

Introducción

El virus desarrollado para esta actividad es un Ransomware. Fue programado en Python y se utilizó una máquina virtual (linux) para probarlo.

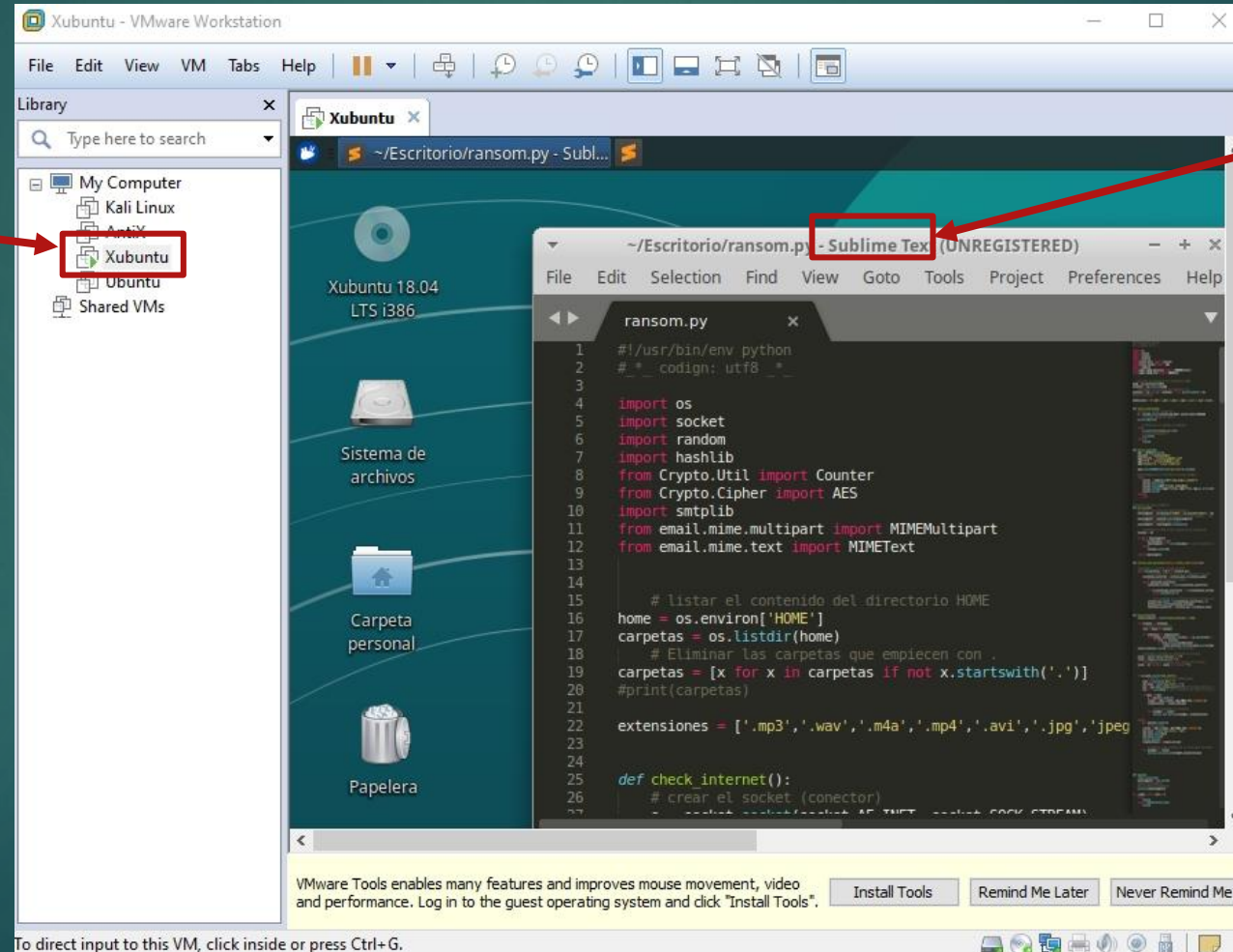
¿Qué es un Ransomware?

El Ransomware es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados.

El atacante pide un 'rescate', normalmente económico para liberar la información encriptada.

