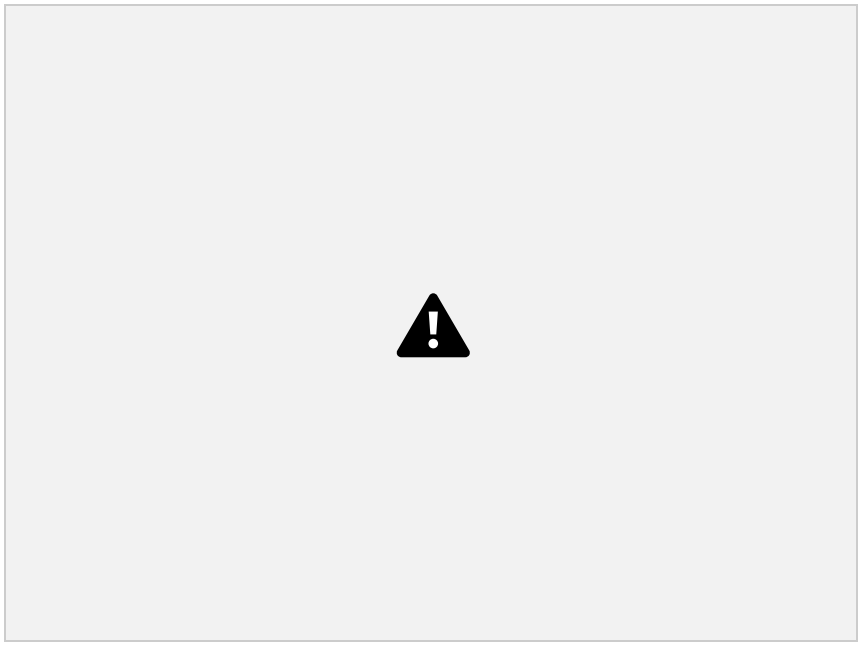
INFORME FORENSE CASO MUEBLES

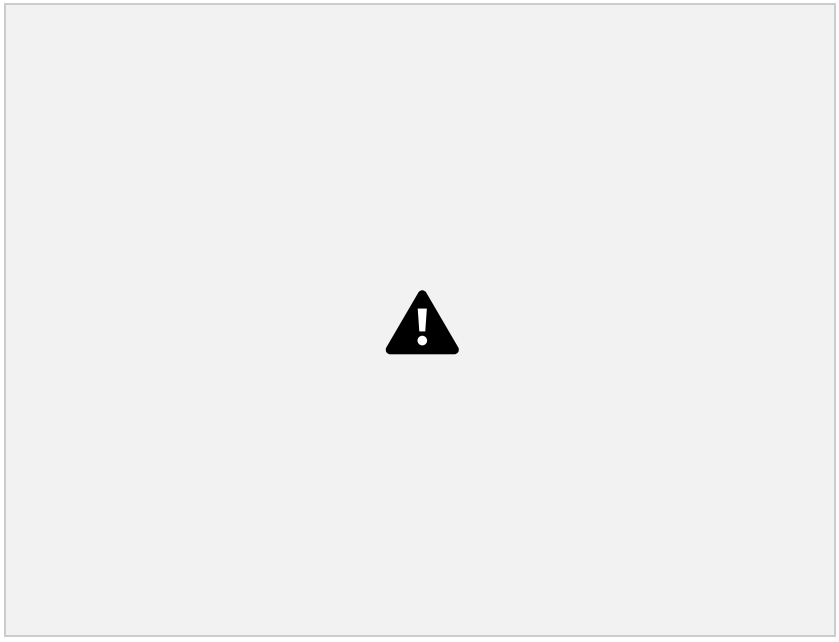
RESUMEN DEL CASO.

El Ing Roberto Cano director general de le empresa Artmuebles la cual diseña y elabora muebles para oficinas, empieza a inquietarse al ver sus diseños expuestos en un empresa de la competencia antes de su lanzamiento. Esto empieza desde el mes de agosto del 2010 hasta la fecha que es 14 de octubre del 2010.
Esto hace presumir que existe una fuga de información de su empresa y uno de sus empleados le está siendo infiel.
Al indagar un poco entre el personal interno le comentan que en la empresa Diseñar que es la competencia de Artmueble, labora la enamorada del Sr Pablo Casares.
Esto hace sospechar ya que el antes mencionado labora en la empresa en el área de despachos.
El Ing. Cano encarga al personal de sistemas que analice algo dentro de los log del servidor de correo electrónico para ver si encontraban algo anormal.
El informe del departamento de sistemas indica que lo único raro de la cuenta del Sr. Casares en que envía a una misma dirección unas 2 veces por semana durante el último mes la imagen de unos perros con el asunto de ahí va otro.
Esto inquieta un poco al Director de la empresa y ordena el análisis del forense de la unidad de almacenamiento de la cual se extrajo una imagen forense y se da para su investigación.
El Ing. Cano nos comenta que requiere se investigue el dispositivo de almacenamiento del Sr. Casares que le fue entregado por la empresa para el trabajo y se busque señales de la información de diseños de los muebles.

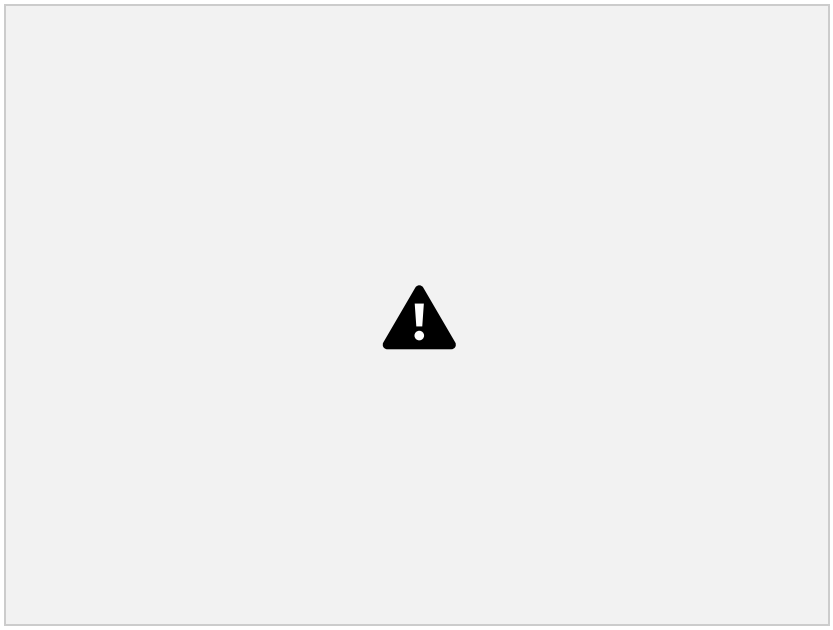
1. Primero abrir el Back Track 5 R 2 crear una carpeta donde se va a guardar la forensia, esta debe estar esterilizada



