


Primera Respuesta: Las etapas iniciales de la Investigación  
Agente Especial Matt Ralls  
Servicio Secreto de los Estados Unidos, Oficina de Campo de Oklahoma City



Once a crime is suspected to have occurred,  
what are the responsibilities of first  
responders?  
How to secure preliminary electronic  
evidence?

Una vez que se sospecha que un delito ha ocurrido, ¿Cuáles son las responsabilidades de los que llegan primero a la escena del delito?  
¿Cómo se asegura la evidencia electrónica preliminar?

# Strategies



- Determine the type of case (fraud, intrusion, theft, child exploitation)
- Identify the sources of electronic evidence
- Preserve electronic evidence (preservation letter)
- Integrate electronic evidence into the investigation (reports, interviews)
- Case Management and investigation plan

## SPANISH TRANSLATION

### Estrategias

Determinar la clase del caso (fraude, intrusión, robo, explotación de niños)

Identificar las fuentes de evidencia electrónica

Conservar la evidencia electrónica (carta de conservación)

Integrar evidencia electrónica en la investigación (informes, entrevistas)

La gestión del caso y plan de investigación

# Getting Started



- Perform traditional investigative steps:
  - Who, What, When, Where, how?
- Is there a victim? Is there a target?
- What crime has been committed? (fraud, intrusion, child exploitation, traditional crime)
- Conduct your traditional criminal checks before leaving the building (+Search Engines)
- Systematic approach/Chaotic approach

Everything comes down to: What is the crime?

Todo llega a: ¿Cuál es el delito?

Comenzar

\*Lleve acabo los pasos de investigación tradicional

-¿quién?, ¿qué?, ¿cuándo?, ¿dónde? ¿cómo?

\*¿Hay una víctima? ¿Hay un blanco?

\*¿Cuál delito ha sido cometido? (fraude, intrusión, explotación infantil, delitos tradicionales).

•Realice sus verificaciones penales tradicionales antes de salir del edificio (+ buscadores)

•Enfoque sistemático/ enfoque caótico

## Initial Stages

### What is the Crime?

| Child Exploitation Case   | Property/Intrusion Case   |
|---|---|
| <ul style="list-style-type: none"> <li>• Conduct criminal history of checks for target or targets</li> <li>• Determine who else has access to system</li> <li>• Is there a possibility of imminent danger ?</li> <li>• Possibility of Flight?</li> <li>• Gather evidence</li> <li>• Obtain legal authority to conduct searches</li> <li>• Interview suspects</li> </ul> | <ul style="list-style-type: none"> <li>• What is the motive?</li> <li>• Determine who has access</li> <li>• Interview Systems Administrators and Other witnesses</li> <li>• What is the purpose of the intrusion (theft/disruption)</li> <li>• Internal vs External Threat</li> </ul> |

History of Target Antecedentes del blanco

-Criminal Penales  
 -Family (Children in Home?) Parientes (¿hay niños en el hogar?)

Possibility of flight: Cullinane, Pine Posibilidad de huida: Cullinane, Pine

What are the security precautions taken to prevent intrusion? ¿Cuáles son las precauciones de seguridad tomadas para prevenir la intrusión?

ie: In a CP Case, an investigator may make the determination to perform a drive-by of the suspect location to determine if wireless encryption is active from the target system

o sea, en un Caso de Pornografía Infantil, un investigador puede tomar la decisión de realizar un paseo en carro del local donde está el sospechoso para averiguar si la encriptación de la red inalámbrica del sistema blanco está activa

Questions to ask administrators: Las preguntas que deben hacerse a los administradores:

What subjects have access to the system? ¿Cuáles sujetos tienen acceso al sistema?

