# Assignment for malware analysis

## Executive Summary

With the development of the Internet and the growth of the computer number, ransomware has become very popular in the Internet. Ransomware is a trojan, which makes users' data assets or computing resources cannot be used normally by harassing, intimidating or even kidnapping users' files, and extorts money from users on this condition. Such user data assets include documents, mails, databases, source code, pictures, compressed files and other files. The ransom form includes real currency, bitcoin or other virtual currencies, which cost a lot of damage.

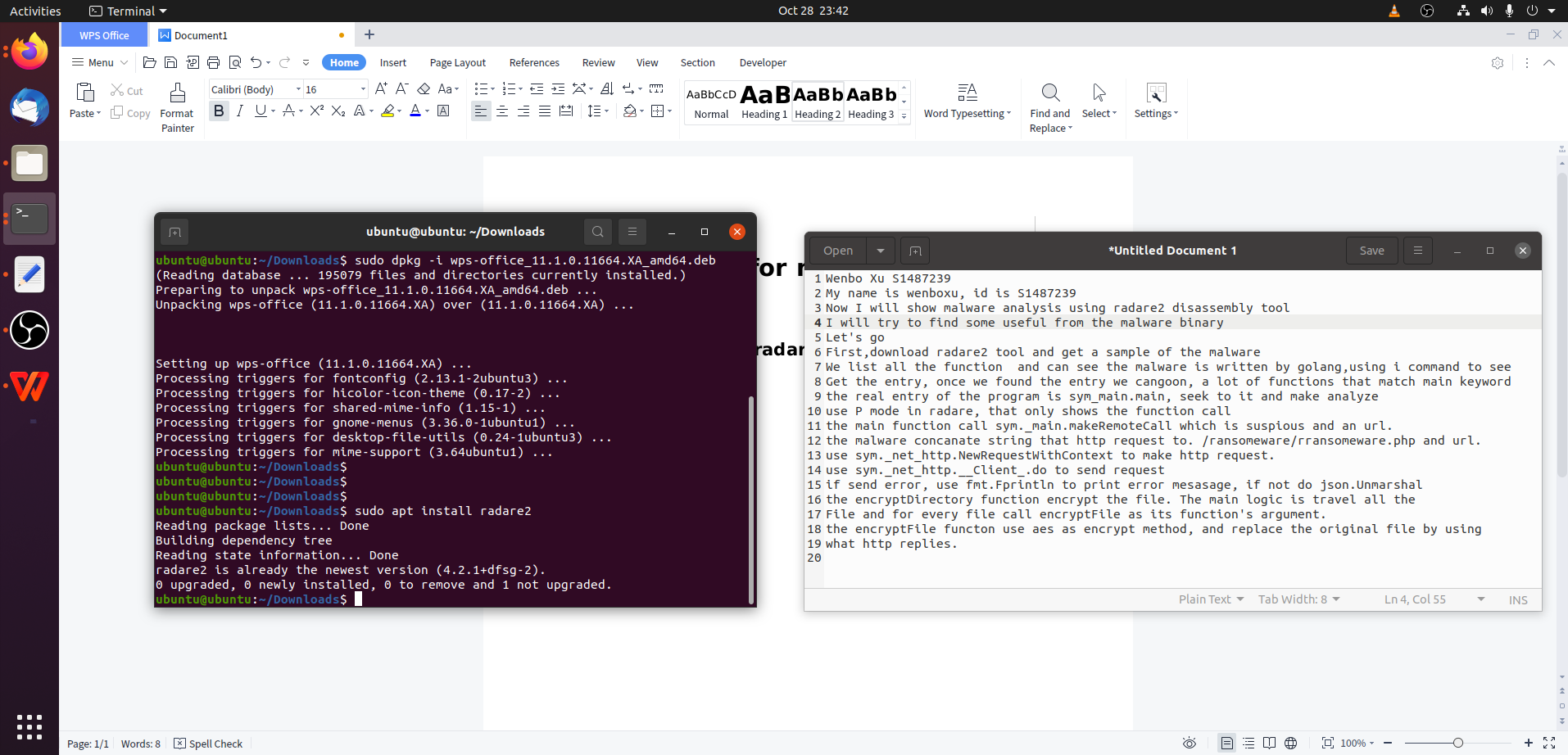
Radare is the very popular tool for the binary analysis. It is open source comparing to the expensive IDA pro, radare2 is totally free we can read code and even modify code from github.

