Universidad Internacional SEK

Análisis jurídico-técnico de la informática forense en el Ecuador y estudio del procedimiento forense aplicado en casos reales

Mario de la Cruz
Directora: Dra. Isabel Maya

Agenda

- Objetivo
- Antecedentes
- Informática Forense
- Análisis jurídico-técnico
- Fases de la Informática Forense
- Análisis de caso
- Conclusiones y recomendaciones

Objetivo

Objetivo

- Realizar análisis jurídico-técnico de la informática forense en el Ecuador y estudio del procedimiento forense aplicado en casos reales

Agenda

- Antecedentes
- Informática Forense
- Análisis jurídico-técnico
- Fases de la Informática Forense
- Análisis de caso
- Conclusiones y recomendaciones

Antecedentes

Antecedentes

- Situación jurídica del Ecuador
- Los Rogues significan el 15% del malware identificado en la web
- Robo de información

Cyberguerra

Cyberguerra

- Stuxnet (febrero 2011)
- Duqu (octubre 2011)
- Flame (mayo 2012)

Agenda

- Informática Forense
- Análisis jurídico-técnico
- Fases de la Informática Forense
- Análisis de caso
- Conclusiones y recomendaciones

Informática forense

¿Qué es?

- La Informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos

Utilidad

- Auditoria
- Resolución de casos

Clasificación

- Análisis en vivo
- Análisis en cadáver

Análisis en vivo

