



PROBAR QUE EL SOSPECHOSO ESTABA A LA COMPUTADORA

Michelle Kane, Abogada Litigante
Sección de Delito Informático y de Propiedad Intelectual
División Penal, Departamento de Justicia



VISTA GENERAL

Probar que el acusado cometió el delito.

El papel de la prueba circunstancial.

Estrategias para recopilar y utilizar las pruebas circunstanciales en casos de Cibercrimen.

Conclusiones.



VISTA GENERAL

Probar que el acusado cometió el delito.

El papel de la prueba circunstancial.

Estrategias para recopilar y utilizar las pruebas circunstanciales en casos de Cibercrimen.

Conclusiones.



- Uno de los más grandes retos en la mayoría de los casos de delito informático es el de probar *quien* estaba usando la computadora.
- Esta comprobación casi siempre dependerá de algún tipo de *prueba circunstancial* .





Escenarios

Transferencia bancaria fraudulenta utilizando la cuenta del sospechoso, rastreada a una dirección IP asignada a la computadora del sospechoso.

Acceso no autorizado a una base de datos restringida desde el terminal de la computadora gubernamental del sospechoso.

Amenazas transmitidas mediante una cuenta de correo electrónico registrada a nombre del sospechoso.



**¿Cómo probar que
el sospechoso lo hizo?**



VISTA GENERAL

Probar que el acusado cometió el delito

El papel de prueba circunstancial

Estrategias para recopilar y utilizar las pruebas circunstanciales en casos de Cibercrimen

Conclusiones



Pruebas Circunstanciales

Definición: pruebas con base en la *inferencia*.

- Los sistemas legales nacionales pueden tratarlas de otra manera, pero generalmente se distinguen de las “pruebas directas”.
- La aserción de un “hecho colateral” que permite que se infiera un hecho clave del caso.

Inferencia de que *el sospechoso cometió el delito.*



Pruebas Circunstanciales

Las pruebas electrónicas pueden conducir a una computadora, pero no a una *persona*.

Sin pruebas directas que vinculan la persona con el delito, busque pruebas circunstanciales de :

- Acceso.
- Conocimiento.
- Oportunidad.
- Motivo.
- Estado mental.



VISTA GENERAL

Probar que el acusado cometió el delito.

El papel de la prueba circunstancial.

Estrategias para recopilar y utilizar las pruebas circunstanciales en casos de Cibercrimen.

Conclusiones.



Acceso

El acceso del sospechoso a los recursos informáticos utilizados para cometer el delito.

- **Computadora (hardware, software, archivos).**
- **Líneas telefónicas o de cable utilizadas para obtener acceso en línea.**
- **Cuentas en línea (correo electrónico, banca en línea, redes sociales).**

Puede ser necesario descartar a otros que tenían acceso



Conocimiento

El *conocimiento* del sospechoso de la información que tiene relación al delito.

- **Experiencia con el programa, sistema o red que fue utilizada o comprometida.**
- **Formación, educación, experiencia o habilidades en Informática.**
- **Familiaridad con los hechos específicos relacionados con el delito.**
- **Posesión de claves.**



Oportunidad

La *oportunidad* del sospechoso para cometer el delito.

- **Uso de una computadora en el momento de realizarse la actividad delictuosa.**
- **No tener coartada creíble.**



Oportunidad

El *motivo* del sospechoso para cometer el delito.

- **Venganza.**
- **Dinero (incluyendo chantaje, extorsión).**
- **Política.**
- **Reto personal.**



Estado mental

El *estado mental* culpable del sospechoso.

- Decepción.
- Ocultación.
- Destrucción de pruebas.



No se olvide de las herramientas tradicionales

La mejor prueba circunstancial puede originarse de tareas tradicionales de detección, tales como:

- Entrevistas del sospechoso y testigos.
- Pruebas físicas.
- Vigilancia.

Las pruebas tradicionales pueden corroborar las pruebas electrónicas



VISTA GENERAL

Probar que el acusado cometió el delito.

El papel de la prueba circunstancial.

Estrategias para recopilar y utilizar las pruebas circunstanciales en casos de Cibercrimen

Conclusiones



Conclusiones

Las pruebas circunstanciales proporcionan el vínculo clave entre el sospechoso y la computadora.

Las pruebas circunstanciales tradicionales complementan a las pruebas electrónicas, formando un caso más fuerte de que el sospechoso era responsable



¿Cómo refutar las tácticas de la defensa?



VISTA GENERAL

Defensas comunes para cibercrímenes.

Las tácticas de la defensa y las maneras de refutarlas.

Conclusiones.



VISTA GENERAL

Defensas comunes para cibercrímenes.

Las tácticas de la defensa y las maneras de refutarlas.

Conclusiones.