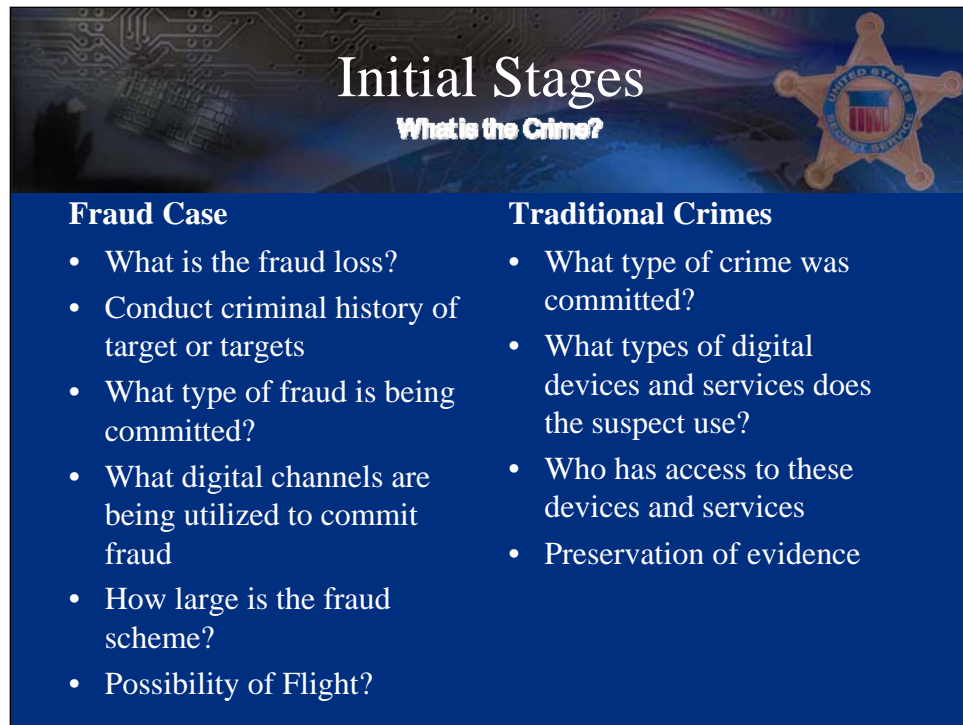
What are the security measures in place? ¿Cuáles son las medidas de seguridad establecidas?

Etapas inicial

- \*¿Cuál es el crimen?
- \*Caso de explotación infantil
- \*realizar un historial criminal del blanco o blancos
- \*determinar quién más tiene acceso al sistema
- \*¿Hay la posibilidad de peligro inminente?
- \*Posibilidad de convertirse en fugitivo
- Recopilar pruebas
- Obtener la autorización legal para realizar registros
- Entrevistar a los sospechosos

Casos de propiedad/intrusión

- \*¿Cuál es el motivo?
- \*Determinar quién tiene acceso
- \*Entrevistar a los administradores de sistemas y a otros testigos
- \*¿Cuál es el propósito de la intrusión (robo/trastorno)?
- \* Amenaza interna vs. externa



The slide features a dark blue background with a circuit board pattern on the left and a rainbow wave on the right. A gold police badge with 'UNITED STATES MARSHAL SERVICE' is in the top right corner. The title 'Initial Stages' is in large white font, with 'What is the Crime?' below it in smaller white font.

| Fraud Case   | Traditional Crimes  |
|--|---|
| <ul style="list-style-type: none"> <li>• What is the fraud loss?</li> <li>• Conduct criminal history of target or targets</li> <li>• What type of fraud is being committed?</li> <li>• What digital channels are being utilized to commit fraud</li> <li>• How large is the fraud scheme?</li> <li>• Possibility of Flight?</li> </ul> | <ul style="list-style-type: none"> <li>• What type of crime was committed?</li> <li>• What types of digital devices and services does the suspect use?</li> <li>• Who has access to these devices and services</li> <li>• Preservation of evidence</li> </ul> |

#### Etapas iniciales

¿Cuál es el delito?

#### Caso de Fraude

- ¿Cuál es la pérdida resultante del fraude?
- Investigar los antecedentes penales del blanco o blancos
- ¿Qué clase de fraude se comete?
- ¿Cuáles canales digitales se utilizan para cometer el fraude?
- ¿Qué tan extenso es el esquema de fraude?
- ¿Posibilidad de huida?

#### Delitos Tradicionales

- \* ¿Qué clase de delito se cometió?
- \* ¿Que clases de dispositivos y servicios digitales utiliza el sospechoso?
- \* ¿Quién tiene acceso a dichos dispositivos y servicios?
- \* ¿Conservación de las pruebas

## Identify Sources of Electronic Evidence

- Divide evidence into 3 categories:
  - Host Based
  - Network Based
  - Other (Includes Interview information)

REDO THIS SLIDE! CONFECCIONAR ESTA LÁMINA DE NUEVO!

