MINISTERIO DEL INTERIOR

GUARDIA CIVIL

LA INVESTIGACIÓN DE LOS DELITOS INFORMÁTICOS EN LA GUARDIA CIVIL

Juan Salom Clotet
Comandante de la Guardia Civil
Jefe del Grupo de Delitos Telemáticos

Jueves 22 de septiembre de 2005

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

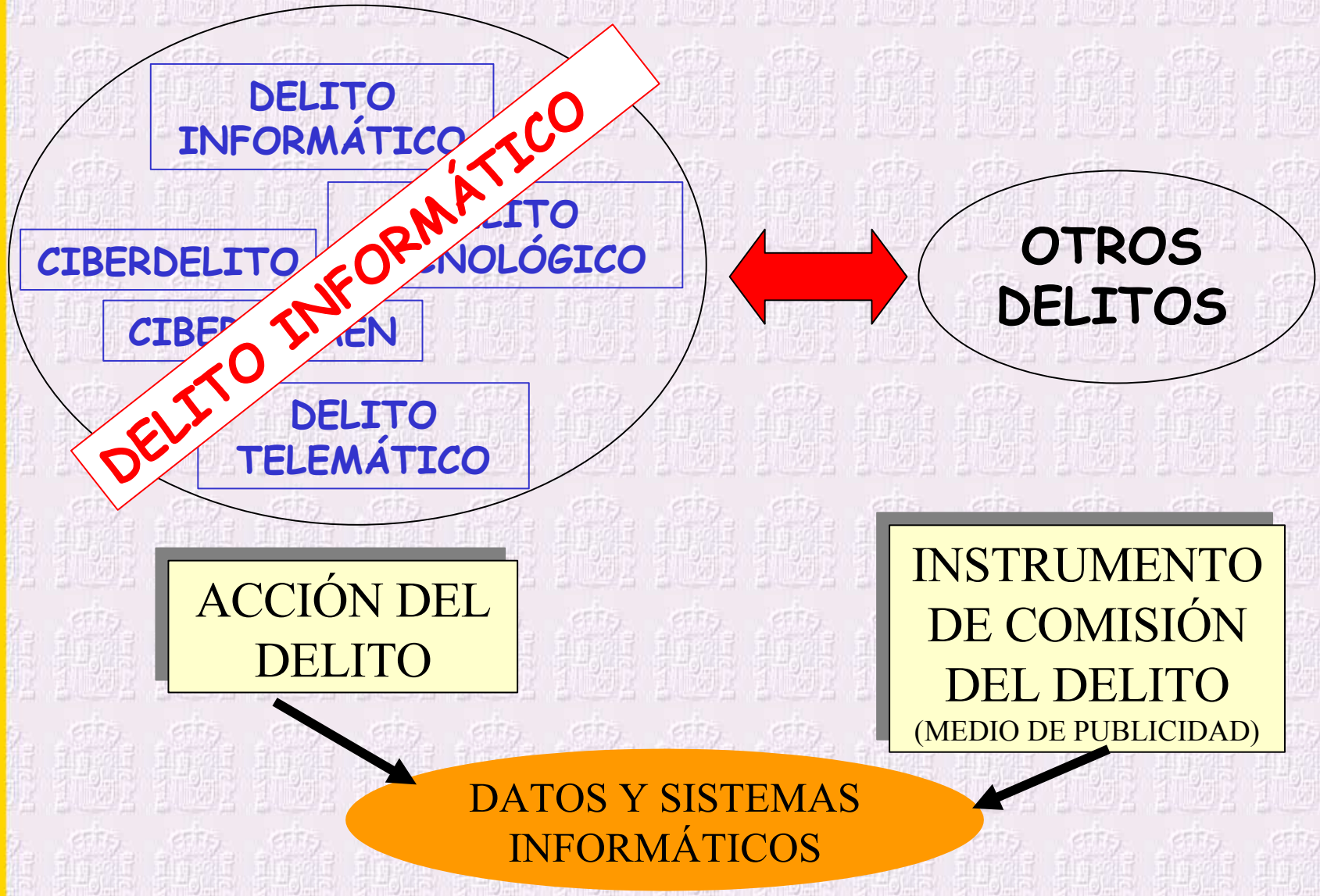
Índice

1. **DELITO INFORMÁTICO**
   - ¿Delito informático?.
   - Convenio Ciberdelincuencia del Consejo de Europa.
   - Respuesta de la Guardia Civil a la delincuencia informática. El GDT
2. **INVESTIGACIÓN DELINCUENCIA INFORMÁTICA**
   - Metodología de investigación.
3. **PROBLEMÁTICA DE LA INVESTIGACIÓN**
   - Conservación de datos de tráfico.
   - Imposibilidad de identificación de usuario.
   - Virtualidad de la prueba informática.
   - Determinación espacial de la Ley penal.
   - Mundo digital desconocido. Judicatura.

