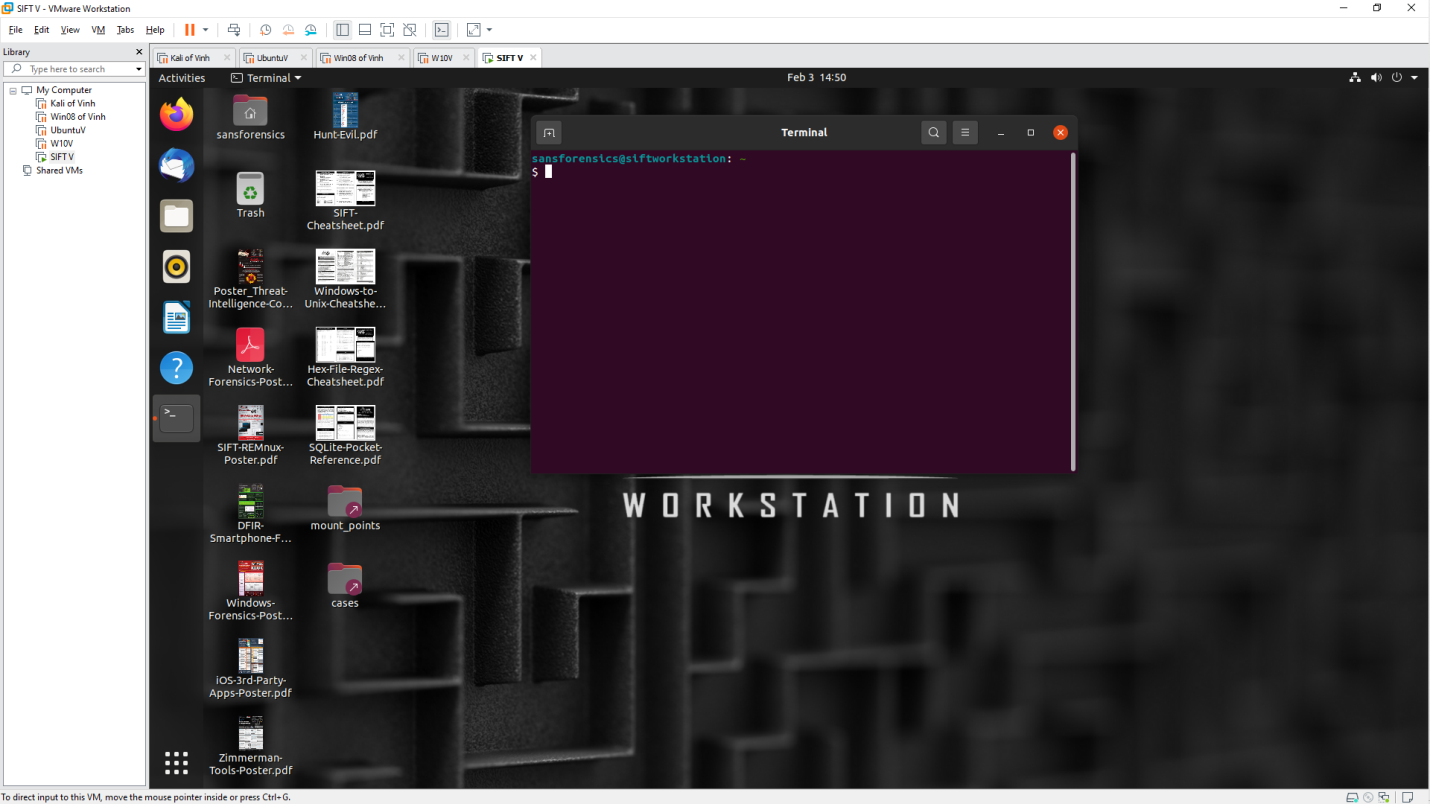
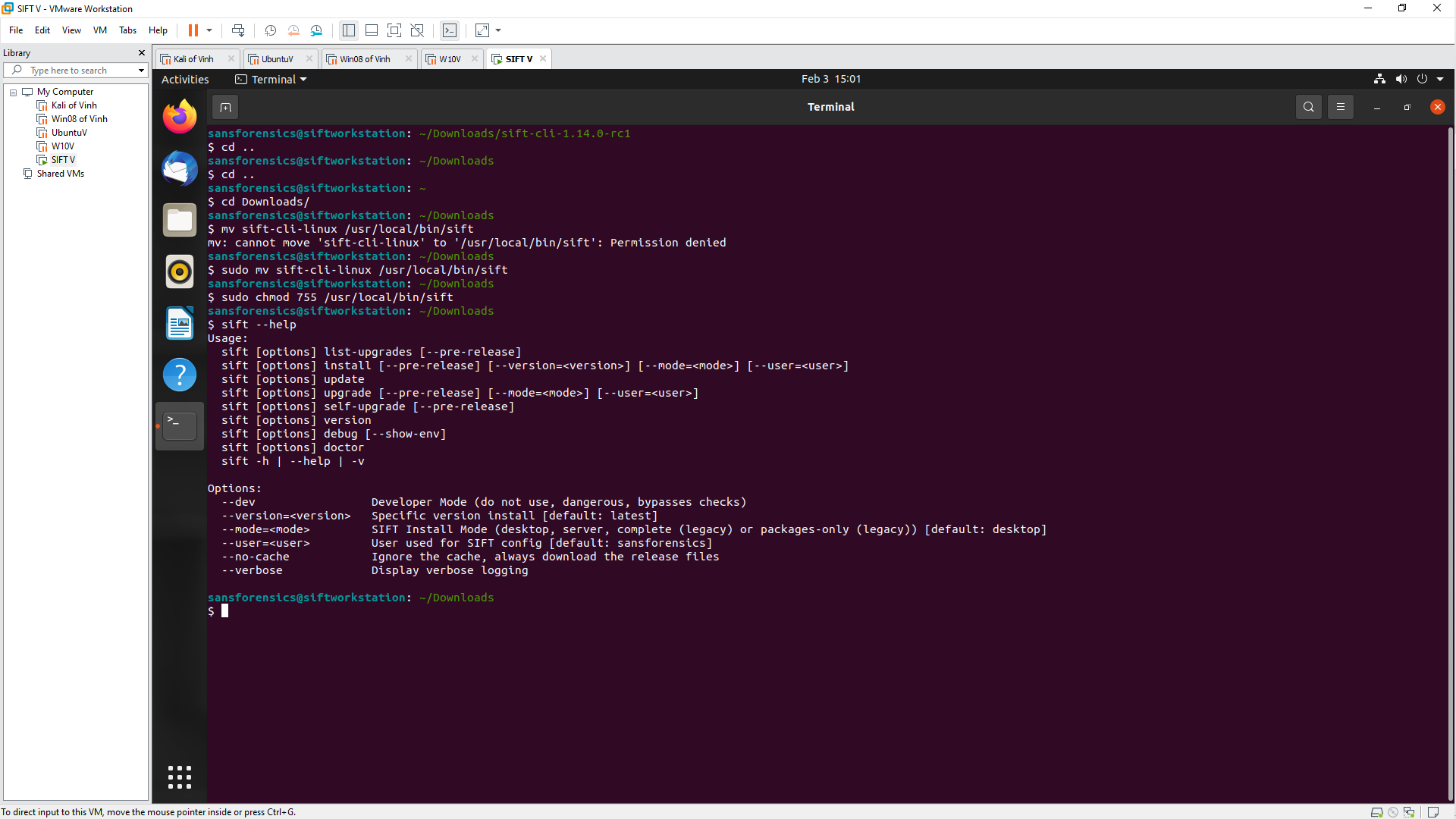
**Instructor Name**: Mai Hoàng Đỉnh

