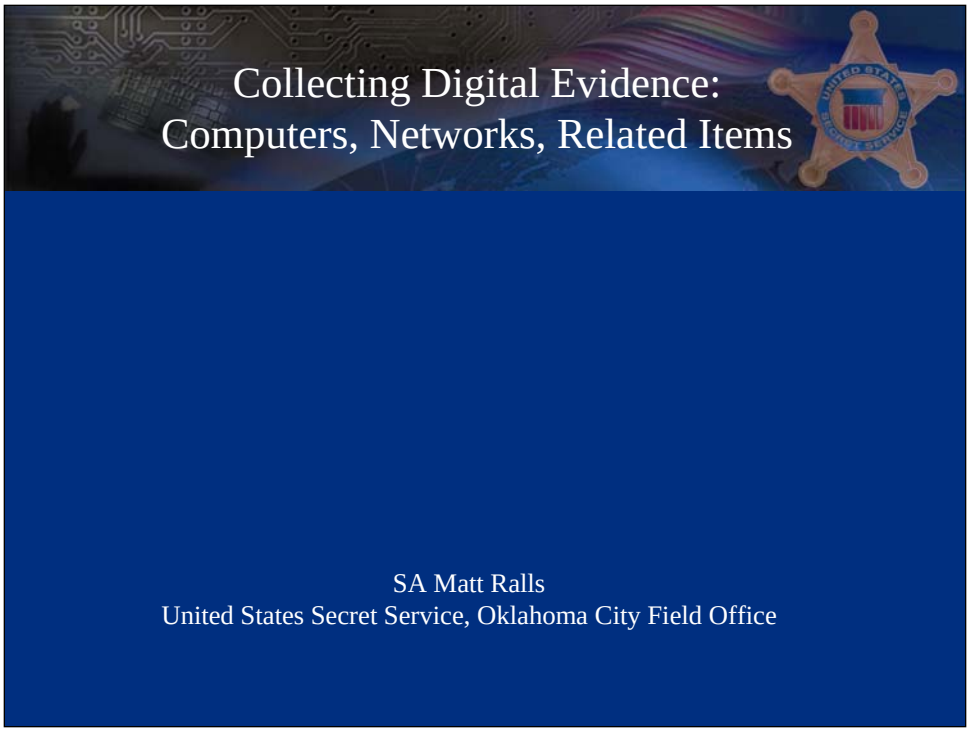


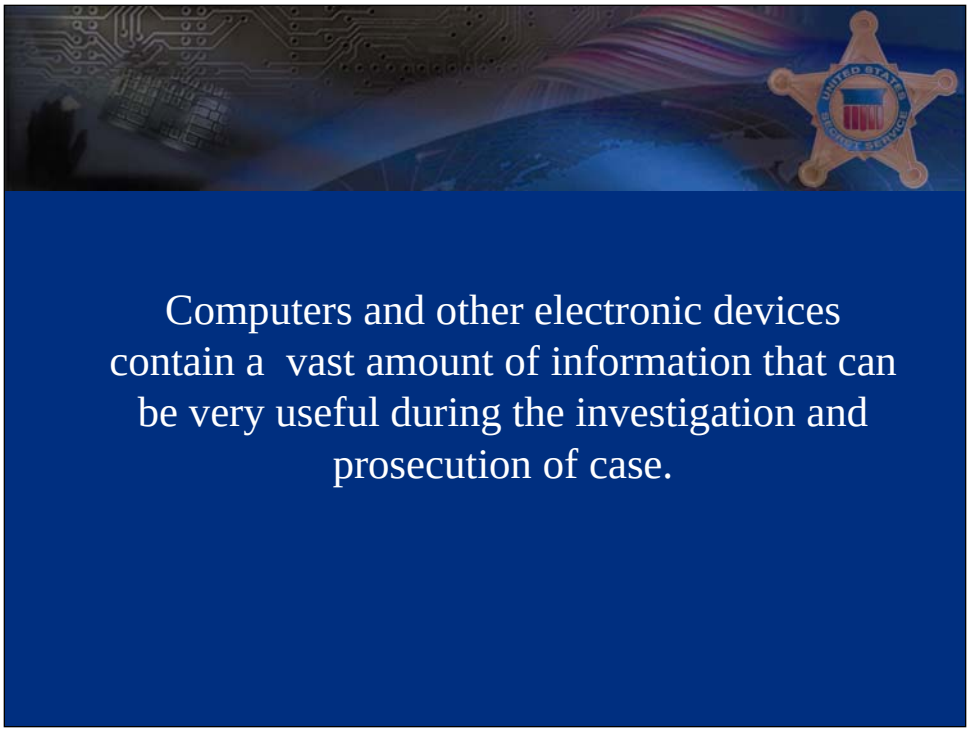
Recolección de evidencia digital

Computadoras, redes, artículos relacionados

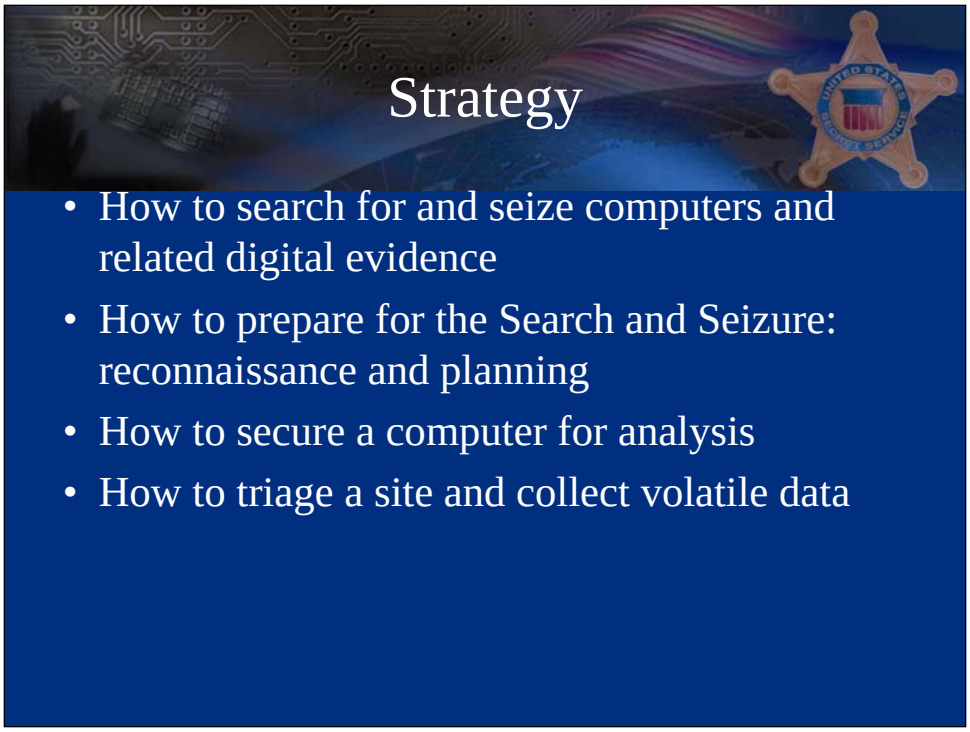
Agregar imagen

Agente Especial Matt Ralls

Servicio Secreto de Estados Unidos, Oficina de Campo de Oklahoma City



Las computadoras y otros artículos electrónicos contienen una enorme cantidad de información la cual puede ser muy útil durante la investigación y enjuiciamiento de un caso.



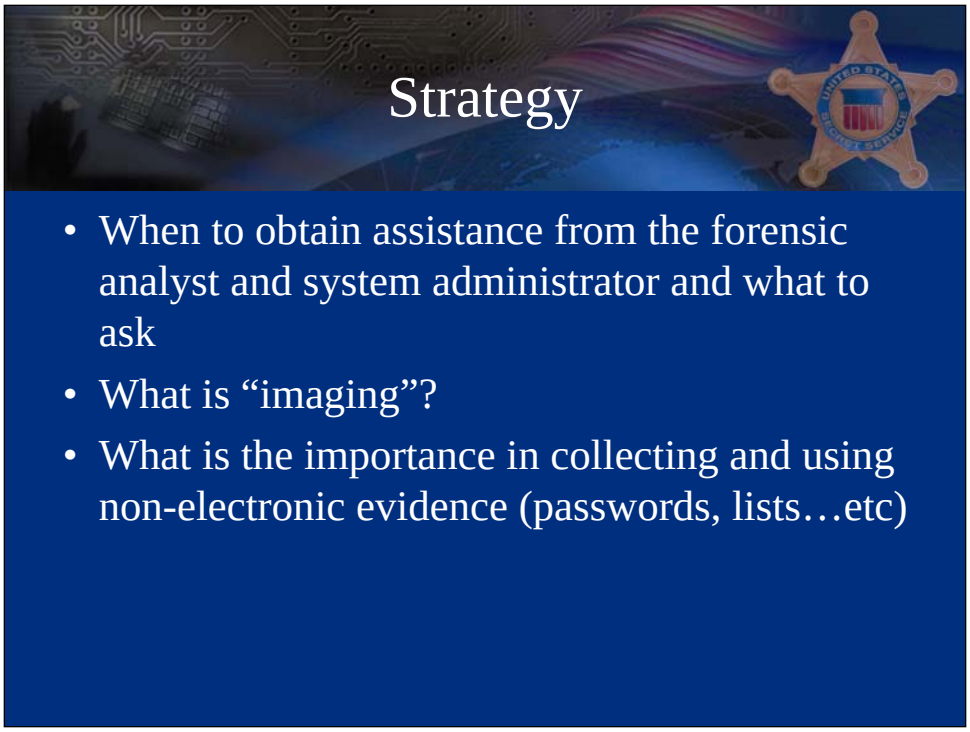
Estrategia

*Cómo buscar y confiscar computadoras y evidencia relacionada

*Cómo prepararse para el registro y confiscación: reconocimiento y la planificación

*Cómo asegurar la computadora para su análisis

*Cómo dar una evaluación preliminar al sitio y recopilar datos volátiles.