Principios Universales

Los acusados en todo el mundo utilizan enfoques similares en los casos de Cibercrimen.

- **Confundir todo.**
- **Implicar la culpabilidad o malos motivos de todos los testigos (menos el acusado)**
- **Hacer creer que la tecnología y pruebas son incomprensibles.**



Tácticas comunes de la defensa de Cibercrimen

Usar la tecnología para generar confusión.

Señalar la carencia de pruebas directas.

Alegar no tener habilidades en lo técnico.

Sugerir que alguien más controlaba la computadora.

**Implicar que las pruebas fueron colocadas por las
autoridades**



VISTA GENERAL

Defensas comunes para Cibercrímenes.

Las tácticas de la Defensa y las maneras de refutarlas.

Conclusiones.



Usar la tecnología para generar confusión

La Defensa:

- Hará aparecer que la tecnología es más complicada de lo que es en realidad.
- Explotará el miedo general de tecnología y computadoras.
- Creará dudas en la mente de la persona buscando los hechos.
- “Si yo no puedo entender los hechos, ¿cómo puedo estar seguro que el acusado lo hizo?”



Usar la tecnología para generar confusión: Respuesta

Simplificar todo.

Presentar y explicar la tecnología en una etapa temprana.

Conocer su audiencia.

Preparar a los testigos para que expliquen la tecnología usando lenguaje claro.

Utilizar ayudas visuales y pruebas.



Usar la tecnología para generar confusión: Respuesta

No se olvide presentar pruebas no electrónicas.

- Testigos de los hechos.
- Registros de vigilancia.
- Pruebas físicas.
- Motivo.
- Comportamiento sospechoso.

Éstas corroborarán las pruebas electrónicas.



Señalar la carencia de pruebas directas o físicas

La Defensa:

- Alegará que su caso depende de la “prueba circunstancial”.
- Señalará la carencia de pruebas físicas, tales como pruebas de ADN o huellas digitales.
- Sugerirá que esto hace que su caso es más débil que uno basado en pruebas “directas”.



Señalar la carencia de pruebas directas o físicas: Respuesta

Alegar (si es posible) que la prueba circunstancial es tan convincente que la prueba directa.

Explicar que la carencia de pruebas “directas” es típica para los casos de delito informático.

Dar énfasis en la carencia de un sospechoso alternativo viable.



Alegar no tener habilidades en lo técnico

La Defensa:

- Alegará que el delito requirió a una persona con pericia especial en computadoras.
- Sugerirá que el acusado no tiene habilidades especiales o no es lo suficiente inteligente para haber llevado a cabo los hechos ilícitos.

Lo anterior a menudo se combina con la primera táctica – generar confusión mediante la tecnología.

“Hacerse el tonto”



Alegar no tener habilidades en lo técnico: Respuesta

Investigar los antecedentes de su acusado en cuanto a lo técnico.

El equipo y software puede demostrar la sofisticación.

Examinar la historia en el Internet para un registro indicando auto-educación.

Entrevistar al sospechoso y sus asociados en cuanto a conocimientos sobre informática.



Sugerir que alguien más controlaba la computadora

La Defensa:

- Alegará que la computadora o el servicio fue secuestrado por un agente desconocido.
- “Un virus tomó control de la computadora y descargó el material del Internet”
- “El correo electrónico fue falsificado”

Lo anterior a menudo se combina con la primera táctica – generar confusión mediante la tecnología.



Sugerir que alguien más controlaba la computadora: Respuesta

Demostrar la manera en que el acceso a la computadora del sospechoso fue limitado.

Demostrar que otros que tenían acceso a la computadora no cometieron el delito.

Explicar (mediante el examinador forense) como es que sabemos que ningún programa ajeno ni otra persona controló la computadora.



Implicar que las pruebas fueron colocadas

La Defensa :

- Atacará la toma de las pruebas electrónicas, la cadena de custodia, y el estudio forense.
- Intentará impugnar al examinador forense y a cada persona que tocó las pruebas.



Implicar que las pruebas fueron colocadas: Respuesta

Demostrar una cadena de custodia segura de los medios digitales.

Presentar registros que indican el momento en que los archivos del sospechoso fueron creados, entrados o modificados.

Describir en el tribunal los dispositivos utilizados para crear imágenes y grabar las pruebas.

Explicar las salvaguardas del proceso forense



CONCLUSIONES

La misma tecnología y pruebas electrónicas pueden ser utilizadas por la defensa para confundir y por el fiscal para iluminar.

Fiscales, agentes de policía e investigadores, trabajando juntos, de manera efectiva pueden anticipar, prepararse para, y refutar las defensas comunes para Cibercrimen.



Preguntas



WWW.CYBERCRIME.GOV

Computer Crime and Intellectual Property Section (CCIPS)
of the Criminal Division of the U.S. Department of Justice