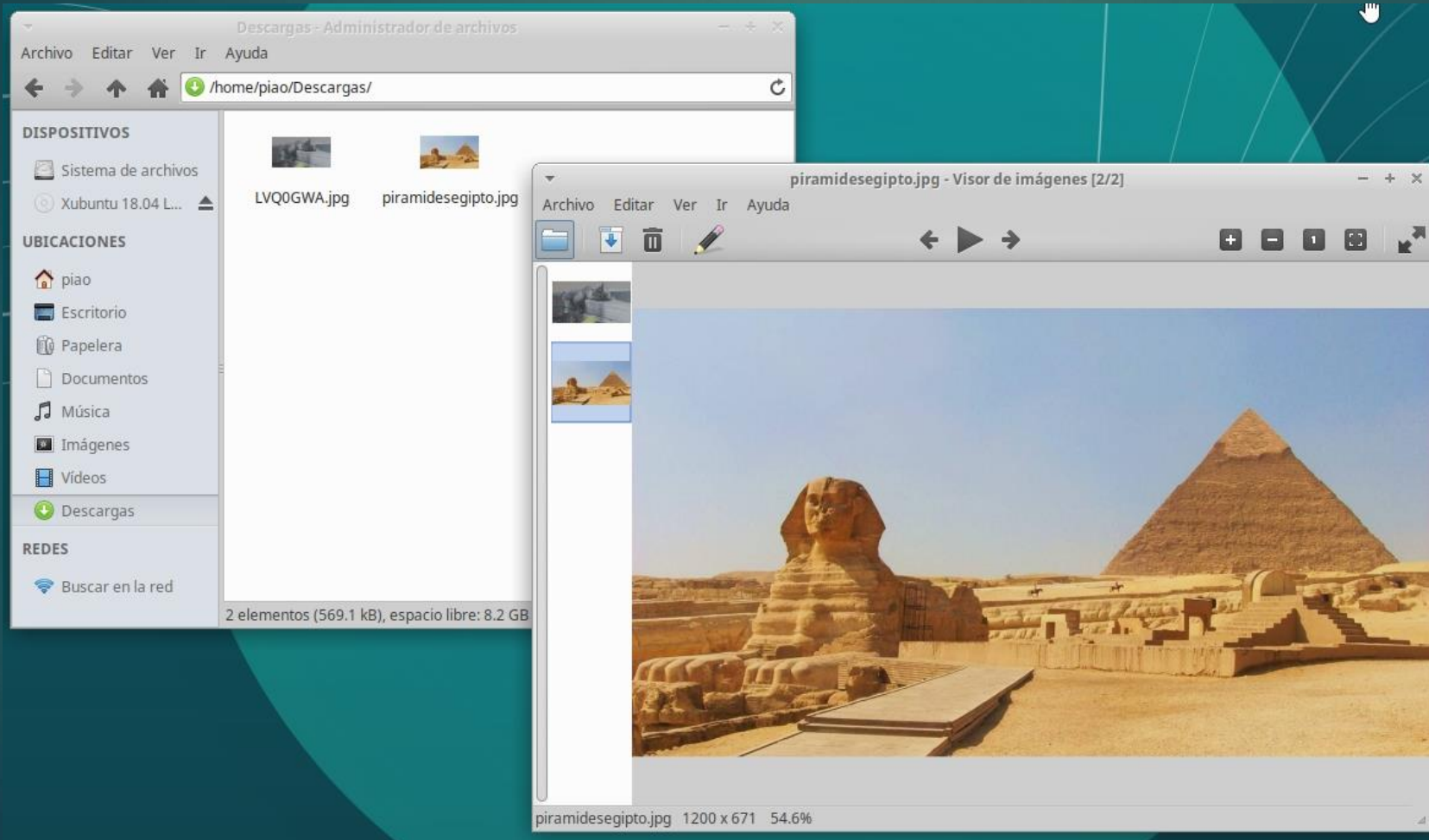
Preparación

Primero instalamos la maquina virtual (Xubuntu) que fue donde se programo y probo el virus. Después instalamos Python y Sublime Text dentro de la maquina virtual.