One of the best ways to simplify a technical investigation is to divide all evidence into 3 categories

Una de las mejores maneras de simplificar una investigación técnica es dividir toda la evidencia en 3 clasificaciones

Host Based: Evidence located on affected or involved system/computer

Basada en el servidor principal

Network Based: Evidence collected from routers, ISP, etc.

Basada en la Red: Pruebas recogidas de routers, ISP, etc.

Other evidence: Nondigital evidence and testimonial information.

Otra evidencia: pruebas no digitales e información de testimonio

### SPANISH TRANSLATION

Identificar Fuentes de Evidencia Electrónica

Dividir la evidencia en 3 categorías

-Basada en el servidor principal

-Basada en la red

-Otras (Incluye información de la entrevista)



# Host Based Information

What information is likely to be on the target/affected system?

| Child Exploitation Case  | Property/Intrusion Case  |
|--|--|
| <ul style="list-style-type: none"> <li>• Emails</li> <li>• Photos/Video</li> <li>• Documents</li> <li>• Chat Logs</li> </ul> | <ul style="list-style-type: none"> <li>• Emails</li> <li>• Server Logs</li> <li>• Documents</li> <li>• Transaction History</li> <li>• Spreadsheets</li> <li>• Scanned Documents</li> <li>• Backup Files</li> </ul> |

Basada en la información del servidor principal

¿Cuál información es más probable que se encuentre en el sistema del sistema blanco/afectado?

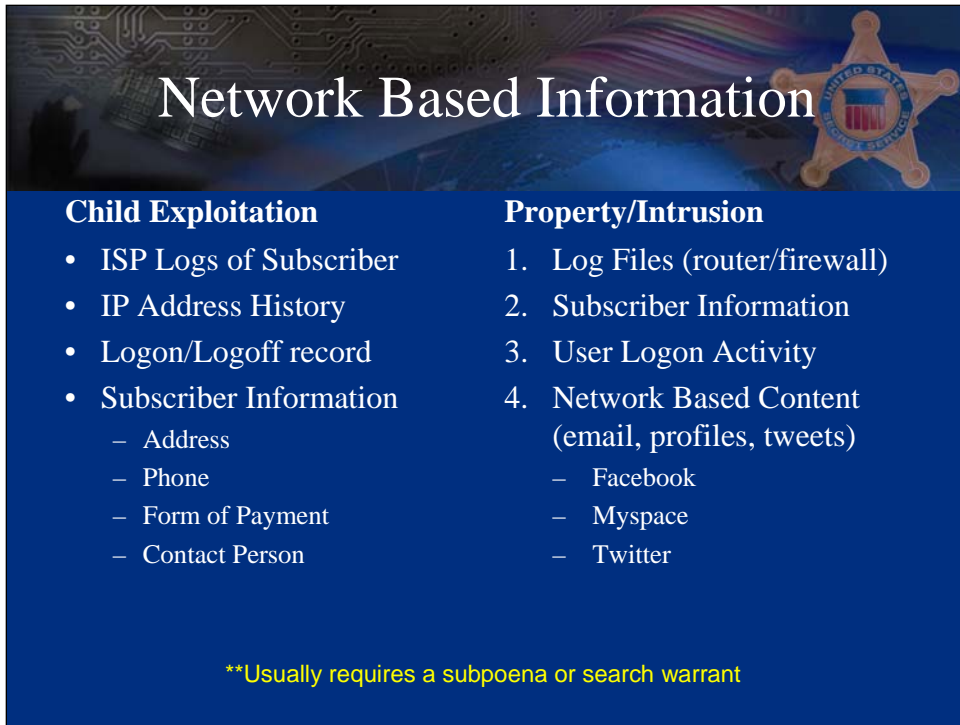
\*Caso de explotación infantil

- Correo electrónico (email)
- fotografías/videos
- documentos
- registros de salones de chat

\*Casos de propiedad/intrusión

- Correo electrónico (email)
- registros de servidores
- documentos
- Historial de transacciones
- Hojas de cálculo
- Documentos “escaneados”
- Archivos de reserva