**Lab Due Date**: 4/2/2023

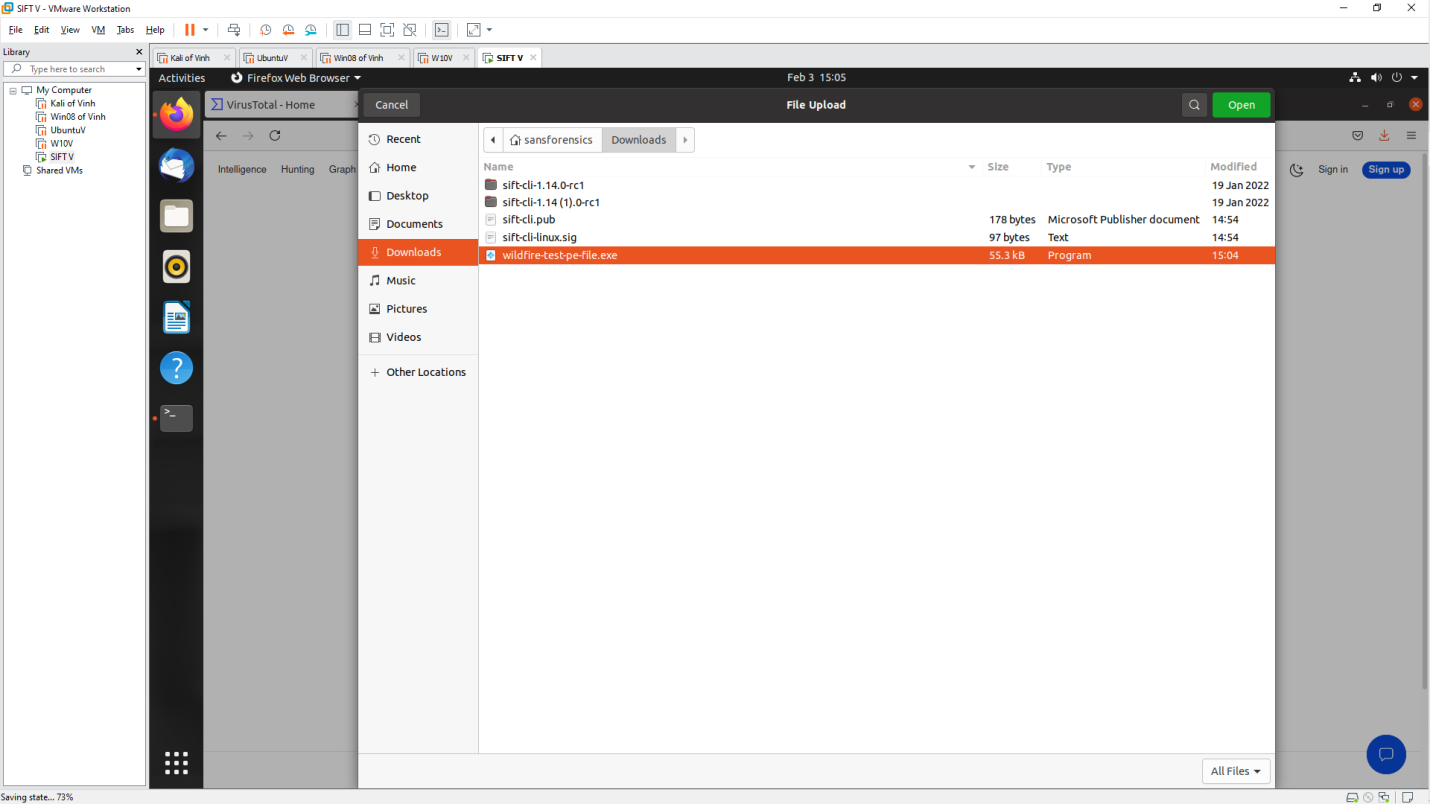
**Purpose**

Setup Sandbox, install SIFT Workstation, use