## Introductions

In this homework I will analysis the malware that written by go by using radare2 tools. I will give a brief discovery of the binary file and do some reversing engineering.

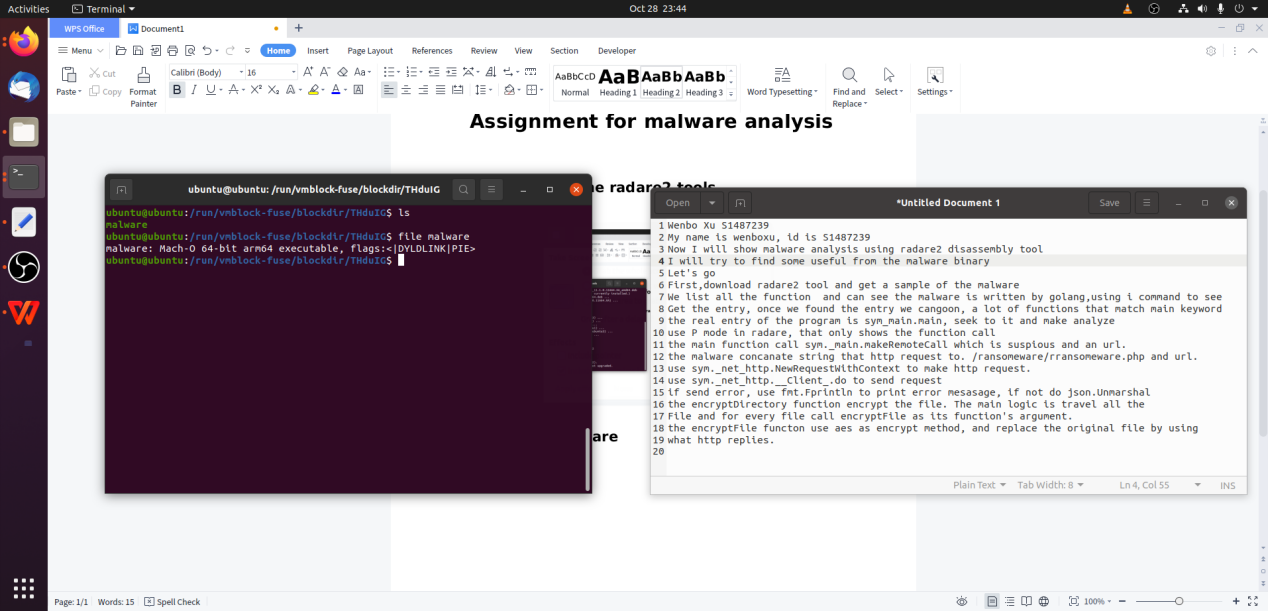
