Servicio Secreto de los Estados Unidos (USSS)

ANÁLISIS FORENSE INFORMÁTICO BÁSICO

REVISIÓN INICIAL DE LAS IMÁGENES INCAUTADAS

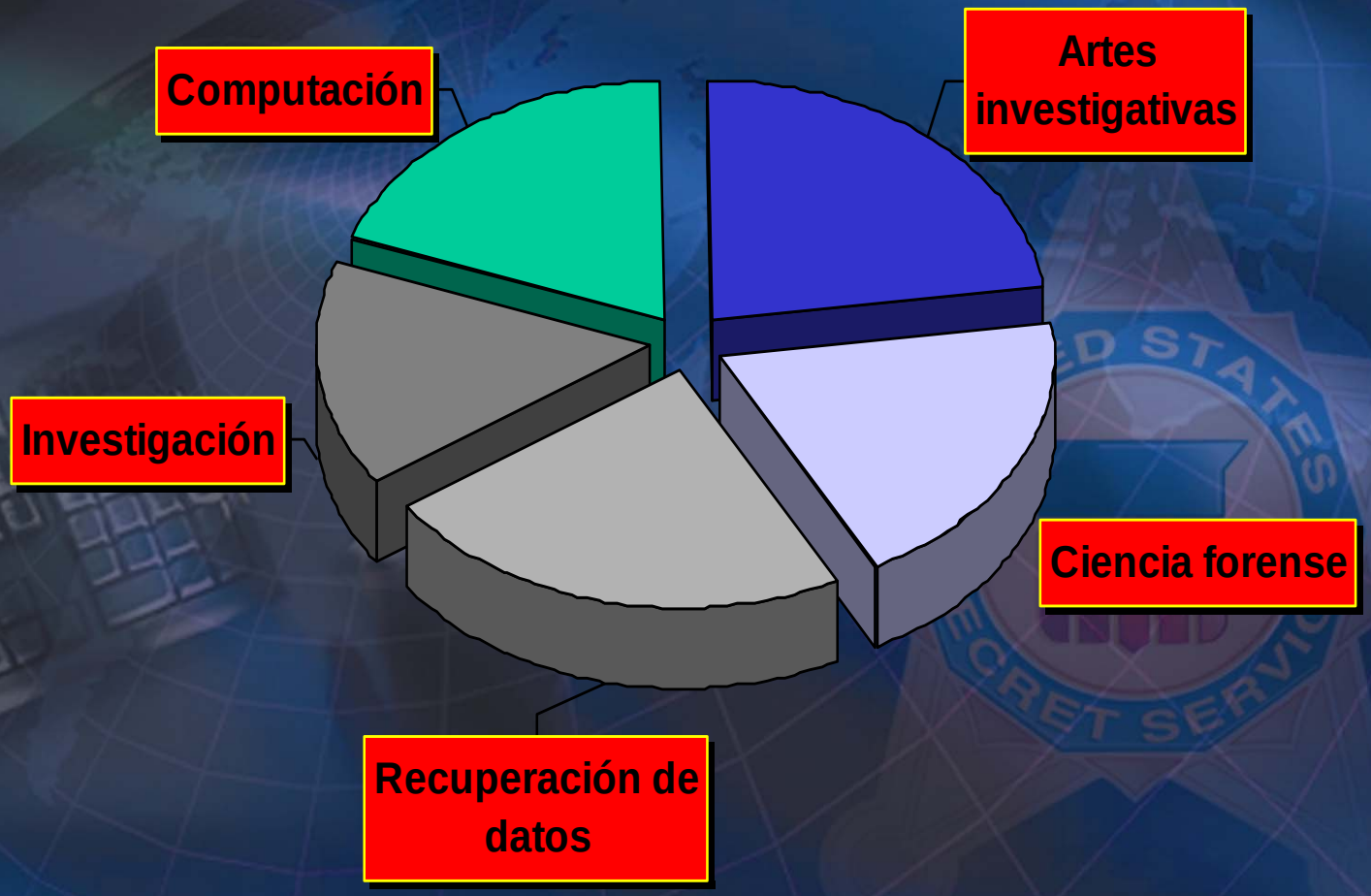
Agente Especial
Jeffrey A. Hill
Jeff.Hill@usss.dhs.gov
Oficina de Campo de Miami

MECTF@usss.dhs.gov

Definición del análisis forense digital

La preservación, identificación, extracción, análisis e interpretación de los datos digitales, hechos con la intención de que los hallazgos sean presentados ante un tribunal.