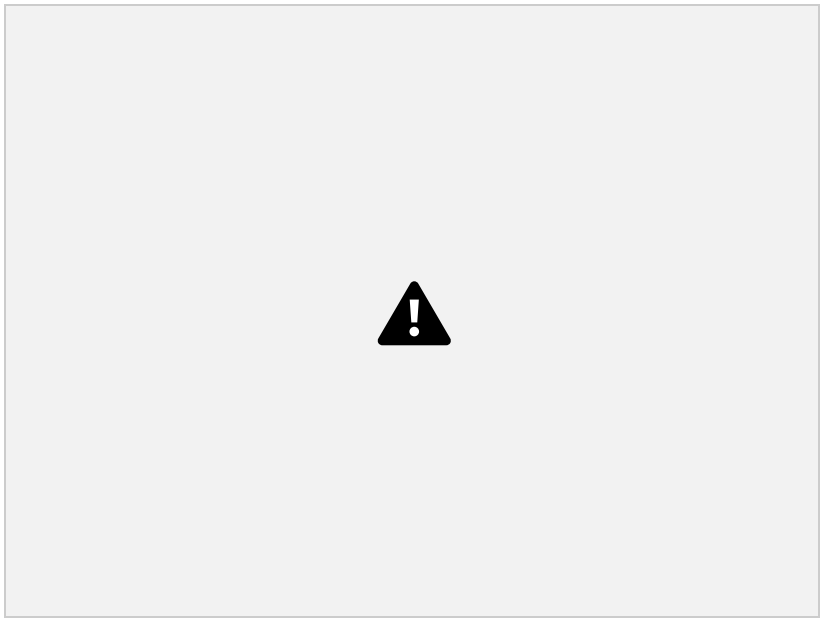
2. Se ingresa a la ruta Back Track – forensics – forensic suites - autopsy



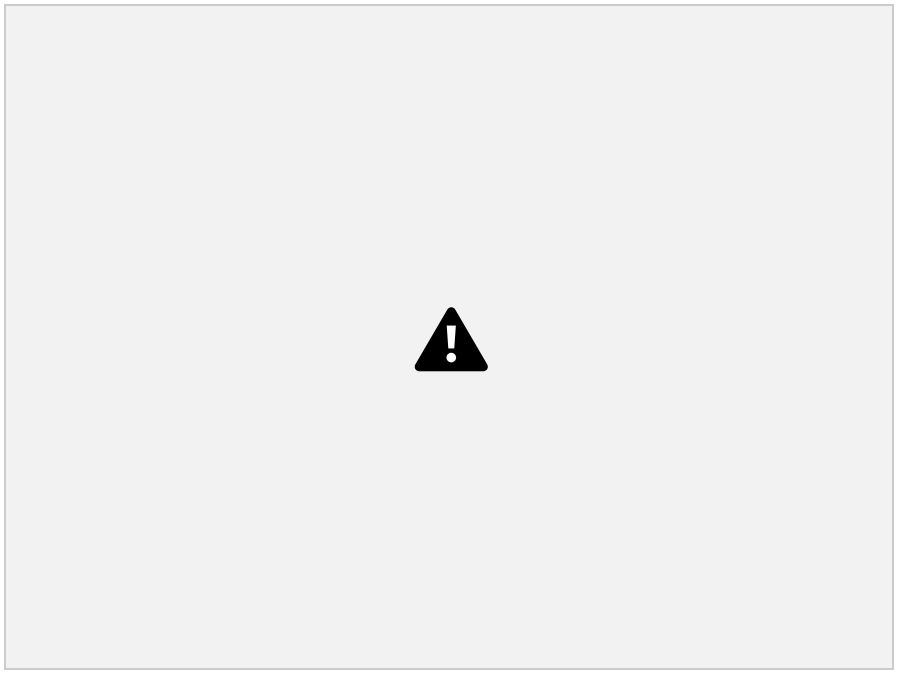
3. Al ingresar a autopsy se le coloca la ruta de donde se va a guardar la forensia se abre el url http://localhost:9999/autopsy



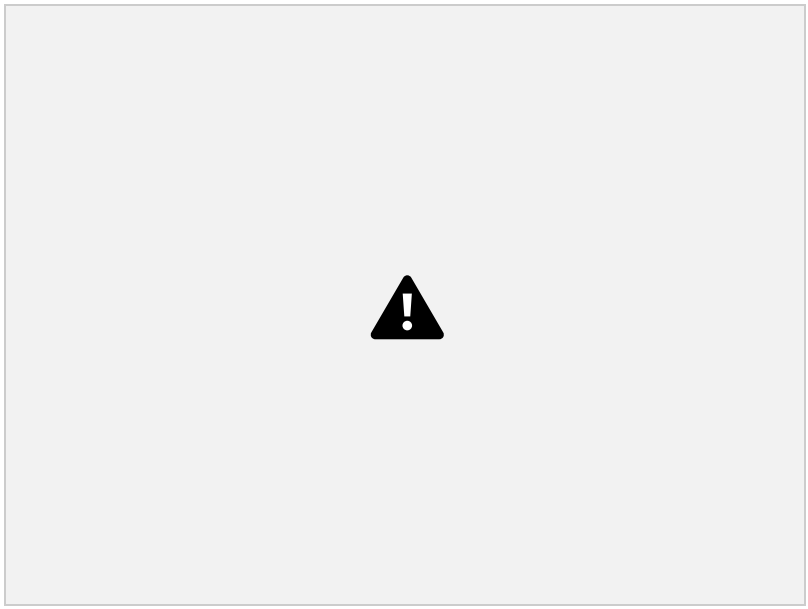
4. Se crea un new case



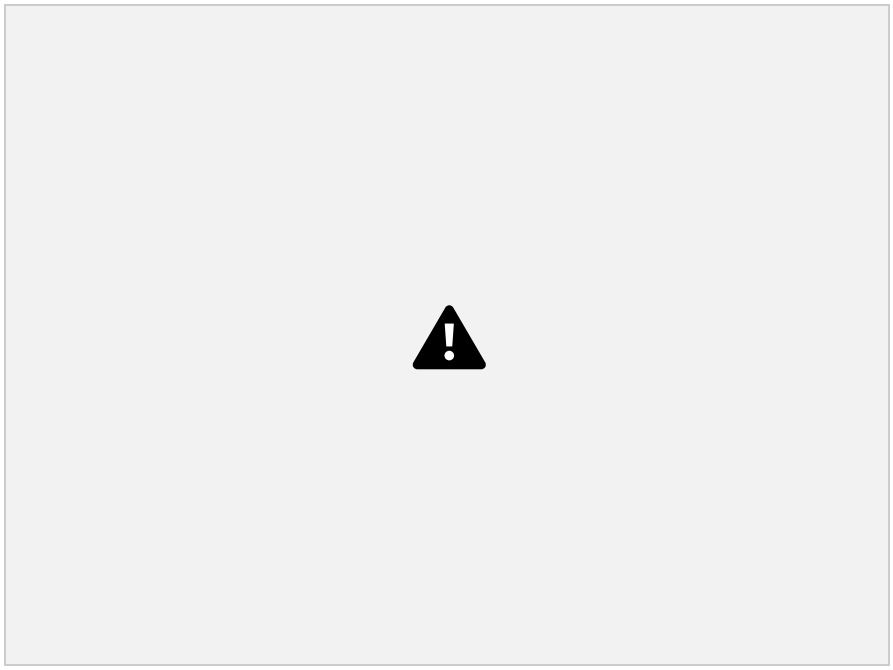
5. Se coloca el nombre del caso a realizar, la descripción y el nombre de la persona que está realizando la forensia