tools to scan malware

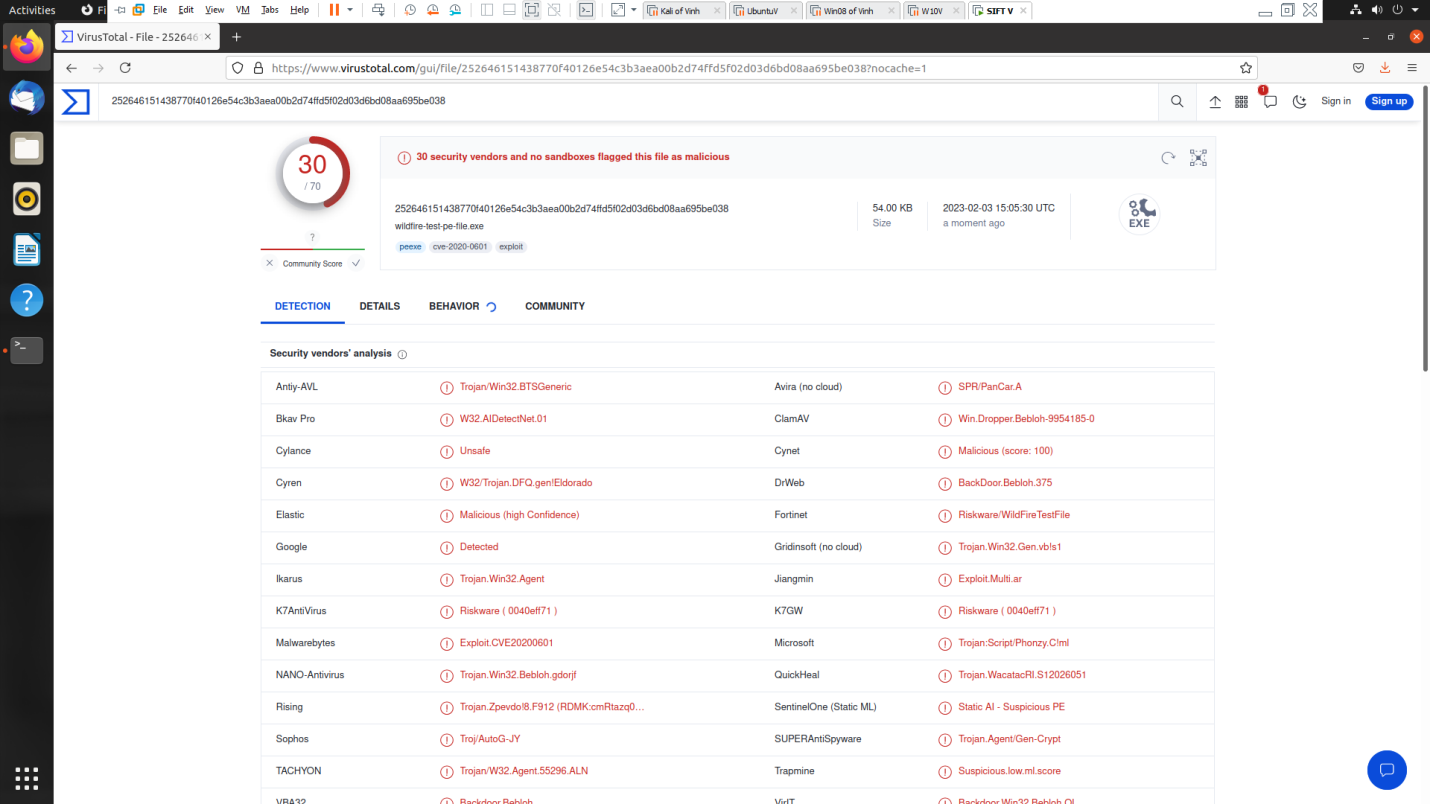
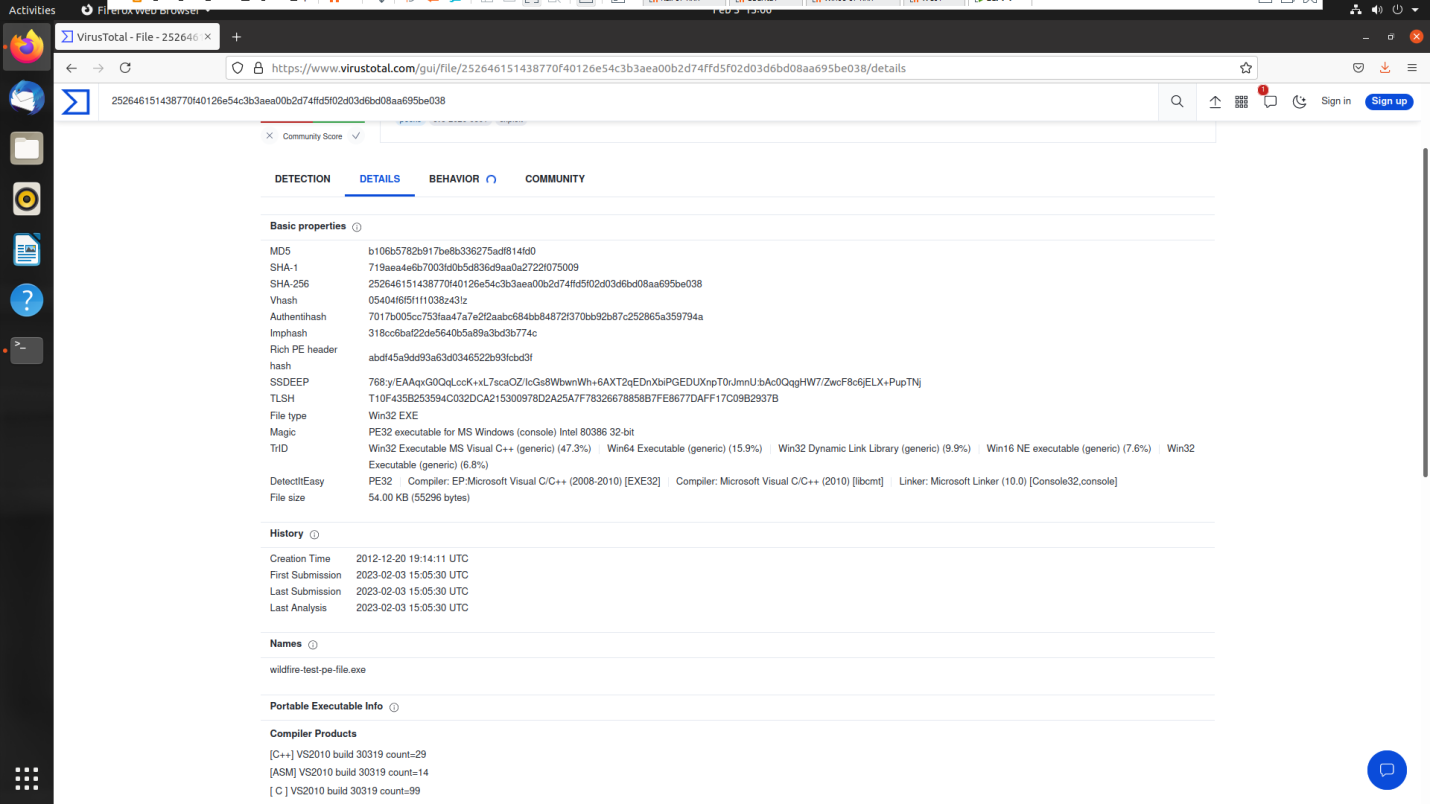
**Install SIFT**

