GOBIERNO DEL
ESTADO DE MÉXICO

TECNOLÓGICO DE ESTUDIOS SUPERIORES
IXTAPALUCA

TECNOLOGICO DE ESTUDIOS SUPERIORES DE IXTAPALUCA

MATERIA:

AUDITORIA DE LA SEGURIDAD INFORMATICA

PROFESOR:

KEVIN RAMIREZ VITE

ESTUDIANTE:

LAMADRID REYNOSO MANUEL

LAGUNA CASTRO GENARO

PEREZ IBARRA GIOVANNI

RAMIREZ OSORIO JAIME

LAURA RAMOS GONZÁLEZ

GRUPO:

1951

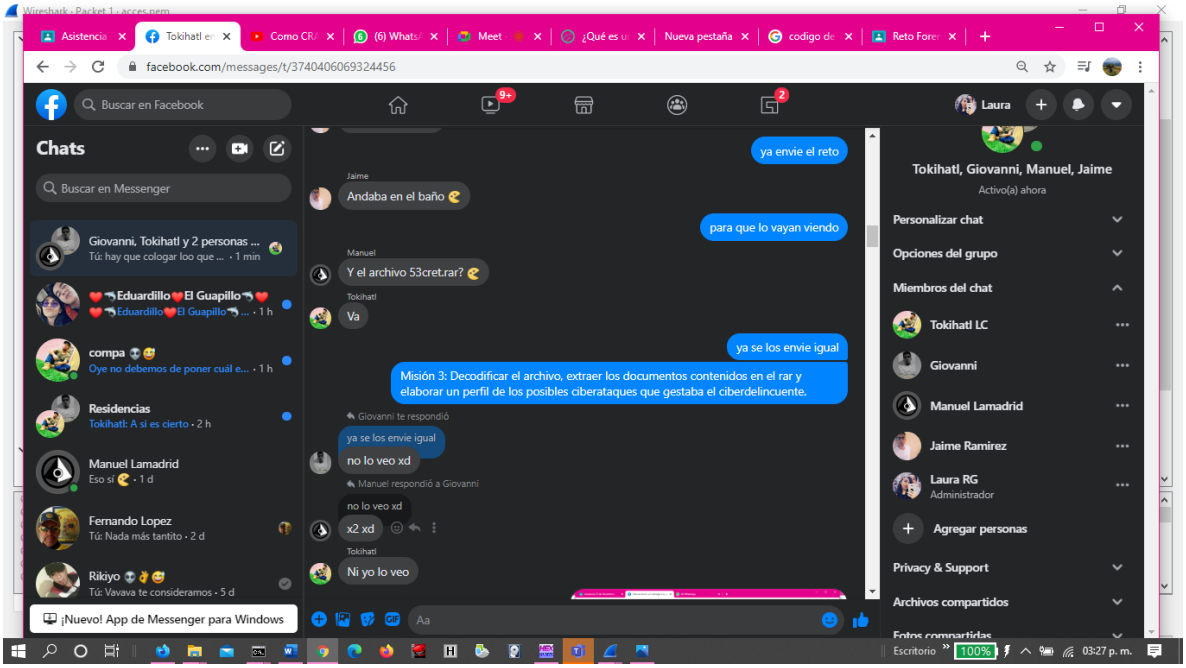
TRABAJO:

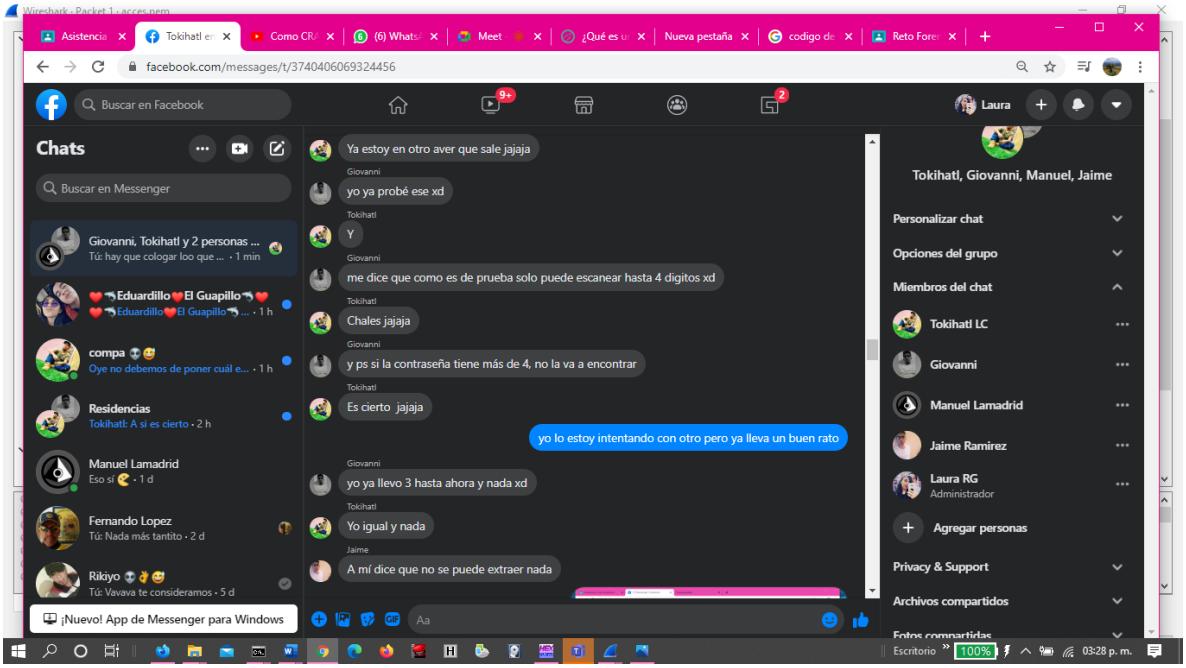
RETO FORENSE 2

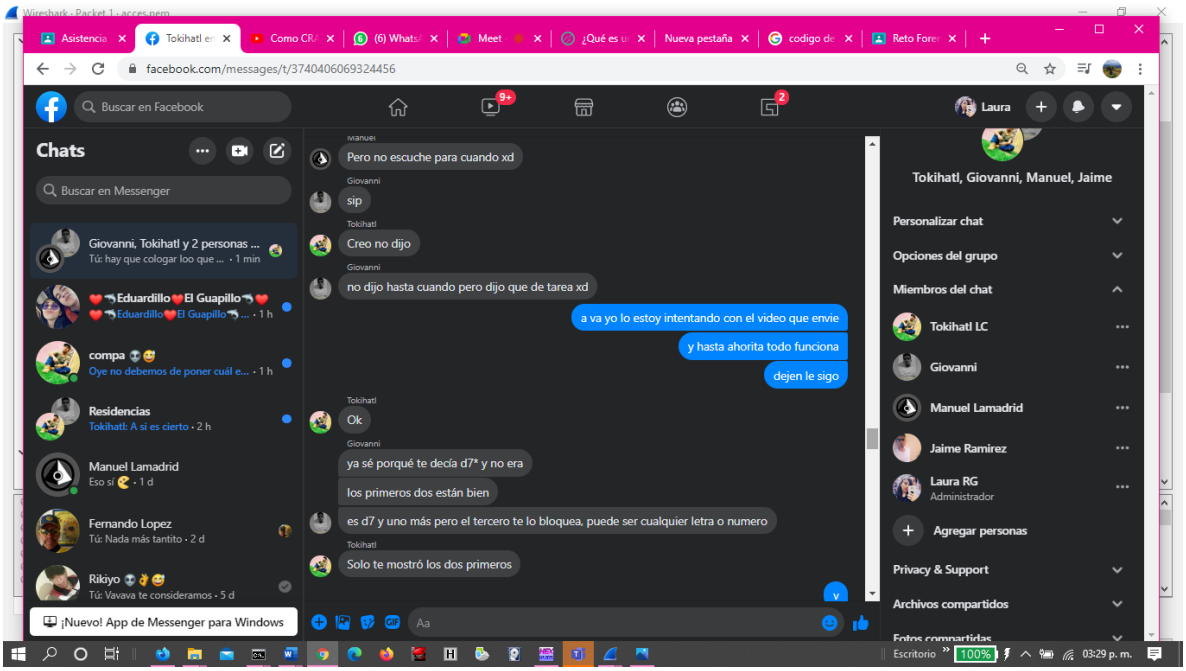
FECHA DE ENTREGA:

25 DE NOVIEMBRE DEL 2020

Conversación del desarrollo de reto

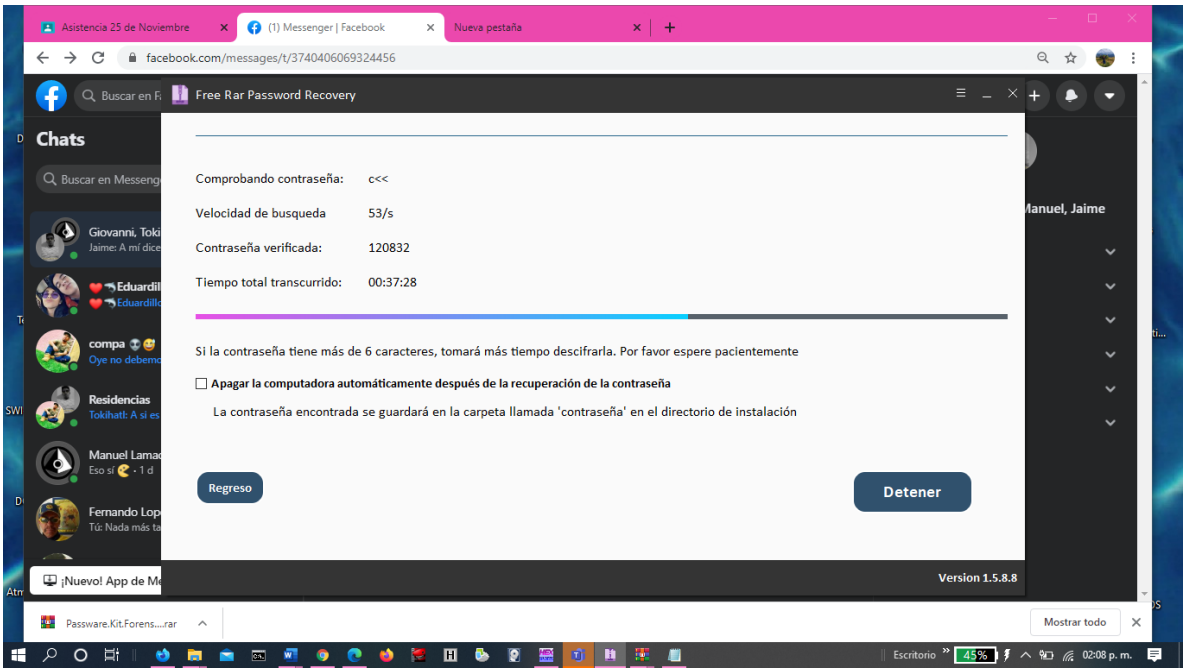




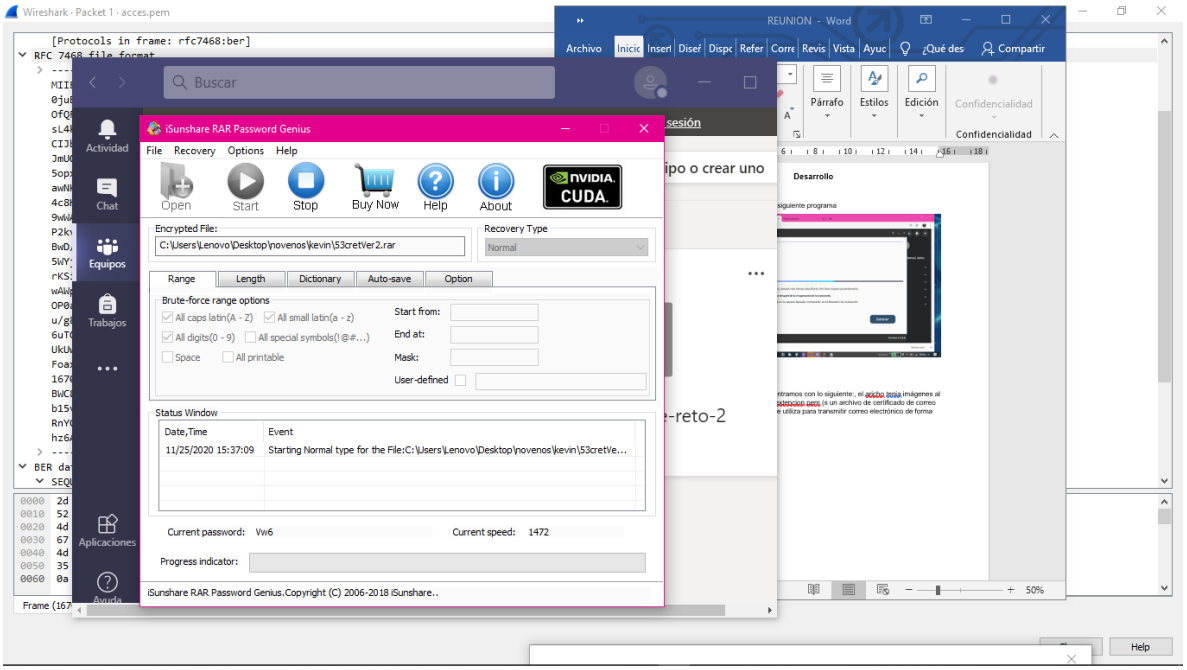

Wireshark · Packet 1 · acces.pcap
Asistencia
Tokihatl en
Como CRA
(6) Whats
Meet
¿Qué es u
Nueva pestaña
codigo de
Reto Fores
facebook.com/messages/t/3740406069324456
Buscar en Facebook
Laura
Chats
Buscar en Messenger
Giovanni, Tokihatl y 2 personas ...
Tú: hay que cologar loo que ... · 1 min
❤️🐬Eduardillo❤️El Guapillo🐬❤️
❤️🐬Eduardillo❤️El Guapillo🐬 ... · 1 h
compa
Oye no debemos de poner cuál e... · 1 h
Residencias
Tokihatl: A si es cierto · 2 h
Manuel Lamadrid
Eso sí · 1 d
Fernando Lopez
Tú: Nada más tantito · 2 d
Rikiyo
Tú: Vavava te consideramos · 5 d
¡Nuevo! App de Messenger para Windows
Manuel
Pero no escuche para cuando xd
Giovanni
sip
Tokihatl
Creo no dijo
Giovanni
no dijo hasta cuando pero dijo que de tarea xd
a va yo lo estoy intentando con el video que envie
y hasta ahorita todo funciona
dejen le sigo
Tokihatl
Ok
Giovanni
ya sé porqué te decía d7* y no era
los primeros dos están bien
es d7 y uno más pero el tercero te lo bloquea, puede ser cualquier letra o numero
Tokihatl
Solo te mostró los dos primeros
Aa
Tokihatl, Giovanni, Manuel, Jaime
Personalizar chat
Opciones del grupo
Miembros del chat
Tokihatl LC
Giovanni
Manuel Lamadrid
Jaime Ramirez
Laura RG
Administrador
Agregar personas
Privacy & Support
Archivos compartidos
Fotos compartidas
Escritorio
100%
03:29 p. m.