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

¿DELITO INFORMÁTICO?



MINISTERIO DEL INTERIOR

GUARDIA CIVIL

¿DELITO INFORMÁTICO?

CONVENIO SOBRE CIBERDELINCUENCIA CONSEJO DE EUROPA

(Copia oficial en castellano en www.guardiacivil.org/telematicos)

Mandato: 1997 Creación Comité de expertos { $3\frac{1}{2}$ años; 25 borradores

Formación: 45 países + EEUU + Canadá + Sudáfrica + Japón

Firmado en Budapest el 23 de noviembre de 2001.

Ratificación: Albania (20-6-02), Croacia (17-10-02), Estonia (12-5-03), Hungría (4-12-03), Lituania (2-03-04), Rumania (12-5-04), Eslovenia (8-9-04) y Macedonia (15-9-04)

Protocolo Adicional al Convenio para criminalizar los actos de racismo y xenofobia cometidos a través de sistemas informáticos (28-01-03)

Medidas de *derecho penal sustantivo* que deberán adoptarse a nivel nacional

Medidas de *derecho procesal* que deberán adoptarse a nivel nacional

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

¿DELITO INFORMÁTICO?

Medidas de *derecho penal sustantivo* que deberán adoptarse a nivel nacional

"Prop Intelec"

"hacking"

"falsificación y fraudes"

"pedofilia"

DELITOS RELACIONADOS CON INFRACIONES DE LA PROPIEDAD INTELECTUAL Y DE LOS DERECHOS AFINES

DELITOS CONTRA LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE DATOS Y SISTEMAS INFORMÁTICOS

- Descubrimiento y revelación de secreto y acceso ilegal (197)
- Apoderamiento de secreto de empresa (278)
- Daños en datos y sistema informático (264)
- Abuso de los dispositivos (270)

DELITOS INFORMÁTICOS

- Falsedad documental (390 y ss.)
- Estafa informática (248)
- Defraudación en fluido telecomunicaciones (255 y 256)

DELITOS RELACIONADOS CON EL CONTENIDO

- Difusión de pornografía infantil (189)
- Provocación sexual y prostitución (186 y 187)
- Amenazas (169), injurias (208) y calumnias (205)
- Apología racismo y xenofobia (607)

GRUPO DE DELITOS TELEMÁTICOS

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

RESPUESTA DE LA GUARDIA FRENTE A LOS DELITOS TECNOLÓGICOS (1)

Año 1996: Creación Grupo Delitos Informáticos

Año 1999: Grupo de Delitos Alta Tecnología

Año 2000: Departamento Delitos Telemáticos

Año 2003: Grupo de Delitos Telemáticos
Departamento de Informática y electrónica
Inicio del proceso de descentralización

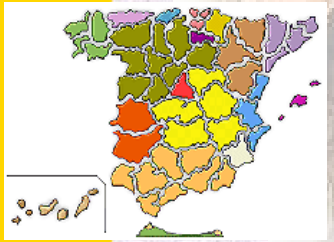
MINISTERIO DEL INTERIOR

GUARDIA CIVIL

RESPUESTA DE LA GUARDIA FRENTE A LOS DELITOS TECNOLÓGICOS (2)

SERVICIO DE POLICÍA JUDICIAL

- LABORATORIO CRIMINALÍSTICA
  - DEPARTAMENTO DE ELECTRÓNICA E INFORMÁTICA
- UNIDAD DE ANÁLISIS
  - SECCIÓN DELINCUENCIA ESPECIALIZADA
- UNIDAD CENTRAL OPERATIVA
  - DROGAS
  - DELINCUENCIA ORGANIZADA
  - DELINCUENCIA ECONÓMICA
  - GRUPO DELITOS TELEMÁTICOS
  - GRUPO APOYO
- U,s TERRRITORIALES
  - U.O.P.J. (Eq. Inves. Tecno.)