**  **

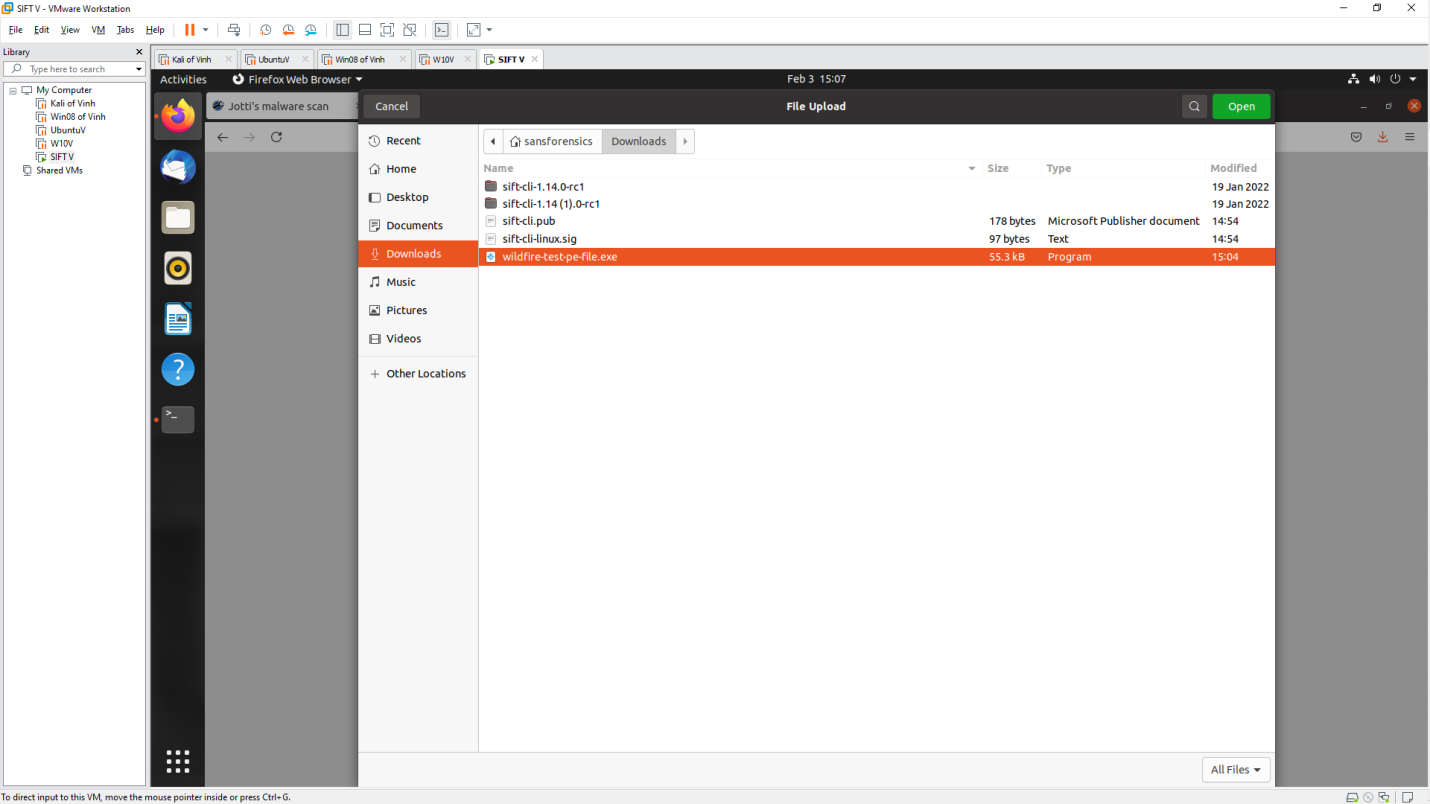
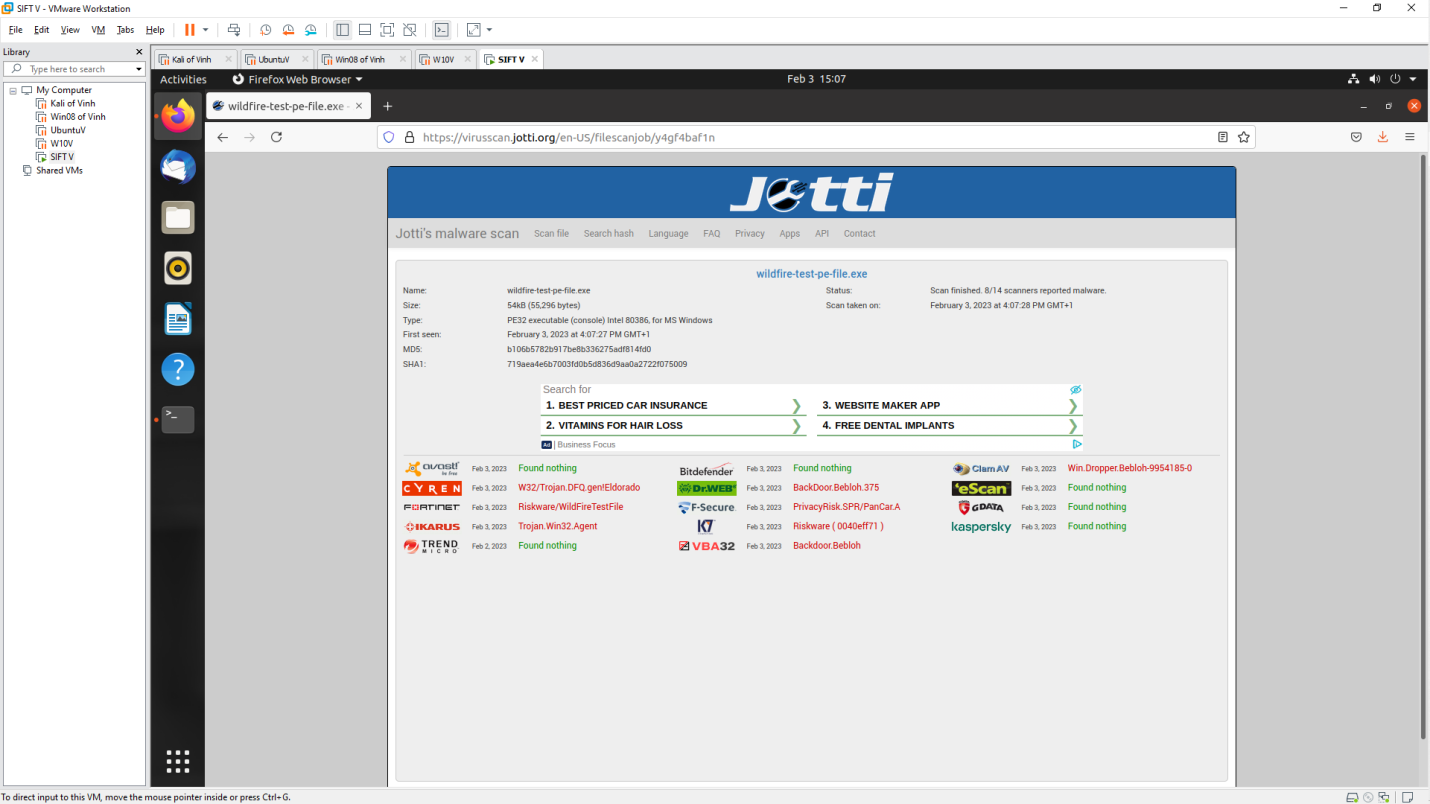
**Download a sample malware**