¿Qué es el análisis forense informático?



Análisis forense informático práctico

- **Muestra pruebas directas en el equipo.**
- **Asocia un equipo con los datos controvertibles.**
- **Muestra pistas de la investigación.**
- **Muestra pruebas circunstanciales que confirman o refutan las alegaciones o las coartadas.**
- **Muestra pruebas derivadas del comportamiento.**

Análisis forense informático práctico

- **Exige que haya una relación con la investigación suficientemente cercana como para entender las metas y las sutilezas del análisis.**

Exige que haya distancia suficiente para permanecer objetivo e imparcial.

Competencia + Objetividad + Confiabilidad = Buen análisis forense

Análisis forense informático aplicado

El uso de la computadora *como una herramienta* o como un arma

El uso de la computadora *como un depósito* de pruebas

El uso de la computadora como un *instrumento de comunicación*

El uso de la computadora *como un blanco* u objetivo

Problemas de almacenamiento en el disco duro

- Aumenta dramáticamente el tiempo que se tarda en adquirir una imagen del disco sospechoso.
- Genera problemas severos al archivar imágenes de los discos duros sospechosos. (Un disco duro de 80 GB ocupará 128 CD-ROMs sin compresión.)
- Limita de manera importante la habilidad de los investigadores para realizar búsquedas en las pruebas digitales.
- Aumenta en gran medida el tiempo necesario para completar un análisis forense informático.

¿QUÉ PODEMOS ENCONTRAR DURANTE EL ANÁLISIS?

-ARCHIVOS BORRADOS

-FRAGMENTOS DE TEXTO

-META-ARCHIVOS MEJORADOS (ENHANCED): ARCHIVOS IMPRESOS CON ANTERIORIDAD

-META-DATOS MEJORADOS (ENHANCED): INFORMACIÓN INCRUSTADA

-INFORMACIÓN SOBRE LA ESTAMPILLA DE FECHA Y HORA

-MENSAJES DE CORREO ELECTRÓNICO Y REGISTROS DE CHAT

-INFORMACIÓN SOBRE EL USO DE INTERNET (HISTORIAL)

-DIVERSOS ARCHIVOS GUARDADOS Y COMPRIMIDOS (ZIP)

-DOCUMENTOS DE ENCRIPTACIÓN BASE 64, ADJUNTOS A LOS CORREOS ELECTRÓNICOS

-IMÁGENES (ACTIVADAS Y BORRADAS)

Consideraciones sobre la volatilidad

- **Remoción o transferencia de archivos**
- **Destrucción o remoción de discos**
- **Destrucción intencional de datos**

Conciencia de las pruebas digitales

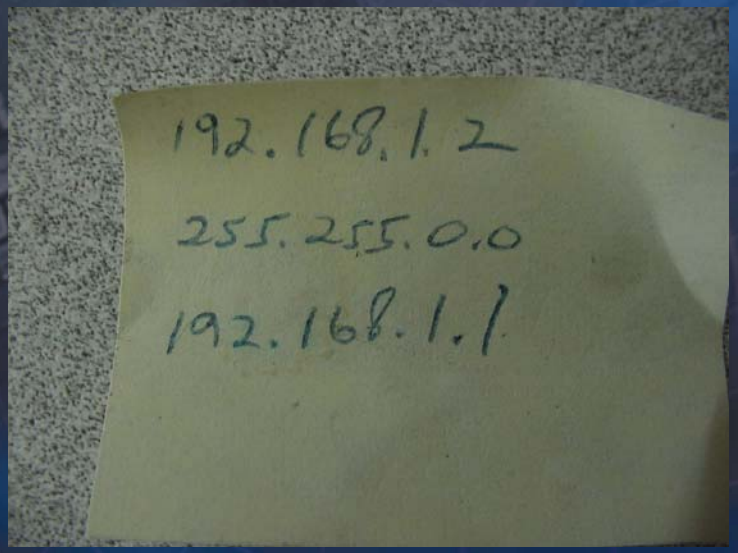
¡El mayor error que un oficial o investigador puede cometer consiste en dejar de ver las posibilidades probatorias!