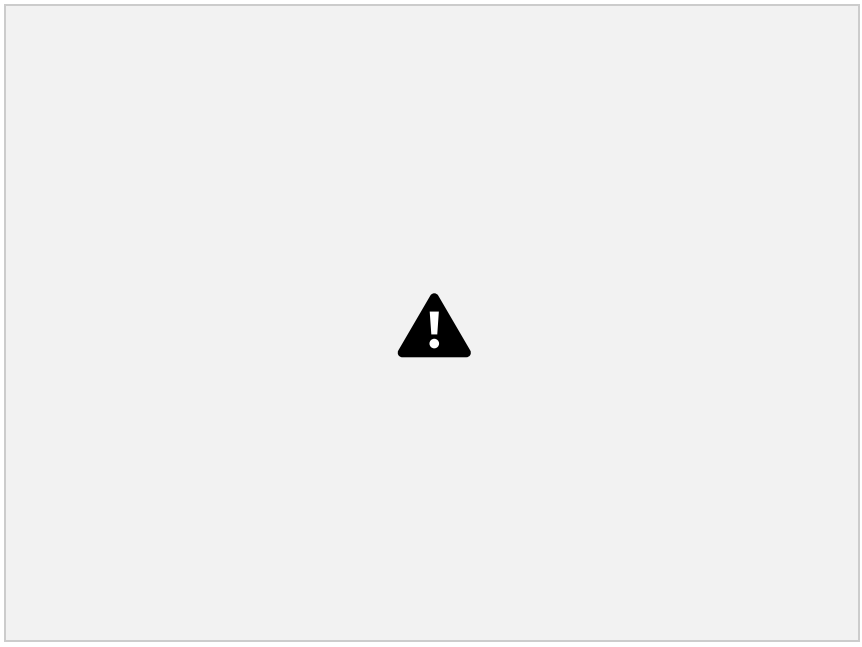
6. Adicional el time zone y zona horario --- add



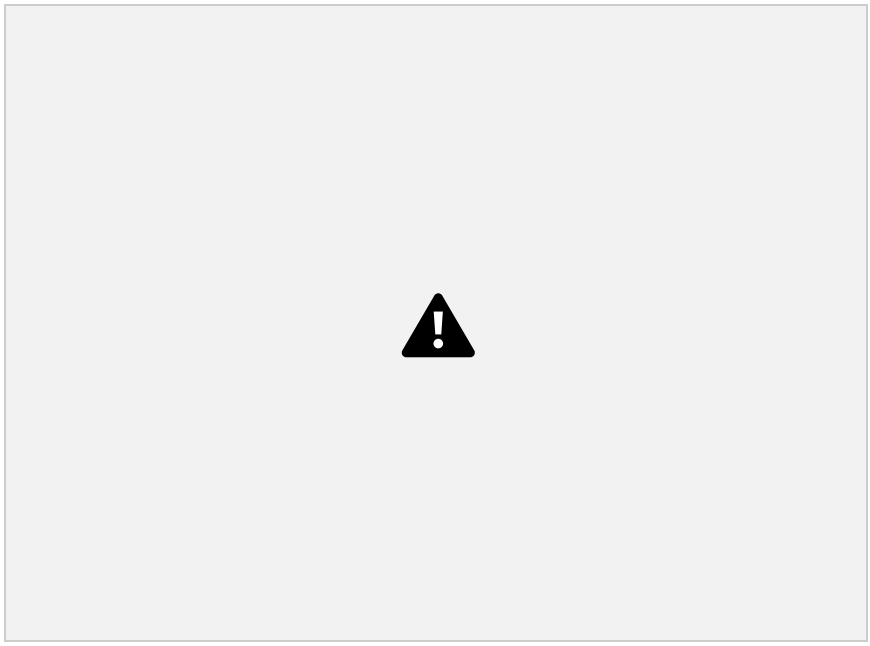
7. Se crea el host en la carpeta donde se va a guardar el caso muebles



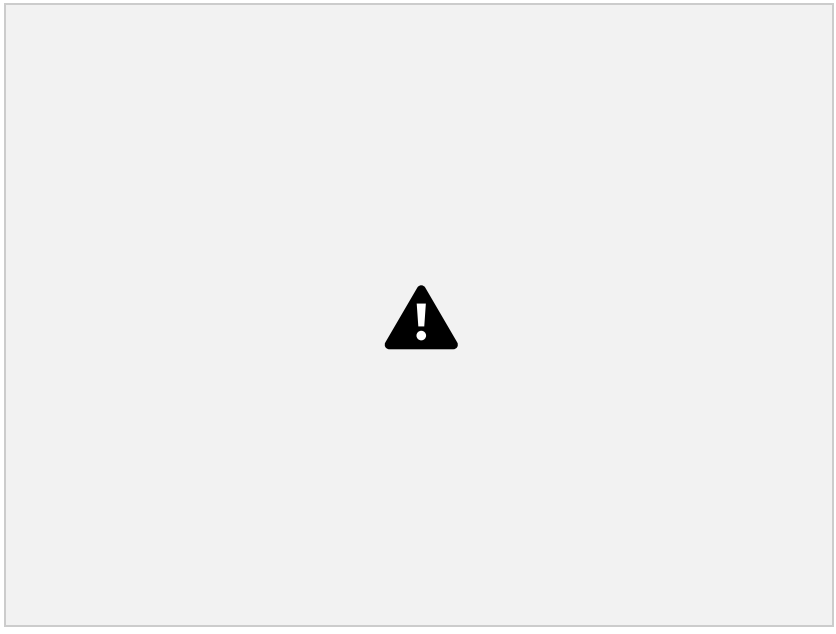
8. En este paso se adiciona la imagen con la opción Add Image File