- Se realiza en el equipo comprometido

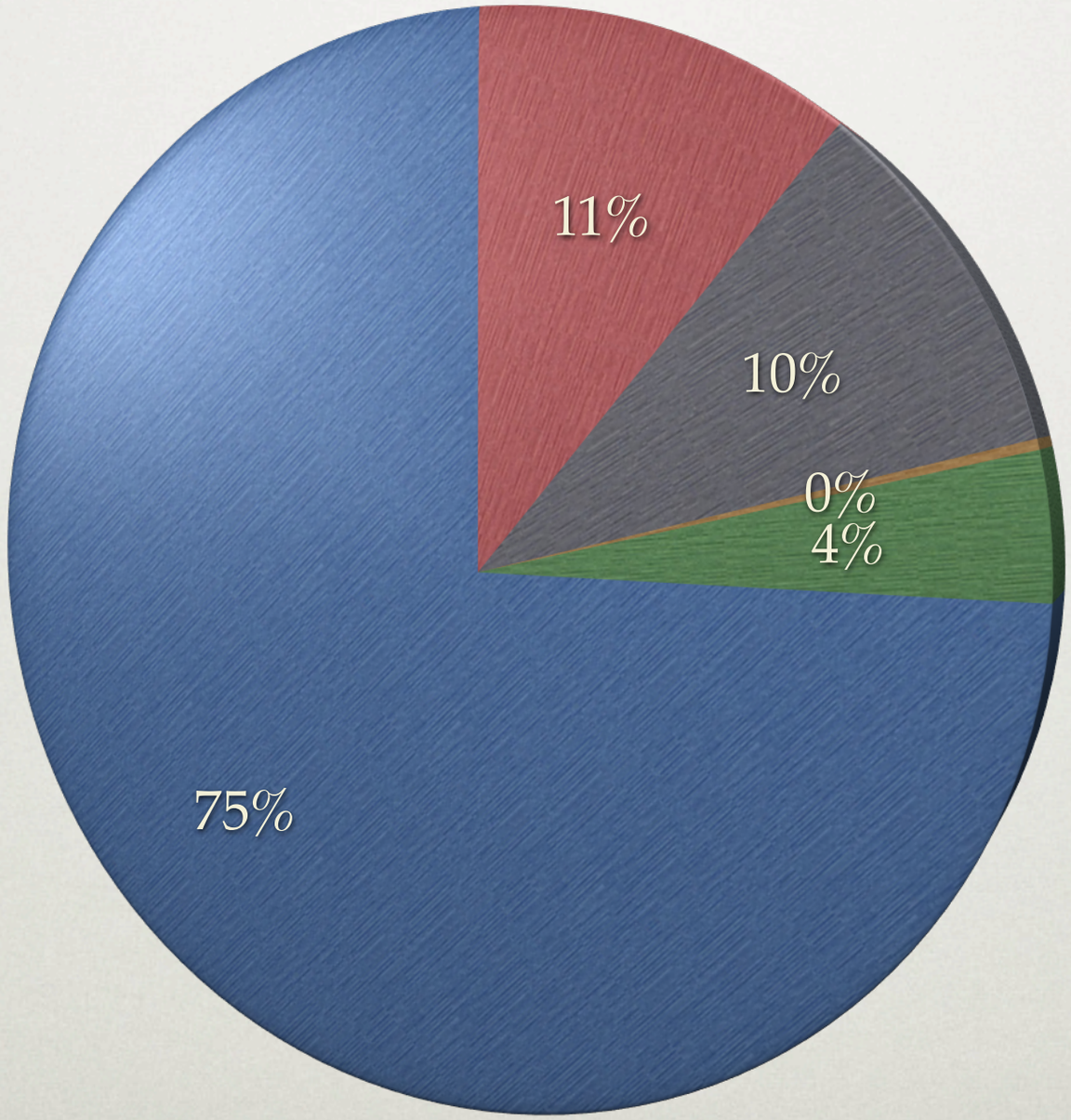
Análisis en cadáver

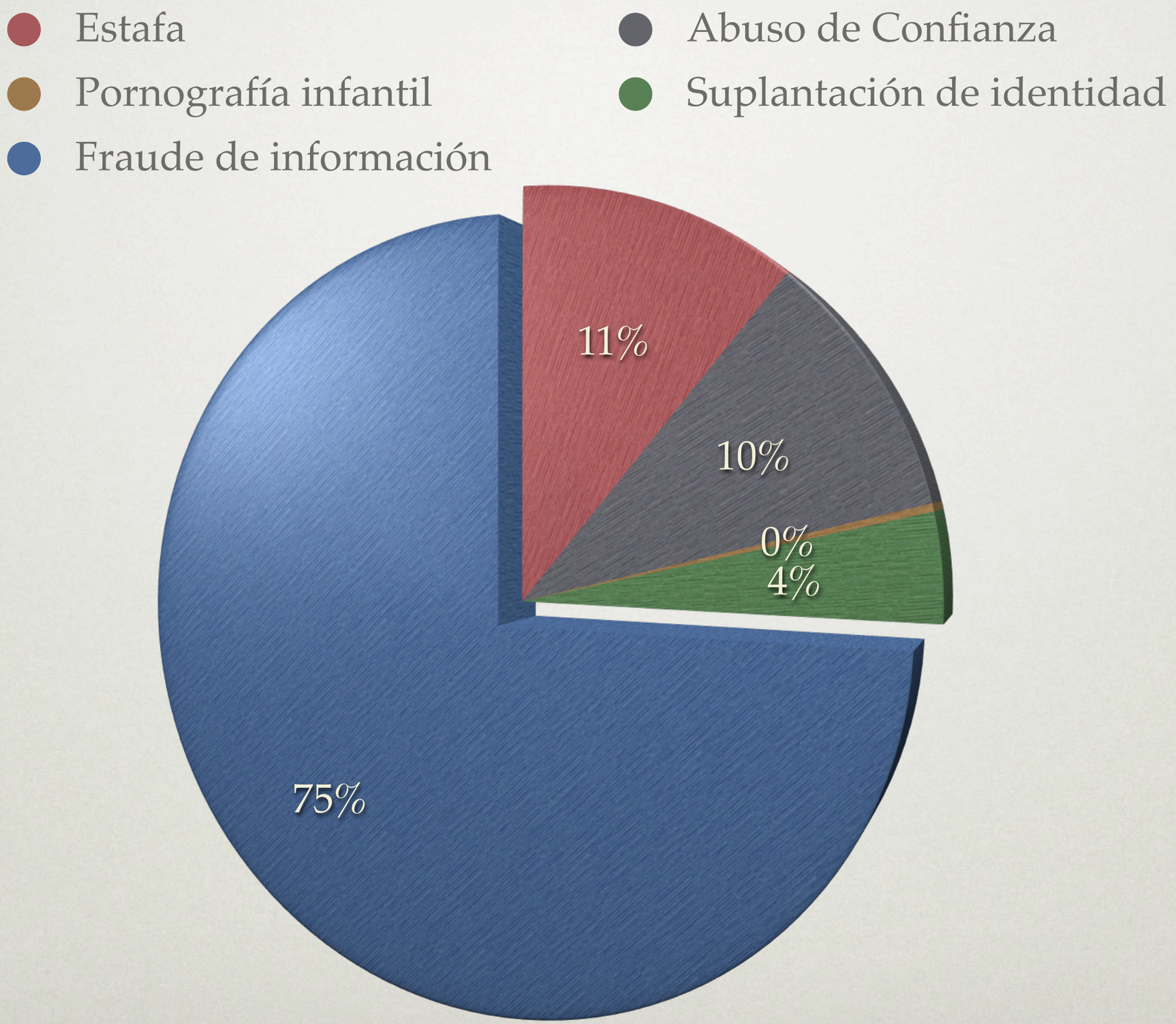
- Se realiza en una imagen del disco

Situación en Ecuador

Delito	Denuncias (2005-2010)
Estafa	861
Abuso de confianza	774
Pornografía infantil	23
Suplantación de identidad	313
Fraude de información	5.803

- Estafa
- Abuso de Confianza
- Pornografía infantil
- Suplantación de identidad
- Fraude de información




Estafa
Abuso de Confianza
Pornografía infantil
Suplantación de identidad
Fraude de información
11%
10%
0%
4%
75%

Agenda

- Análisis jurídico-técnico
- Fases de la Informática Forense
- Análisis de caso
- Conclusiones y recomendaciones

Análisis jurídico-técnico

Análisis jurídico

Cuerpos legales

Código Penal	Regula toda actitud dolosa
Código Civil	Intercambio comercial
Ley de Comercio Electrónico, Firmas Digitales y Mensajes de datos	Regula mensajes de datos

Interjudicialidad

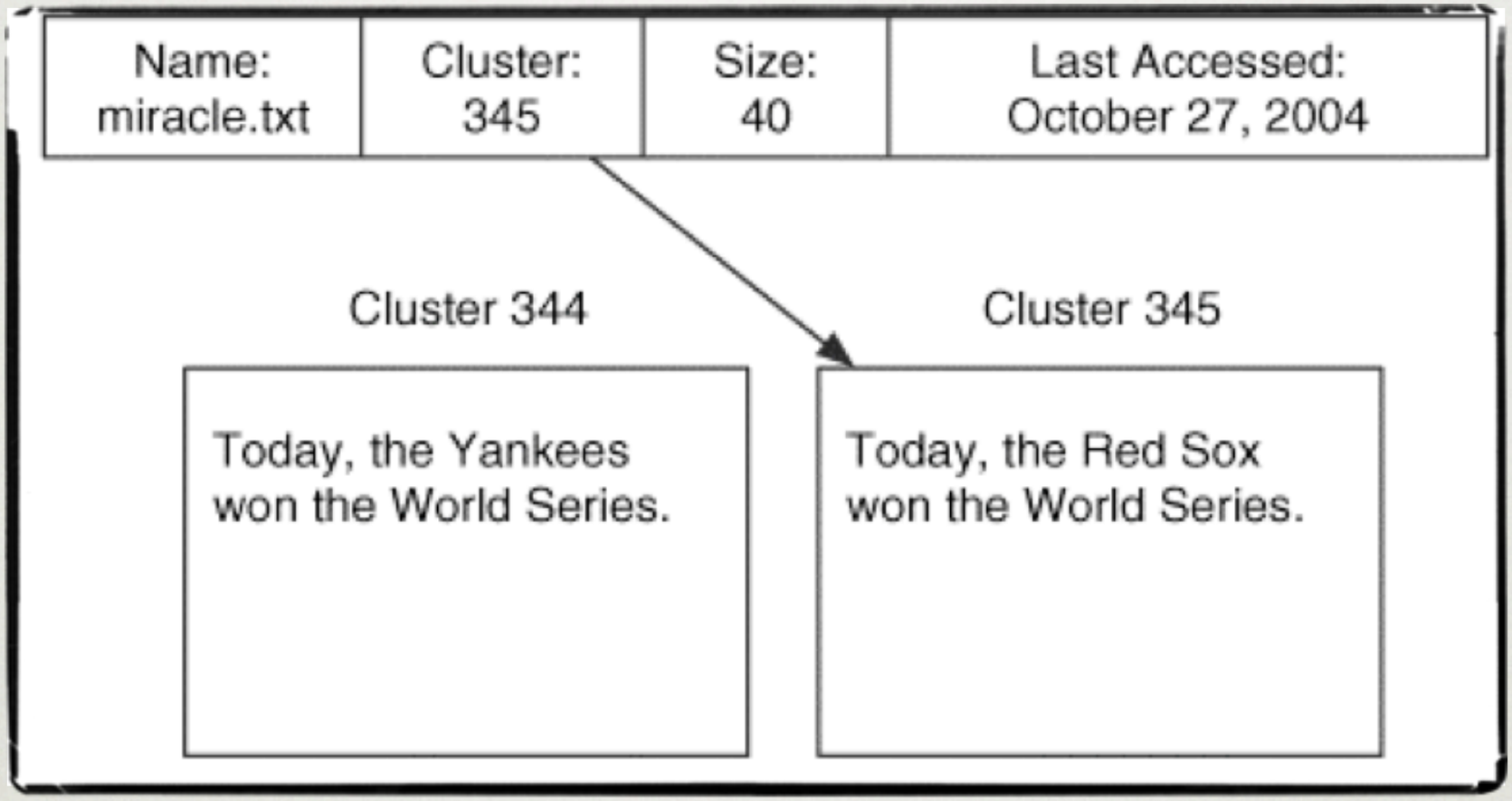
- Delito: tipificado en el Código Penal
- Reconocido como medio del delito: Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos
- Indemnización económica: Código Civil

Análisis técnico

Guía general

Datos esenciales y no esenciales

Esenciales	No esenciales
Confiables	No fiable
Necesario para proceso de lectura/escritura	Conveniencia