Conciencia de las pruebas digitales

- Piensen en la computadora como una herramienta de comunicación
- Piensen en la computadora como un diario personal o como un registro de actividades
  - ¿Diario de intereses?
  - ¿Pasatiempos?
  - ¿Aficiones a la hora de comprar?
  - ¿Pensamientos – fantasías?

Conciencia de las pruebas digitales

- **Pruebas no-electrónicas**
  - Huellas dactilares
  - Cabello
  - Fluidos corporales (¿usar guantes?)



Sellos de garantía del caso

Cuentas y otros datos impresos

Información sobre la salida del teléfono

Papel (con claves)

REVISIÓN INICIAL DE UNA IMAGEN INCAUTADA

Proceso inicial de revisión

- HITOS

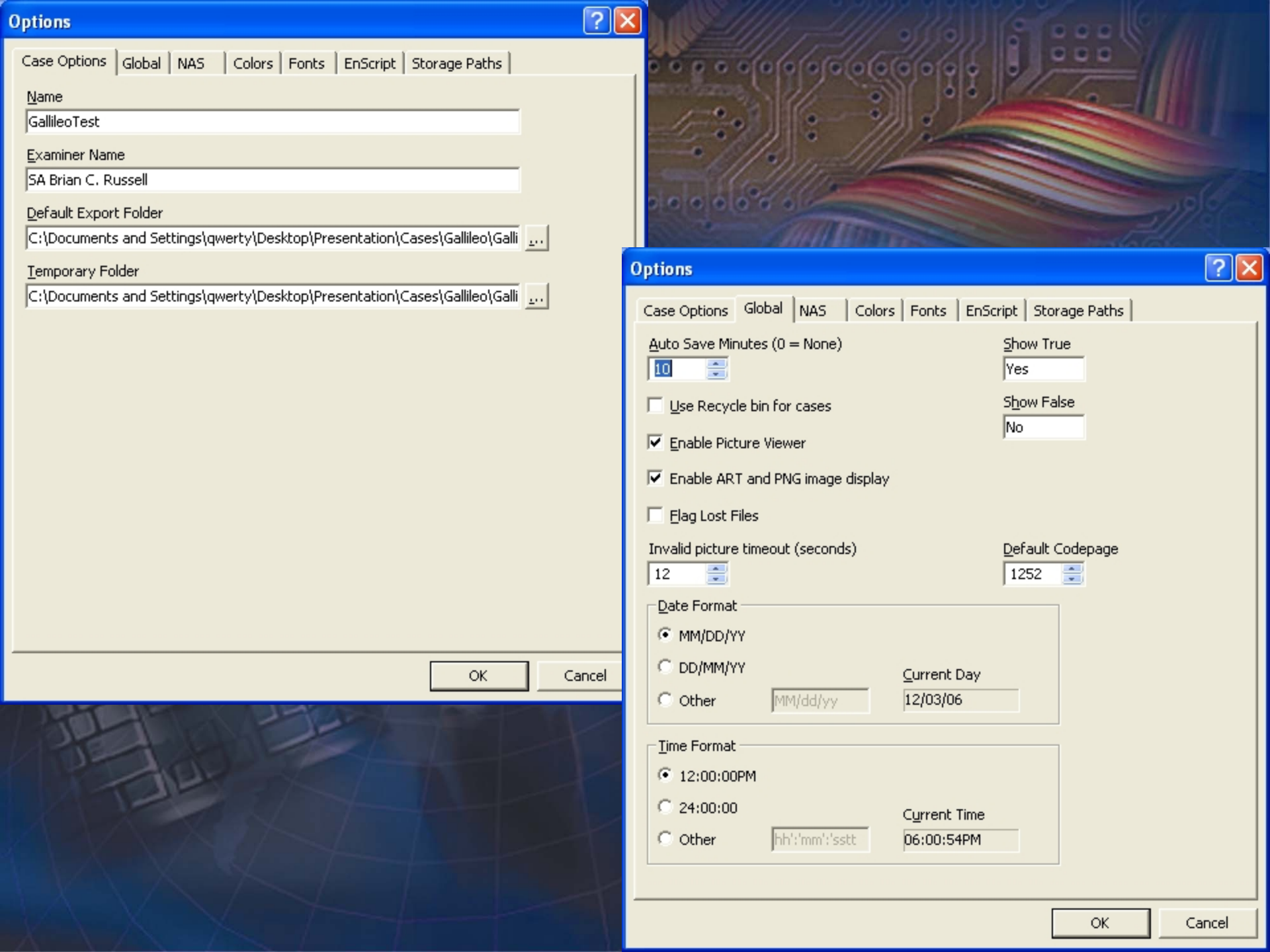
- ***¡¡¡Siéntese con el agente asignado al caso para determinar el alcance de la investigación!!!***
- Identificar la facultad legal para revisar los medios (orden de un juez, consentimiento, otros ….)
- Obtener una explicación sobre el caso
- Determinar qué pruebas se espera encontrar en los medios