****

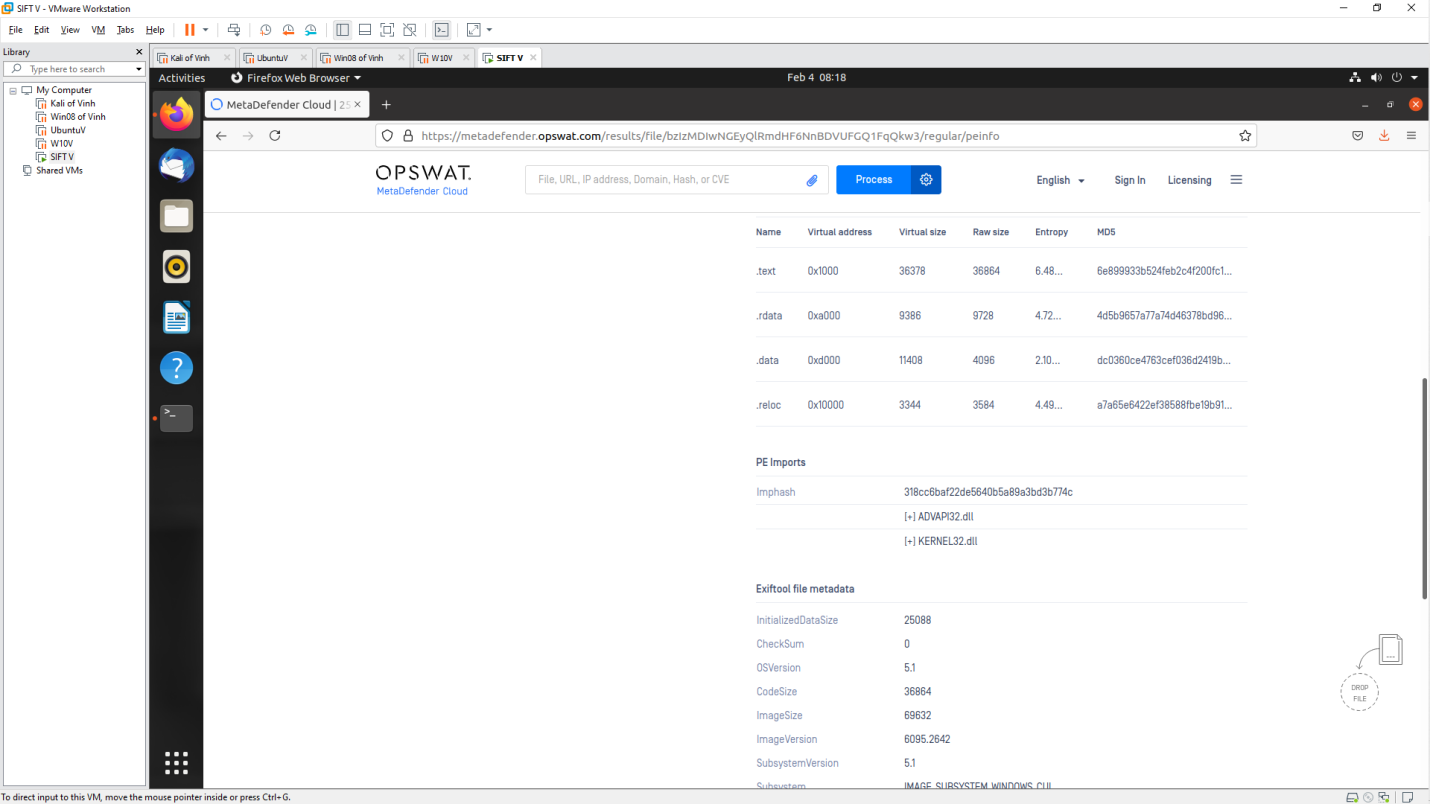
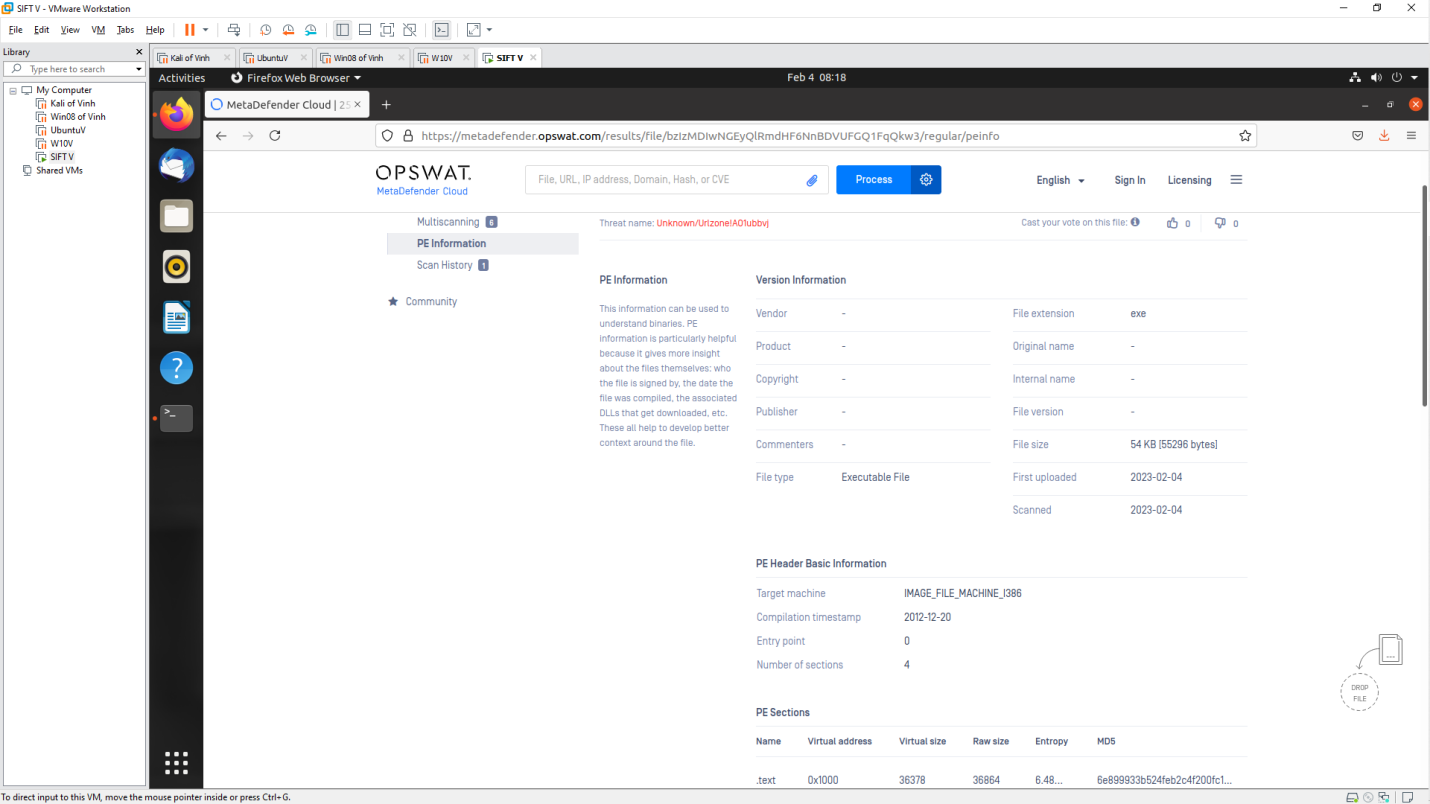
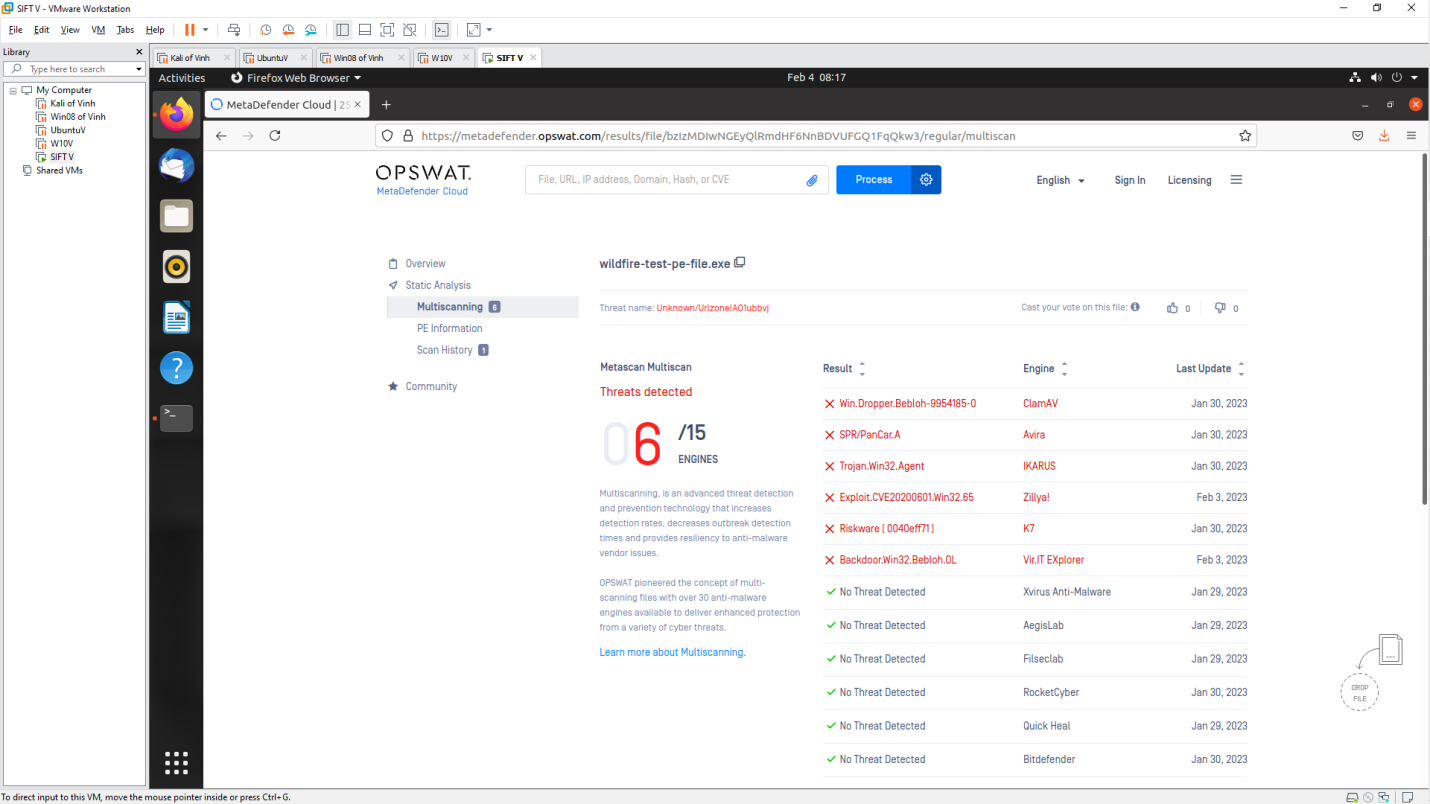