Datos esenciales y no esenciales

Dirección de disco: esencial
Fecha de acceso: No esencial

Herramienta

```
# dd if=disk-9.dd bs=512 skip=20482875 count=1 | xxd
0000000: 088c 039a 5f78 7694 8f45 bf49 e396 00c0 ....._xv..E.I....
0000016: 889d ddc0 6d36 60df 485d adf7 46d1 3224 ....m6`.H]..F.2$
0000032: 3829 95cd ad28 d2a2 dc89 f357 d921 cfde 8)...(.....W.!..
0000048: df8e 1fd3 303e 8619 641e 9c2f 95b4 d836 ....0>..d../...6
[REMOVED]
0000416: 3607 e7be 1177 db5f 11c9 fba1 c913 1a3d 6....w._.......=
0000432: da81 143d 00c7 7083 9d42 330c 0287 0001 ...=..p..B3.....
0000448: c1ff 0bfe ffff 3f00 0000 fc8a 3801 0000 ......?.....8...
0000464: c1ff 05fe ffff 3b8b 3801 7616 7102 0000 ......;.8.v.q...
0000480: 0000 0000 0000 0000 0000 0000 0000 0000 ................
0000496: 0000 0000 0000 0000 0000 0000 0000 55aa ..............U.
```

Comando dd

Adquisición de imagen de disco

```
# istat -f fat fat-4.dd 4
Directory Entry: 4
Allocated
File Attributes: File, Archive
Size: 8689
Name: RESUME-1.RTF
```

ISTAT

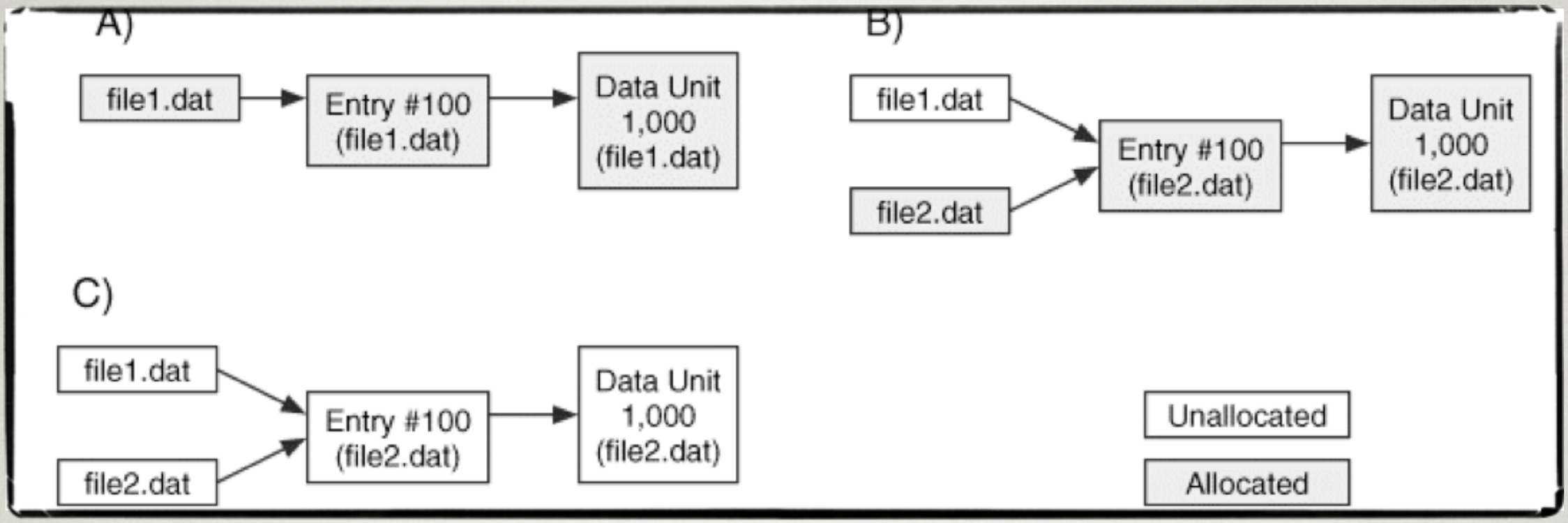
Información relacionada con el archivo/directorio

```
# istat -f fat fat-4.dd 4
Directory Entry: 4
Allocated
File Attributes: File, Archive
Size: 8689
Name: RESUME-1.RTF

Directory Entry Times:
Written:        Wed Mar 24 06:26:20 2004
Accessed:       Thu Apr 8 00:00:00 2004
Created:        Tue Feb 10 15:49:40 2004

Sectors:
1646 1647 1648 1649 1650 1651 1652 1653
1654 1655 1656 1657 1658 1659 1660 1661
1662 1663
```

```
# icat -f openbsd openbsd.dd 1921 | xxd
0000000: 8107 0000 0c00 0401 2e00 0000 0200 0000 ................
0000016: 0c00 0402 2e2e 0000 8c07 0000 1400 0809 ................
0000032: 6669 6c65 312e 7478 7400 93e7 8d07 0000 file1.txt.......
0000048: 1400 0809 6669 6c65 382e 7478 7400 93e7 ....file8.txt...
0000064: 8e07 0000 2800 0809 6669 6c65 372e 7478 ....(...file7.tx
0000080: 7400 93e7 8f07 0000 1400 0809 6669 6c65 t............file
0000096: 362e 7478 7400 93e7 9007 0000 1400 0809 6.txt............
0000112: 6669 6c65 352e 7478 7400 93e7 9107 0000 file5.txt.......
0000128: 2800 0809 6669 6c65 342e 7478 7400 93e7 (...file4.txt...
0000144: 9207 0000 1400 0809 6669 6c65 332e 7478 ........file3.tx
[REMOVED]
```

ICAT

Información del nodo-i



Espacios ocupado-libres del disco

Proceso de creación y borrado de archivos

```
# ffind -f linux-ext3 ext3.dd 69458
/dir1/abcdefg.txt
```

FFIND

Búsqueda de archivos/directorios

```
Wed Aug 11 2004 19:31:58      34528 .a. /system32/ntio804.sys
                              35392 .a. /system32/ntio412.sys
[REMOVED]
Wed Aug 11 2004 19:33:27       2048 mac /bootstat.dat
                               1024 mac /system32/config/default.LOG
                               1024 mac /system32/config/software.LOG
Wed Aug 11 2004 19:33:28     262144 ma. /system32/config/SECURITY
                             262144 ma. /system32/config/default
```