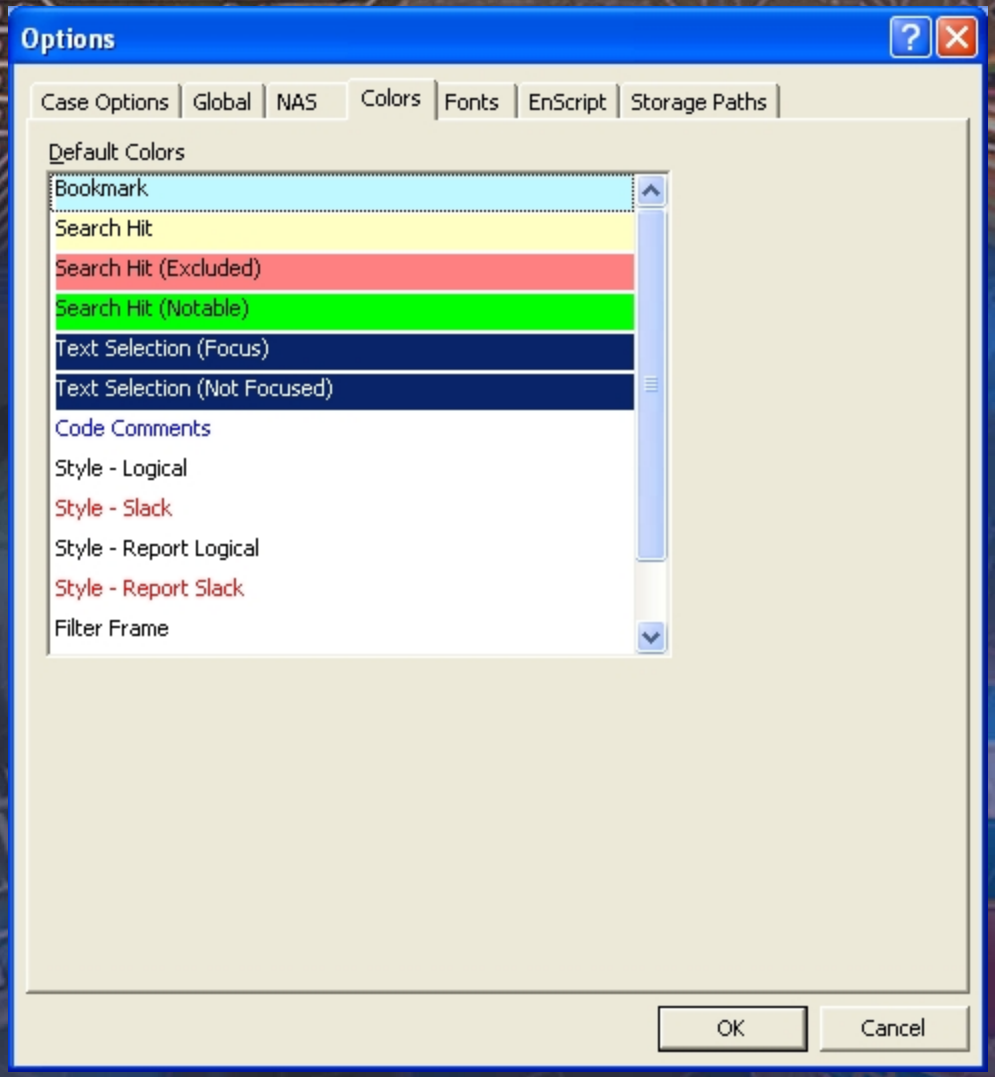
- ***Crear una carpeta de destino en el disco duro de la computadora forense o de análisis***
- Identificar qué disco almacenará el archivo de imagen del disco duro tomado como prueba
- Cree una carpeta en este disco duro para guardar la imagen (normalmente, el disco duro esclavo interno forense)
- En esta carpeta, cree dos carpetas adicionales (***Exportar*** y ***Basura***)