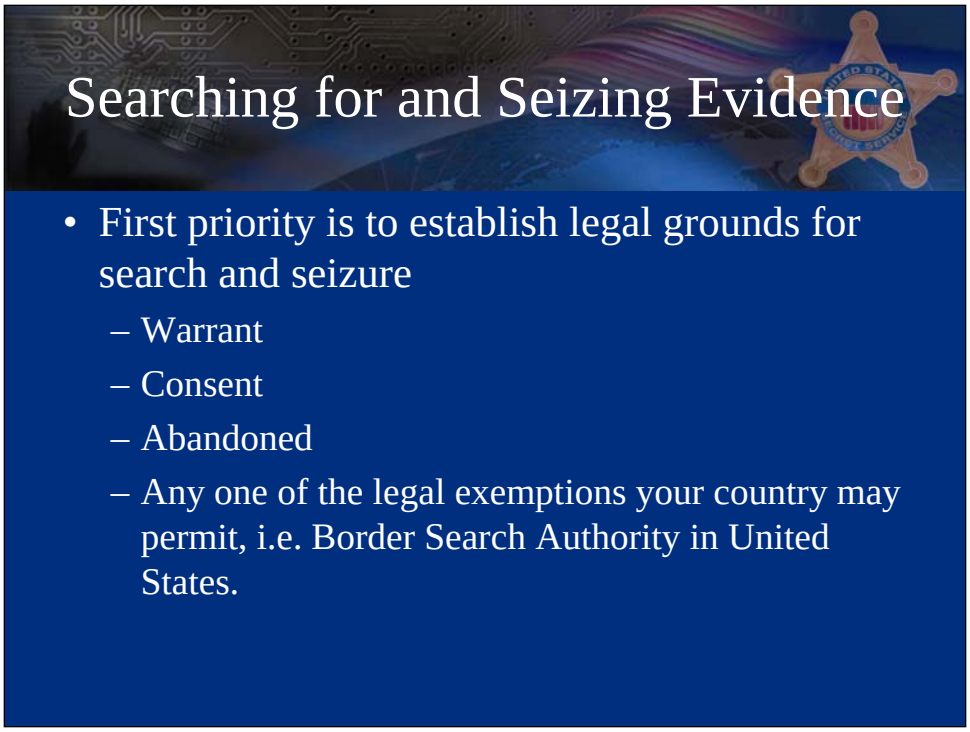


Estrategia

*Cuándo debe buscar asistencia del analista forense y del administrador de sistemas y qué se debe preguntar

*¿Qué es “tomar las imágenes”

*¿Cuál es la importancia de recolectar y usar evidencia no electrónica (contraseñas, registros, etc.)?



Buscar y confiscar evidencia

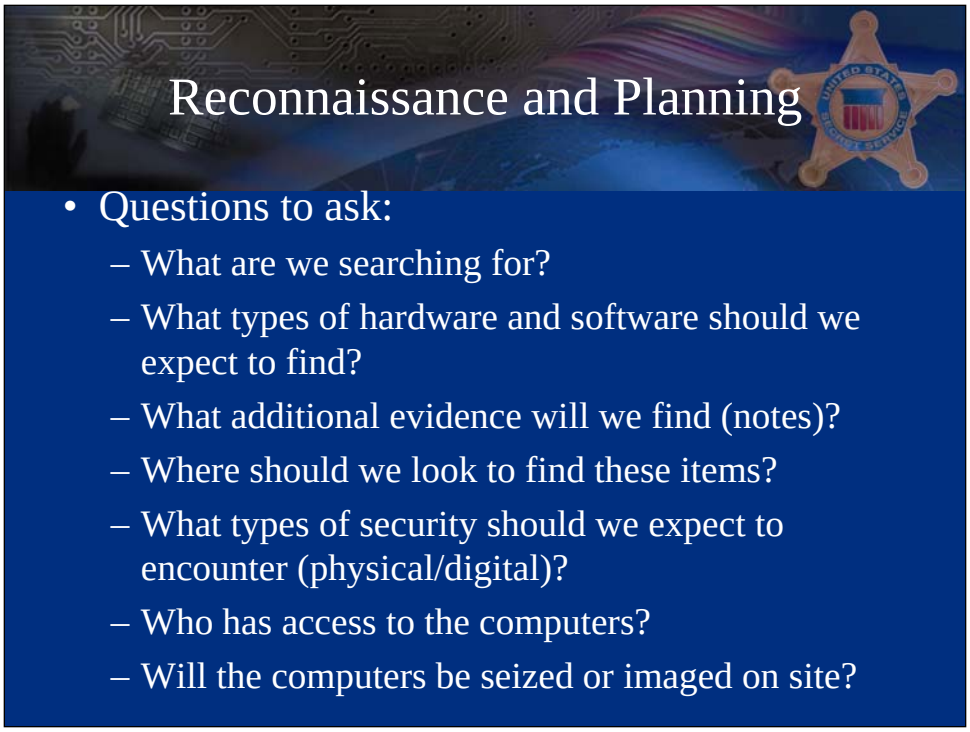
*La primera prioridad es establecer la base legal para poder registrar y confiscar

-orden de cateo

-consentimiento

-abandono

-cualquiera de las exenciones legales que su país permita, es decir, Autoridad de Registro de la Frontera en EE.UU.



Reconocimiento y planificación

*Preguntas que deben hacerse:

-¿Qué estamos buscando?

-¿Qué clases de hardware y software esperamos encontrar?

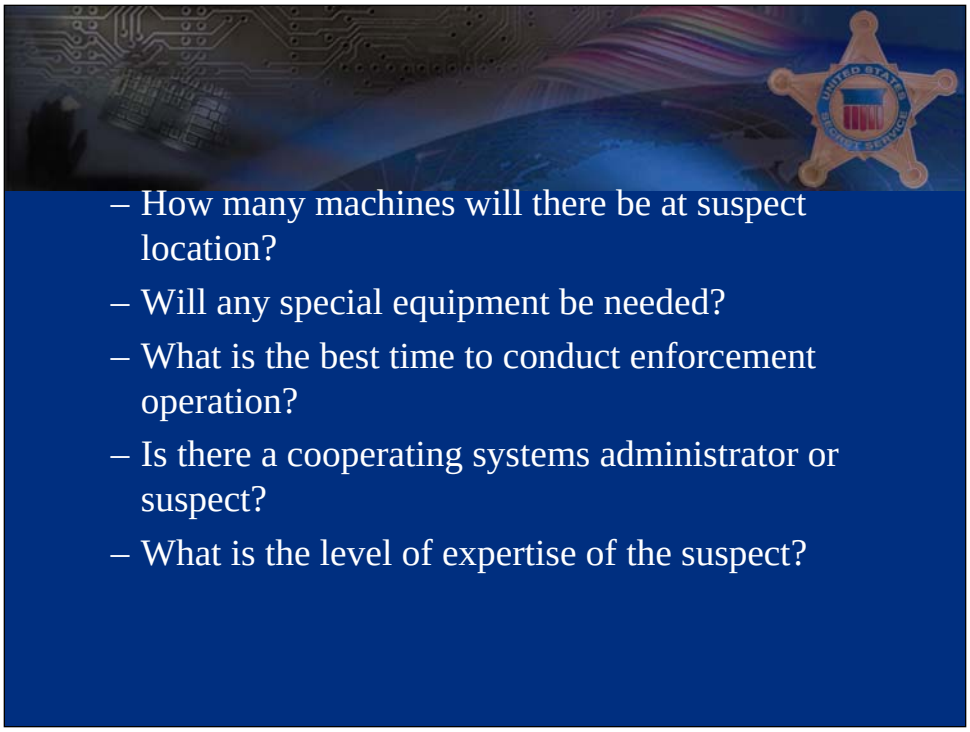
-¿Qué pruebas adicionales encontraremos (notas)?

-¿Dónde debemos buscar para encontrar esas pruebas?

-¿Qué clases de seguridad esperamos encontrar (física/digital)?

-¿Quién tiene acceso a las computadoras?

-¿Serán las computadoras confiscadas o tomadas las “imágenes” en la lugar donde se cometió el delito?



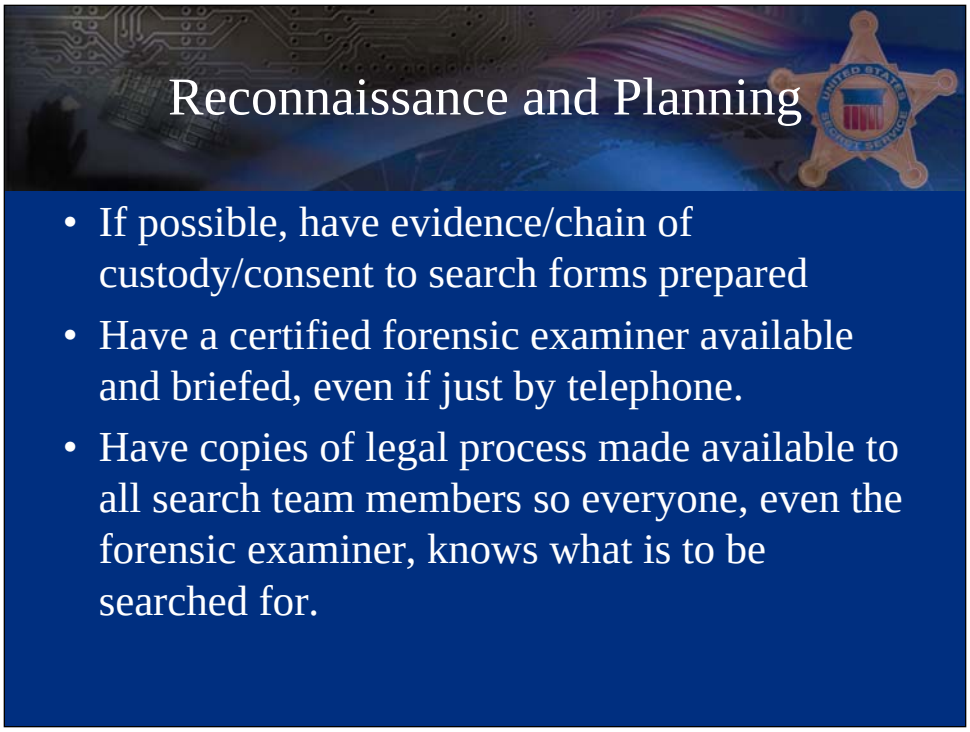
¿Cuántas máquinas hará en el lugar sospechoso?