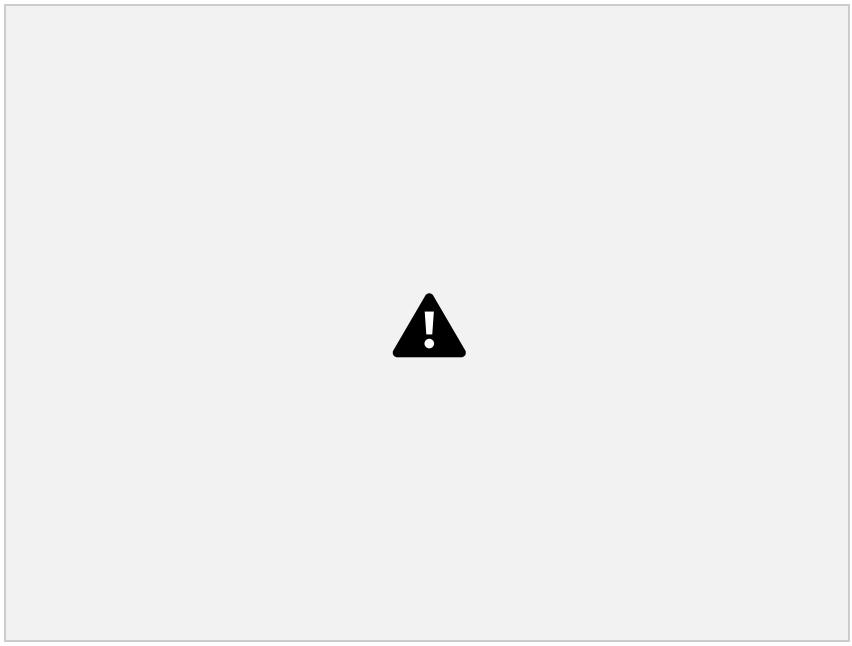
9. En la consola se adiciona una imagen en el usb para que se puede visualizar la imagen a revisar



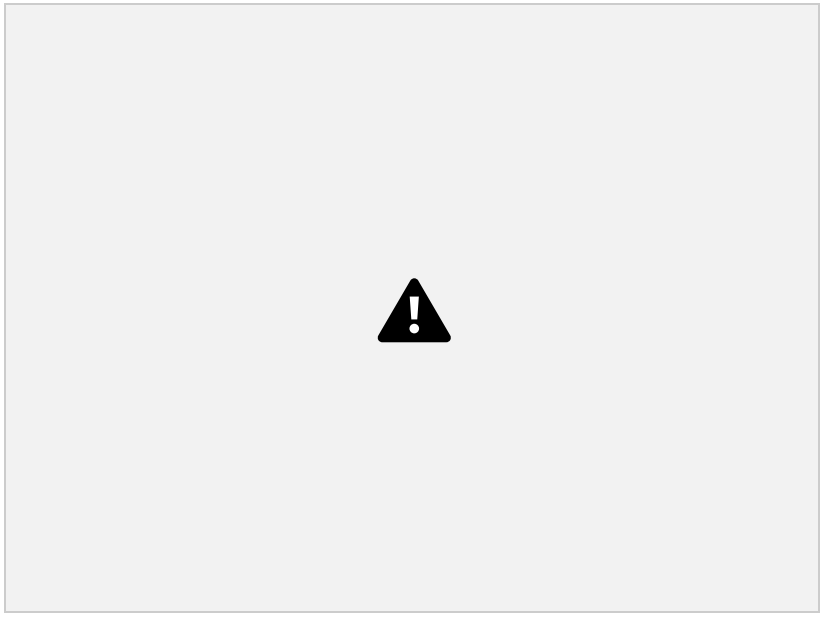
10. Se vuelve a el caso y se coloca la ruta anteriormente creada



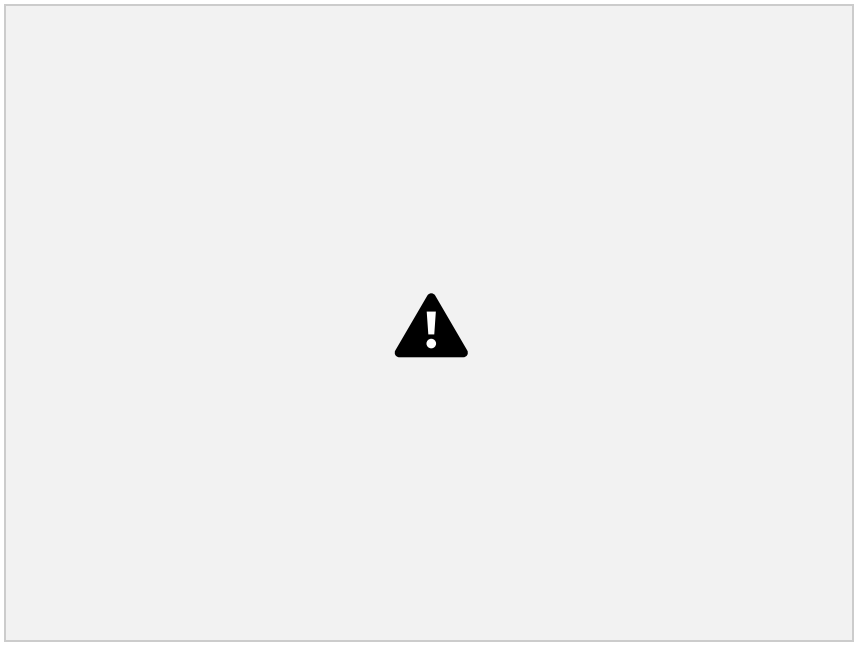
11. Se detallan cual método se va a utilizar para verificar la integridad de la imagen cargada, en este caso escogemos calculate y Add



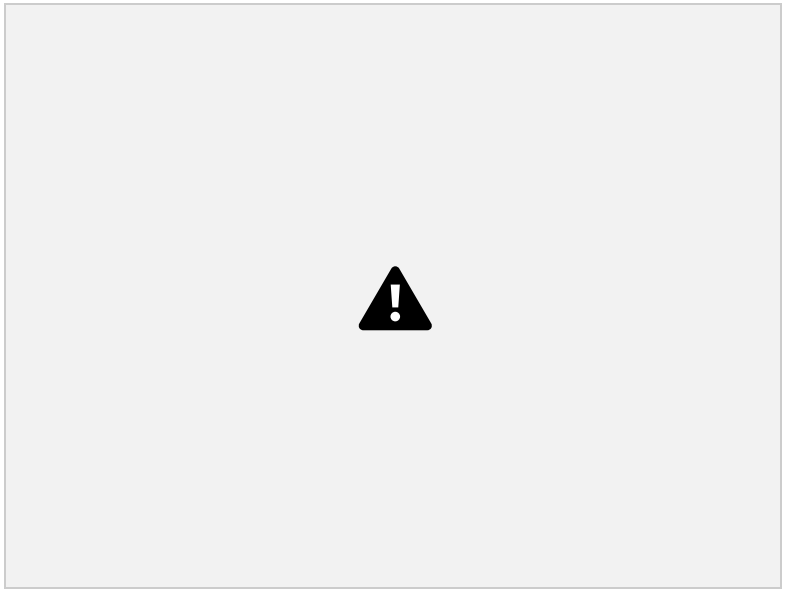
12. Se verifica que se haiga cargado correctamente la imagen