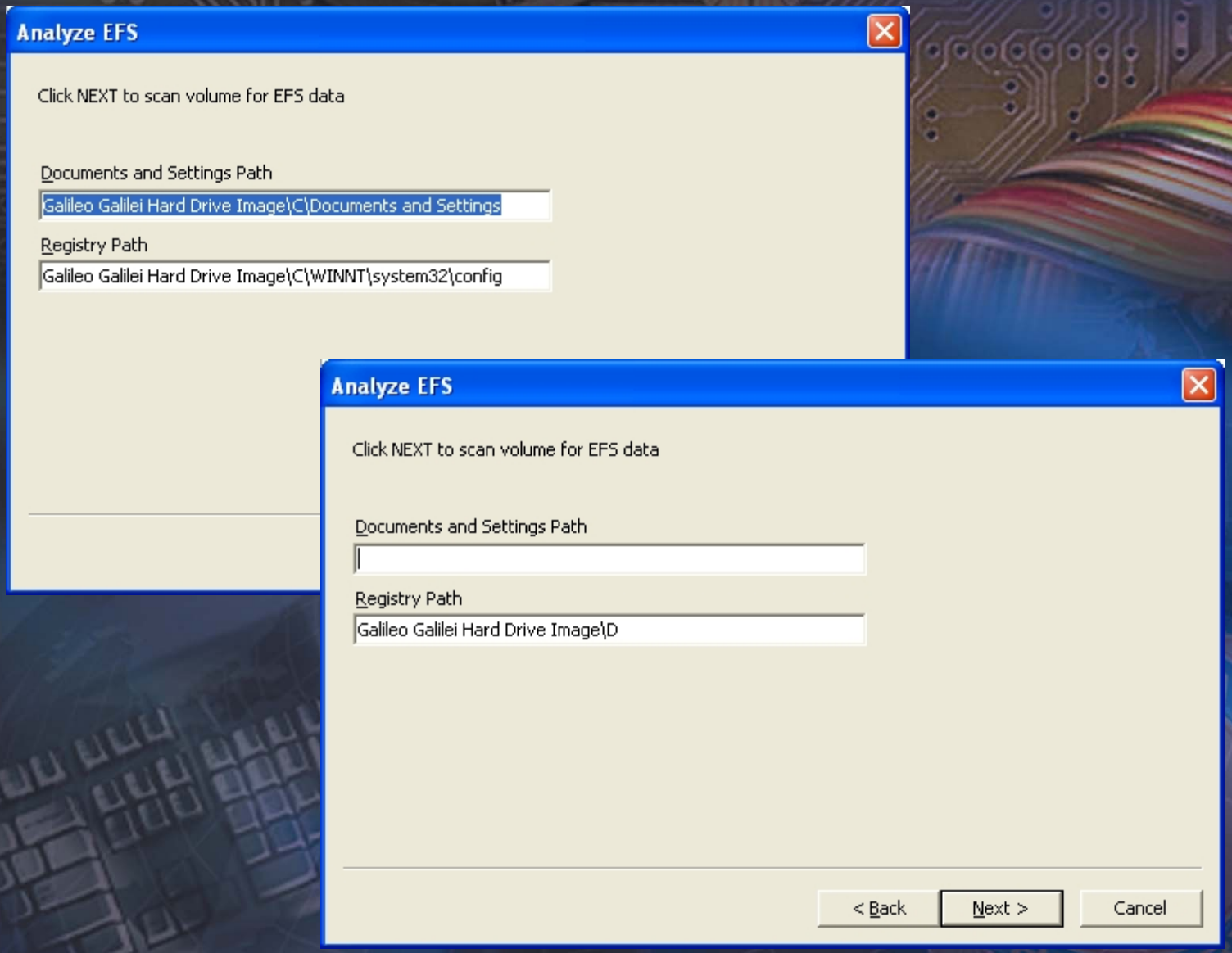
Proceso inicial de revisión

- ***Abra EnCase y Abra Nuevo Caso***
- Empiece bajo ***Archivo*** y luego seleccione ***Nuevo***
- Llene las celdas correspondientes a Crear Nuevo Caso
- Identifique la carpeta estándar para exportar (usando el botón de menú descolgante, identifique la carpeta ***Exportar*** creada al inicio de este proceso)
- Identifique la carpeta temporal (usando el botón de menú descolgante, identifique la carpeta ***Basura*** creada al inicio de este proceso)
- Llene las celdas correspondientes a Crear Nuevo Caso

- ***Añada Archivo de Pruebas***
- Empiece bajo ***Archivo*** y luego seleccione ***Añadir*** y ***Archivo de Pruebas***
- Escoja el archivo de pruebas creado durante el proceso de adquisición


Options
Case Options
Global
NAS
Colors
Fonts
EnScript
Storage Paths
Name
GallileoTest
Examiner Name
SA Brian C. Russell
Default Export Folder
C:\Documents and Settings\qwerty\Desktop\Presentation\Cases\Gallileo\Galli
Temporary Folder
C:\Documents and Settings\qwerty\Desktop\Presentation\Cases\Gallileo\Galli
OK
Cancel
Options
Case Options
Global
NAS
Colors
Fonts
EnScript
Storage Paths
Auto Save Minutes (0 = None)
10
Use Recycle bin for cases
Enable Picture Viewer
Enable ART and PNG image display
Flag Lost Files
Invalid picture timeout (seconds)
12
Show True
Yes
Show False
No
Default Codepage
1252
Date Format
MM/DD/YY
DD/MM/YY
Other
MM/dd/yy
Current Day
12/03/06
Time Format
12:00:00PM
24:00:00
Other
hh':'mm':'sstt
Current Time
06:00:54PM
OK
Cancel