MINISTERIO DEL INTERIOR

GUARDIA CIVIL

FUNCIONES DEL GDT

- Desarrollo de investigaciones relacionadas con la delincuencia informática.
- Apoyo a aspectos técnicos del resto de investigaciones de la UCO.
- Formación del personal de los equipos de investigación tecnológica de las distintas Comandancias.
- Dirección técnica de los Equipos de investigación tecnológica.
- Representar y promover la participación de la Guardia Civil en foros y encuentros internacionales sobre cibercrimen.
- Punto de contacto de cooperación internacional en el ámbito de cibercrimen

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

UNIDAD DE POLICÍA JUDICIAL

UNIDAD CENTRAL

GDT

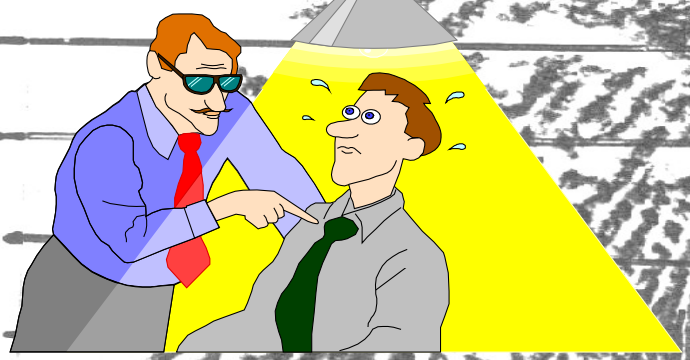
GUARDIA CIVIL

- Conocimientos de informática
- Conocimientos técnica procesal penal
- Experiencia investigadora
- Relaciones internacionales
- Prestigio y confiabilidad en la judicatura
- Proyección temporal en la investigación
- Discreción

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

INVESTIGACIÓN DEL DELITO



OBJETIVO INVESTIGACIÓN

"Identificar y localizar delincuente"

"Asegurar y presentar las pruebas del delito"

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

Investigación tecnológica + clásica

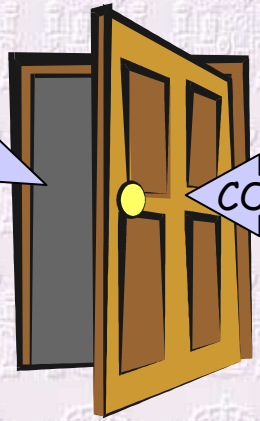
OPERADORA

PROVEEDOR DE ACCESO

PRESTADOR DE SERVICIOS

abonado

ACCESO



COMUNICACIÓN

equipo

USUARIO

Web
Chat
Foros
Telefonía
Mail
Comercio electrónico
Consultoría
...

"DATOS DE TRÁFICO"

Núm. IP (198.23.55.255)

FECHA Y HORA

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

METODOLOGÍA DE INVESTIGACIÓN POLICIAL (1)

¿cómo?

IDENTIFICACIÓN
OBTENCIÓN DE PRUEBAS

1. FASE PREVIA. ¿qué ha pasado?

1. FASE DE INVESTIGACIÓN. ¿cómo y quién lo ha hecho?

1. FASE DE INCRIMINACIÓN. Asegurar y presentar la prueba

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

METODOLOGÍA DE INVESTIGACIÓN POLICIAL (2)

1. FASE PREVIA. ¿qué ha pasado?

- Denuncia – Conocimiento delito público
- Recogida de evidencias del delito (~inspección ocular)

  Recuperación de logs, mensajes, backups, imágenes (volcado), …

  Penalidad añadida a la víctima.

  Auxilio administradores de sistemas afectados.

  Acreditar el delito.

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

METODOLOGÍA DE INVESTIGACIÓN POLICIAL (3)

1. FASE PREVIA. ¿qué ha pasado?
1. **FASE DE INVESTIGACIÓN. ¿cómo y quién lo ha hecho?**

- Análisis de evidencias y búsqueda de indicios de autoría
- Búsqueda de información (ayudas externas) y referencias identificativas (vanidad)
- Resolución de "datos de tráfico" de indicios y referencias identificativas (ISP,s)
- Identificación y localización (teléfono)
- Vigilancia
- Interceptación de telecomunicaciones (teléfono, e-mail, sniffers, ADSL)