Desarrollo

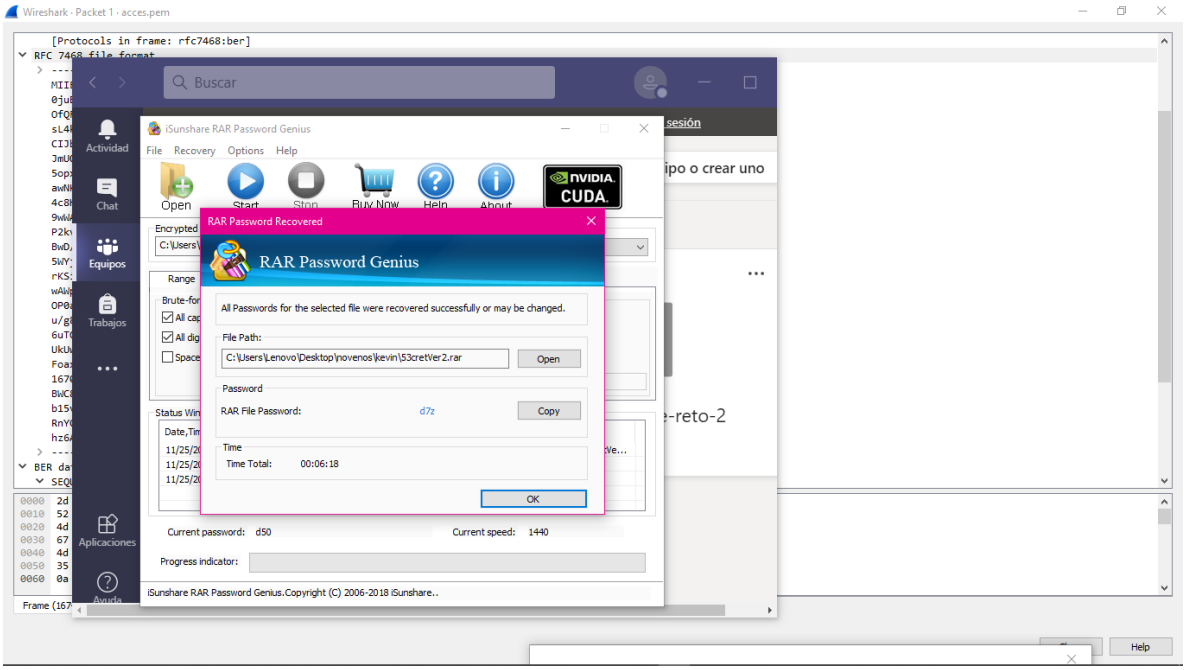
Extraemos la contraseña con el siguiente programa