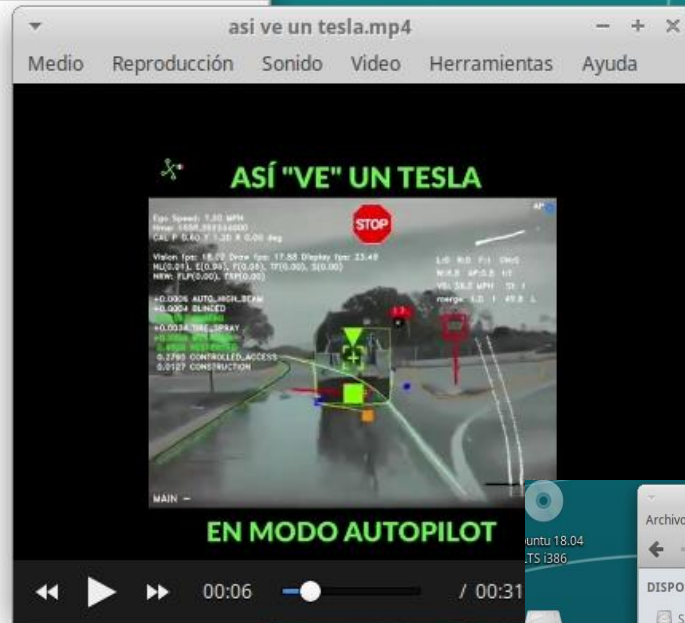
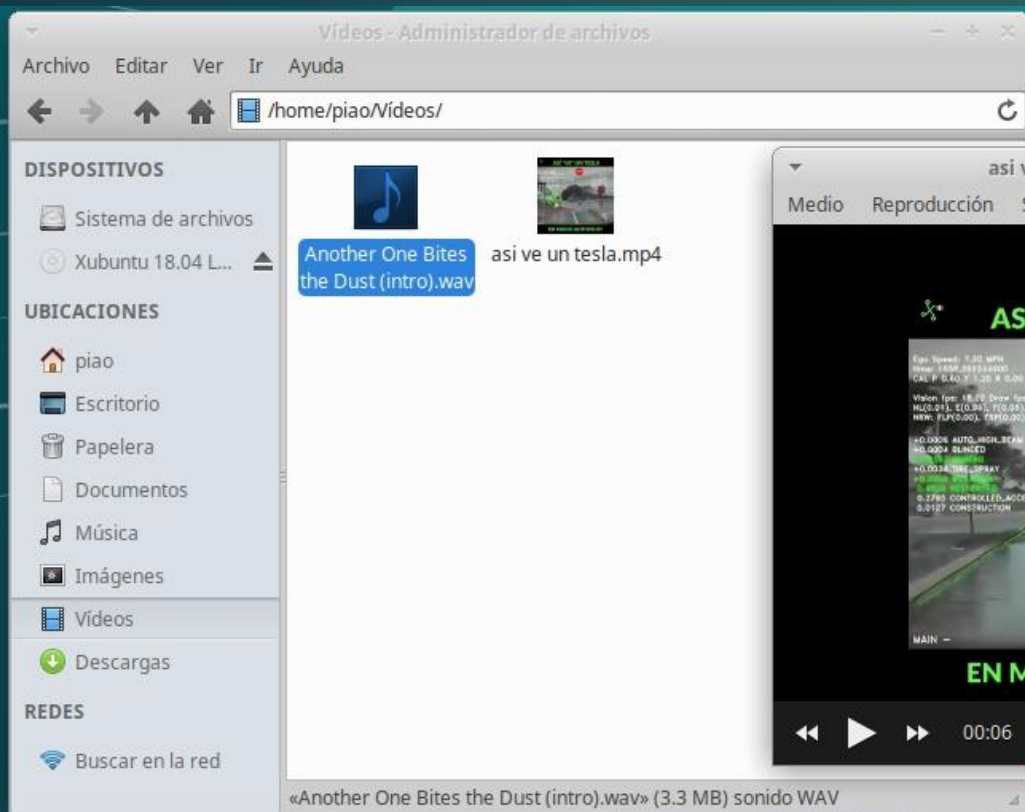