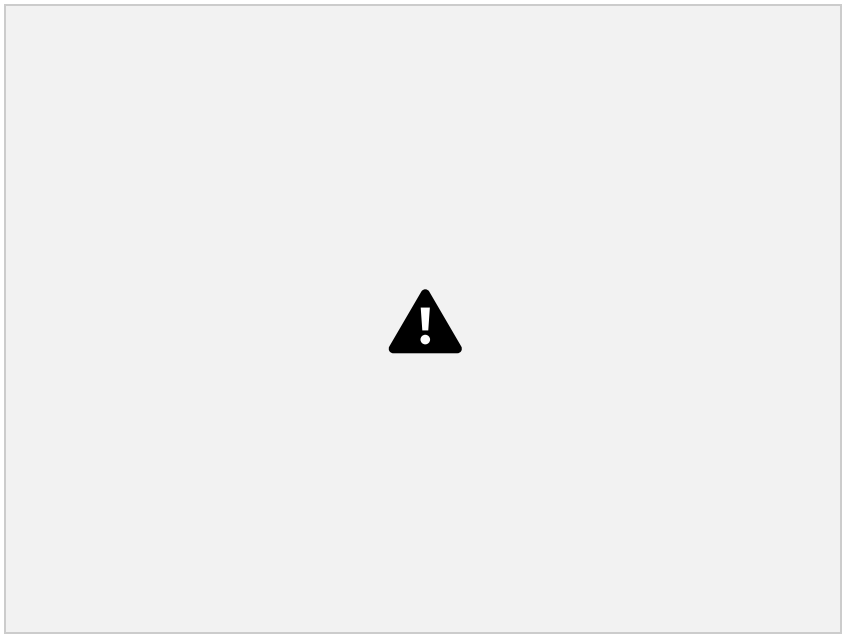
13. En el campo Analyze para que se pueda ver que existe en la imagen



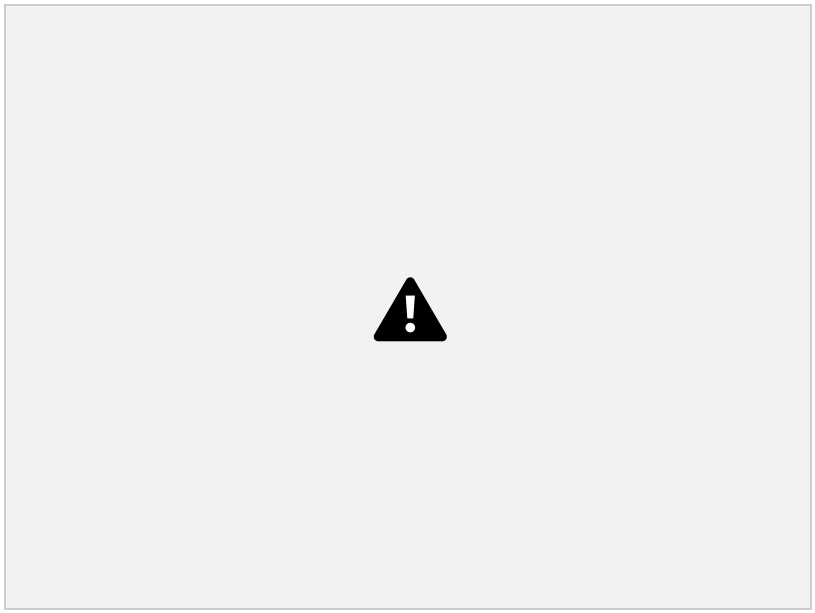
14. En esta pantalla se visualiza lo que contiene la imagen examinada



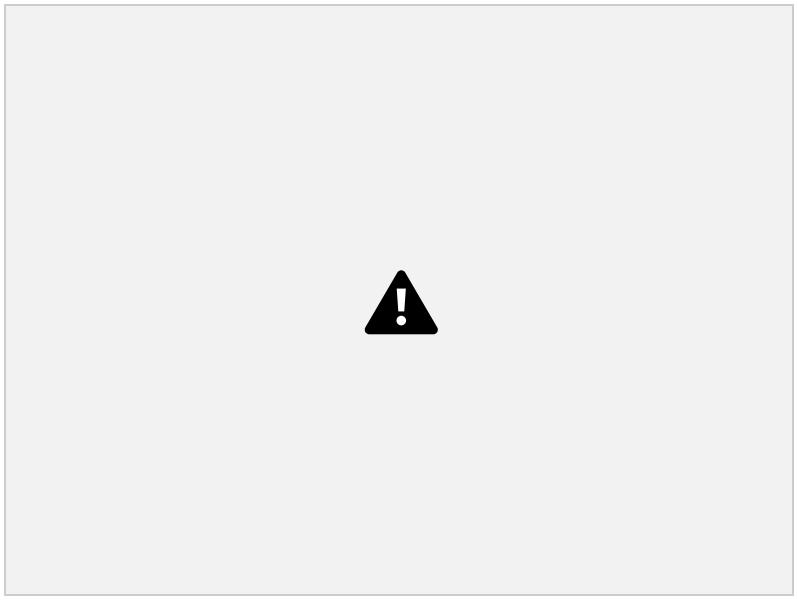
15. Para poder analizar una fecha específica se puede realizar por la opción File Activity Time Line. Al ingresar a esta opción se selecciona la imagen a analizar y Ok



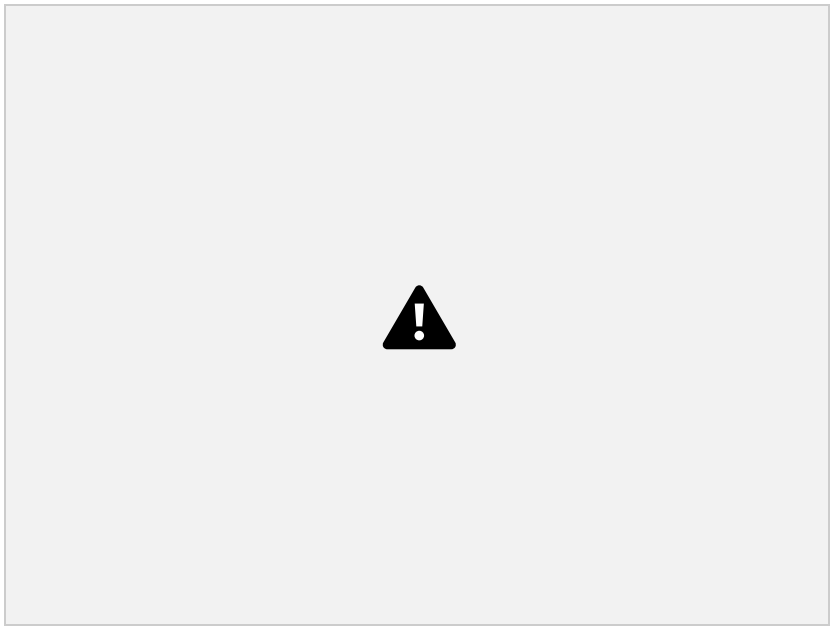
16. Se visualiza el time line que se esta creando