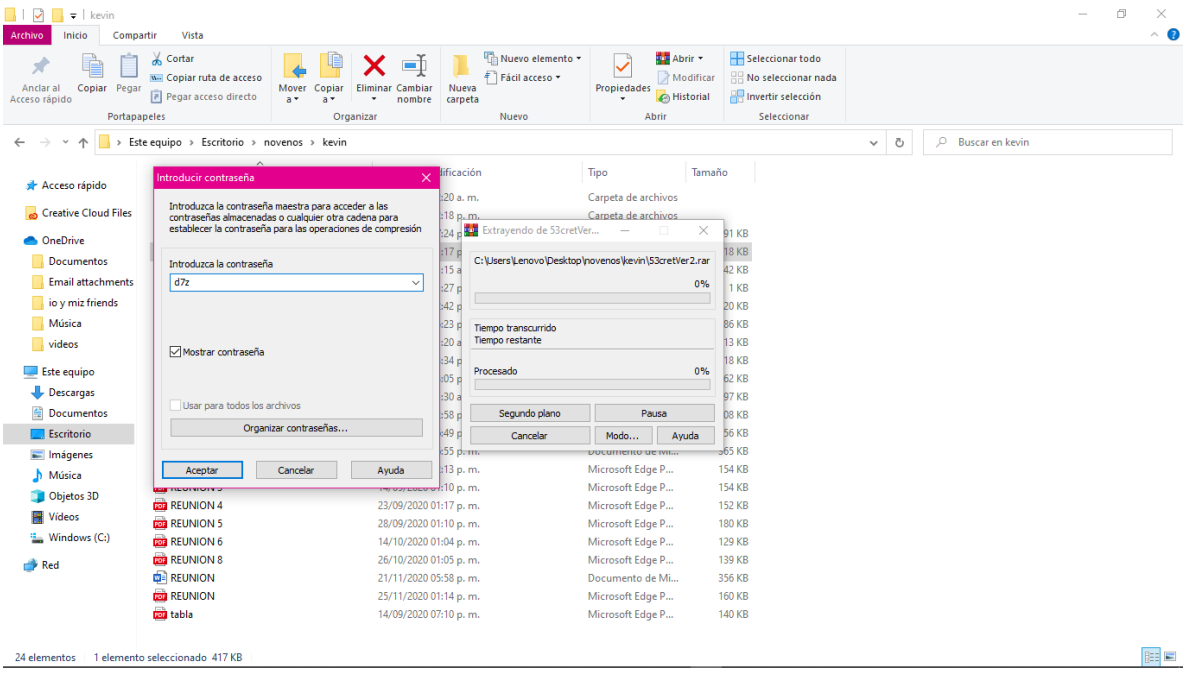
Igual lo intentamos con password genius



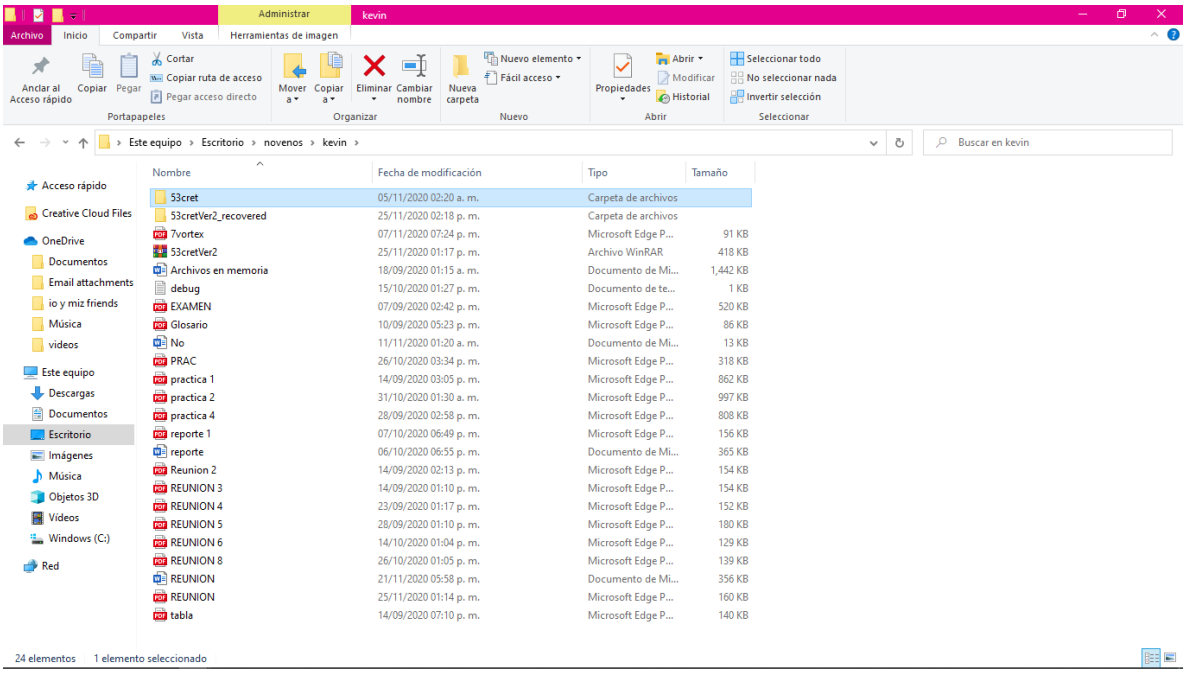