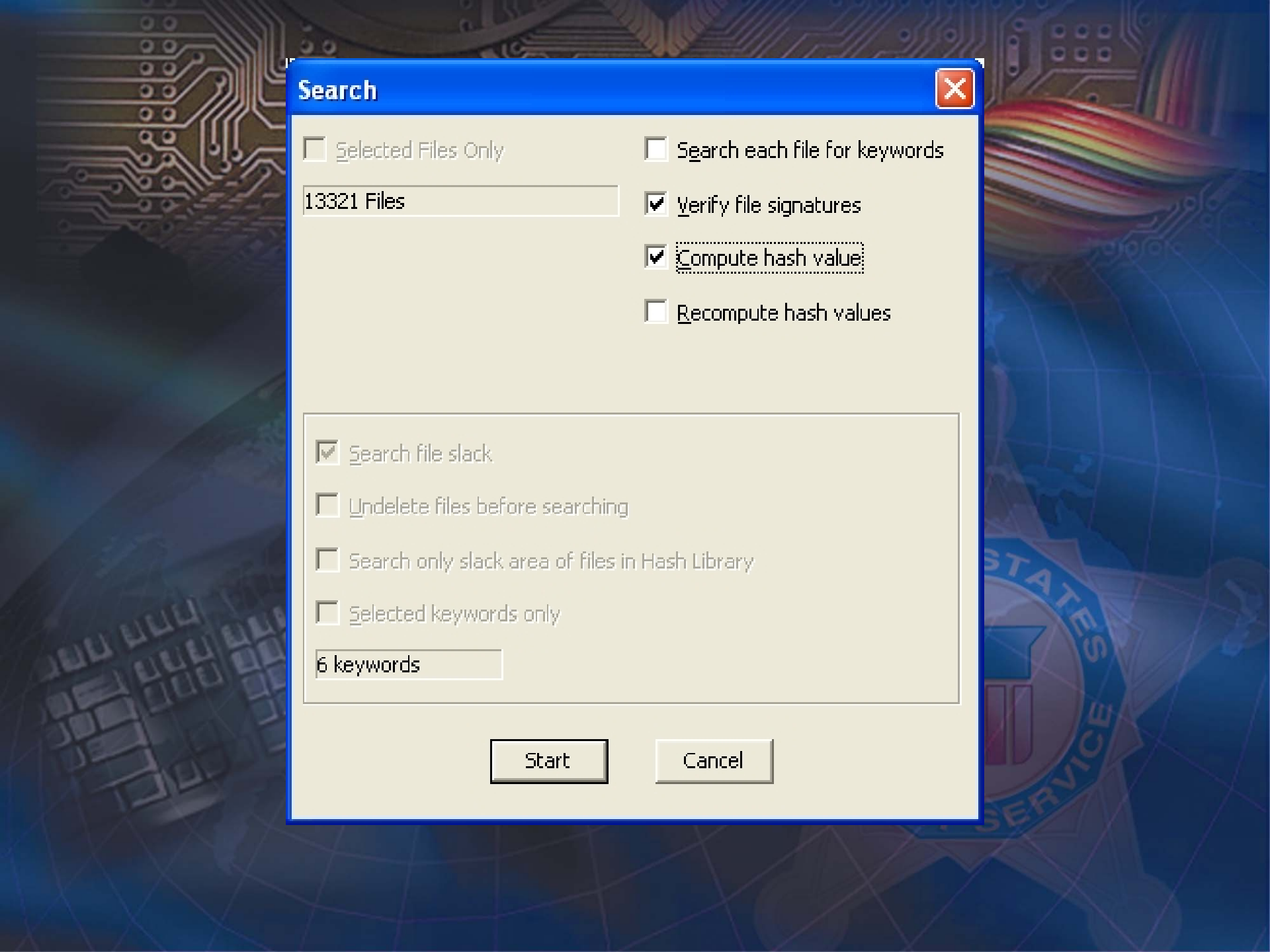

Options
Case Options
Global
NAS
Colors
Fonts
EnScript
Storage Paths
Default Colors
Bookmark
Search Hit
Search Hit (Excluded)
Search Hit (Notable)
Text Selection (Focus)
Text Selection (Not Focused)
Code Comments
Style - Logical
Style - Slack
Style - Report Logical
Style - Report Slack
Filter Frame
OK
Cancel


Analyze EFS
Click NEXT to scan volume for EFS data
Documents and Settings Path
Galileo Galilei Hard Drive Image\C\Documents and Settings
Registry Path
Galileo Galilei Hard Drive Image\C\WINNT\system32\config
Analyze EFS