¿Será necesario tener algún equipo especial?

¿Cuándo es mejor realizar una operación de orden público?

¿Tenemos un administrador de sistemas o sospechoso cooperador?

¿Cuál es el nivel de pericia del sospechoso?

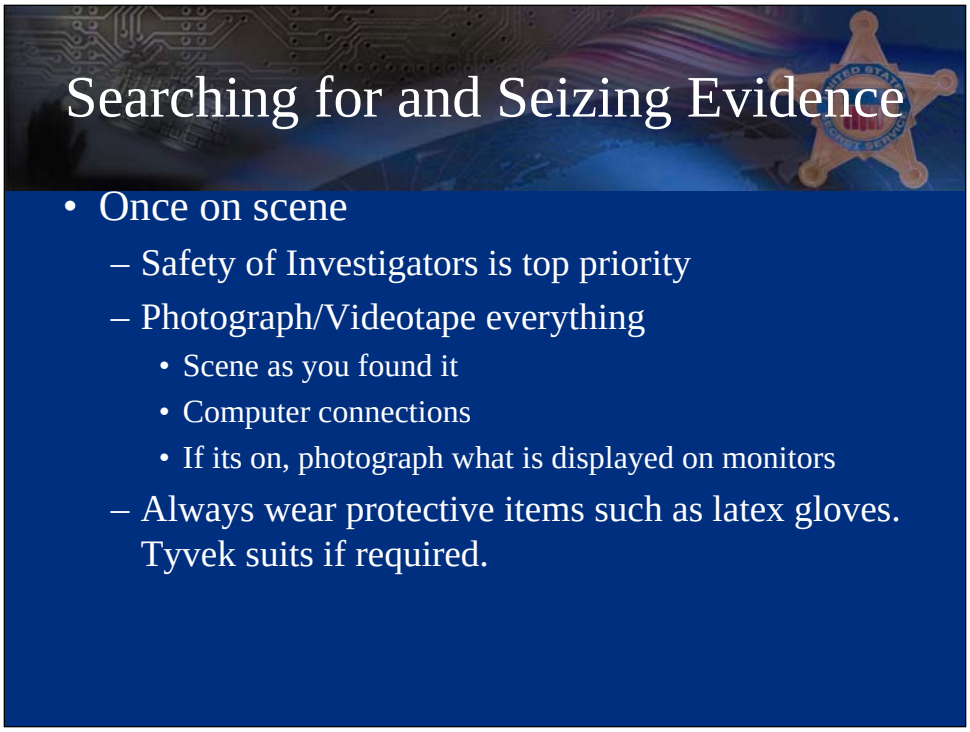


Reconocimiento y planificación

*Si es posible, tener formularios de evidencia/cadena de custodia/ consentimiento de registro ya confeccionados.

*Tener disponible un examinador forense certificado e informado, aunque sea sólo por teléfono.

*Proveer copias del proceso legal a todos los miembros del equipo de registro para que todos, hasta el examinador forense, sepan qué es lo que se está buscando.



Buscar y confiscar evidencia

*Una vez en el lugar

-La seguridad de los investigadores es la prioridad principal

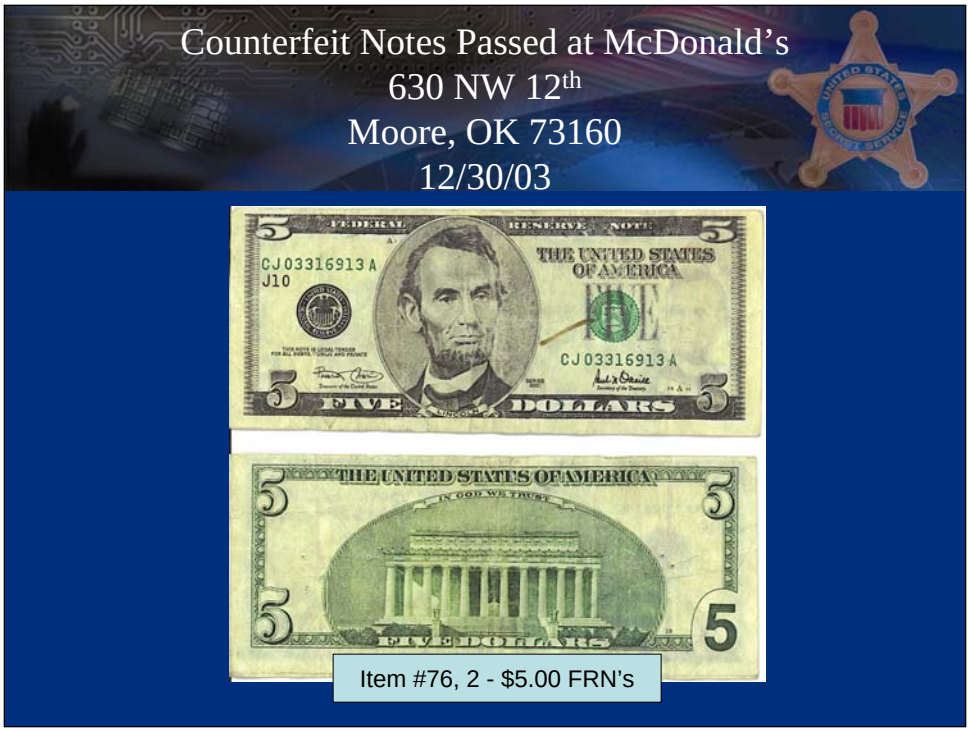
*Fotografiar/tomar video de todo

-El lugar del incidente así como lo encontró

-Conexiones de la computadora

-Si la computadora está prendida, fotografíe la pantalla

*Siempre usar equipo de protección, tal como guantes de látex. Traje Tyvek si es necesario.



Billetes falsos pasados en el McDonald's de

630 NW 12th

Moore, OK 76160

30 diciembre 2003

Foto tomada durante un registro por consentimiento de la recámara de Alroy Cameron Cox

8101 NW 84th, Oklahoma City, OK 73132

31 diciembre 2003

31 diciembre 2003 La computadora de Alroy Cameron Cox con una FRN [Nota de la Reserva Federal] mostrada en la pantalla.

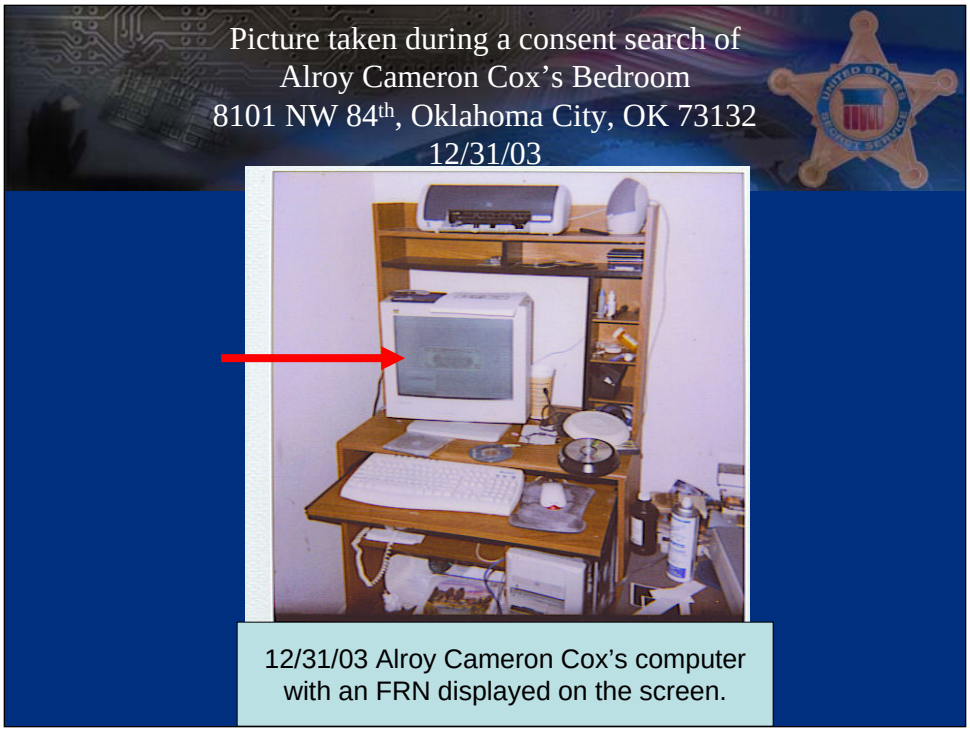


Foto tomada durante un registro por consentimiento de la recámara de Alroy Cameron Cox

8101 NW 84th, Oklahoma City, OK 73132

31 diciembre 2003

31 diciembre 2003 La computadora de Alroy Cameron Cox con una FRN [Nota de la Reserva Federal] mostrada en la pantalla.