## Downloading the radare2 tools

using apt install in ubuntu

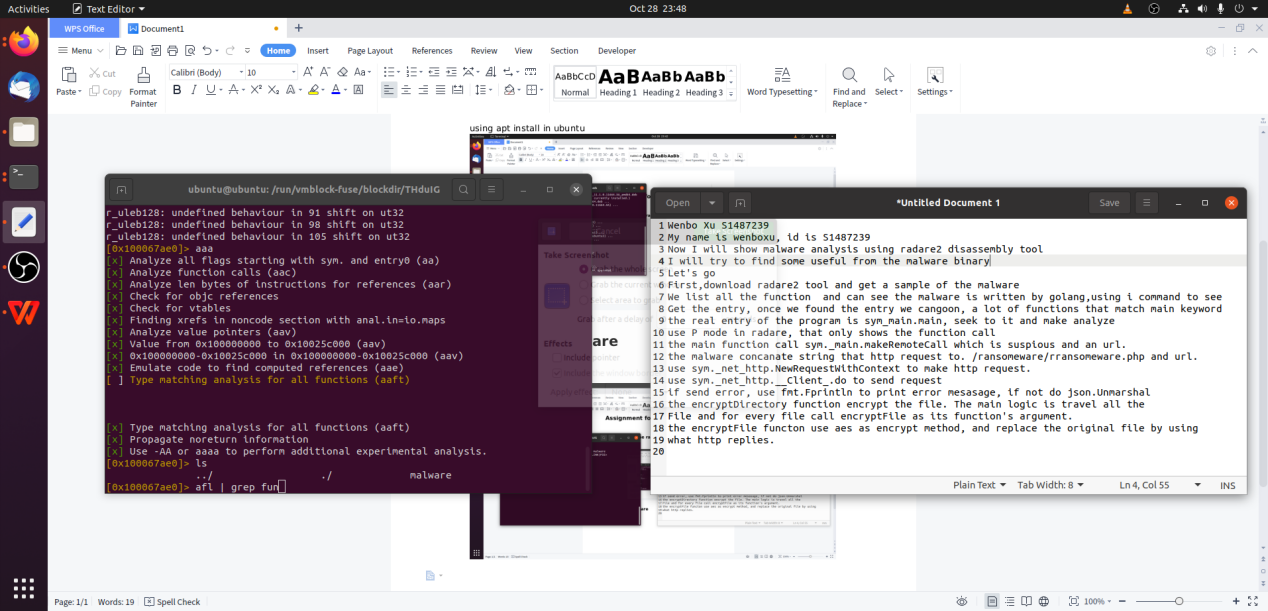


## Aanalysis malware

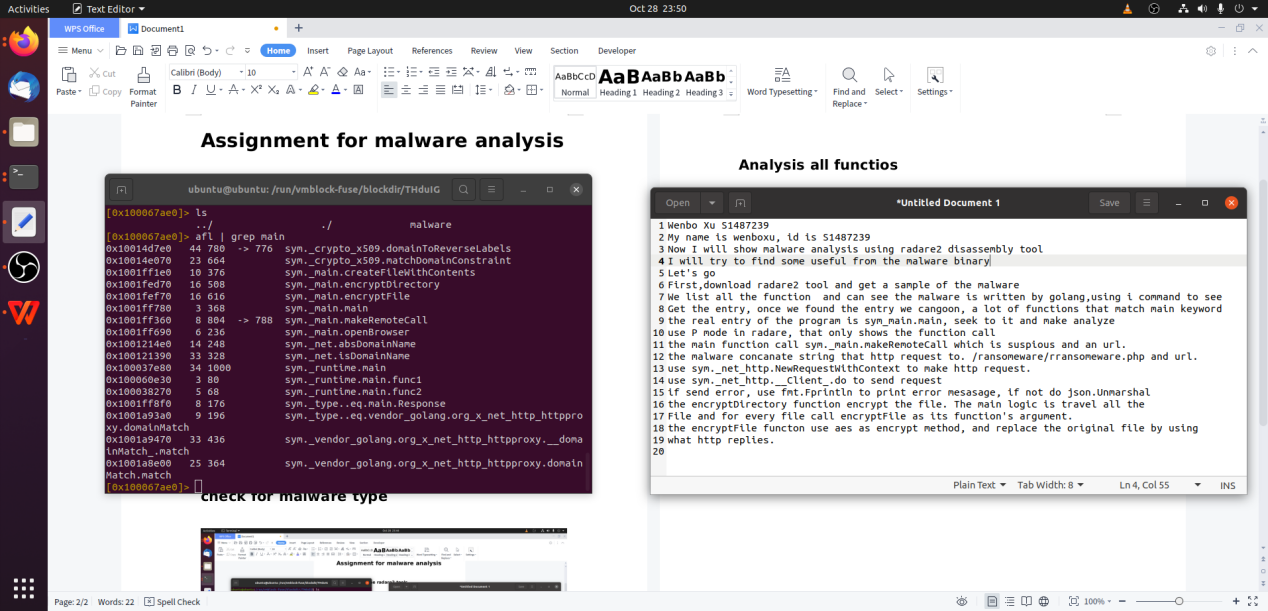
### check for malware type



### Analysis all functios