# Network Based Information

|   |  |
|---|--|
| <p><b>Child Exploitation</b></p> <ul style="list-style-type: none"> <li>• ISP Logs of Subscriber</li> <li>• IP Address History</li> <li>• Logon/Logoff record</li> <li>• Subscriber Information             <ul style="list-style-type: none"> <li>– Address</li> <li>– Phone</li> <li>– Form of Payment</li> <li>– Contact Person</li> </ul> </li> </ul> | <p><b>Property/Intrusion</b></p> <ol style="list-style-type: none"> <li>1. Log Files (router/firewall)</li> <li>2. Subscriber Information</li> <li>3. User Logon Activity</li> <li>4. Network Based Content (email, profiles, tweets)             <ul style="list-style-type: none"> <li>– Facebook</li> <li>– Myspace</li> <li>– Twitter</li> </ul> </li> </ol> |
|---|--|

\*\*Usually requires a subpoena or search warrant

Network Based Data: Router information, IP Data, etc.

Datos basados en la red: Información de routers, datos del IP [protocolo del Internet], etc.

**\*Explotación infantil**

- El registro de suscriptores del ISP [proveedor de servicio]
- El historial de la dirección IP
- Registro de entradas y salidas del sistema
- Información del subcriptor
  - dirección
  - teléfono
  - forma de pago
  - persona de contacto

**\*propiedad/allanamiento**

1. Archivos de registro (router/contrafuegos)
2. Información del subcriptor
3. Actividad de entradas del usuario
4. Contenido basado en la red (correo electrónico, perfiles, tweets)
  - Facebook
  - Myspace
  - Twitter

**\*\* Usualmente requiere un citación u orden de allanamiento)**

# Preserving Electronic Evidence



## Child Exploitation

- Screen Capture software
- Email preservation from Service Provider
- Direct to Law Enforcement Computer (P2P)
- Seizure of digital evidence
- Obtaining an image (exact copy) of evidence

## Property/Intrusion

- Screen Capture software
- Email preservation from Service Provider
- Direct to Law Enforcement Computer (P2P)
- Seizure of digital evidence
- Obtaining an image (exact copy) of evidence

Volatile Data is data that will “disappear” once the system is powered down

Los datos volátiles es información que “desaparecerá” una vez se apague el sistema

May Include: system date and time, applications currently running, network state, currently established network connections.

Puede incluir: fecha y hora en el sistema, aplicaciones actualmente en uso, estado de la red, conexiones a la red actualmente establecidas

Live Imaging is described as “making a copy” of a logical file structure on a system that is on.

More on imaging later...

Se describe a la formación de imágenes en vivo como “hacer una copia” de una estructura lógica de archivos en un sistema prendido. En los casos cuando la víctima ha reportado un delito, la formación de imágenes en vivo del sistema afectado puede ser una opción para conservar el escenario del delito “tal como está”.

Vamos a hablar más sobre la formación de imágenes más tarde....

In cases where the subject may be utilizing email to commit an offense, certain legal process may be required to require the email provider to preserve email.

En los casos que el sujeto puede estar utilizando el correo electrónico para cometer un delito, pueden requerirse algunos procesos legales para exigir que el proveedor del correo electrónico conserve el correo electrónico.

Preservar la evidencia electrónica

\*

Software de captura de pantalla

Conservar el correo electrónico de proveedor de servicio

Enviar la evidencia directamente a la computadora del cuerpo de policía (P2P)

Decomiso de evidencia digital

Obtener un imagen (copia exacta) de la evidencia

\*propiedad/intrusión

Software de captura de pantalla

Conservar el correo electrónico de proveedor de servicio

Enviar la evidencia directamente a la computadora del cuerpo de policía (P2P)

Decomiso de evidencia digital

Obtener un imagen (copia exacta) de la evidencia

# Preserving Electronic Evidence

- Whichever option you choose:
  - You must collect data in a forensically sound manner.
  - You must protect the integrity of the data

Conservar la evidencia electrónica

Cualquier opción que usted decida usar:

-debe de recolectar la información de una manera que siga los reglamentos en materia forense

-debe de proteger la integridad de la información

# Forward Edge 2



## FORWARD EDGE II



United States Department  
of Homeland Security  
United States  
Secret Service

Interactivo de formación y recursos para luchar contra los crímenes de Electrónica