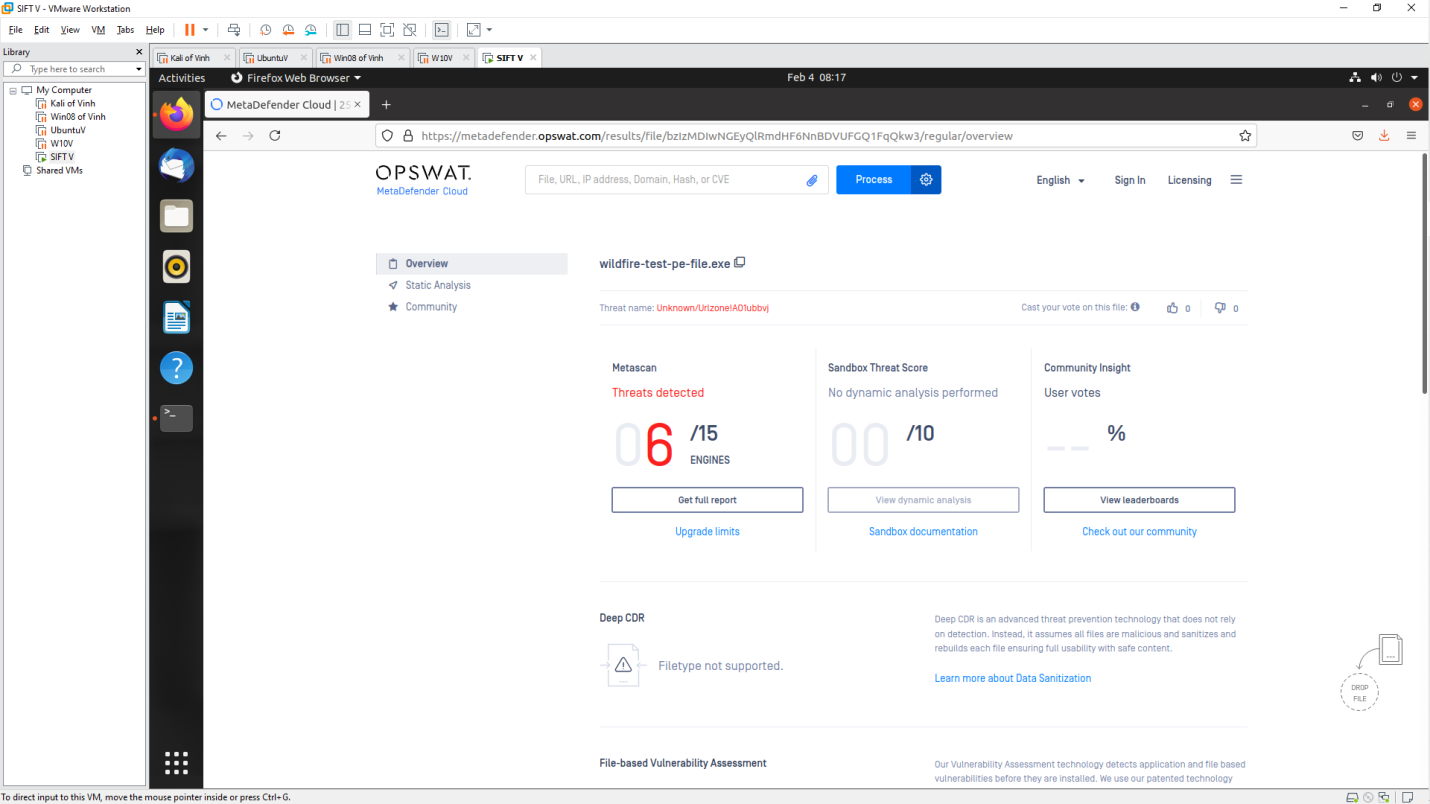
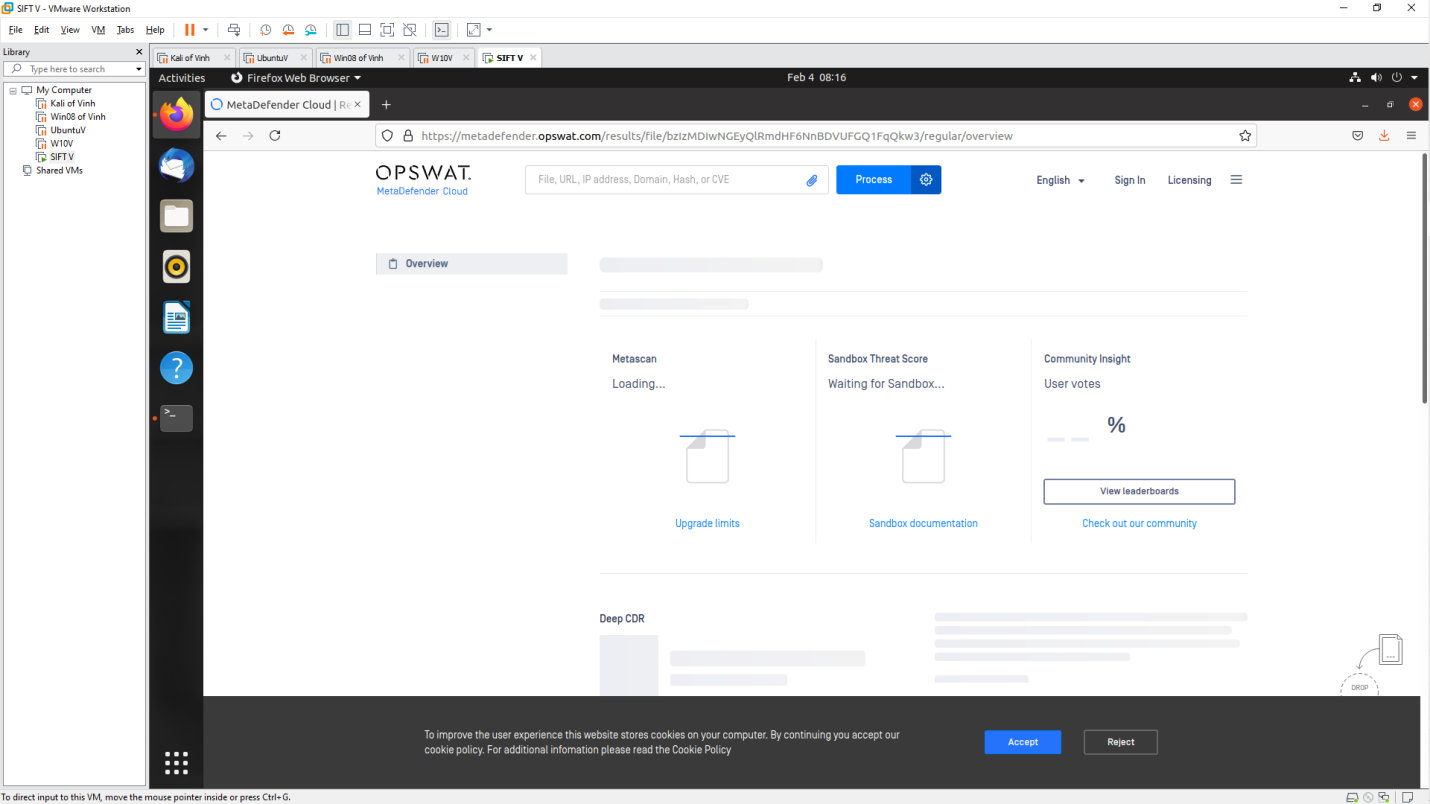
**Upload to virustotal**