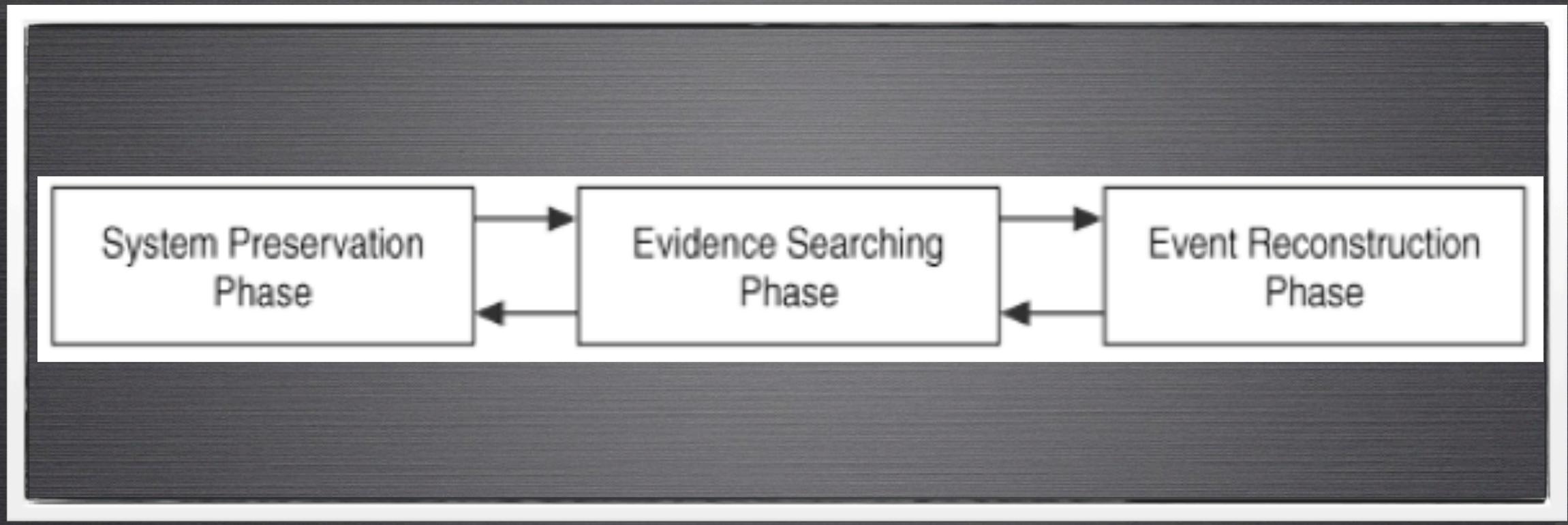
MACTIME

Marcas de tiempo

Agenda

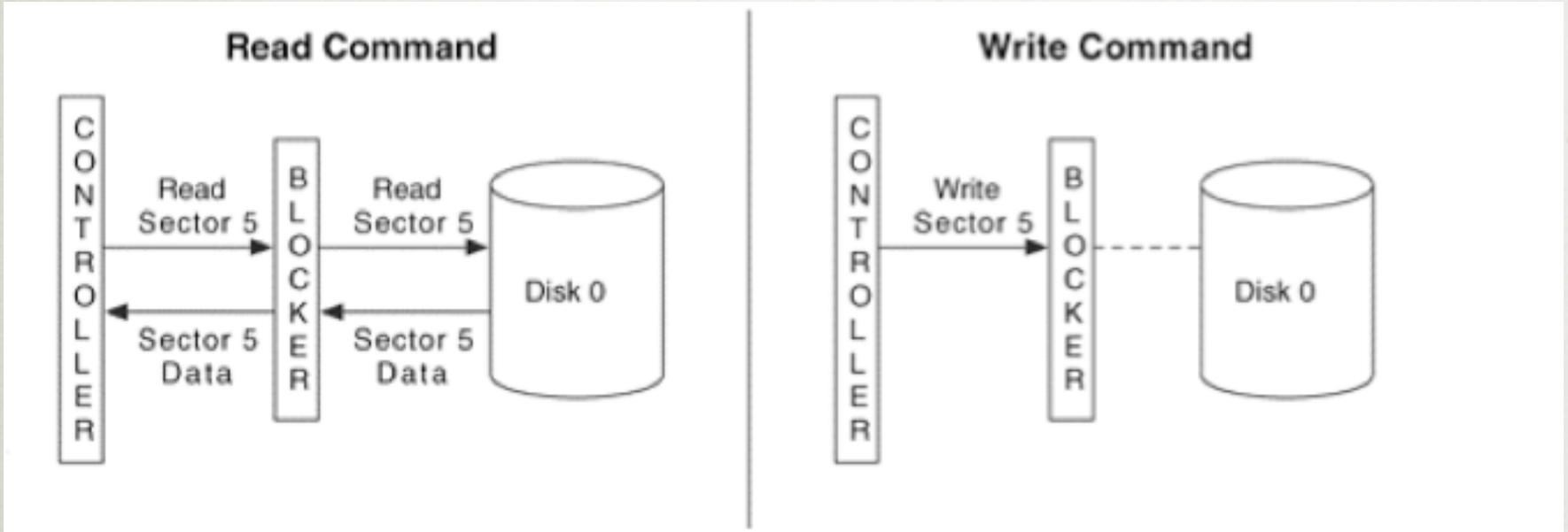
- Fases de la Informática Forense
- Análisis de caso
- Conclusiones y recomendaciones