Click NEXT to scan volume for EFS data
Documents and Settings Path
Registry Path
Galileo Galilei Hard Drive Image\D
< Back
Next >
Cancel

Proceso inicial de revisión

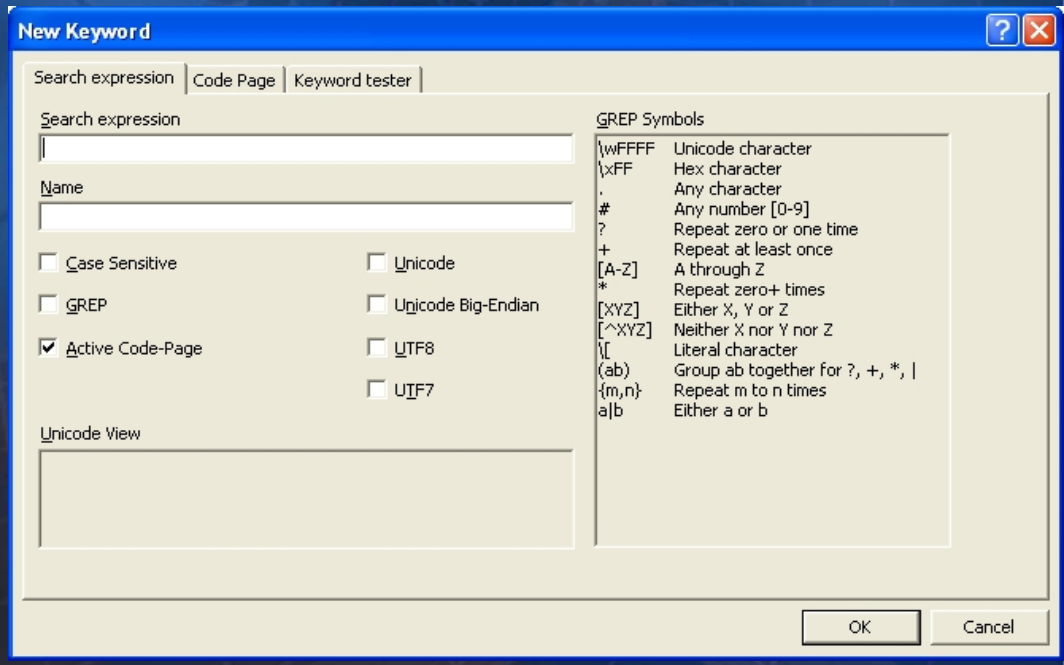
- ***Recuperar las carpetas perdidas***
- Haga click en el volumen en el que quiera buscar, con el botón **derecho** del mouse (es necesario buscar en cada volumen por separado)
- Seleccione ***Recuperar Carpetas***
- Revise la información resultante listada en la carpeta virtual Carpetas Recuperadas, ubicada en la parte inferior del directorio del volúmenes