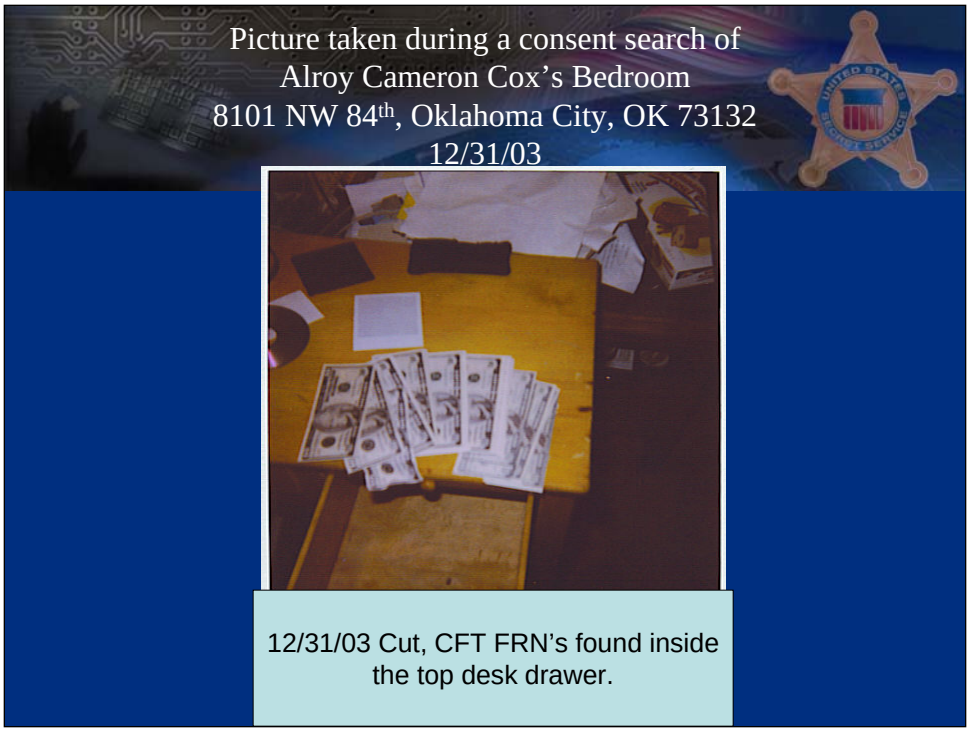


Foto tomada durante un registro por consentimiento de la recámara de Alroy Cameron Cox

8101 NW 84th, Oklahoma City, OK 73132

31 diciembre 2003

31 diciembre 2003 FRNs [Notas de la Reserva Federal] falsas encontradas en el cajón superior del escritorio.

Foto tomada durante un registro por consentimiento de la recámara de Alroy Cameron Cox

8101 NW 84th, Oklahoma City, OK 73132

31 diciembre 2003

31 diciembre 2003 Tabla con cuchilla usada para cortar las FRNs [Notas de la Reserva Federal] falsas.

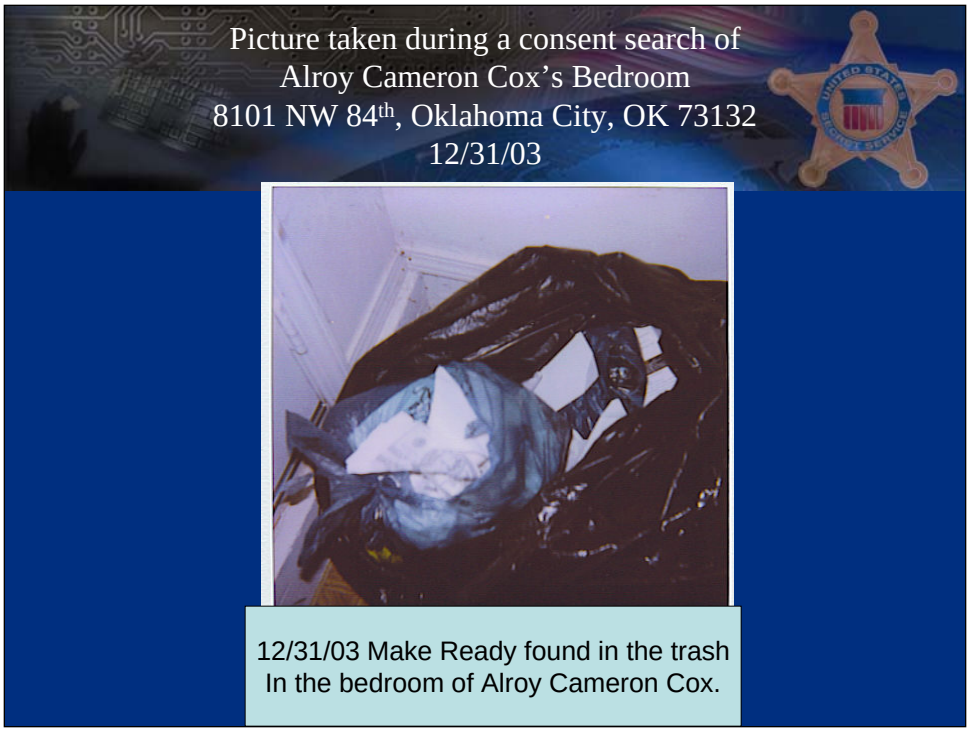
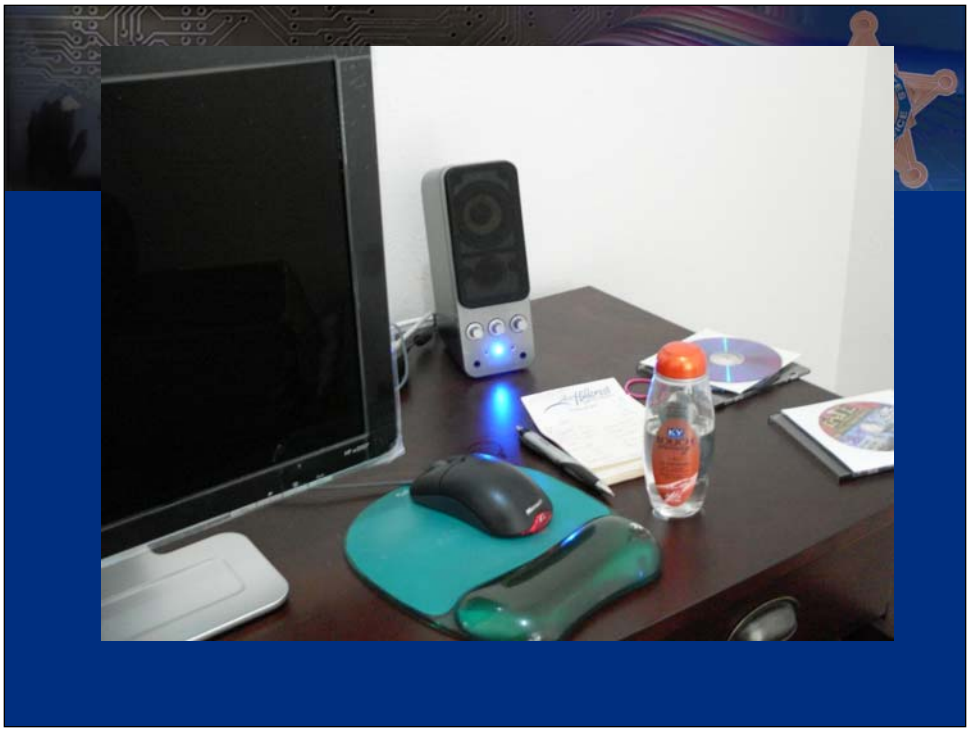


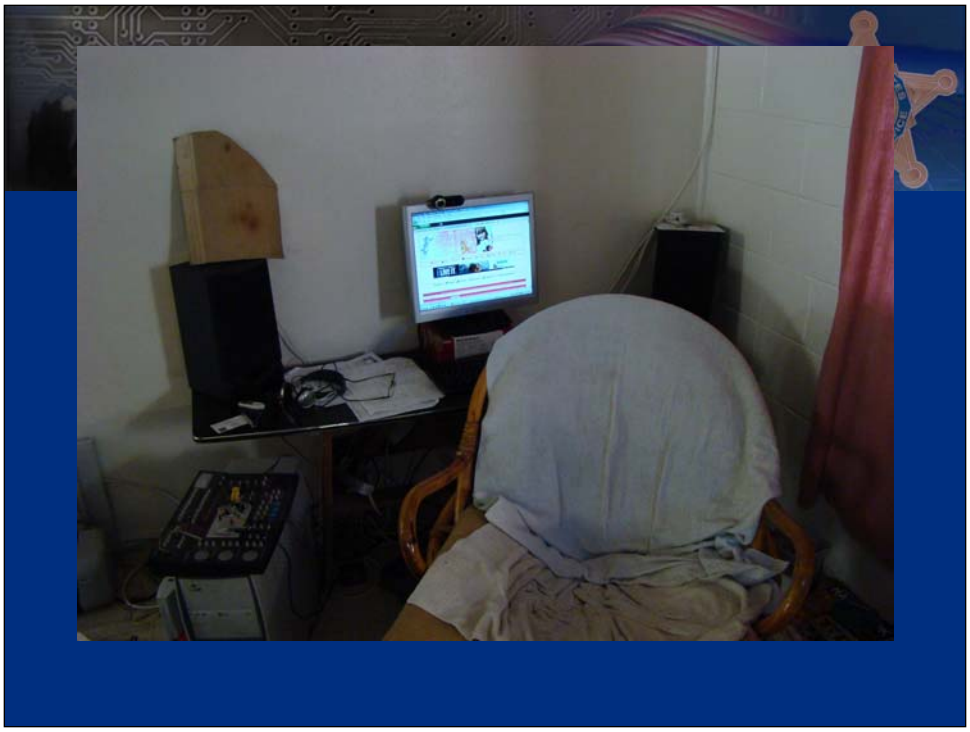
Foto tomada durante un registro por consentimiento de la recámara de Alroy Cameron Cox