Verificar que los archivos funciones correctamente

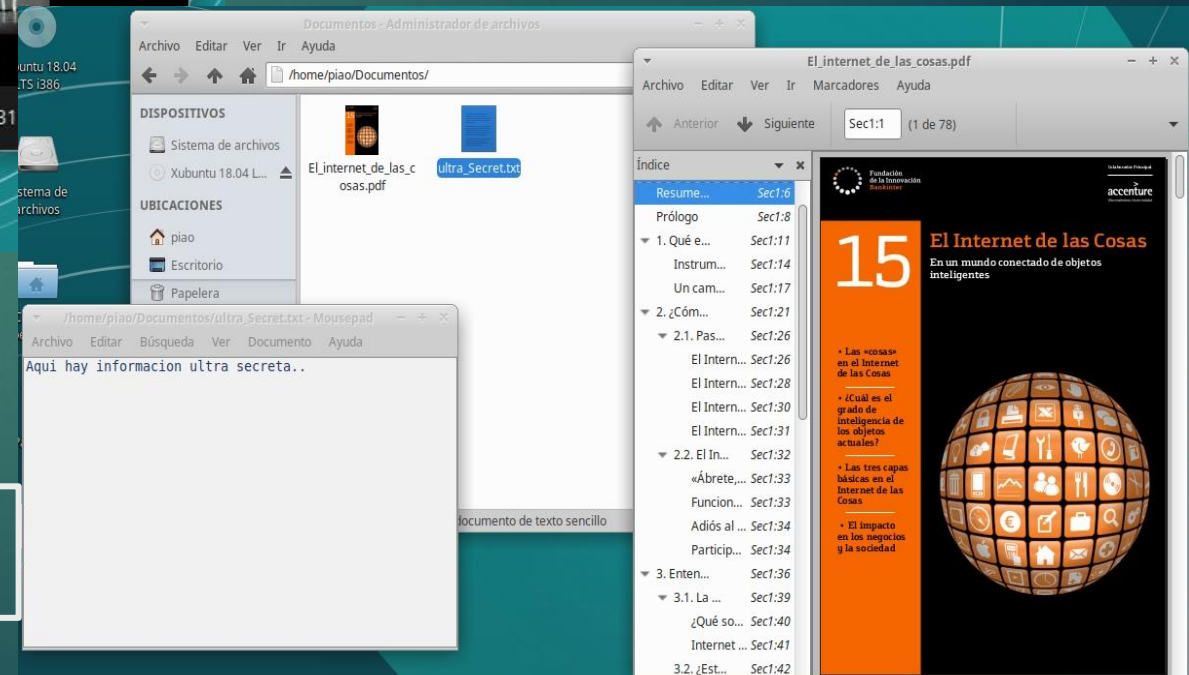
Primero agregamos varios archivos de diferentes tipos en diferentes carpetas y verificamos que se abren correctamente. Estos archivos son los que encriptaremos después con el ransomware.



Imágenes



Videos y
audio




Archivos de texto
y pdf

Funcionamiento del Ransomware

Este ransomware utiliza una encriptación de clave simétrica, es decir, genera una clave con el algoritmo 'sha512' para encriptar los archivos, y después esa clave se nos envía por email para utilizarla en la descriptación de los mismos.

Explicación general de lo que hace el ransomware:

- Primero se verifica que exista conexión a internet para poder enviar la clave por email.
- Después recorre las diferentes carpetas que existan en el sistema comenzando por la carpeta raíz ('home' en este caso).
- Verifica los archivos que se encuentran en cada carpeta comparando la extensión de estos con una lista de extensiones dentro del programa.
- Cuando la extensión de un archivo coincide con alguna extensión en la lista, el programa procede a abrirlo en modo binario y encriptar la información por bloques de 16 caracteres con el algoritmo sha256.