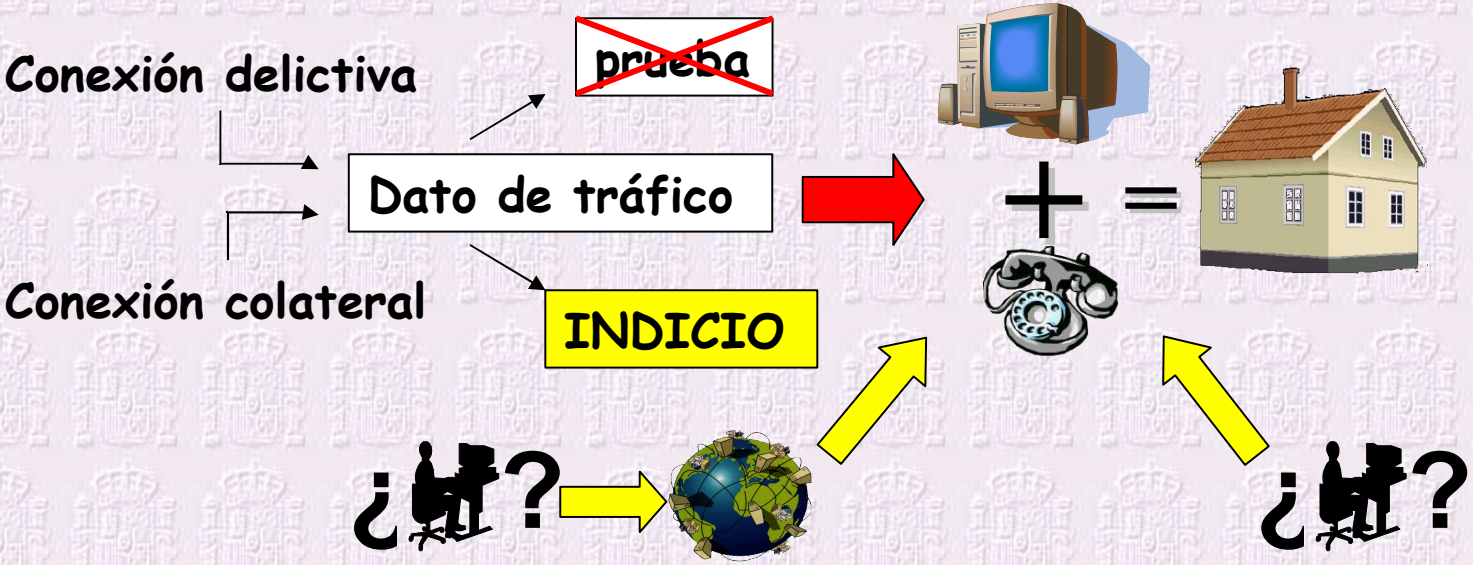
MINISTERIO DEL INTERIOR

GUARDIA CIVIL

METODOLOGÍA DE INVESTIGACIÓN POLICIAL (4)

1. FASE PREVIA. ¿qué ha pasado?

1. FASE DE INVESTIGACIÓN. ¿cómo y quién lo ha hecho?



MINISTERIO DEL INTERIOR

GUARDIA CIVIL

METODOLOGÍA DE INVESTIGACIÓN POLICIAL (5)

¿PRUEBA INFORMÁTICA?

PRUEBA DE INDICIOS

(STS 202/98 y 437/98)

- **PLURALES**
- **ACREDITADOS**
- **COHERENTES ENTRE SI**
- **ENLACE PRECISO Y DIRECTO** entre indicio y hecho determinante de la responsabilidad según las reglas de la lógica y la experiencia.

- **Datos de tráfico de las conexiones de autoría o relacionadas**
- **Sistema informático intervenido**
- **Activos patrimoniales defraudados**
- **Objetos vinculados al delito**

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

METODOLOGÍA DE INVESTIGACIÓN POLICIAL (6)

1. FASE PREVIA. ¿qué ha pasado?
1. FASE DE INVESTIGACIÓN. ¿cómo y quién lo ha hecho?
1. **FASE DE INCRIMINACIÓN. Asegurar y presentar la prueba**

    1) Registro e incautación (protocolo validación de la prueba)

    2) Análisis forense de sistema y soportes intervenidos

    3) Informe policial incriminatorio

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

REGISTRO E INCAUTACIÓN DE LA PRUEBA (1)

OBJETIVO DEL REGISTRO DOMICILIARIO

- Intervención de dispositivos informáticos susceptibles de contener indicios de criminalidad.
- Obtención de indicios que vinculen equipo y usuario (ubicación, titularidad, declaración, …)
- Intervención de sistemas para decomiso de los efectos del delito.