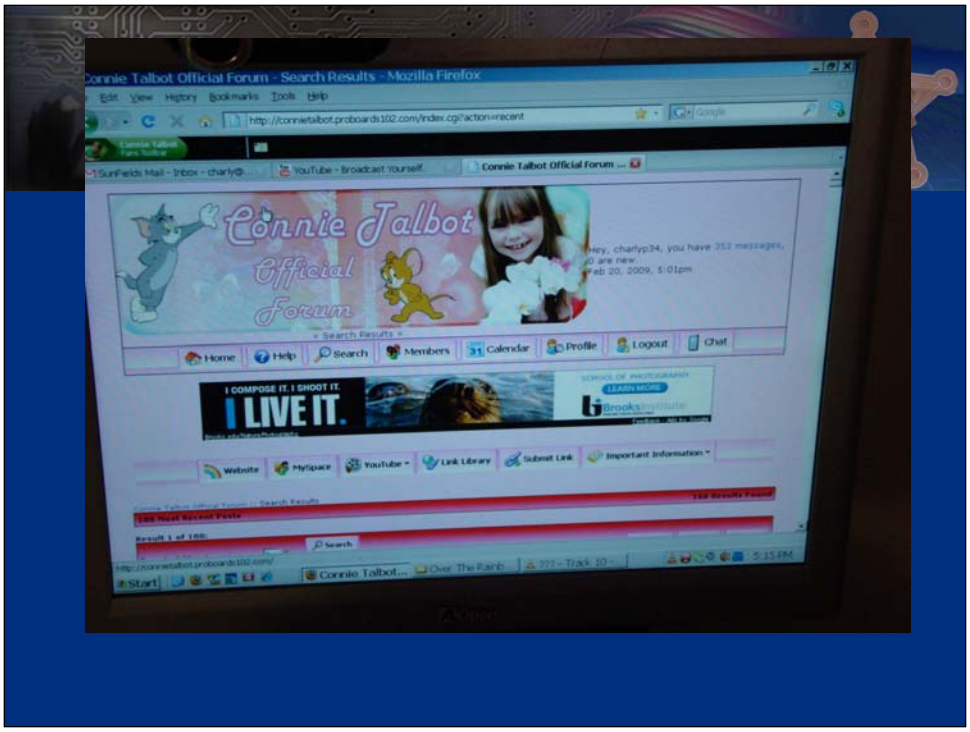
8101 NW 84th, Oklahoma City, OK 73132

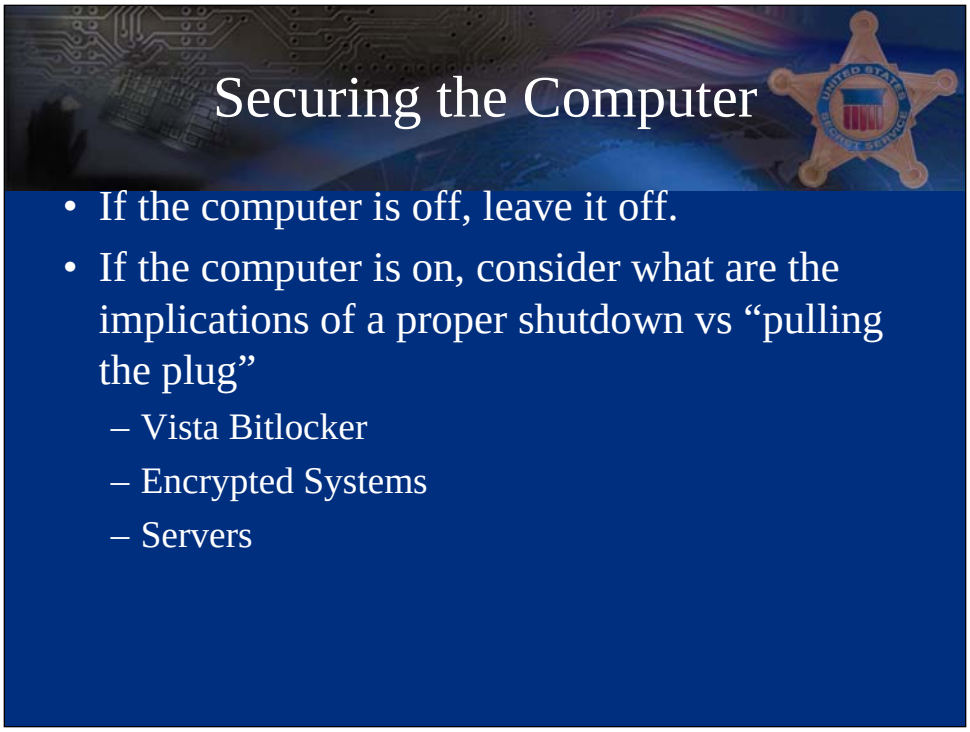
31 diciembre 2003

31 diciembre 2003. "Make Ready" [un proceso de preparación para imprimir] encontrado en la basura en la recámara de Alroy Cameron Cox






Connie Talbot Official Forum - Search Results - Mozilla Firefox
Connie Talbot Official Forum
Home
Help
Search
Members
Calendar
Profile
Logout
Chat
I COMPOSE IT. I SHOOT IT.
I LIVE IT.
Website
MySpace
YouTube
Link Library
Submit Link
Important Information



Asegurar la computadora

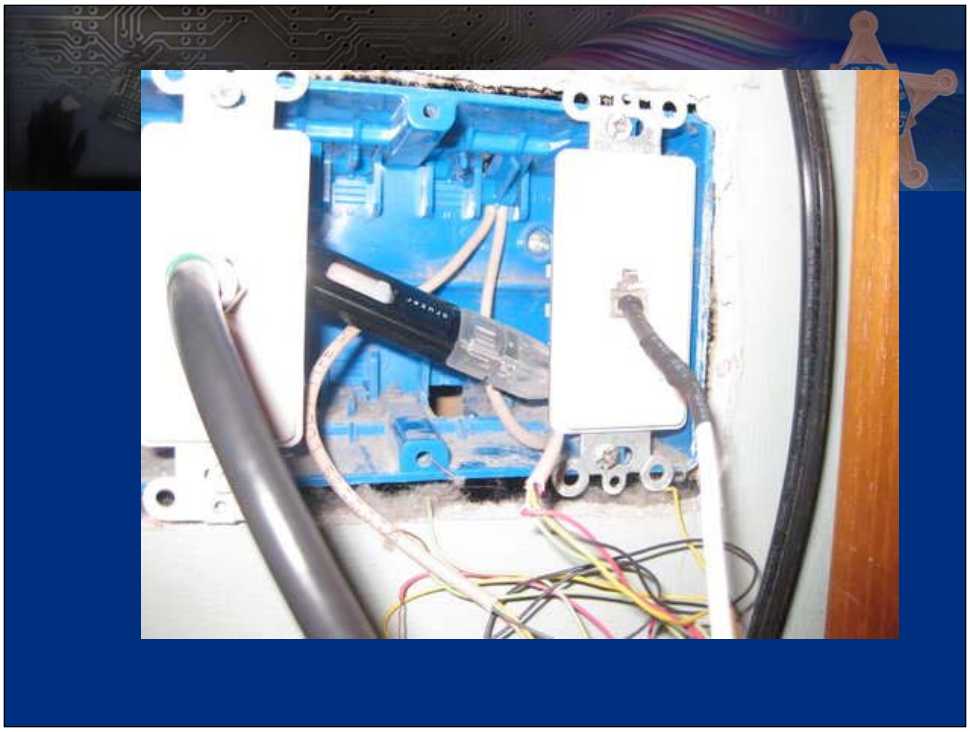
*Si la computadora está apagada, debe dejarla apagada

*Si la computadora está encendida, debe tomar en cuenta las consecuencias de apagarla correctamente vs. “jalar el enchufe”

-Vista Bitlocker

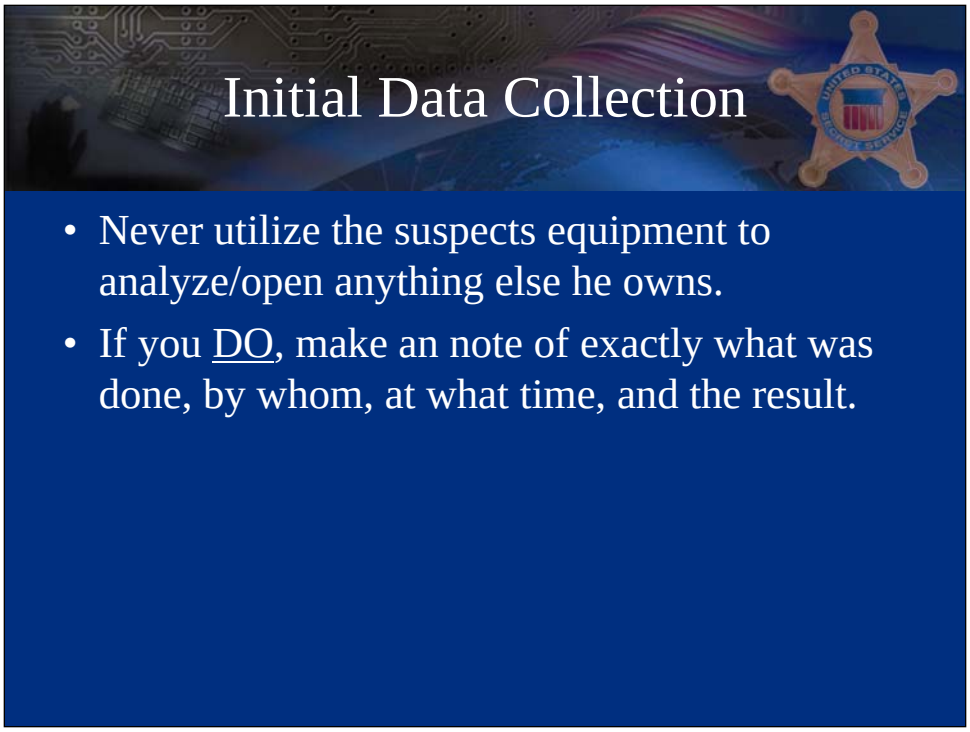
-sistemas codificados

-servidores



CAT5 linked USB Thumb Drive.