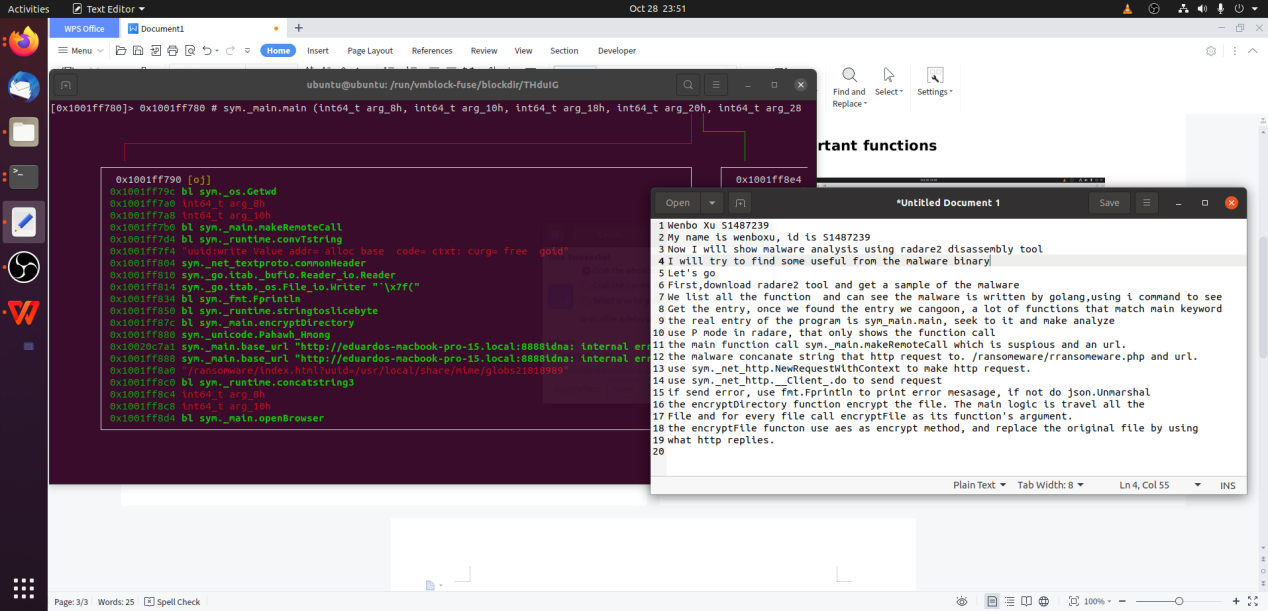
### Find important functions



### Main function

The mannfunction makes a remote call that commuiicates with the attacker’s host,

And then use encrypt function to encypt all the files.