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

REGISTRO E INCAUTACIÓN DE LA PRUEBA (2)

PROBLEMÁTICA DEL REGISTRO DOMICILIARIO

- Medida restrictiva de derecho fundamental: Necesidad de JUSTIFICACIÓN y PROPORCIONALIDAD del registro frente al mal causado (juicio de necesidad, idoneidad y proporcionalidad).
- Incomprensión del alcance de la intervención (rechazo a la intervención de diverso material tecnológico)
- Desconocimiento generalizado de formas y necesidades de precinto.
- Secretario judicial, ¿fedatario público o instructor?

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

ANALISIS DE MATERIAL INTERVENIDO (1)

OBJETIVO DEL ANÁLISIS

- Localización, identificación y aseguramiento de cuantas evidencias se hallen para construir la prueba de indicios.

- Localización, identificación y aseguramiento de cuantas evidencias se hallen que vinculen equipo informático, usuario e indicios .

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

ANALISIS DE MATERIAL INTERVENIDO (2)

PRÁCTICA DEL ANÁLISIS DEL MATEIAL INFORMÁTICO

2. Volcado de dispositivos de almacenamiento de información (imagen o copia bit a bit) (principio de contradicción y mínima injerencia en la prueba) (backup, copia de ficheros)
    - Equipos informáticos intervenidos
    - Dispositivos intervenidos de almacenamiento de información digital removible.
3. Estudio TÉCNICO POLICIAL "TP", sobre todo el material intervenido
    - Equipos informáticos intervenidos (volcados u originales protegidos)
    - Backups o copias de ficheros de información
    - Dispositivos de almacenamiento de información digital intervenidos
    - Documentación intervenida

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

ANALISIS DE MATERIAL INTERVENIDO (3)

PROBLEMÁTICA DEL PROCESO DE ANÁLISIS

- Desconocimiento generalizado en el estamento judicial.
- Ausencia de protocolo de volcado y análisis homologados.
- Sistemas hardware, software, no homologados.
- Sistemas propietarios, no open source
- Sistemas lentos con elevadas incidencias. (Firma digital, Timestamping).
- Sistemas caros (HD). Se mantiene la identidad digital.
- Limitaciones por cifrado.
- Posibilidad de falsificación de indicios (coartadas).

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

INFORME POLICIAL INCRIMINATORIO

- Descripción del conjunto de evidencias electrónicas que interrelacionadas conducen por un razonamiento lógico a una conclusión de culpabilidad.

- Traducción del lenguaje técnico informático a un lenguaje coloquial y comprensible para profanos en la materia.

- Descripción de los protocolos de actuación utilizados en el proceso de análisis.

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

Problemática de la investigación

1. CONSERVACIÓN DE LOS DATOS DE TRÁFICO

No conservación = impunidad

Excepto Activo patrimonial (Fraudes)

LEY 34/02 "LSSIyCE"

Artículo 12. Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas.

1. Los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses, en los términos establecidos en este artículo y en su normativa de desarrollo.

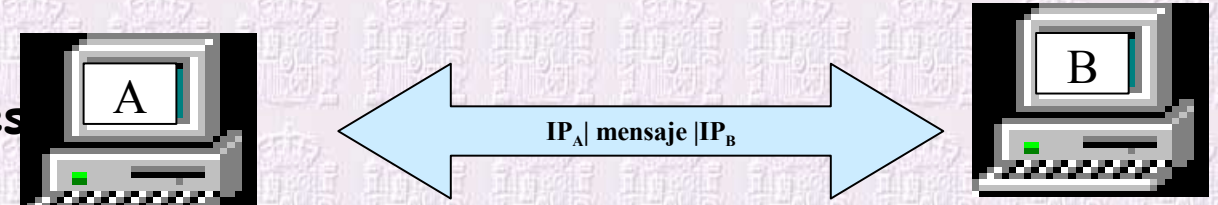
MINISTERIO DEL INTERIOR

GUARDIA CIVIL

Problemática de la investigación

1. IMPOSIBILIDAD DE IDENTIFICACIÓN DEL USUARIO

- Empresas
- Universidades
- Cibercafés
- Conexiones a redes WiFi
- Telefonía prepago



= IMPUNIDAD

AUSENCIA de legislación administrativa sobre cibercafés, telefonía prepago, …

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

Problemática de la investigación

VIRTUALIDAD DE LA PRUEBA INFORMÁTICA

¿PRUEBA INFORMÁTICA?

POSIBILIDAD DE FALSIFICACIÓN

Diseño de coartadas

Carga de la prueba

FACILIDAD DE ELIMINACIÓN

Sistemas borrados

HD formateados

CIFRADO ESTEGANOGRAFÍA

Inaccesibilidad

¿Negativa = indicio?