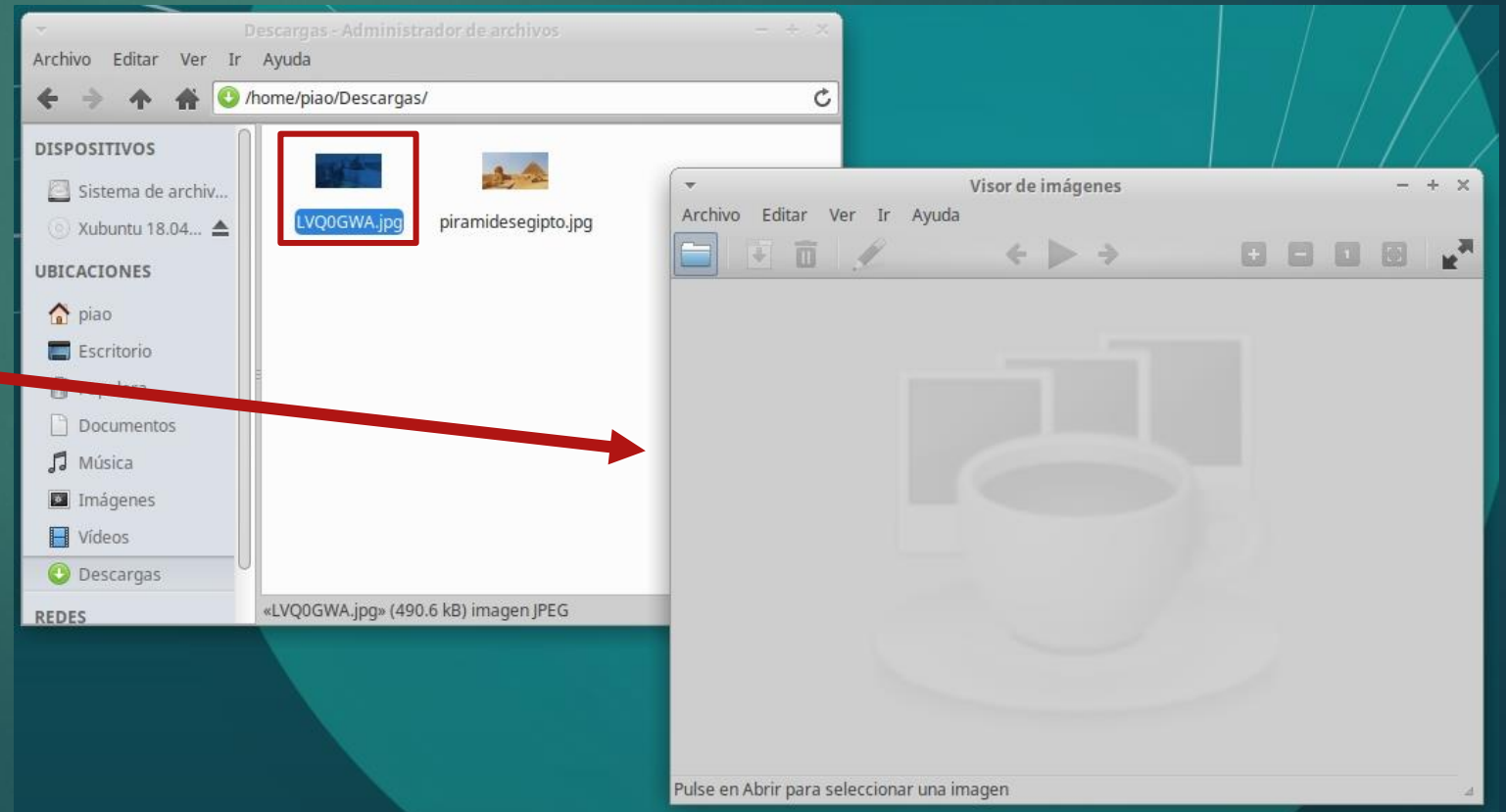
- 
- Después de recorrer todas las carpetas del sistema y encriptar los archivos que encuentra, el programa genera una clave de 32 caracteres que se enviara por email.
 - Una vez hecho todo esto, los archivo quedan inutilizables, no es posible abrirlos ya que todos sus caracteres fueron cambiados en modo binario, por lo que ninguna aplicación los reconoce.
 - Para recuperar los archivos, al ejecutar nuevamente el programa, pedirá una clave, que es la que nos llegara por email.
 - Una vez que escribamos la clave correcta, el programa descripta los archivos para que se puedan volver a abrir con normalidad.

Ejecución del Ransomware

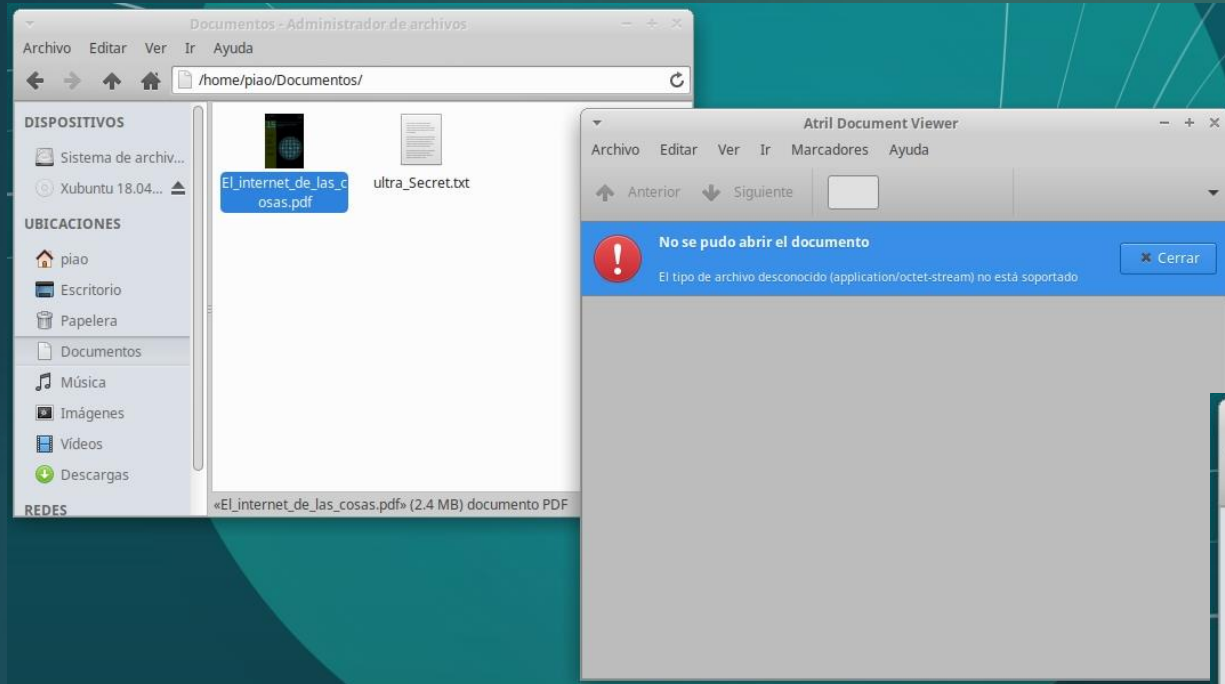
```
Terminal - piao@xubuntu-ram: ~/Escritorio
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
piao@xubuntu-ram:~/Escritorio$ python ransom.py
```