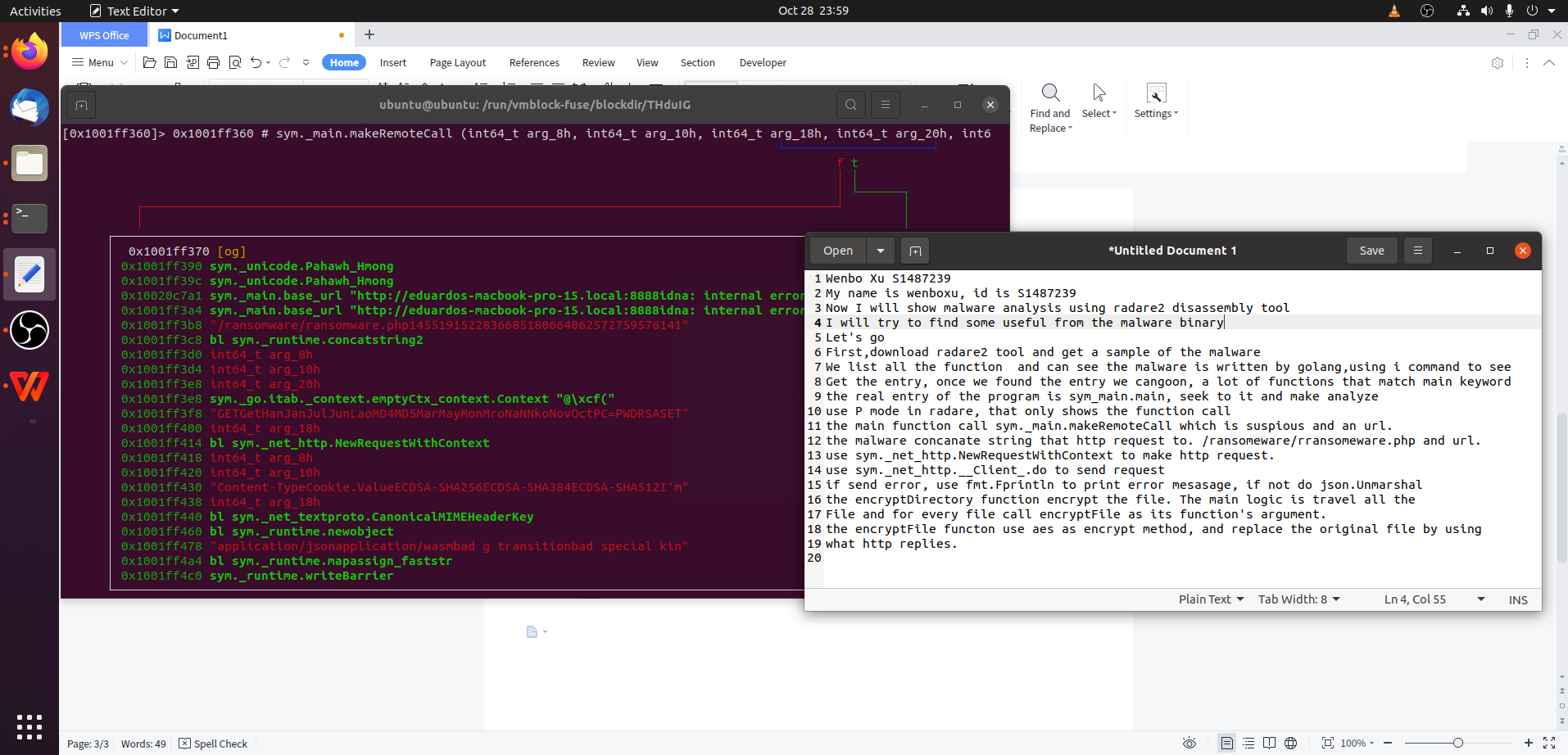


## Remote call function

Here are many strings object in this function.

