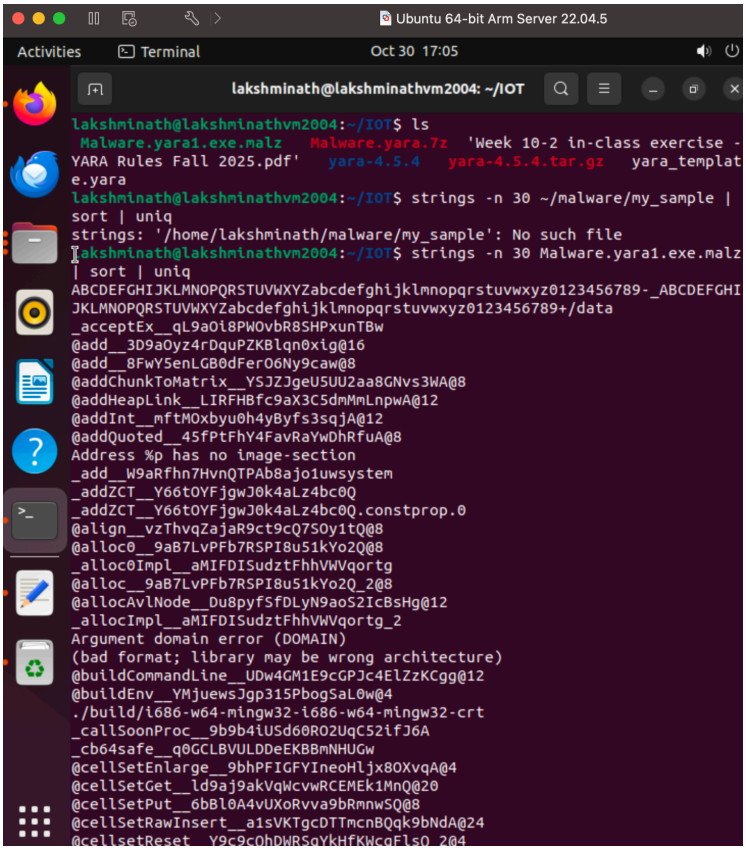
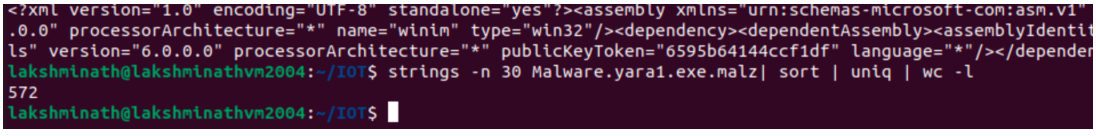
IOT Inclass Exercise Week10_2 YARA
Lakshminath Reddy Alamuru
SUID: 367982169

Task-1

Extracted the strings from malware sample file given in the task.
I showed the strings which are at least 30 characters.



The total number of strings are 572 with length greater than 30 in this case.



Task-2
For the task-2, I have created a myrule1.yar file with two extracted string from the task-1

```
rule myrule1 {
    meta:
        description = "Detect malware strings from sample Malware.yara1.exe.malz"
        author      = "Lakshminath Alamuru"
        date        = "10-30-2025"
        hash1       = "e128283461b14224459e966abf317c070d50aae7a531d64"

    strings:
        // Example unique strings extracted from your malware sample
        $s1 = "_acceptEx__qL9aOi8PWOvbR8SHPxunTBw" ascii
        $s2 = "@add__3D9aOyz4rDquPZKBlqn0xig@16" ascii
        $mz  = {4D 5A}    // MZ magic number for PE files

    condition:
        // Check if at least 2 of the defined strings are present
        (uint16(0) == 0x5A4D) and       // MZ at offset 0 (little-endian)
        (#s1 + #s2 >= 2)                // at least 2 of the defined strings
}
```

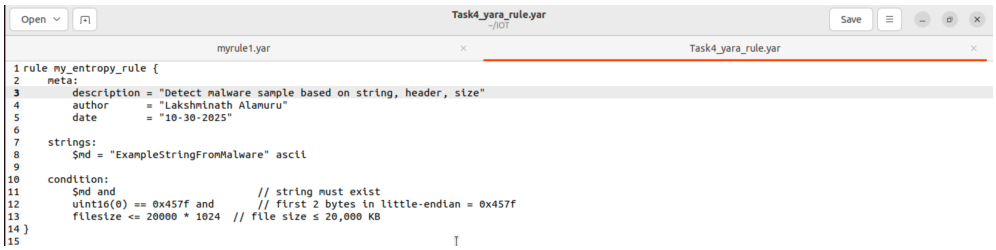
Task-3
Test the yara rule against the malware file that has given in exercise

```
rule myrule1 {
    meta:
        description = "Detect malware strings from sample Malware.yara1.exe.malz"
        author      = "Lakshminath Alamuru"
        date        = "10-30-2025"
        hash1       = "e128283461b14224459e966abf317c070d50aae7a531d64"

    strings:
        // Example unique strings extracted from your malware sample
        $s1 = "_acceptEx__qL9aOi8PWOvbR8SHPxunTBw" ascii
        $s2 = "@add__3D9aOyz4rDquPZKBlqn0xig@16" ascii
        $mz  = {4D 5A}    // MZ magic number for PE files

    condition:
        $mz at 0 and (#s1 + #s2 >= 2) // at least 2 of the defined strings and $mz at 0
}
```

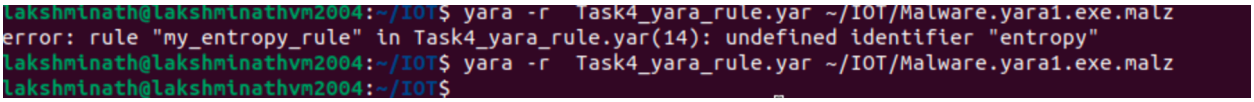
```
lakshminath@lakshminathvm2004:~/IOT$ yara myrule1.yar ~/IOT/Malware.yara1.exe.malz
error: rule "myrule1" in myrule1.yar(18): unreferenced string "$mz"
lakshminath@lakshminathvm2004:~/IOT$ yara myrule1.yar ~/IOT/Malware.yara1.exe.malz
myrule1 /home/lakshminath/IOT/Malware.yara1.exe.malz
lakshminath@lakshminathvm2004:~/IOT$
```

myrule1.yar file is has run against malware file successfully here. It seems no condition strings are found here.

Task-4



Run the Task4_yara_rule.yar file again malware file didn't get any output. Seems the conditions are not met.



Observations:

I got to know how to write war file and can check for the conditions met for string matching and file size checking as well. At least in the conditions that I have taken, those are not met. But it is successful learning for me about yara rules in detail.