Fases de la Informática Forense



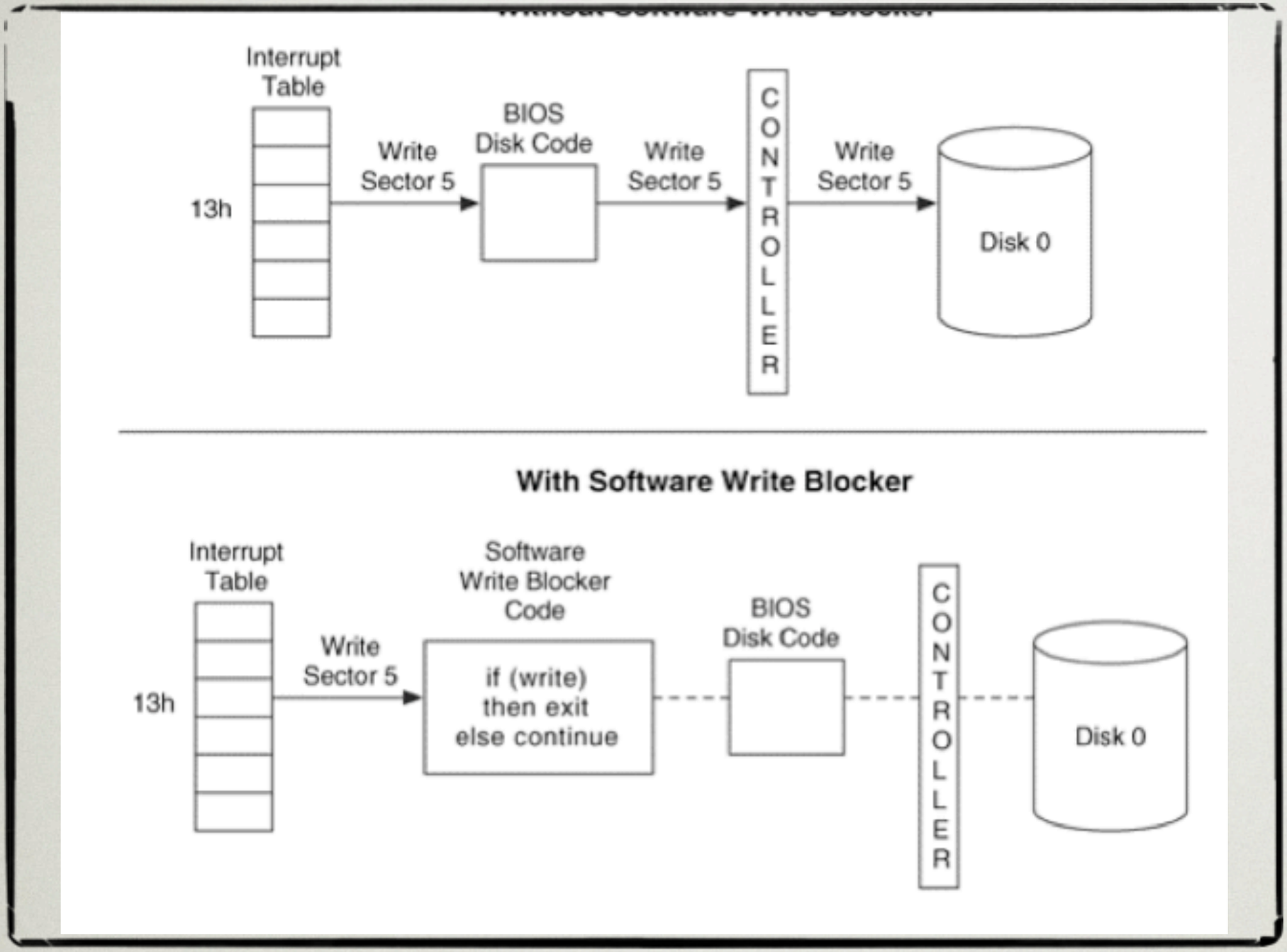
Etapas del proceso forense

Preservación del sistema



Bloqueador de escritura

Hardware



Bloqueador de escritura

Software

Búsqueda de evidencia

```
# dd if=/dev/hda of=/mnt/hda.dd bs=2k
# dd if=/dev/hda of=/dev/hdd bs=2k
```

```
# sigfind -o 510 55AA disk-9.dd
Block size: 512 Offset: 510
Block: 63 (-)
Block: 64 (+1)
Block: 65 (+1)
Block: 69 (+4)
Block: 70 (+1)
Block: 71 (+1)
Block: 75 (+4)
Block: 128504 (+128429)
Block: 293258 (+164754)
[REMOVED]
```

```
# mmls -t dos bsd-disk.dd
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000062   0000000062   Unallocated
02:  00:00   0000000063   0002056319   0002056257   Win95 FAT32 (0x0B)
03:  00:01   0002056320   0008209214   0006152895   OpenBSD (0xA6)
04:  00:02   0008209215   0019999727   0011790513   FreeBSD (0xA5)
```

Reconstrucción del evento

Reconstrucción del evento

- Relacional
- Funcional
- Temporal

Agenda

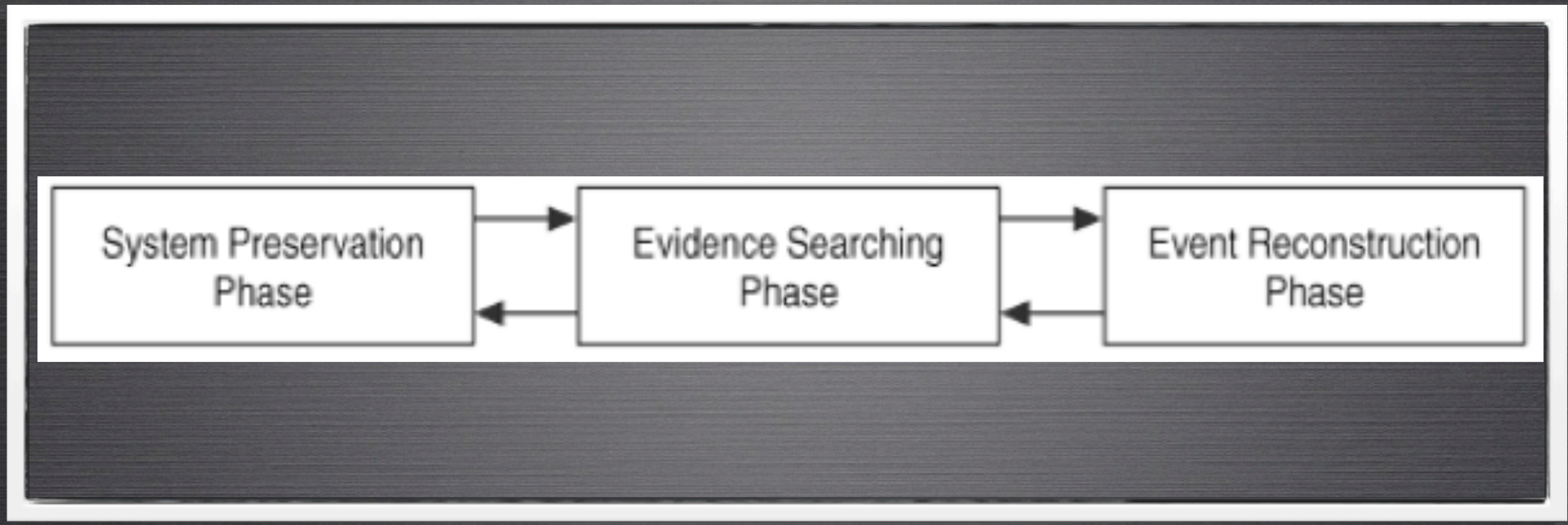
- Análisis de caso
- Conclusiones y recomendaciones

Análisis de caso

Caso por injurias

Caso por injurias

- Caso nacional
- Se usa el correo electrónico como medio para cometer delito.