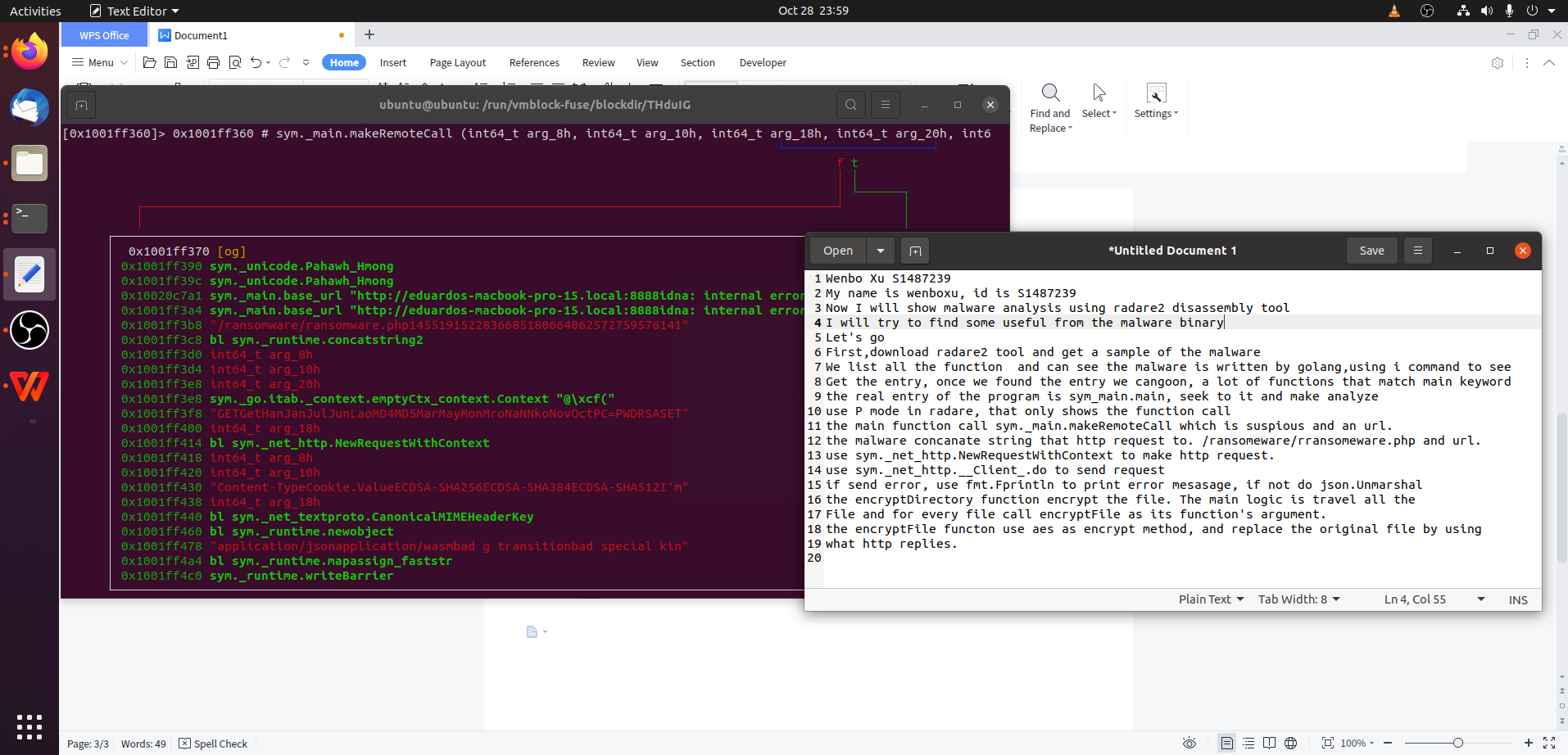
URL and port number show’s attacker’s host.

The http new\_request\_\_with\_context function make preparation for the http request.



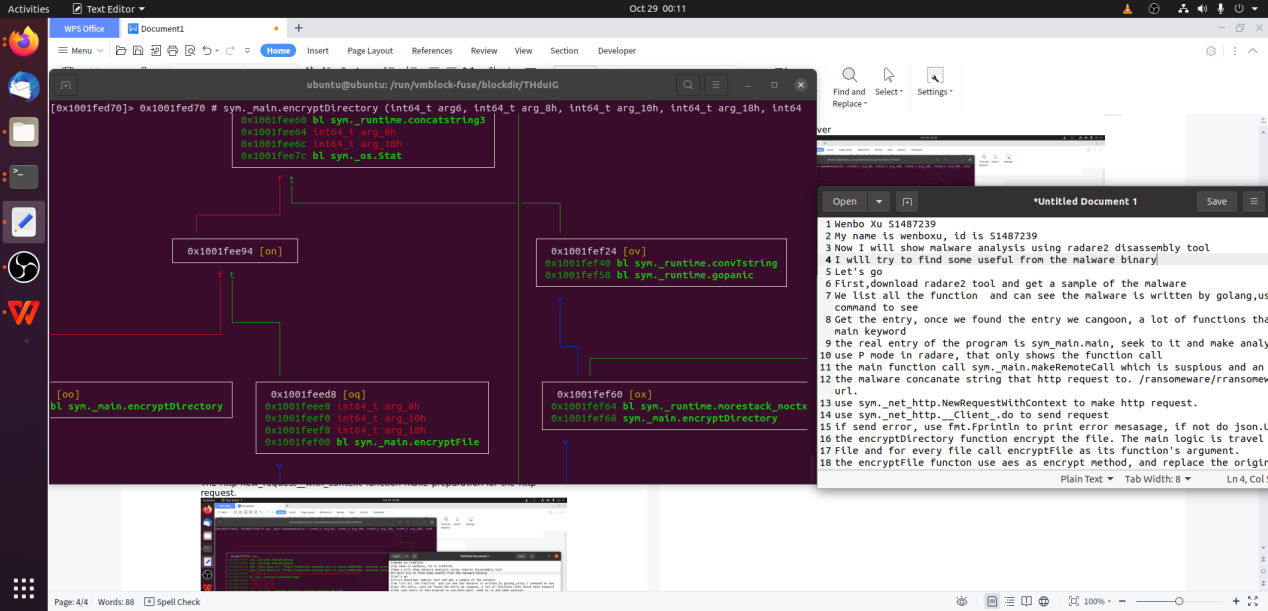
then use do\_client function to send request