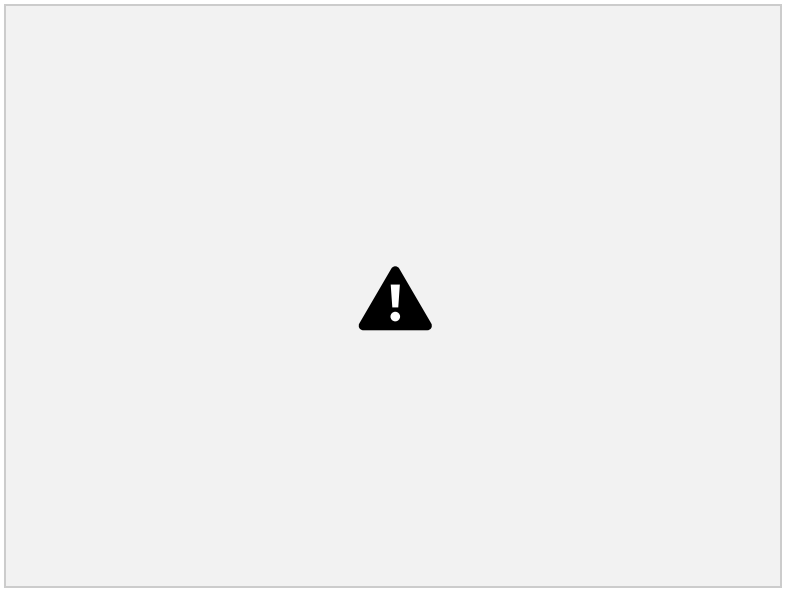
17. Se selecciona el rango de fechas a revisar

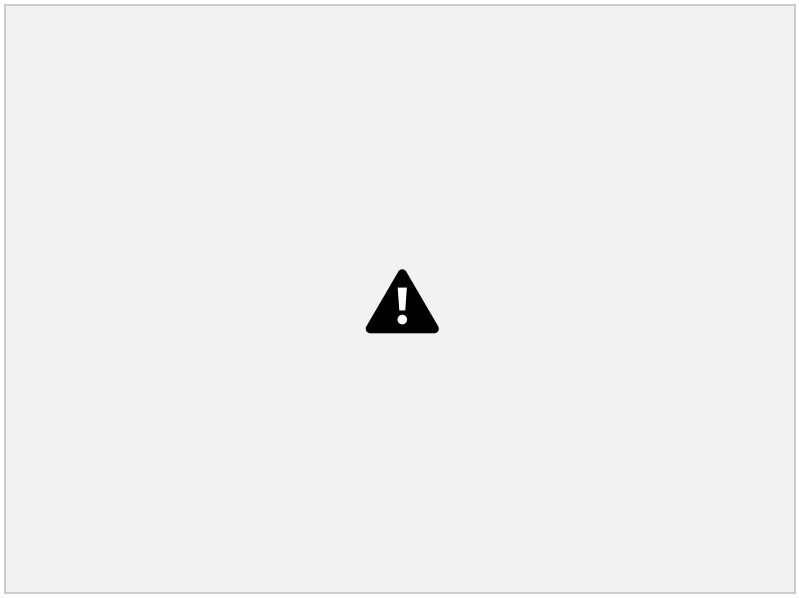


18. Se visualiza el time line que se creo



19. Estos son los archivos que se encuentran en el rango de fechas especificadas y los cuales se va a investigar





CONCLUSION

Se concluye basándome en la evidencia encontrada en la forensia de la imagen proporcionada

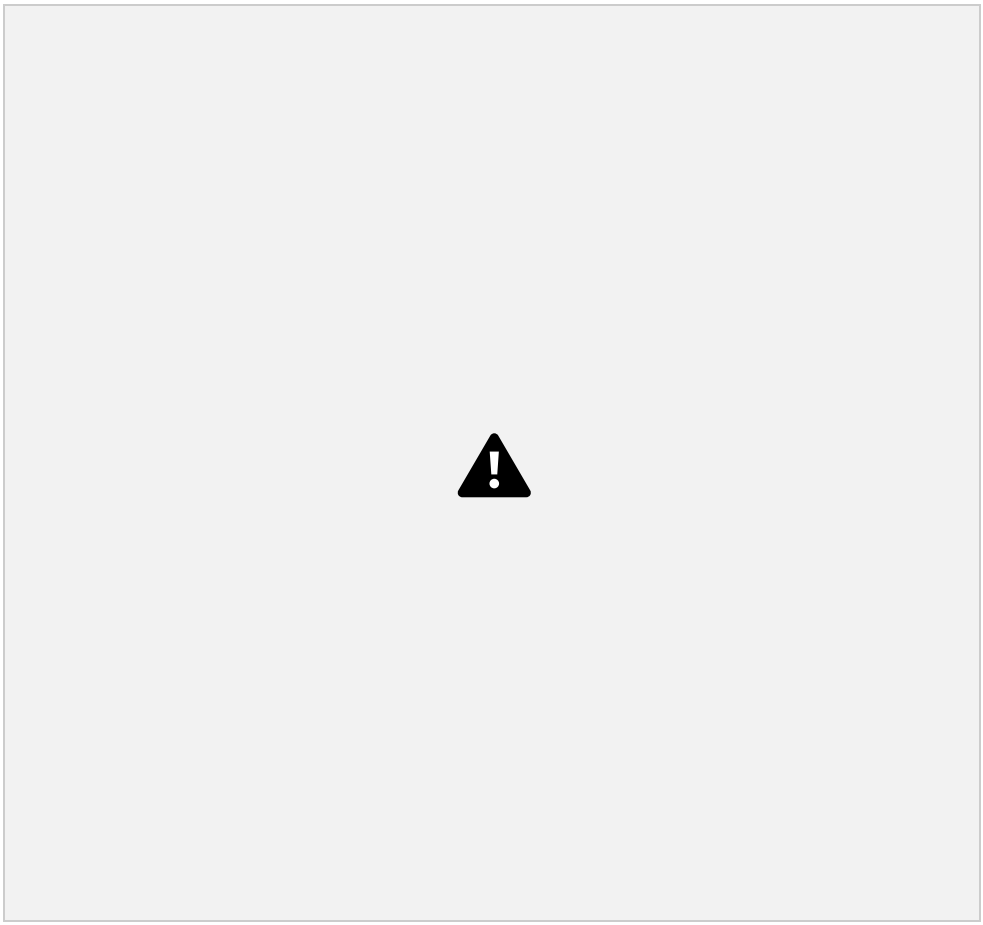
por la empresa Artmuebles, se evidencio que el Sr Pablo Casare quien labora en la empresa en los rangos de Fecha de Agosto de 2010 hasta la fecha de 14 de Octubre de 2010, lo siguiente

- El computador del Sr Pablo Casare se evidencia que se enviaban correos a su novia con fotos de Perros donde se adjuntaba los diseños de los muebles
- También se encontró el programa Xiao Stenography el cual es utilizado para ocultar información dentro de imágenes