** **

**Upload Jotti**

** **

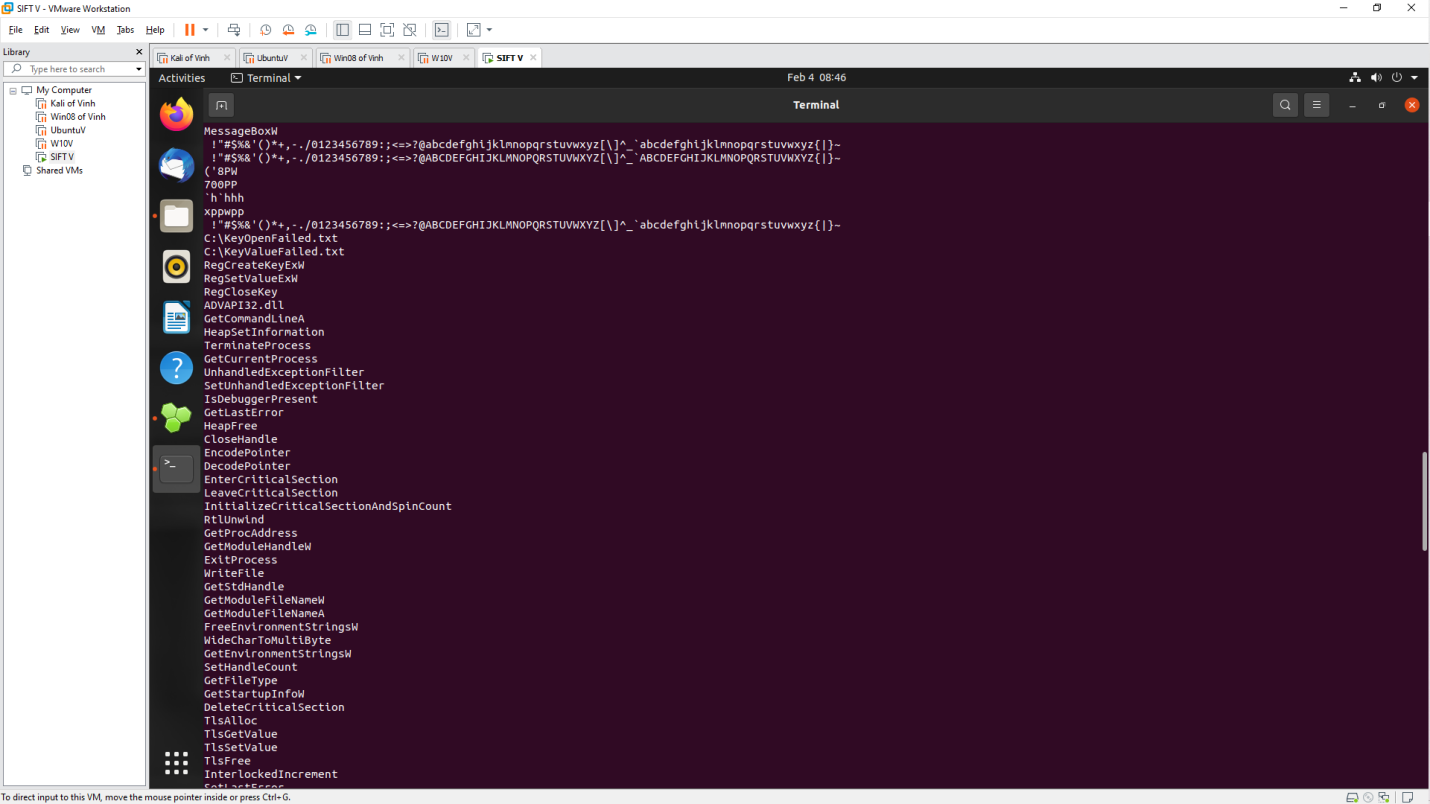
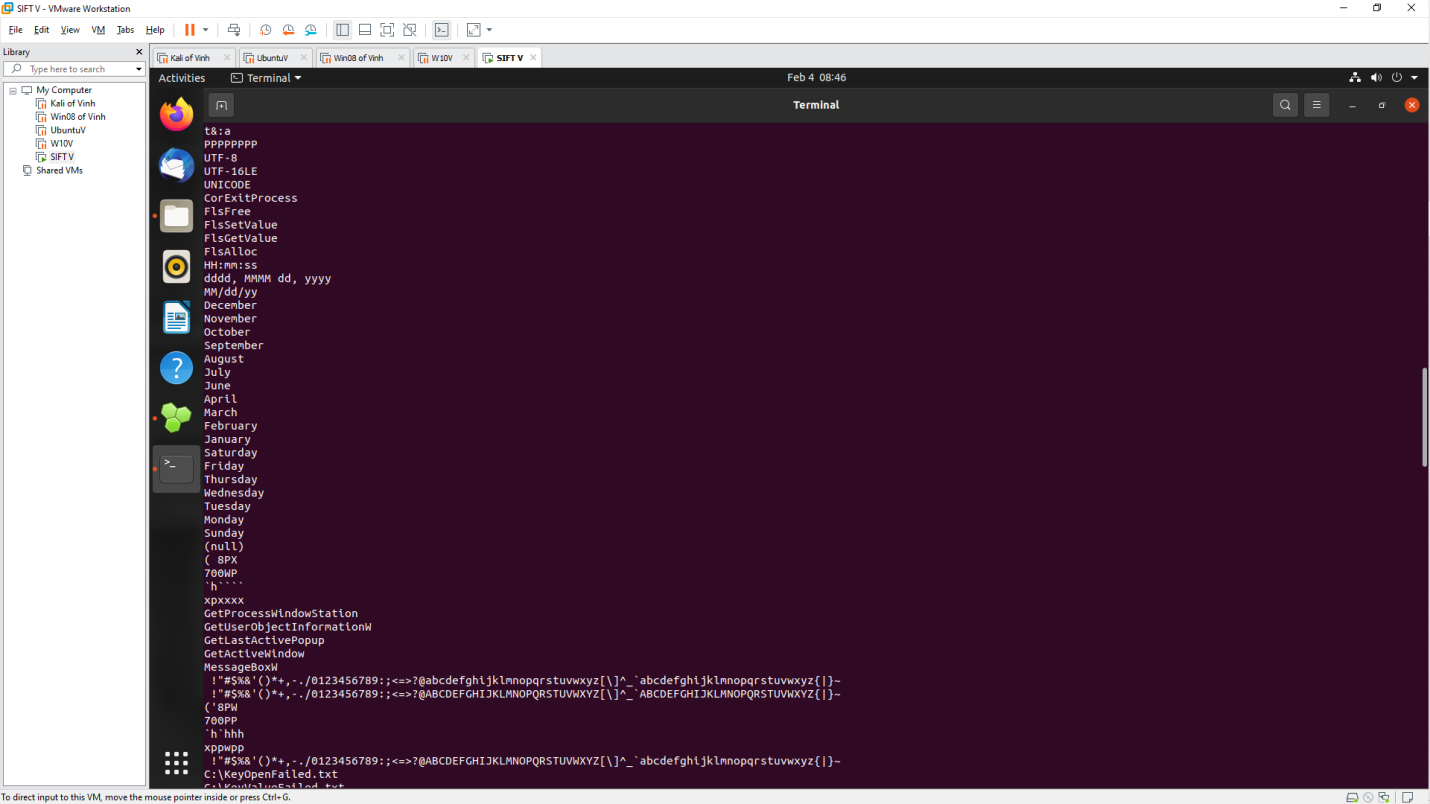
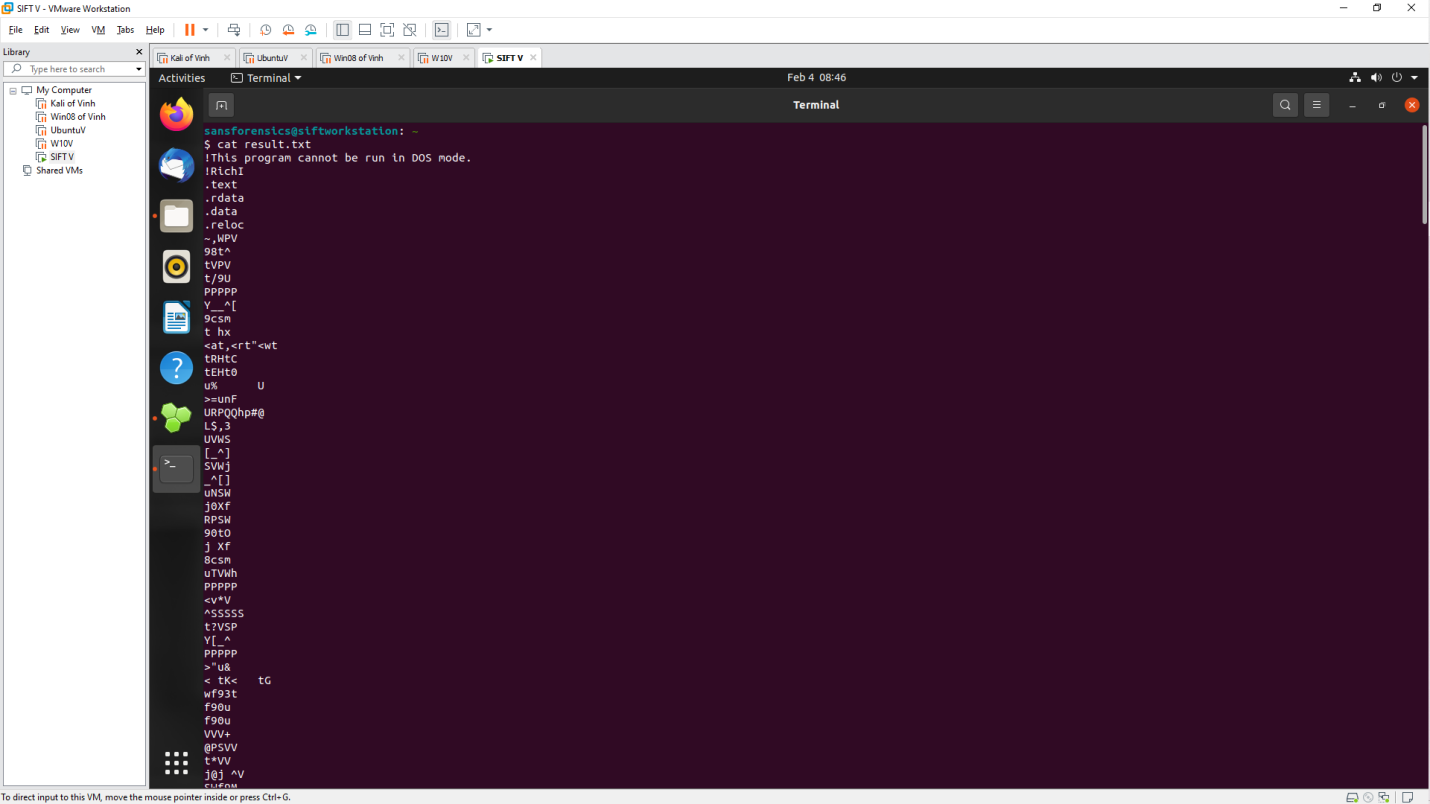
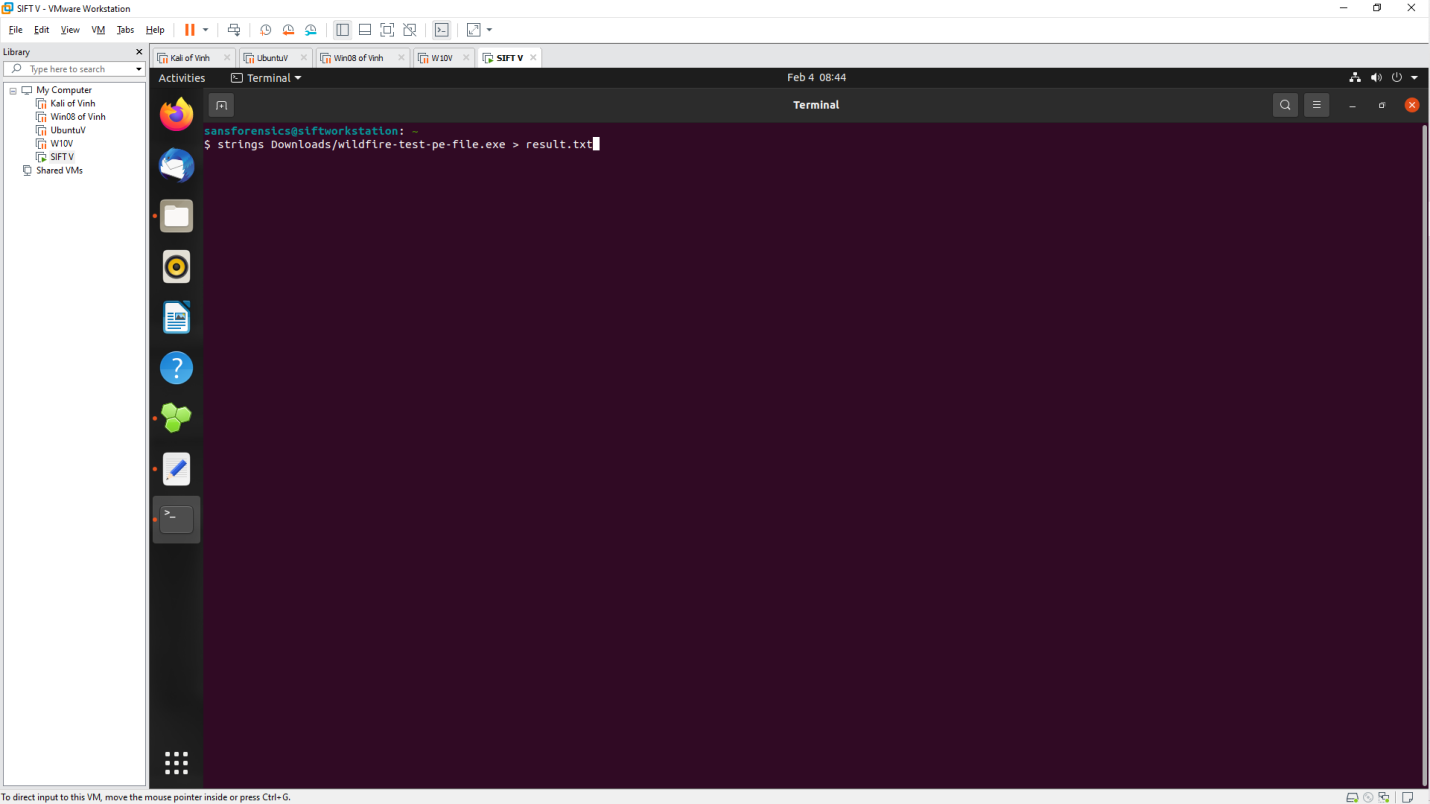
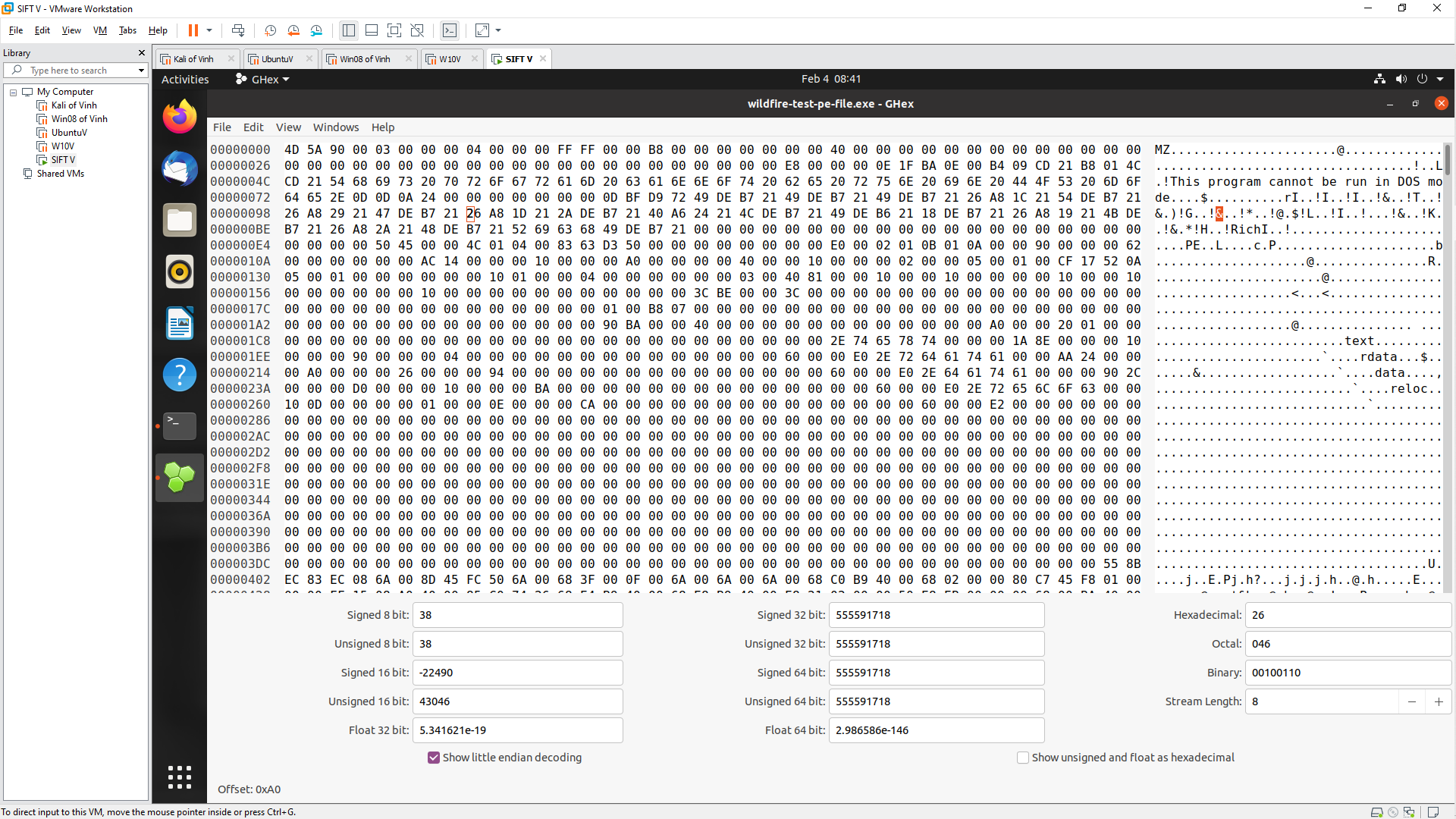
**MetaDefender**

****

**Conclusion**

- Virustotal is the website used to scan Malware most effectively when it gives the most results, history of malware. Meanwhile, Jotti gives more results than MetaDefender but the specific information of MetaDefender is clearer than Jotti

**Use tools on SIFT Workstation**

****