Una vez ejecutado el ransomware, intentamos abrir los archivos

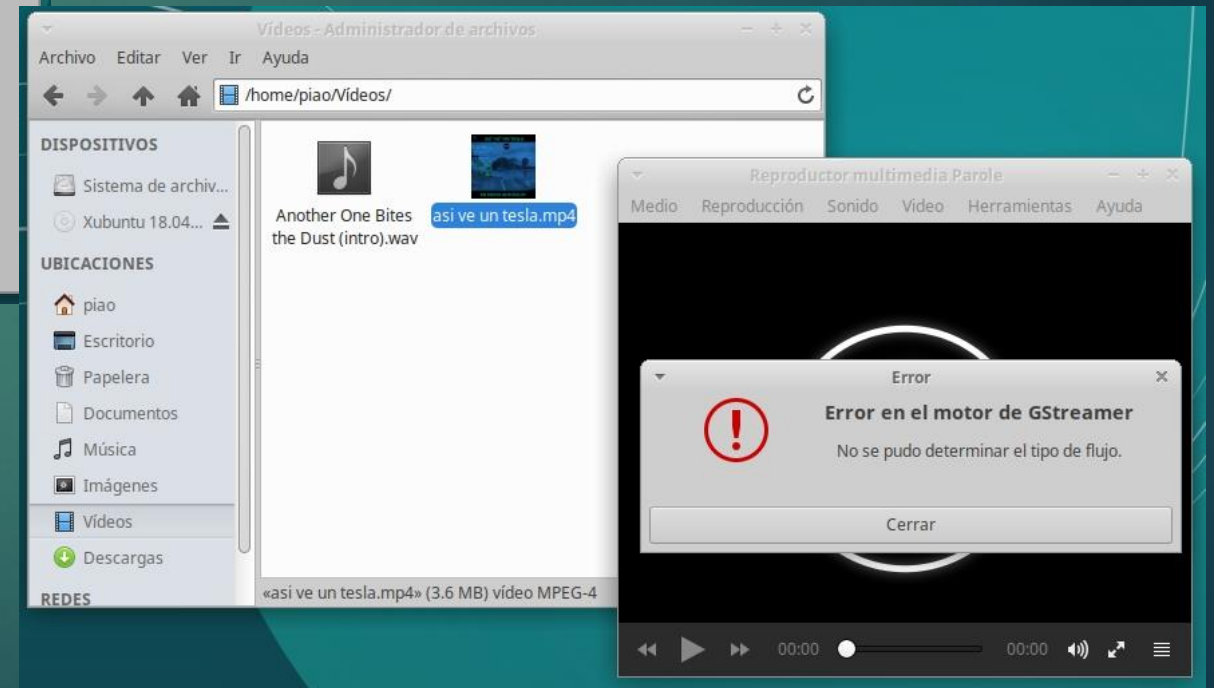
Al verificar los archivos todo parece normal, pero al intentar abrir una imagen, el visor de imágenes no reconoce el archivo y no lo puede abrir