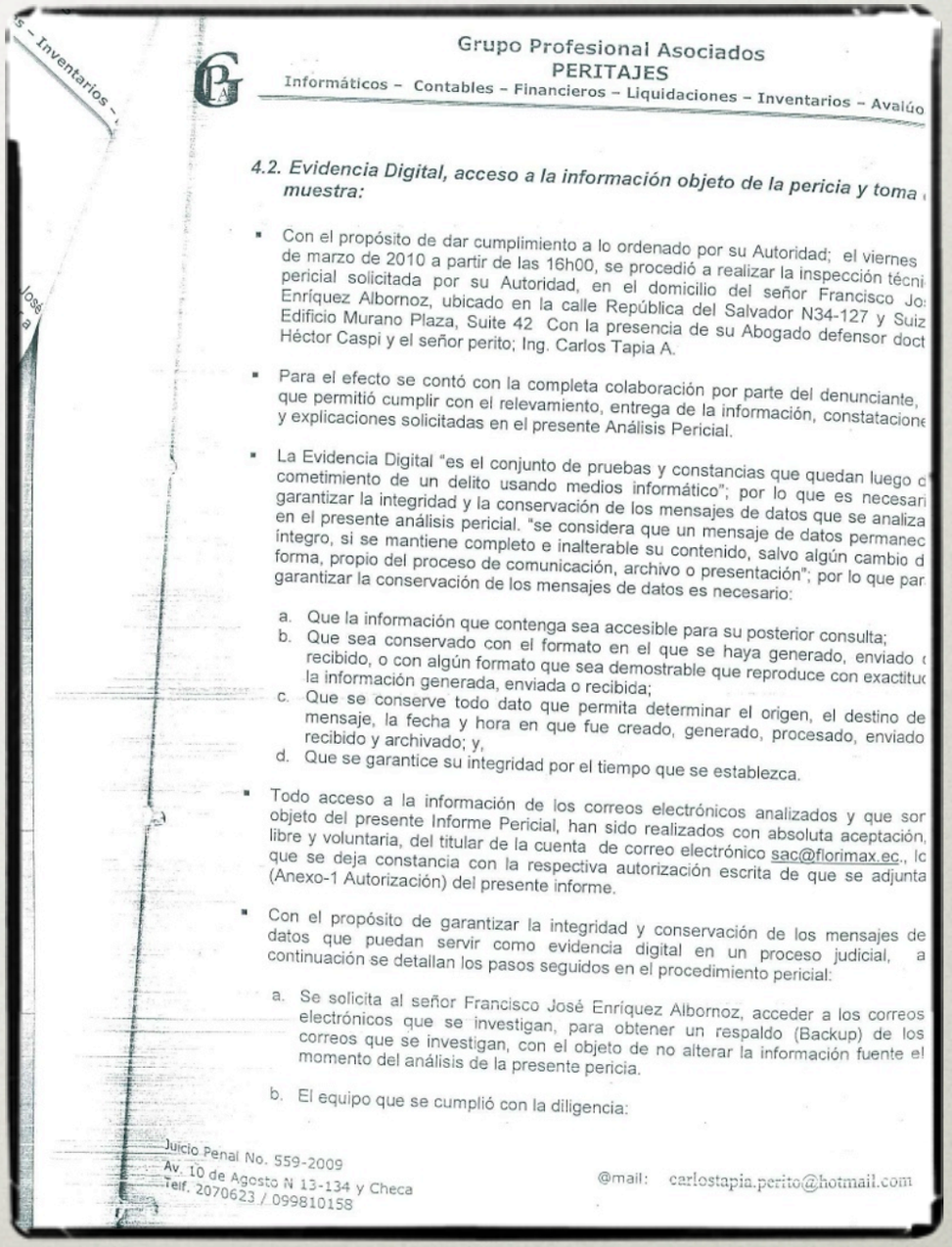


Etapas del proceso forense

Preservación del sistema

Fase de preservación del sistema

- Se realiza respaldo de la bandeja de entrada
- Se genera carpeta en el escritorio en donde se guardan correos, cabeceras y capturas de pantalla



Grupo Profesional Asociados
PERITAJES
Informáticos – Contables – Financieros – Liquidaciones – Inventarios – Avalúo

4.2. Evidencia Digital, acceso a la información objeto de la pericia y toma muestra:

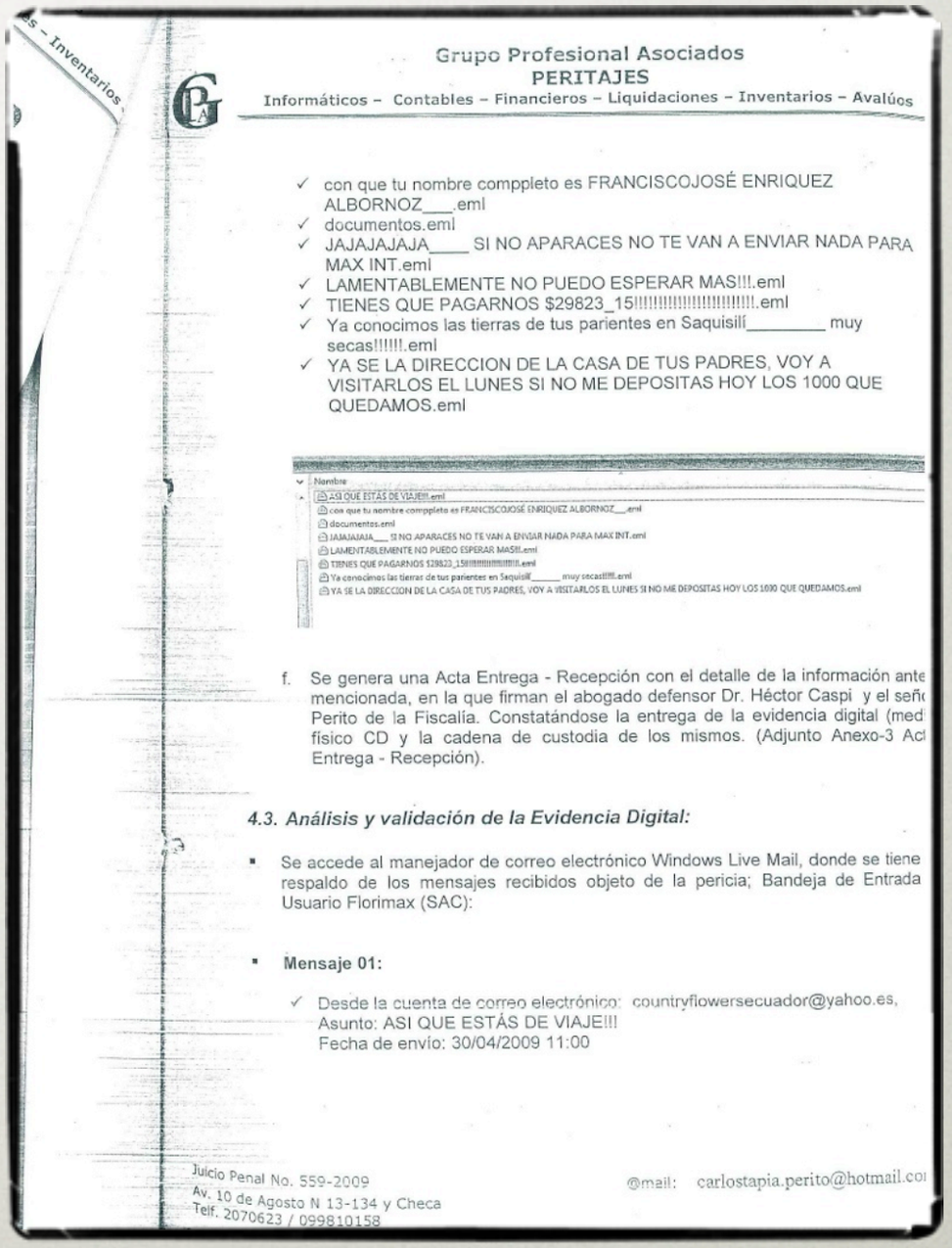
- Con el propósito de dar cumplimiento a lo ordenado por su Autoridad; el viernes de marzo de 2010 a partir de las 16h00, se procedió a realizar la inspección técni pericial solicitada por su Autoridad, en el domicilio del señor Francisco Jos Enríquez Albornoz, ubicado en la calle República del Salvador N34-127 y Suiz Edificio Murano Plaza, Suite 42 Con la presencia de su Abogado defensor doct Héctor Caspi y el señor perito; Ing. Carlos Tapia A.
- Para el efecto se contó con la completa colaboración por parte del denunciante, que permitió cumplir con el relevamiento, entrega de la información, constataciones y explicaciones solicitadas en el presente Análisis Pericial.
- La Evidencia Digital "es el conjunto de pruebas y constancias que quedan luego c cometimiento de un delito usando medios informático"; por lo que es necesari garantizar la integridad y la conservación de los mensajes de datos que se analiza en el presente análisis pericial. "se considera que un mensaje de datos permanec íntegro, si se mantiene completo e inalterable su contenido, salvo algún cambio d forma, propio del proceso de comunicación, archivo o presentación"; por lo que par garantizar la conservación de los mensajes de datos es necesario:
  a. Que la información que contenga sea accesible para su posterior consulta;
  b. Que sea conservado con el formato en el que se haya generado, enviado recibido, o con algún formato que sea demostrable que reproduce con exactitu la información generada, enviada o recibida;
  c. Que se conserve todo dato que permita determinar el origen, el destino de mensaje, la fecha y hora en que fue creado, generado, procesado, enviado recibido y archivado; y,
  d. Que se garantice su integridad por el tiempo que se establezca.
- Todo acceso a la información de los correos electrónicos analizados y que son objeto del presente Informe Pericial, han sido realizados con absoluta aceptación, libre y voluntaria, del titular de la cuenta de correo electrónico sac@florimax.ec., lo que se deja constancia con la respectiva autorización escrita de que se adjunta (Anexo-1 Autorización) del presente informe.
- Con el propósito de garantizar la integridad y conservación de los mensajes de datos que puedan servir como evidencia digital en un proceso judicial, a continuación se detallan los pasos seguidos en el procedimiento pericial:
  a. Se solicita al señor Francisco José Enríquez Albornoz, acceder a los correos electrónicos que se investigan, para obtener un respaldo (Backup) de los correos que se investigan, con el objeto de no alterar la información fuente el momento del análisis de la presente pericia.
  b. El equipo que se cumplió con la diligencia:

Juicio Penal No. 559-2009
Av. 10 de Agosto N 13-134 y Checa
Telf. 2070623 / 099810158
@mail: carlostapia.perito@hotmail.com

Búsqueda de evidencia

Fase de búsqueda de evidencia

- 20 de abril del 2009 al 26 de febrero del 2010
- Se accede al CD de respaldo desde la aplicación de correos



Grupo Profesional Asociados
PERITAJES
Informáticos – Contables – Financieros – Liquidaciones – Inventarios – Avalúos

- ✓ con que tu nombre comppleto es FRANCISCOJOSÉ ENRIQUEZ ALBORNOZ___.eml
- ✓ documentos.eml
- ✓ JAJAJAJAJA____ SI NO APARACES NO TE VAN A ENVIAR NADA PARA MAX INT.eml
- ✓ LAMENTABLEMENTE NO PUEDO ESPERAR MAS!!!.eml
- ✓ TIENES QUE PAGARNOS $29823_15!!!!!!!!!!!!!!!!!!!!!!!!!!!.eml
- ✓ Ya conocimos las tierras de tus parientes en Saquisilí_____ muy secas!!!!!!.eml
- ✓ YA SE LA DIRECCION DE LA CASA DE TUS PADRES, VOY A VISITARLOS EL LUNES SI NO ME DEPOSITAS HOY LOS 1000 QUE QUEDAMOS.eml

Nombre
ASI QUE ESTÁS DE VIAJE!!!.eml
con que tu nombre comppleto es FRANCISCOJOSÉ ENRIQUEZ ALBORNOZ___.eml
documentos.eml
JAJAJAJAJA____ SI NO APARACES NO TE VAN A ENVIAR NADA PARA MAX INT.eml
LAMENTABLEMENTE NO PUEDO ESPERAR MAS!!!.eml
TIENES QUE PAGARNOS $29823_15!!!!!!!!!!!!!!!!!!!!!!!!!!!.eml
Ya conocimos las tierras de tus parientes en Saquisilí_____ muy secas!!!!!!.eml
YA SE LA DIRECCION DE LA CASA DE TUS PADRES, VOY A VISITARLOS EL LUNES SI NO ME DEPOSITAS HOY LOS 1000 QUE QUEDAMOS.eml

f. Se genera una Acta Entrega - Recepción con el detalle de la información ante mencionada, en la que firman el abogado defensor Dr. Héctor Caspi y el seño Perito de la Fiscalía. Constatándose la entrega de la evidencia digital (med físico CD y la cadena de custodia de los mismos. (Adjunto Anexo-3 Act Entrega - Recepción).

4.3. Análisis y validación de la Evidencia Digital:

- Se accede al manejador de correo electrónico Windows Live Mail, donde se tiene respaldo de los mensajes recibidos objeto de la pericia; Bandeja de Entrada Usuario Florimax (SAC):

- **Mensaje 01:**

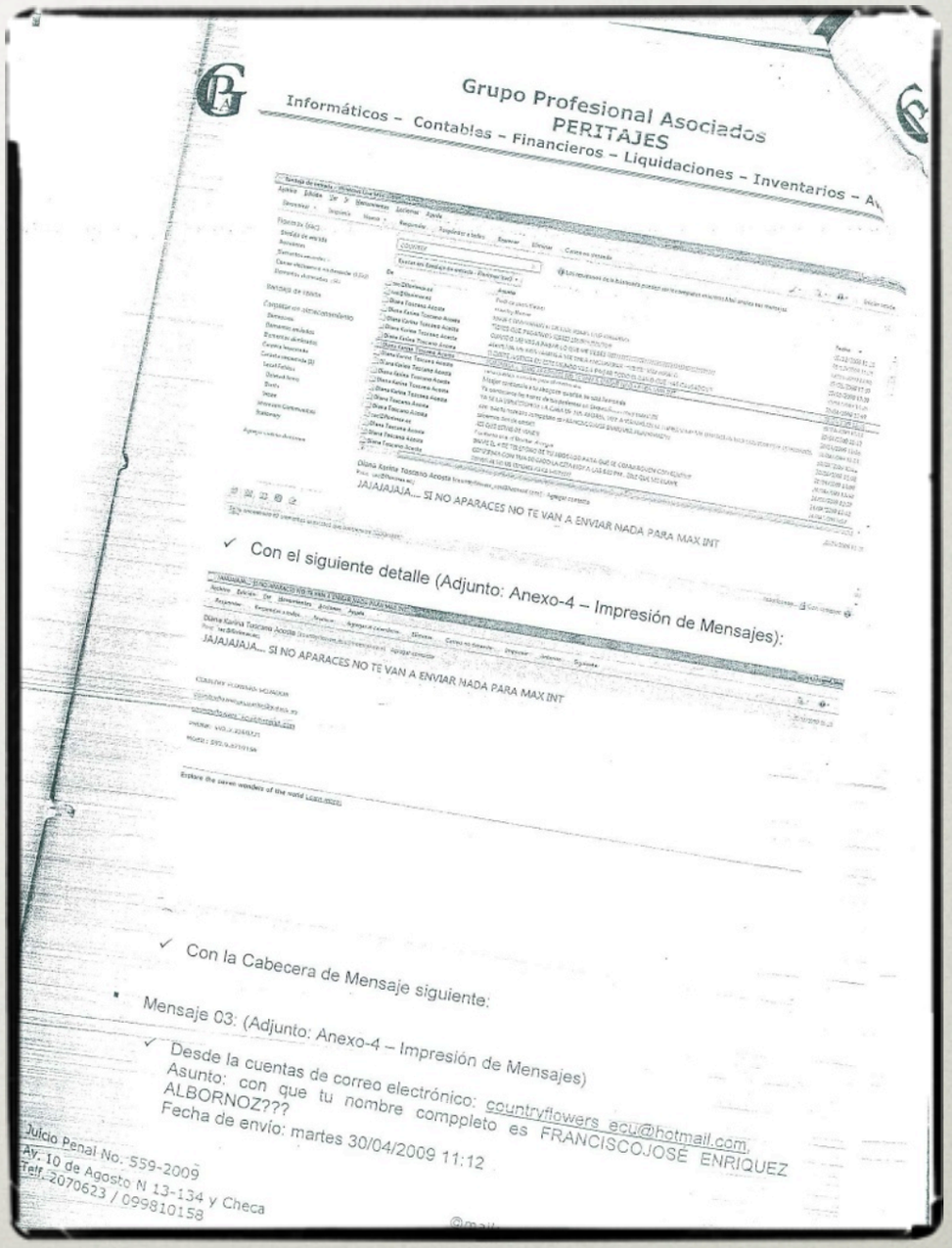
✓ Desde la cuenta de correo electrónico: countryflowersecuador@yahoo.es,
Asunto: ASI QUE ESTÁS DE VIAJE!!!
Fecha de envío: 30/04/2009 11:00