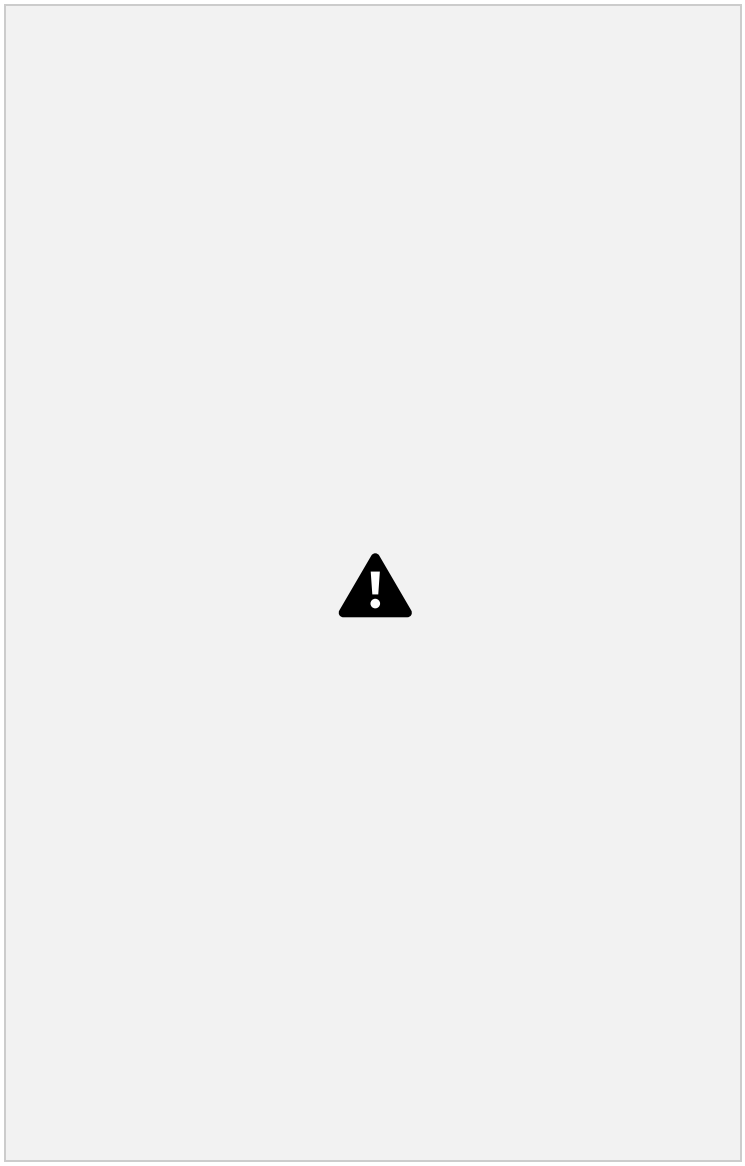
OBSERVACIONES

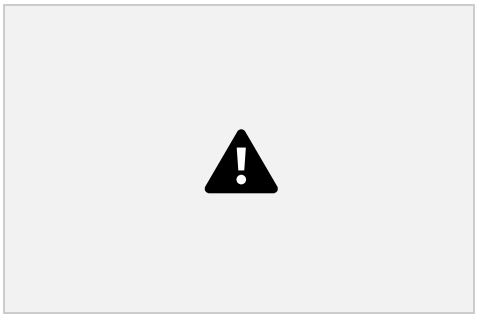
Se observa que el Sr Pablo Casare es dueño y que utiliza el computador, no se encontró evidencia que otra persona haiga accedido a este.

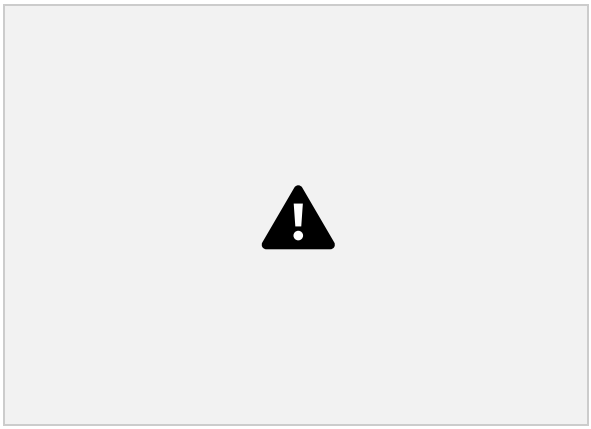
EVIDENCIA ENCONTRADA

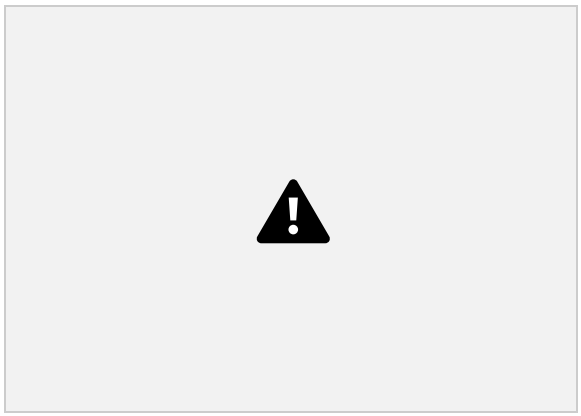


Se revisó la siguiente imagen encontrando oculta el documento Work con los diseños