Lo mismo ocurre con los demás archivos



Al intentar abrir un pdf, la aplicación no lo reconoce



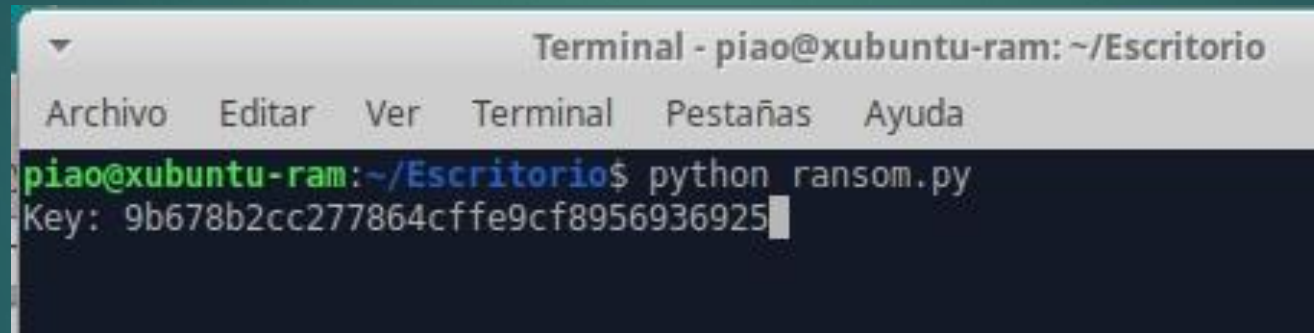
Los mismo ocurre al intentar abrir un video

Desencriptar los archivos

Ya vimos que los archivos están encriptados y quedaron inutilizables, ahora verifiquemos que la clave que nos llegó por mail funciona para desencriptarlos.

Abrimos nuestro mail y vemos que la contraseña está ahí.

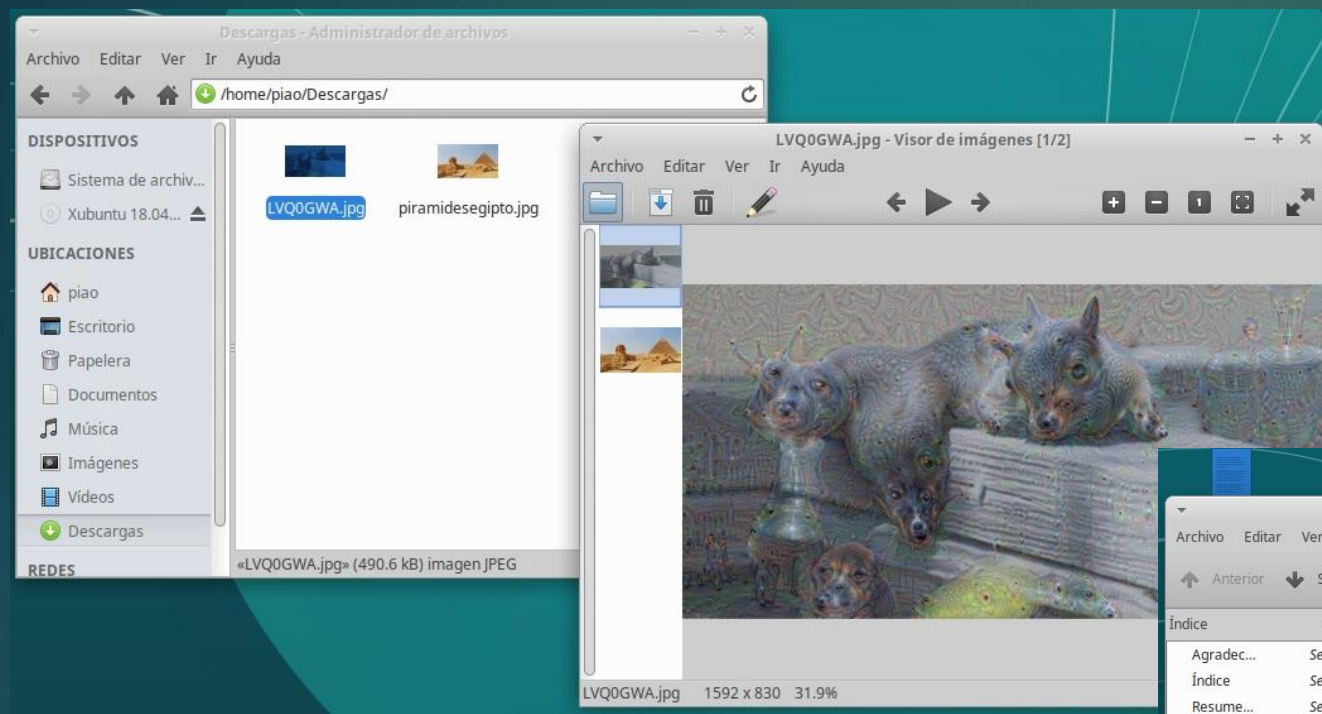
Al volver a ejecutar el programa nos pedirá la clave. La pegamos.