remote call to server



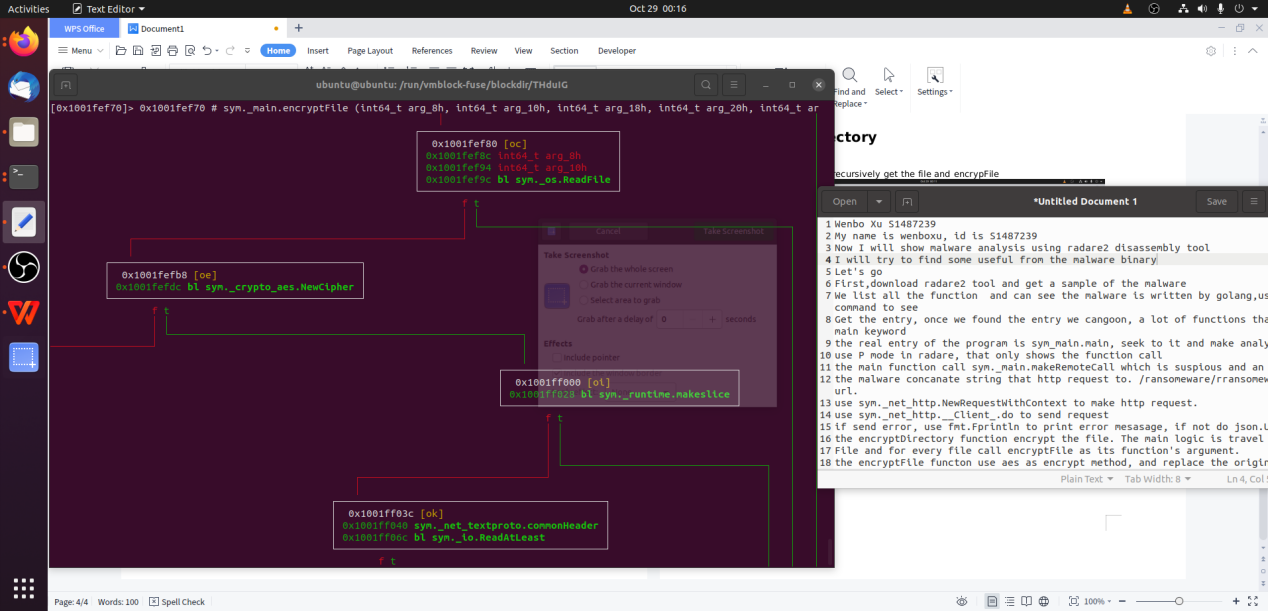
## Encrypt directory

Get all directory flle, recursively get the file and encrypFile



## Encrypt File

The function use aes crypto method to encrypt the data and replace the file



## Conclusion

Analyzing the basic information of the binary. Linux provides some basic tools that discovery the information of the binary. Using file command to see the file type of the file, this command will give the executable format and arch data. Use readelf to get the file header, such as session header and programs header, which is something helpful for us to analyze the malware.