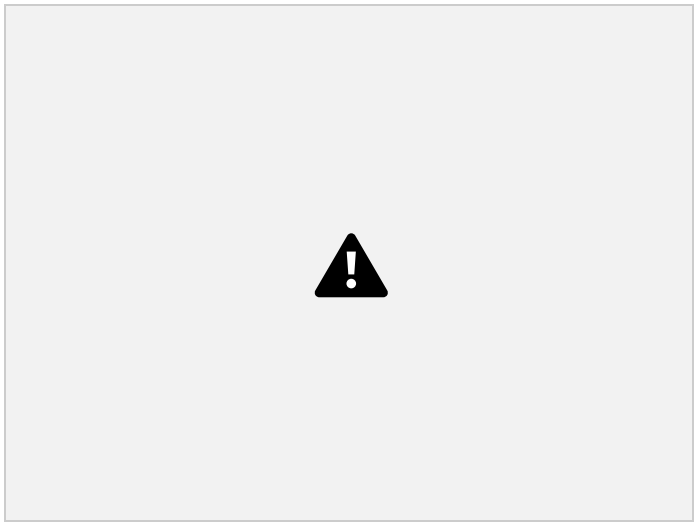


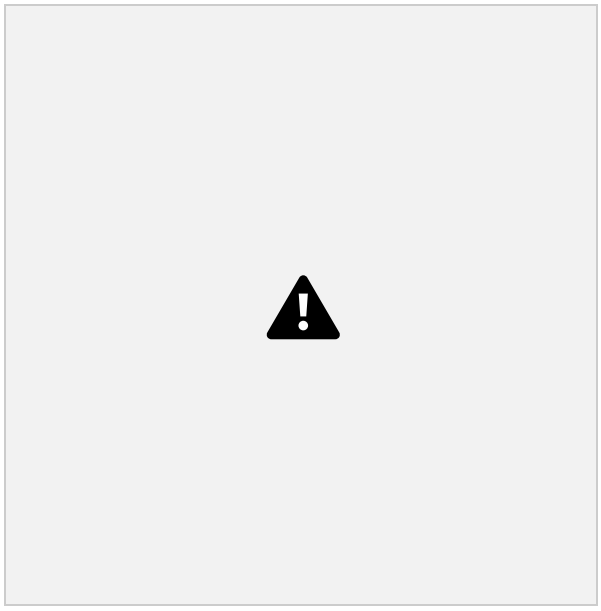


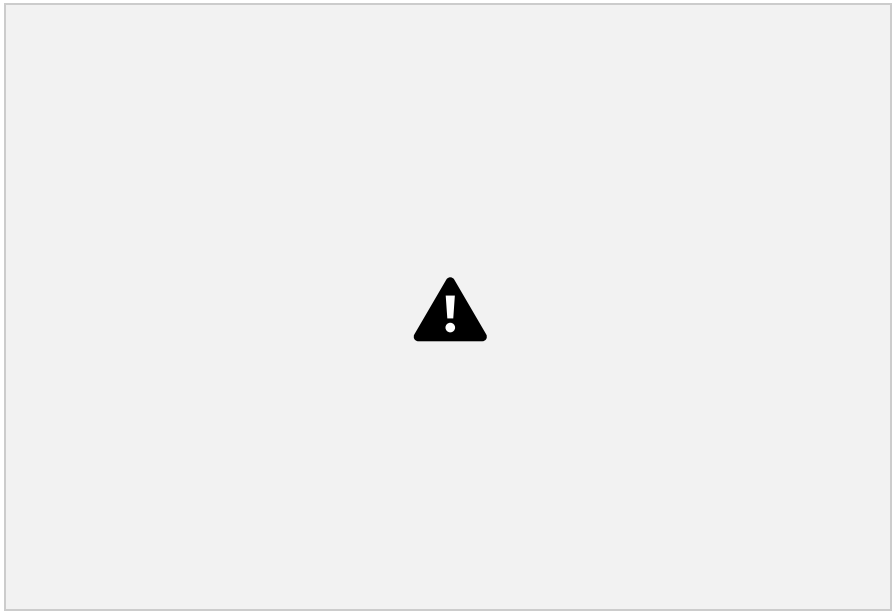




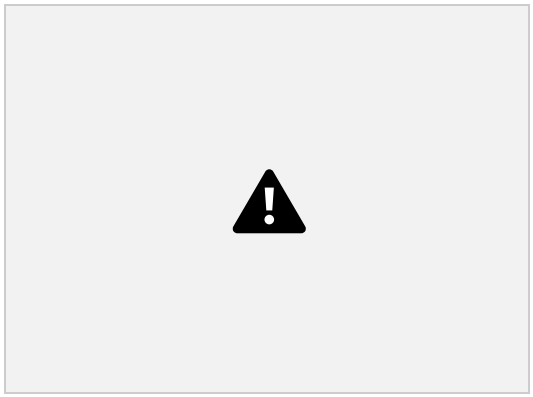
Diseños ArtMUebles

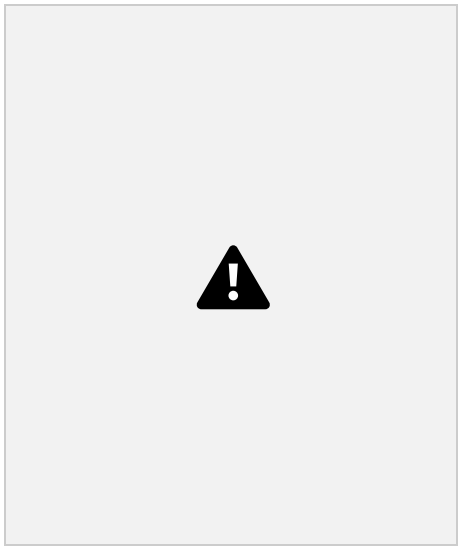


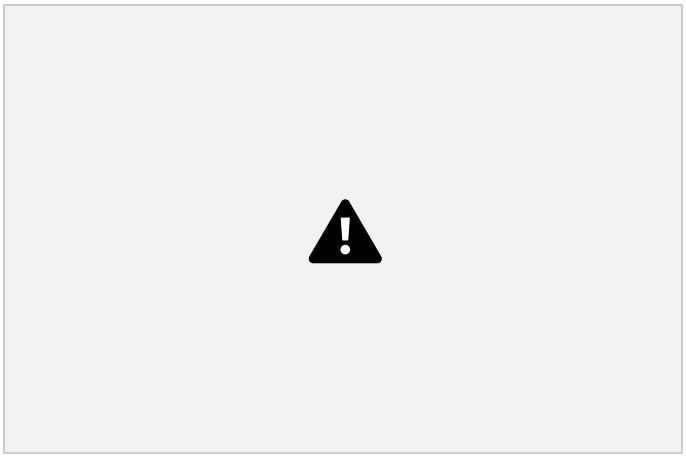


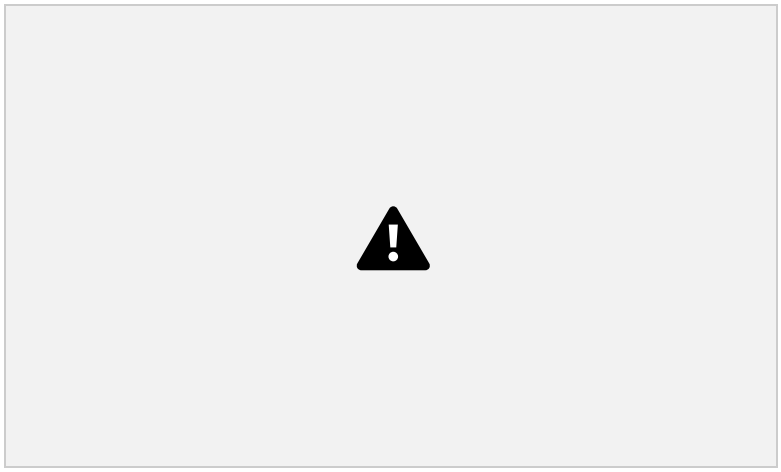


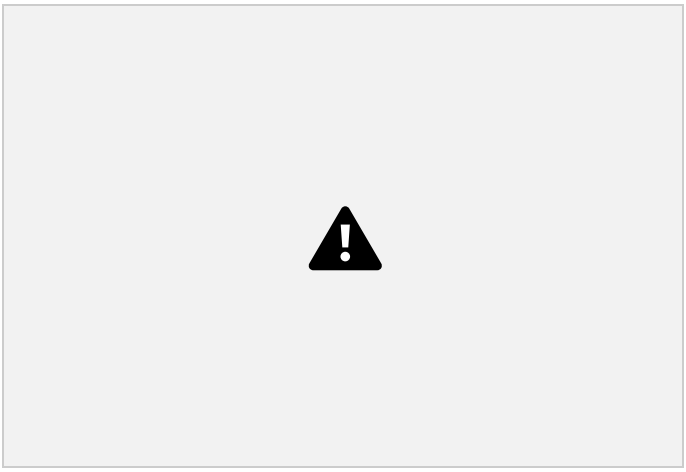
Se evidencia que en la foto superior tiene encriptado un documento con los diseño de los muebles











Las demás imágenes no tienen información oculta. Adicional se encontraron 3 canciones las cuales no tienen información oculta.