A screenshot of a terminal window titled "Terminal - piao@xubuntu-ram: ~/Escritorio". The window has a menu bar with "Archivo", "Editar", "Ver", "Terminal", "Pestañas", and "Ayuda". The terminal shows the command "python ransom.py" being executed, followed by the prompt "Key: 9b678b2cc277864cffe9cf8956936925" with a cursor at the end.

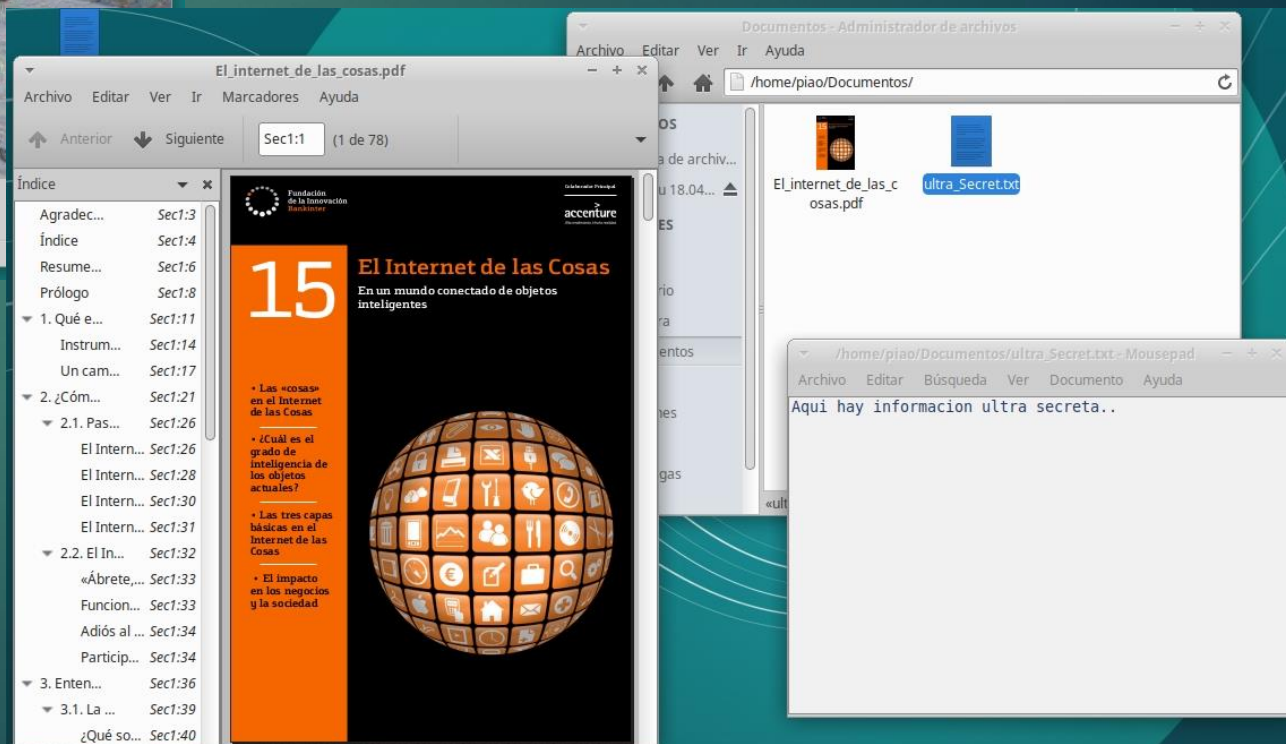
```
Terminal - piao@xubuntu-ram: ~/Escritorio
Archivo  Editar  Ver    Terminal  Pestañas  Ayuda
piao@xubuntu-ram:~/Escritorio$ python ransom.py
Key: 9b678b2cc277864cffe9cf8956936925
```

Al hacer esto el programa comienza a desencriptar los archivos.

Verificamos entonces que los archivos se puedan abrir normalmente.



Imágenes



Archivos de
texto y pdf