[INICIO](#) | [Solicitar una copia](#) | [GUÍA DE CAMPO](#) | [ESCENARIOS](#) | [CRÉDITOS](#) | [Carta del Director](#) | [COMENTARIOS](#)

### Edge II Forward Promo Video



Play Promo >>

Flash Video

Windows Media

[¿Qué es el borde II?](#)

### Adelante Edge II Guía de Campo



CONTINENTAL UNITED STATES

[Guía en línea para los investigadores](#)

### Access eLibrary



El Servicio Secreto de Estados Unidos eLibrary sitio web es un sitio web seguro para la aplicación de la ley y la delincuencia financiera investigadores calificados. Es una colección única de recursos de bases de datos sobre una variedad de temas. ELibrary la Web se basa en la promesa de que el intercambio de información puede hacer que la aplicación de la ley y la delincuencia financiera, incluso los investigadores más eficaces.

## Case Management and Electronic Evidence Integration

- Confer with a forensic examiner
- What agencies/services are available to process this data?
- Case management is a priority

Forensic Examiners are extremely busy and may need to make special arrangements, special equipment purchases. If it's a server type environment the examiner may have to seek assistance in handling a network environment.

Los Examinadores forenses están muy ocupados y puede requerirse que hagan arreglos especiales o que compren equipo especial. Si es un entorno de servidores, puede que el examinador tenga que buscar ayuda en gestionar el entorno de redes.

CP Case: In USL NCMEC Caso de Pornografía Infantil: en USL NCMEC

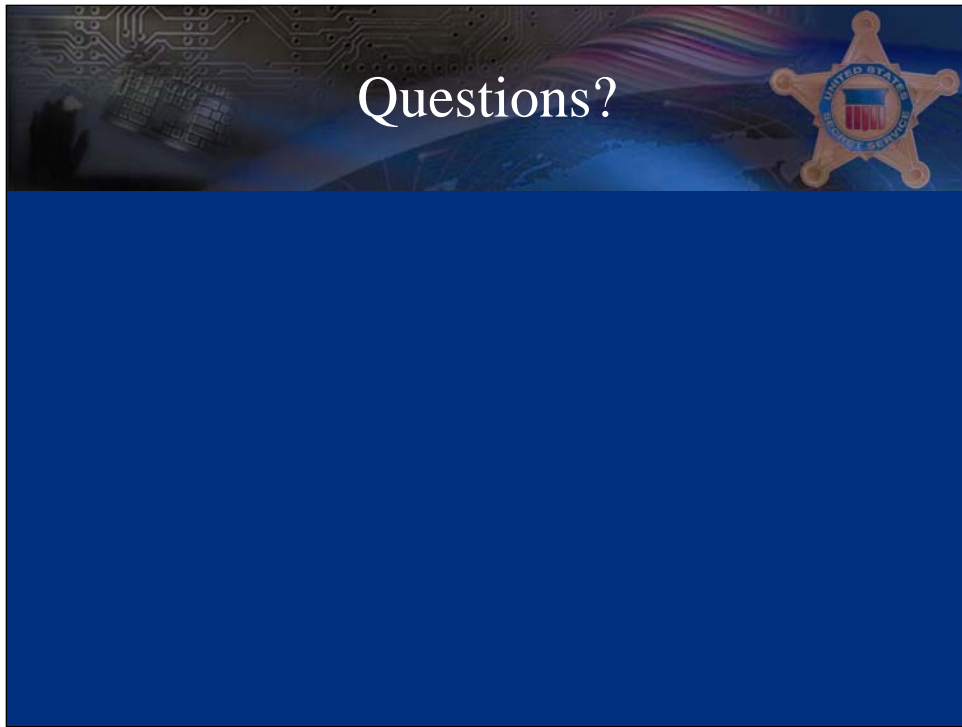
Property Type Crime: respective agency (In US: ICE, FBI,) Delito de Propiedad: la agencia competente (en EE.UU.: ICE, FBI)

La integración de la gestión del caso y la evidencia electrónica

\*Consulte con un examinador forense

\*¿Cuáles agencias/servicios están disponibles para procesar esta información?

\*La gestión del caso es la prioridad.



¿Preguntas?