= IMPUNIDAD

Problemática de la investigación

DETERMINACIÓN ESPACIAL DE LA LEY PENAL

ACCIÓN ⟷ RESULTADO

Diferencia espacio - temporal

1º Espacio jurídico español

Problema de competencia ¿Qué Tribunal Penal debe perseguir hechos?

2º Diferentes espacios jurídicos

Problema de legislación aplicable y de competencia

Problemática de la investigación

DIFICULTAD DE COMPRENSIÓN DEL MUNDO DIGITAL Y LAS REDES DE COMUNICACIONES

- Desconocimiento de la Judicatura ¿Jurisdicción especializada?
- Cultura social = "Travesuras de niños" (hacktivismo, hacking blanco o ético)
- Aplicación de pena accesoria del decomiso (art 127 C.P.)

ESPACIOS DE IMPUNIDAD EN LAS TI

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

Dirección General
Guardia Civil

C/ Guzmán El Bueno, 110
28003 Madrid (España)

www.guardiacivil.org
delitostelematicos@guardiacivil.org

Tel. 91 514 64 00
Fax. 91 514 64 02

MINISTERIO DEL INTERIOR

GUARDIA CIVIL

Noticias: Hacker absuelto del ataque al puerto de Houston - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Multimedia

Dirección http://www.delitosinformaticos.com/seguridad/noticias/106658942584633.shtml

Ir Vínculos

delitosinformaticos.com

Servicios
. Adecuación a LSSI
. Consultas jurídicas
. Protección Datos
. Contratos
. Propiedad Intelectual
. Firma Electrónica
. Defensa Jurídica
. Reclamaciones
Información
. Noticias
. Archivo noticias
. Denuncias
. Mapa del WEB
. Seguridad/PGP
Comunidad
. Agenda
. Boletín
. Lista correo
. Buzón sugerencias
. Publica tu artículo
. Encuesta
. Antivirus
. Utilidades
. Bibliografía
Temas
. Portada
. Audiovisual
. Ciberderechos
. Delitos
. E-commerce
. Estafas
. Firma Electrónica
. Fiscalidad
. Hacking
. LSSI

Búsqueda Búsqueda avanzada

Noticias

- Hacker absuelto del ataque al puerto de Houston [19-10-03]

Un hacker británico fue absuelto el pasado viernes de la acusación de haber atacado y dejar sin servicio los sistemas del puerto de la ciudad estadounidense de Houston, uno de los más grandes del mundo, en septiembre de 2001. Aaron Caffrey, que ahora tiene 19 años, ha alegado que su ordenador fue secuestrado y que él no tenía conocimiento del ataque.

Hace dos años, los sistemas del puerto de de Houston se vieron afectados por un ataque DoS, que dejó sin servicio la web que consultan los pilotos de las embarcaciones y demás personal del puerto, y que contiene información crítica necesaria para realizar sus trabajos. Tras varios meses de investigación, todo apuntaba hacia Aaron Caffrey que vive en Shaftsbury y es ligeramente autista, como autor del ataque. Se le acusó de infectar el ordenador central del puerto de Houston, mientras planeaba la distribución masiva de un programa, cuyo fin era asaltar electrónicamente a una mujer que insultó a su novia americana en un chat público. En la organización de su venganza, el código se le había escapado de las manos y atacó inadvertidamente los sistemas del puerto.

Caffrey dijo pertenecer a un grupo de hackers conocido como Allied Haxor Elite, y confesó haber violado la seguridad de muchos servidores siempre con el consentimiento de sus legítimos dueños. Decía actuar siempre con el fin de comprobar la seguridad de los sistemas.

Su defensa consistió en alegar que su máquina había sido infectada con algún tipo de software que realizó el ataque sin su conocimiento. Afirmó rotundamente que no tenía nada que ver con el ataque, y que en todo caso, él mismo era la víctima de un intento de suplantación de identidad, pues habían conseguido realizar un ataque desde su propio sistema sin su conocimiento. Podía incluso proporcionar los apodos de los hackers que consiguieron secuestrar su conexión: Dry Ice y Friction. Cuando su ordenador fue confiscado, no hubo forma de demostrar que allí hubiese instalado un "caballo de troya" o programa de control remoto, a lo que Caffrey, que testificó en su propio juicio como experto, alegó que el software podía estar programado para autodestruirse sin dejar rastro una vez cumplido su objetivo.

La corte de Southwark Crown ha decidido finalmente que Caffrey no es culpable del ataque, aceptando la (muy

Internet