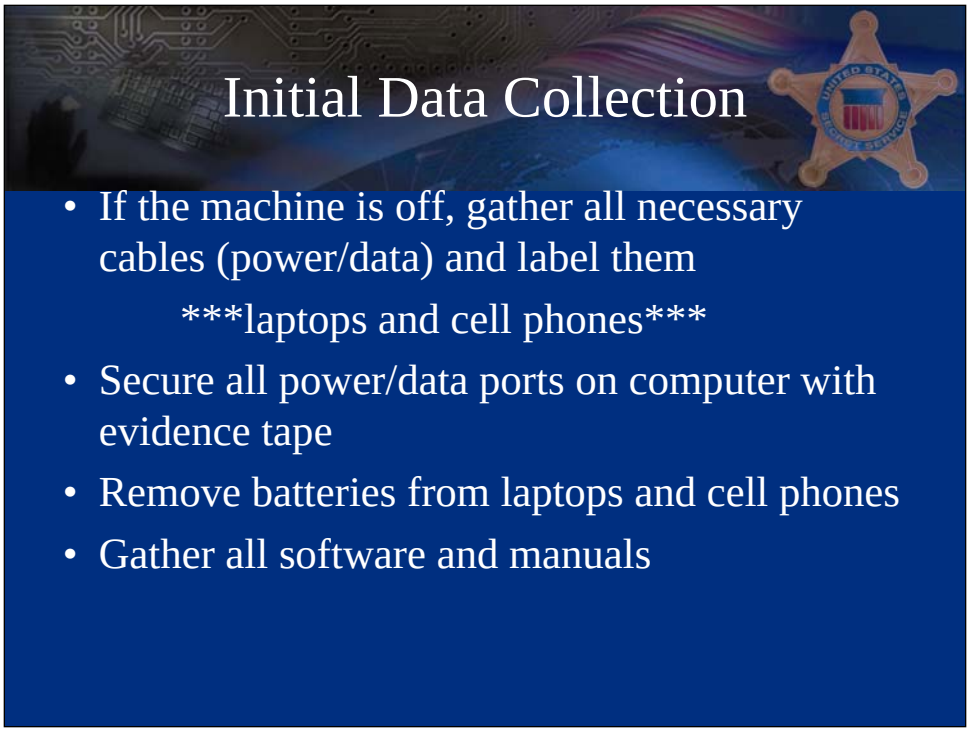
Llave de memoria USB enlazada a una línea CAT5



Recolección inicial de datos

*Nunca debe usar el equipo del sospechoso para analizar o abrir cualquier otra cosa de la cual él sea propietario.

*Si usted hace algo, debe tomar nota de exactamente qué se hizo, quién lo hizo, a qué hora y el resultado.



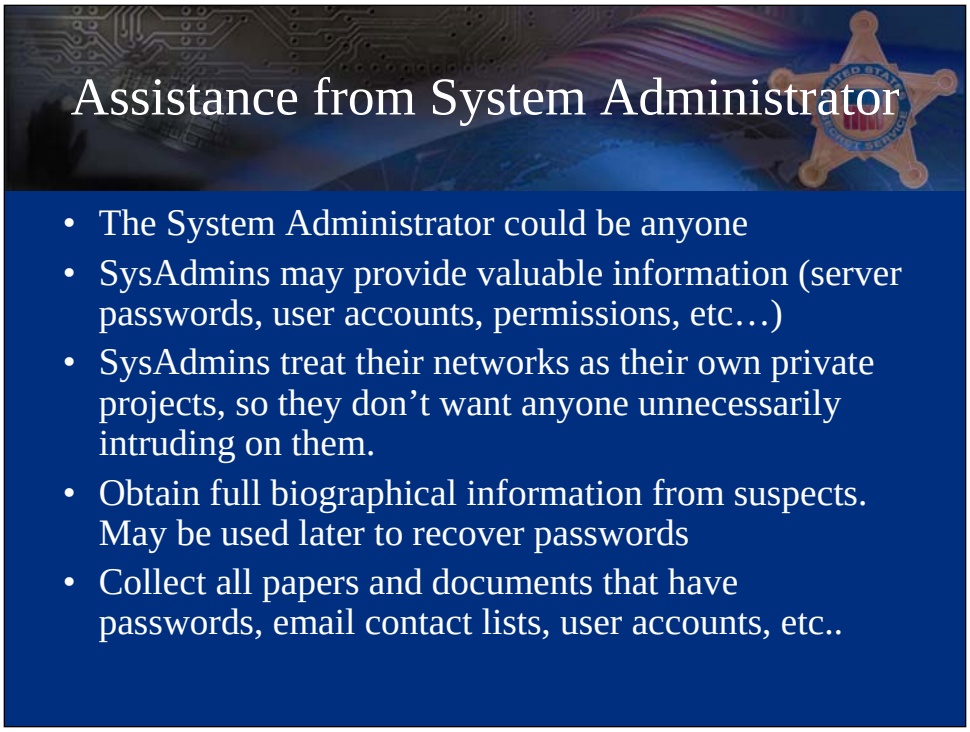
Recolección inicial de datos

*Si el equipo está apagado, debe juntar todos los cables necesarios (de alimentación/de datos) y etiquetarlos con la información necesaria.

*Debe asegurar todos los puertos de alimentación y de datos usando cinta adhesiva para evidencia

*Debe sacar la batería de las computadoras portátiles y teléfonos celulares

*Recopilar todo el software y los manuales

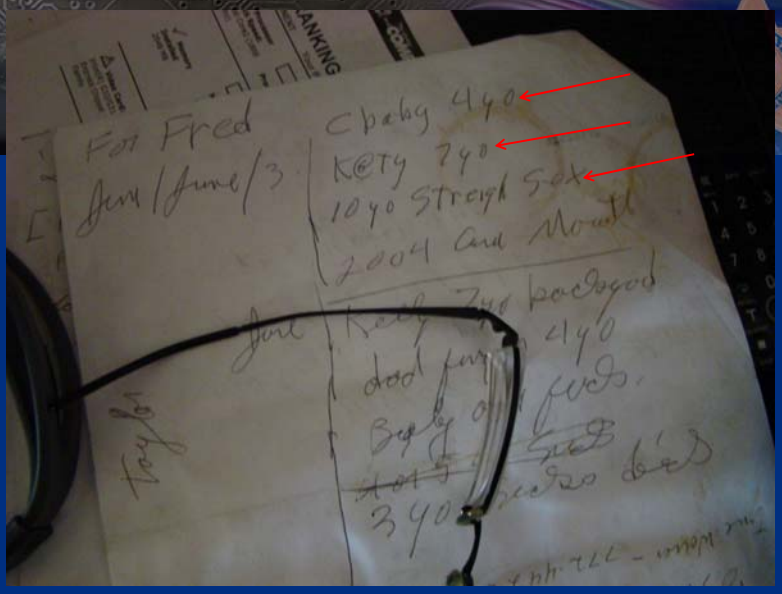


The System Admin can be anyone: from the Systems Administrator of a large corporate server to the guy who installed the operating system on his laptop.
El Administrador del sistema puede ser cualquier persona; desde el administrador de sistemas de un servidor grande corporativo hasta la persona que instaló el sistema operativo en su computadora portátil.
-Discuss SSA Nunez case where a sysop intentionally gave wrong passwords to server.
-Hablar del caso de SSA [Agente del Servicio Secreto] Núñez en el cual un operador del sistema dio contraseñas incorrectas al servidor a propósito.
-In cases where the suspect is the System Administrator, the term is not so much assistance as a full interrogation:

En los casos en que el sospechoso es el administrador del sistema, el término no es tanto "ayuda" como una "interrogación plena".
--While being cognizant of legal ramifications, try to obtain as much information as possible *At the Scene* to try to determine his level of computer knowledge, passwords, encryption.
-Mientras teniendo en cuenta las ramificaciones legales, debe intentar de obtener cuanta información posible "en sitio" para tratar de determinar su nivel de conocimientos de informática, contraseñas y codificación
--How was he doing what he was doing? ¿Cómo llevó a cabo lo que estaba haciendo?
--The majority of us use passwords which are derived from things/people we know. Spouses names, pets names, license plate numbers, birthdays…etc.
-La mayoría de nosotros utilizamos contraseñas derivadas de cosas/personas que conocemos. Nombre del esposo/esposa, nombre del mascota, número de placa de automóvil, cumpleaños… etc.
-- Discuss Baker Case
- Hablar del caso de Baker

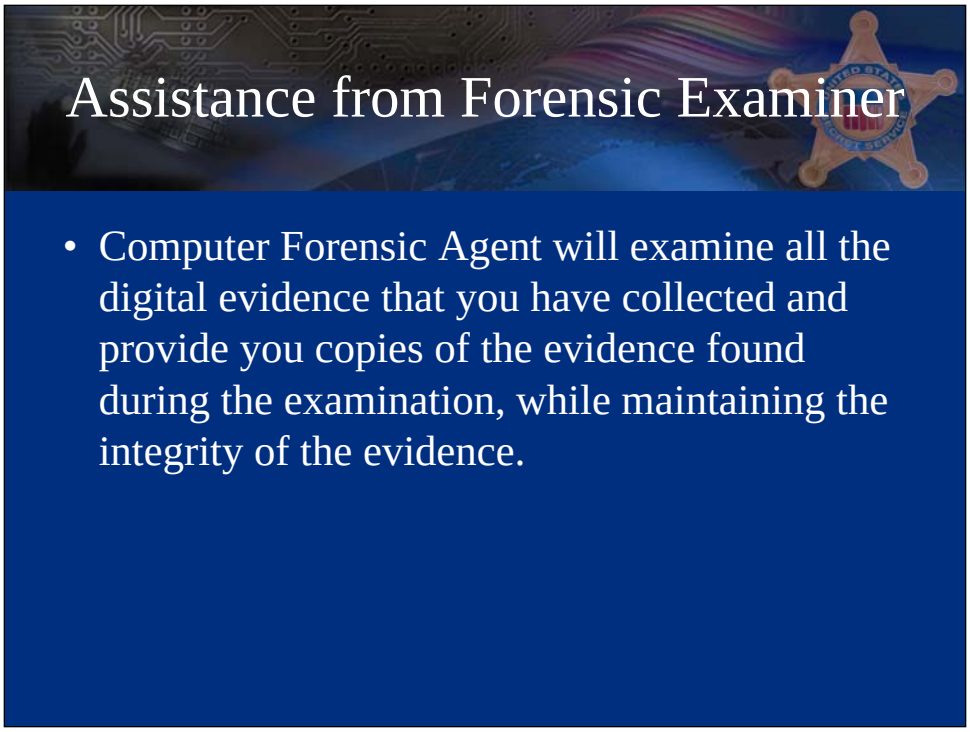
***Asistencia del administrador de sistema
*El administrador de sistema puede ser cualquier persona
*Los administradores de sistema pueden proporcionar información valiosa (contraseñas de los servidores, cuentas de los usuarios, permisos, etc.).
*Los administradores de sistemas tratan a sus redes como sus proyectos privados y no quieren intrusos innecesarios en sus proyectos.
*Obtenga la información biográfica completa de los sospechosos, la cual puede utilizarse más tarde para recuperar contraseñas

Juntar todos los papeles y documentos que tienen contraseñas, listas de contactos de correo electrónico, cuentas de usuarios, etc...