- ***Calcule los valores de dispersión (*hash*) / Firmas (se usan para filtrar los archivos conocidos)***
- Empiece bajo ***Herramientas*** y luego seleccione ***Buscar***
- Escoja ***Verificar archivos de firma*** y ***Calcular el valor hash***, luego ***Empezar análisis***
- Revise la información resultante listada en la ventana ***Tabla*** en EnCase


Search
Selected Files Only
13321 Files
Search each file for keywords
Verify file signatures
Compute hash value
Recompute hash values
Search file slack
Undelete files before searching
Search only slack area of files in Hash Library
Selected keywords only
6 keywords
Start
Cancel

Proceso inicial de revisión

- ***Realice búsquedas por palabra clave / GREP***
- Se encuentra en la sección ***Palabras clave*** del programa EnCase
- Se usa normalmente para identificar las instancias de:
- Nombres de víctimas
- Nombres de sospechosos
- Números de seguridad social
- Números de tarjeta de crédito
- Números telefónicos
- Otros identificadores misceláneos



Proceso inicial de revisión

- ***Realizar búsquedas por E-Script***
- Diseñado para obtener información oculta, borrada, o no-asignada (*unallocated*)
- Archivos comunes que exigen búsquedas por E-Script:
- Archivos .EMF (documentos impresos con anterioridad, que ya no están visibles en la estructura normal de archivos de un sistema operativo)
- Archivos de imagen borrados (.BMP, .JPG, etc.…)
- Historial de Internet / vínculos (se obtiene de los archivos .DAT de Internet)
- Direcciones de correo electrónico (identificará correos electrónicos con nombres de dominio de 2° o 3er nivel)
- ***Búsquedas por Vista de Galería***
- Útil para identificar rápidamente las imágenes de archivos en medios de almacenamiento más pequeños

Proceso inicial de revisión

- ***Índice de Texto Completo (usando FTK)***
- ***NOTA:*** No lo realice cuando esté añadiendo inicialmente pruebas a un archivo del caso (trabará la computadora de pruebas)
- FTK tiene la capacidad de preparar un índice de todas las cadenas de texto ubicadas en un medio de almacenamiento
- Le permite a un analista adelantar búsquedas de cadenas de caracteres de manera instantánea

- ***Busque archivos de correos electrónicos (usando FTK)***
- FTK tiene una poderosa habilidad propia para recuperar correos electrónicos completos a partir de los medios de almacenamiento
- (es una capacidad mucho más poderosa que la de Encase)

Vínculos en Internet

- MECTF@USSS.DHS.GOV
- www.ectaskforce.org
- www.secretservice.gov
- www.ectf.usss.gov
- www.cert.org
- www.forwardedge2.com
- www.forwardedge2.com/pdf/bestPractices.pdf

Agente Especial
Jeff Hill

Servicio Secreto de los Estados Unidos
Oficina de Campo de Miami
(305) 863-5000
Jeff.Hill@usss.dhs.gov
MECTF@usss.dhs.gov


Q&A
Sesión de preguntas y respuestas