La contraseña que nos arroja es d7z



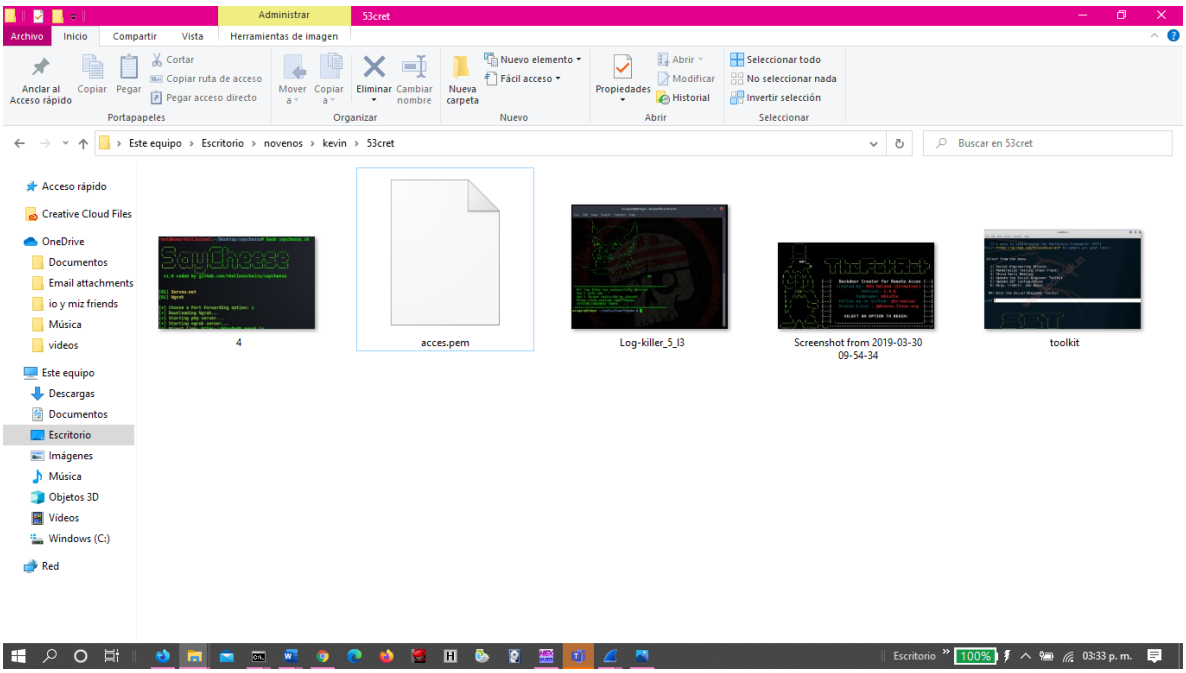
Colocamos la contraseña que nos arrojo el software