For Fred
Jan/June/3
Cbaby 440
KCTY 740
1040 Straight Sex
2004 and Mouth
440
340

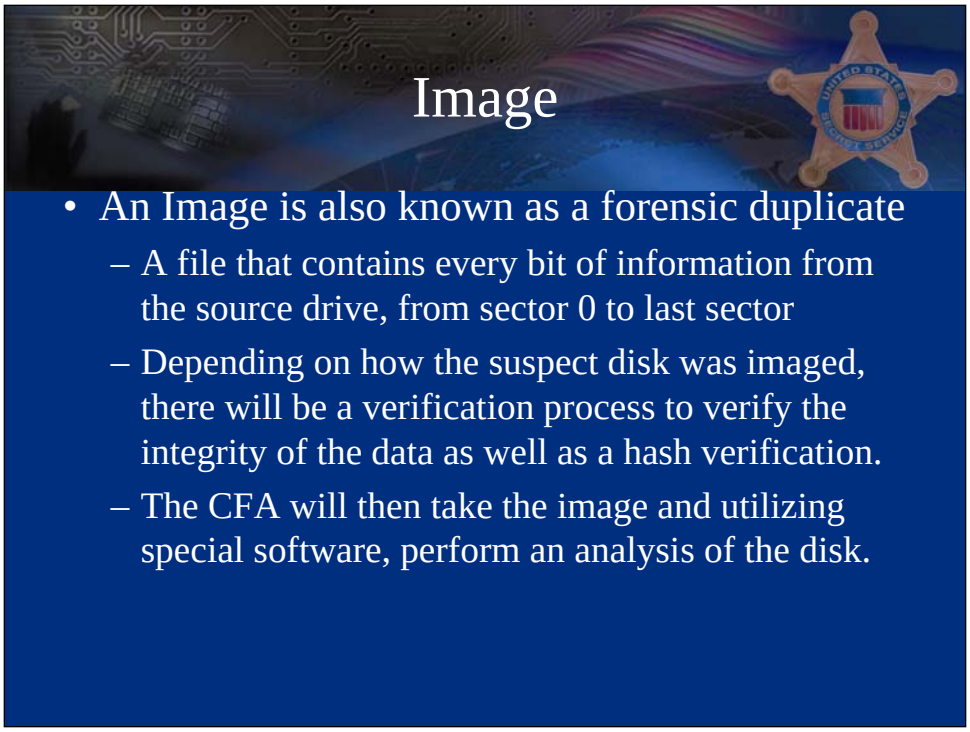

11/08/2002


NetApp Filer



Asistencia del examinador forense

*El Agente Forense de Informática examinará toda la evidencia digital que se ha recolectado y le proporcionará copias de las pruebas encontradas durante la examinacion, mientras mantiene la integridad de la evidencia.



"Imagen" (imaginática)

*Una imagen también se conoce como un duplicado forense

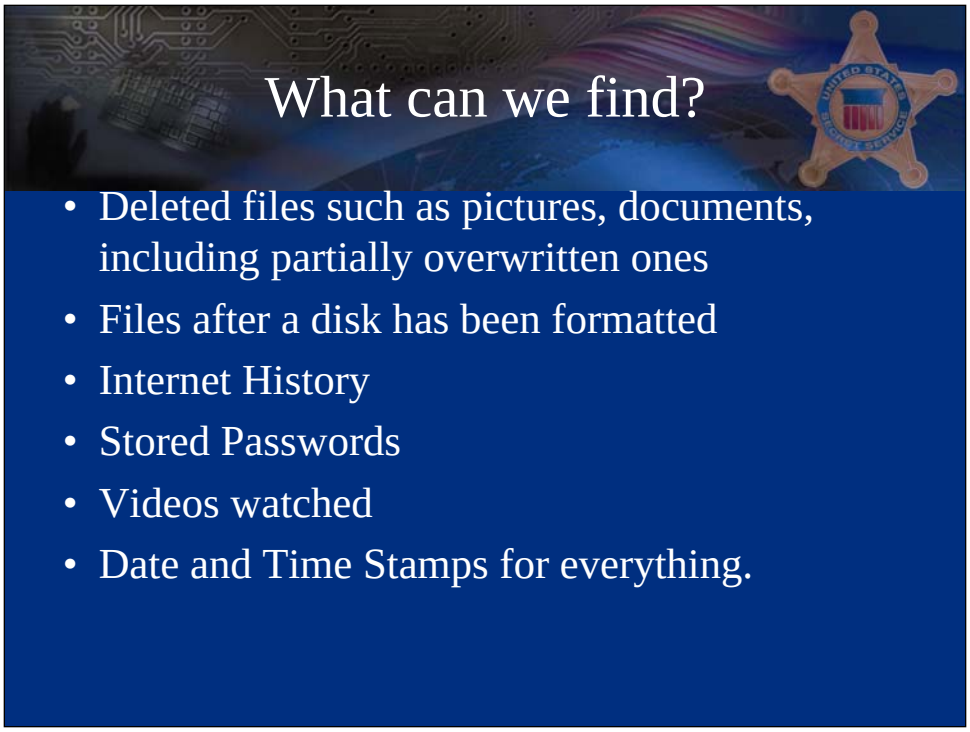
-Un archivo que contiene cada pedacito de información de la unidad fuente, desde el sector 0 hasta el último sector.

-Dependiendo de la manera en que el disco del sospechoso fue duplicado, se realizará un proceso de verificación para confirmar la integridad de los datos como también una comprobación del valor *hash*.

-El Agente Forense de Informática tomará la imagen y, utilizando un software especial, hará un análisis del disco.

"Imagen"

*Todas las "imágenes" de *bitstreams* se deberán hacer con un bloqueador que no permite escribir, basado en el hardware o el software, el cual previene la modificación a los medios del sospechoso.



This is just a partial list. Ask the audience what else they believe may be stored on their computers pertaining to the case they will be working on:

Chat logs, Emails, notes, letters, images of signatures, documents, on-line banking software

Esta es solamente una lista parcial. Pregunte a la audiencia qué más creen que puede almacenarse en las computadoras pertenicientes al caso en el cual van a trabajar.

Registros de chat, correo electrónico, cartas, imágenes de firmas, documentos, software para banca en línea.

¿Qué podemos encontrar?

*Archivos suprimidos, tales como fotografías, documentos, incluyendo los que están parcialmente superpuestos

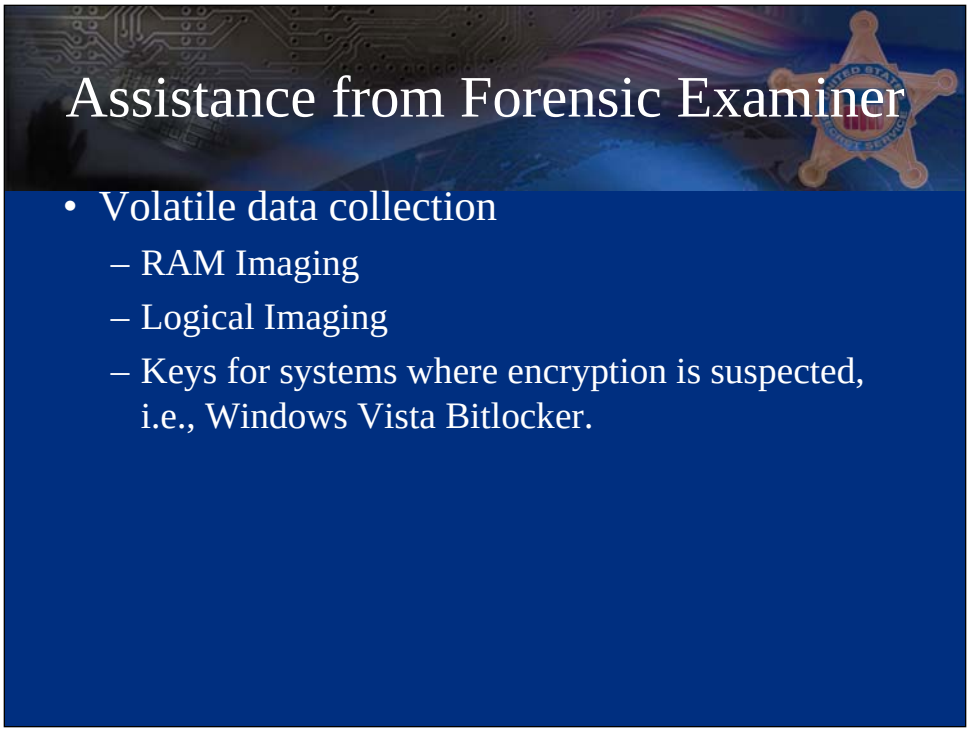
*Archivos después de que el disco ha sido formateado

*El historial del uso del internet

*Contraseñas guardadas

*Videos previamente vistos

* Registro de fecha y hora de todo



Discuss the importance of only having a qualified CFA perform these tasks

Hablar de la importancia de que solamente un Agente Forense de Informática debe llevar a cabo estas tareas.