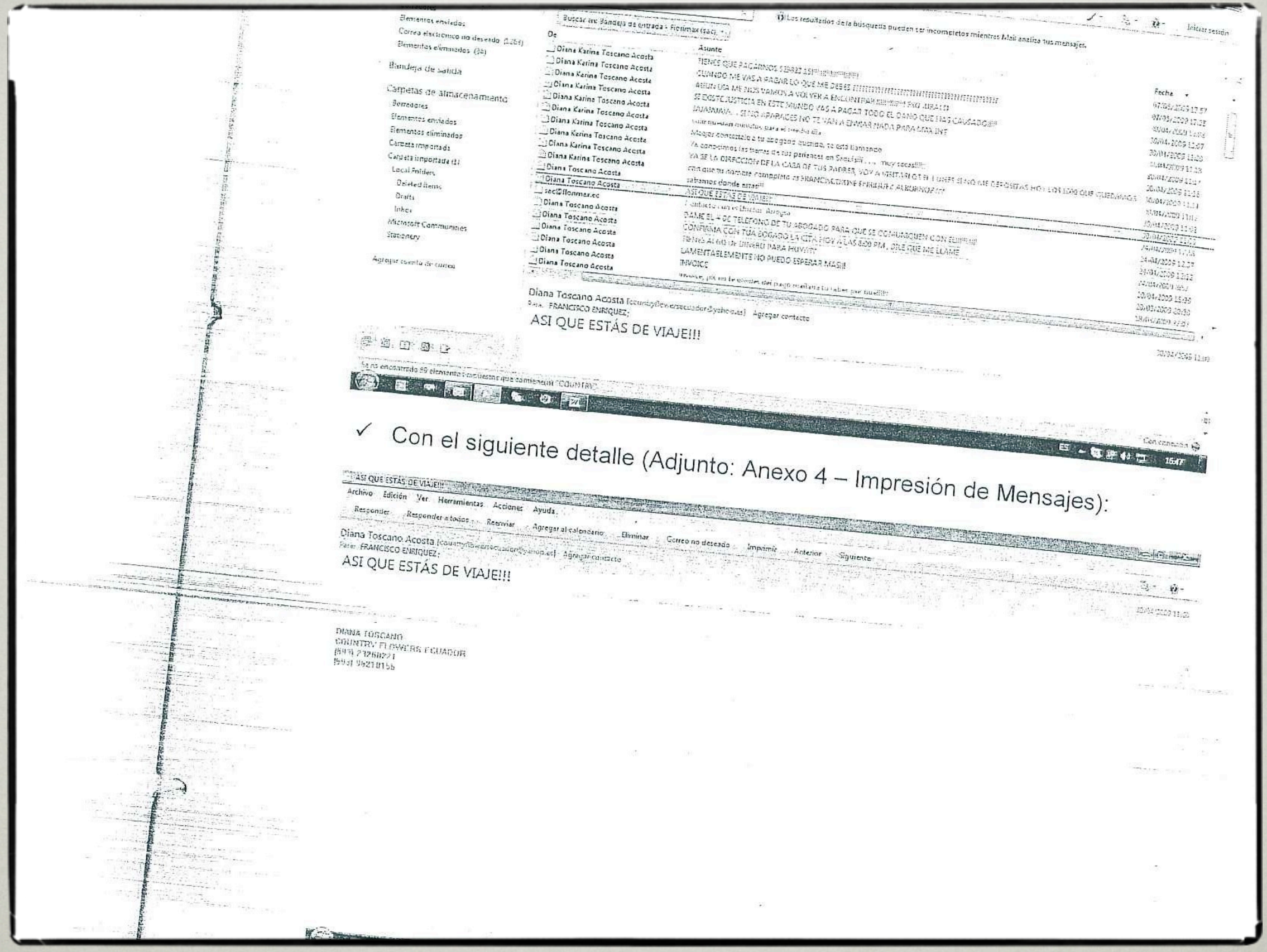
Juicio Penal No. 559-2009
Av. 10 de Agosto N 13-134 y Checa
Telf. 2070623 / 099810158

@mail: carlostapia.perito@hotmail.co

Fase de búsqueda de evidencia

- Información de cabecera se verifica origen, destino y firma digital





✓ Con el siguiente detalle (Adjunto: Anexo 4 – Impresión de Mensajes):

Reconstrucción del evento

- Los e-mails (1 al 8) fueron originalmente disparados desde las siguientes direcciones IP: 190.152.45.211, 190.11.3.72, 87.4.162.91 y 190.152.26.203 de acuerdo a información obtenida de las cabeceras de los (8) mensajes.

- El presente análisis pericial se centró en los tres (8) correos electrónicos recibidos por el Sr. Francisco José Enríquez Albornoz; en su cuenta de correo electrónico sac@florimax.ec; desde las cuentas de correos electrónico countryflowers_ecu@hotmail.com, y countryflowersecuador@yahoo.es, pertenecientes a la Sra. Diana Karina Toscano Acosta.

- No son contundentes las conclusiones y recomendaciones de la empresa de peritaje

- En tal sentido falla el juez a favor de la enjuiciada y desestima la demanda presentada

Agenda

- Conclusiones y recomendaciones

Conclusiones y recomendaciones

Conclusiones

- Gran impacto de medios tecnológicos en la vida cotidiana

- Escaso avance en materia de peritaje informático

- El respetar los estándares internacionales y las cadenas de custodia

- El Código Penal es el marco legal que regula cualquier actividad o actitud atípica y que vaya en perjuicio del Estado Ecuatoriano

Recomendaciones

- Capacitar y formar a técnicos calificados en administración de sistemas informáticos, protección y rastreo de la información gubernamental

- Implementar tecnología de protección de información

- La Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos debe ampliarse

La Ingeniería forense se desenvuelve y progresa en el contexto de estas nuevas situaciones. Como disciplina de integración con capacidad de crear su propio bagaje conceptual, contribuye a la elaboración de una ciencia en sí misma, individual, integradora y por sobre todo, transdisciplinaria, capaz de generar innovaciones de utilidad general.

Ing. Aníbal Oscar Garcia

Gracias