Nos aparece la carpeta siguiente

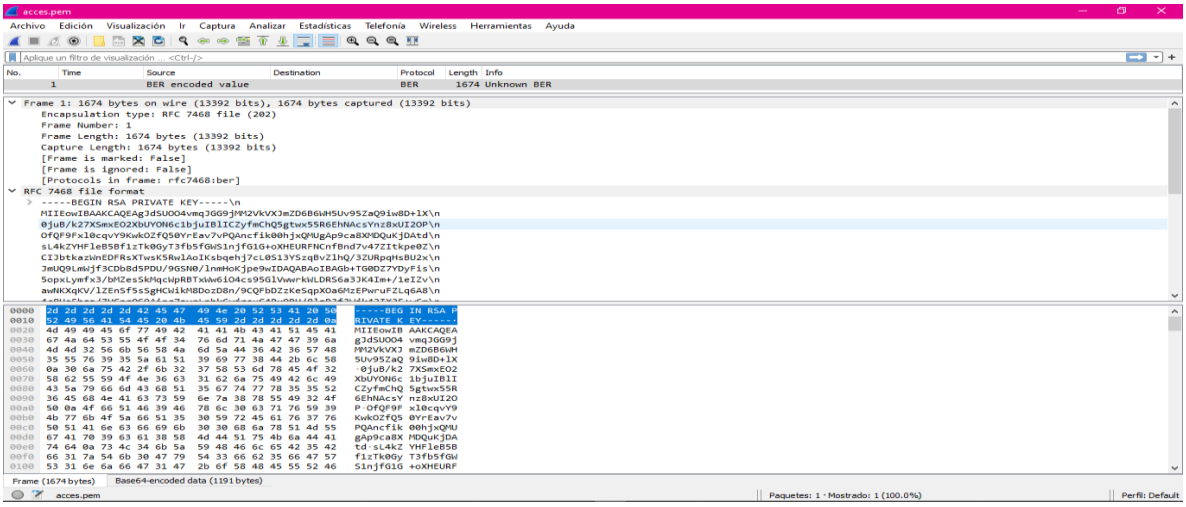


Al extraer el archivo nos encontramos con lo siguiente:, el archivo tenía imágenes al igual que un documento con extensión pem (s un archivo de certificado de correo mejorado de privacidad que se utiliza para transmitir correo electrónico de forma privada.)



información sobre PEM La función de integridad de datos del formato de certificado de correo mejorado de privacidad utiliza compendios de mensajes RSA-MD2 y RSA-MD5 para comparar un mensaje antes y después de su envío, a fin de garantizar que no haya sido manipulado durante el proceso. Al principio de un archivo PEM hay un encabezado que dice ——BEGIN[label]——, y el final de los datos es un pie de página similar a este: —— END[etiqueta]———-. La sección “[label]” describe el mensaje, por lo que podría ser PRIVATE KEY, CERTIFICATE REQUEST, or CERTIFICATE.

Abrimos el archivo con wireshark



al abrir el archivo nos aparece los encabezado de prívate key