

Mobile Telephones as Electronic Evidence




SA Matt Ralls

United States Secret Service, Oklahoma City Field Office

Teléfonos celulares como evidencia electrónica.

Agente Especial Mat Ralls

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



Cell phones are everywhere. What information can investigators obtain from this device and how can they preserve it for evidentiary purposes?

El teléfono celular se encuentra en todas partes. ¿Qué información pueden obtener los investigadores de este dispositivo y cómo la pueden conservar para los propósitos de evidencia?

Strategies



- What kind of evidence resides on mobile phones
- How to search and seize mobile phones
- What kind of evidence is held by service providers

Estrategias:

¿Qué clase de evidencia se encuentra en los teléfonos celulares?

Cómo registrar y confiscar teléfonos celulares

¿Qué clase de evidencia tienen los proveedores de servicio celular?

Where do You Encounter Cell Phones?

- Field Interviews
- Arrests
- Search Warrants
- Everywhere



¿Dónde se encuentran los teléfonos celulares?

Entrevistas en el campo
Arrestos
Ordenes de allanamiento
Por todas partes

Cell Phone Considerations



- Always consider every cell phones as evidence
- Determine if the suspect has one early in the investigation
- Remove and store the cell phone in a secure place when interviewing suspects (officer safety and securing data)
- Never let the suspect use their phone during an interview, treat it just like a computer

Consideraciones sobre teléfonos celulares

- Siempre considerar que todo teléfono celular es evidencia
- Determinar en las etapas tempranas de la investigación si el sospechoso tiene teléfono celular
- Remover y almacenar el teléfono celular en un lugar seguro cuando está entrevistando a los sospechosos (seguridad del agente y aseguramiento de los datos)
- Nunca permitir que el sospechoso utilice su teléfono durante una entrevista, tratarlo como si fuera computadora

Evidence Residing on Mobile Phones

- Call History –
 - received calls
 - dialed numbers
 - missed calls
 - call dates and durations
- Text Messages
- Contacts
- Datebook
- Scheduler
- Calendar
- To Do List
- Videos
- Pictures of Contraband
- Email
- Deleted Text Messages
- GPS Way Points

Discuss Eagle Pass SANCHEZ case where load car driver was communicating with scout via cell phone.

Hablar del caso de SÁNCHEZ en Eagle Pass, en el cual el conductor del automóvil con la carga estaba comunicándose con la persona de reconocimiento por medio de un teléfono celular.

Evidencia que se encuentra en los teléfonos celulares

Los registro de llamadas

- llamadas recibidas
- números marcados
- llamadas perdidas
- fechas y duraciones de llamadas

Mensajes de texto

Listas de contactos

Agenda

Programador

Calendario

Lista de Quehaceres

Videos

Fotos de Contrabando

Correos electrónicos

Mensajes de texto tachados

Puntos de ruta de GPS

When to examine a cell phone

- During initial interview
 - Consent/Search Incident to Arrest
 - make notes/documentation
 - need for immediate information
- By a forensic Examiner
 - Consent/Search Incident to Arrest/Warrant
 - Pull the Battery/Cell Phone Protective Bags
 - Power Cords/Data Cords

Cuando debe examinar un teléfono celular

- Durante la entrevista inicial
 - Consentimiento/Registro concomitante con el arresto
 - Apuntar notas/ documentación
 - La necesidad de información inmediata
- Por un examinador forense
 - Consentimiento/Registro concomitante con el arresto
 - Sacar la pila/ Bolsas protectoras para teléfonos celulares
 - Cables de alimentación/ cables de datos

Cell Phone Examinations



- Cell phones technology is extremely proprietary
- There is NO one certain way to analyze a cell phone.

Unlike computers, where two major operating systems exist in the world today, cell phones are extremely proprietary, with each manufacturers phone software differing from that of another and often from within the same maker of phones

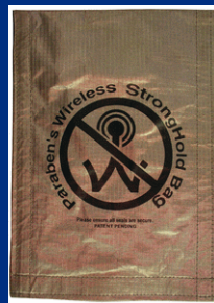
A diferencia de las computadoras, para las cuales existen dos sistemas operativos mayores en el mundo, los teléfonos celulares son extremadamente exclusivos - el software de cada proveedor se distingue de el de otros, muchas veces dentro del mismo fabricante de teléfonos.

La tecnología de los teléfonos celulares es muy exclusiva.

No hay una manera cierta/única de analizar un teléfono celular.

Searching and Seizing Mobile Phones (#1)

1. Maintain Power
2. Get the Phone “Off the Grid” utilizing a Faraday bag or even a paint can.
3. Seize power cords, data cables, manuals and media cards
4. Get the device to a forensic examiner as quickly as possible



Registrar y confiscar teléfonos celulares (#1)

1. Mantener la pila del celular con carga eléctrica
2. Poner el teléfono “incomunicado de las torres de la señal de servicio” utilizando una bolsa de efecto Faraday o una lata de pintura vacía.
3. Decomisar los cables de alimentación y de datos, los manuales y tarjetas de memoria.
4. Llevar el dispositivo a un examinador forense lo antes posible.



Llevarse todo.

Searching and Seizing Mobile Phones (#2)

- If there will be a delay until the phone gets analyzed, turn it off.
- Remove Battery
- Do not turn on the phone.



Registrar y confiscar teléfonos celulares (#2)

Si hará una demora en analizar el teléfono, debe apagarlo.

Retirar la pila del celular

No prender el teléfono.

Searching and Seizing Mobile Phones (#3)

- Sometimes, the only option you have is to “do it the old fashioned way”.
 - Take notes, pictures

Registrar y confiscar teléfonos celulares (#3)

A veces, la única opción que hay es "hacerlo a la antigua".
Tomar fotos y apuntar notas.

Reminders For All Methods:

- Take Everything
- Isolate the phone from the Network
- Do not remove media cards, SIM cards, etc
- Don't forget about latent prints, DNA and other trace evidence

13

Recordatorios para todos métodos utilizados:

Llevar todo con usted

Aislar el teléfono de la red

No retirar las tarjetas de memoria, tarjetas de SIM (tarjeta que le da la autenticidad al celular), etc

No olvidarse de las huellas digitales latentes, ADN y otros vestigios de evidencia

Evidence Held By Service Providers



- Depending on the legal process utilized, you may obtain:
 - Subscriber Information
 - Billing Information
 - Call Tolls, which will include the numbers involved in the call, date, time, etc.

Evidencia que tienen los proveedores de servicio celular.

Dependiendo del proceso legal que se utilizó, usted puede obtener

Información del suscriptor

Información de facturación

Registros de llamadas, los cuáles incluirán los números implicados en la llamada, la fecha, la hora, etc.

Questions?



- www.faradaybag.com
- www.cellbrite.com
- www.paraben.com
- www.ramseytest.com

¿Preguntas?