Asistencia del examinador forense

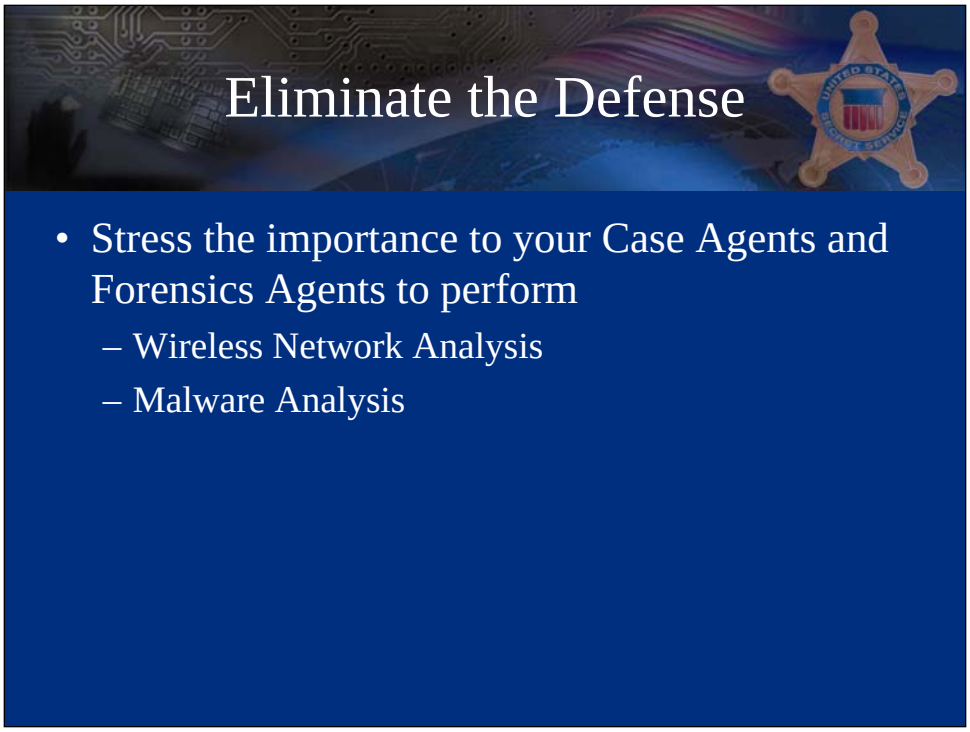
*Recoleccion de datos inestables

-"Imagenes" de memoria de acceso aleatorio

-Toma de imagenes lógica

-Claves para los sistemas donde se sospecha de codificación

p. ej. Windows Vista Bitlocker



Wireless network analysis eliminated SOD hacked into my open network defense

El análisis de la red inalámbrica eliminó la defensa de SOD [alguna otra persona] entró por *hacking* a mi red abierta.

Malware analysis eliminates the “a virus put all this porn on my computer” defense

El análisis de software malicioso elimina la defensa de “un virus colocó toda esta pornografía en mi computadora”.

Even if viruses are found, a full explanation of what the virus does is available at symantec.com or mcaffee.com.

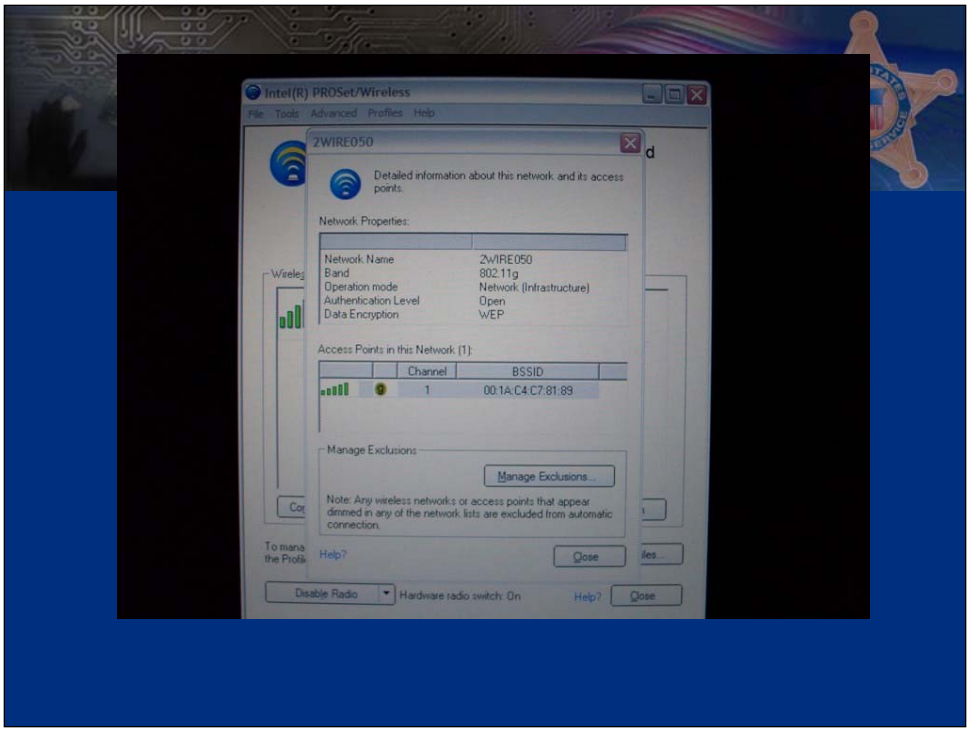
Aun cuando se encuentran virus, se dispone de una explicación completa de lo que hace el virus en los sitios symantec.com o mcaffee.com.

Eliminar las estrategias de defensa

*A su agente encargado del caso y a los agentes forenses, debe poner énfasis en la importancia de que realicen:

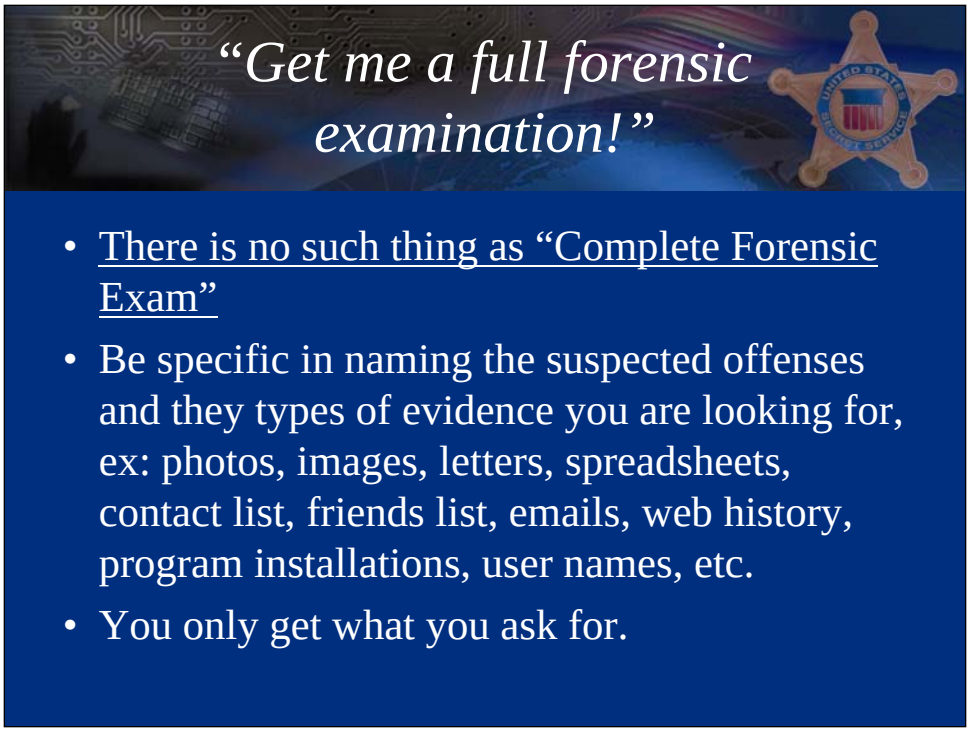
-un análisis de la red inalámbrica

-un análisis de software malicioso



Screen shot of Search Warrant showing WEP encryption active on a CP suspect. Eliminates SODDI network Intrusion defense.

Imagen de pantalla de una orden de allanamiento, la cual muestra codificación activa sobre un sospechoso de pornografía infantil. Elimina la defensa de intrusión a la red de SODDI [lo hizo alguna otra persona].



As the knowledge of the forensic field has increased, so has the belief from many prosecutors that a CFA can perform all exams on a machine.

Al incrementarse el conocimiento en materia forense, también se ha incrementado la opinión de muchos fiscales de que un Agente Forense de Informática puede realizar todos los estudios sobre una máquina.

Often times, providing a CFA a keyword list of suspects, bank names, account numbers is the best way to find the data a case agent may need.

Muchas veces, el proporcionarle al Agente Forense de Informática una lista de sospechosos, nombres de bancos y números de cuentas es la mejor forma de encontrar los datos que puede requerir el agente del caso.

¡"Deme un estudio forense completo"!

•No hay tal cosa como "una investigación forense completa"

•Debe estar específico en nombrar los delitos sospechados y las clases de evidencia que usted está buscando, por ejemplo: fotos, imágenes, cartas, hojas de cálculo, listas de contactos, listas de amigos, correo electrónico, el historial del uso del Internet, instalación de programas, nombres de usuario, etc.

•Sólo consigue lo que pide.

¿Preguntas?