INCIDE - Seminarios Análisis Forense

¿Quién se ha llevado mi archivo?

colaborador de: GILO

GRUPO WINTERMAN

29 marzo 2012

Licencia de uso

– Esta obra está bajo una licencia Reconocimiento-No comercial-Sin obras derivadas 2.5 España de Creative Commons. Para ver una copia de esta licencia, visite

http://creativecommons.org/licenses/by-nc-nd/2.5/es/

o envie una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.

Breve presentación

- Abraham Pasamar
  - Ingeniero Superior y Master Seguridad Informática
  - Socio Director INCIDE (2005, Grupo Winterman)
- INCIDE
  - Objetivo: Lucha contra Fraude Empresarial
  - Analistas de información , consultores legales, ingenieros expertos en análisis forense y laboratorio forense tecnológicamente puntero
  - Ofrecemos una gestión integral de los procesos en los que se requiere Prueba Electrónica
  - Experiencia acumulada:
    - más de 800 casos atendidos
    - más de 400 investigaciones realizadas
    - más de 300 informes periciales emitidos

3

AGENDA

- Sospechosos habituales
- Motivaciones
- Métodos empleados
- Contexto legal
- Casos prácticos
- Metodología y buenas prácticas forenses

Sospechosos habituales

- Empleados descontentos
- Potenciales ex-empleados y futura competencia
- Socios (minoritarios, poco implicados)
- Directivos (poco implicados, poco reconocimiento)
- Pluri-Empleados
- Competencia

5

Motivaciones

- Interno:
  - Conflicto laboral (venganza, ira, odio)
  - Aprovechamiento del trabajo ajeno
  - Atribución errónea de la propiedad intelectual (desconocimiento del delito)
  - Ánimo de lucro
- Externo:
  - Ánimo de lucro, inteligencia competitiva y competencia desleal

Métodos empleados

- Navaja de Ockham:
  - <<Dos teorías en igualdad de condiciones que tienen las mismas consecuencias, la teoría más simple tiene más probabilidades de ser correcta que la compleja>>
  - Es decir, si nos roban la información tendemos a pensar que alguien muy rico ha contratado a **Lisbeth Salander** que con su programa **Asphyxia** se ha introducido en nuestros sistemas, pero lo cierto es, que la experiencia nos dice que somos descuidados con la seguridad y no solemos desconfiar de los empleados y compañeros hasta que ocurre algo ...

7

Métodos empleados

- Errores habituales:
  - Acceso compartido en red y local
  - Facilitamos los passwords a terceros
  - Usamos los mismos passwords para diferentes servicios y niveles de seguridad
  - Permitimos el acceso local a nuestros equipos
  - AV no actualizados
  - No pensamos antes de hacer click (ing. social)

8

Métodos empleados

- Errores habituales:
  - Falta de conciencia sobre el poder de los administradores de sistemas
  - Falta de conciencia sobre el poder de los administradores de sistemas
  - Uso de ordenadores no seguros (familiares, cybercafé)
  - Malas practicas (recordar passwords, passwords fáciles, vacíos, descarga programas raros, etc.)
  - Mala protección/clasificación de información (seg. logica/sistemas)

9

Métodos empleados

- USB (discos memorias teléfonos)
- CD/DVD
- Fotos
- Impresora/Papel
- Bluetooth/WiFi (vía móvil, agenda, ipad)
- Internet (Gmail, hotmail, dropbox,.....)
  - Eludir filtros: zips con contraseña, cambio extensiones, etc
- Software espía convencional (comercial), Troyanos,...

Marco Legal

- **Art. 197.1 CP**: descubrimiento y revelación de secretos (1 a 4 años y multa 12 a 24 meses)
  - Apoderamiento mails, papeles, cartas u otros documentos
  - Interceptar telecomunicaciones
  - Utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido, imagen o cualquier otra señal de comunicación
- **Art. 197.6 CP**(tipos agravados. 3 a 5 años): realización de hechos con fines lucrativos

11

Marco Legal

- **Sentencia 534/10**

FALLO

CONDENO a [redacted] como autor criminalmente responsable de un delito de revelación de secretos, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a la pena de prisión de 3 años y multa de 20 meses a razón de 10 euros día con responsabilidad personal subsidiaria en caso de impago, así como al pago de las costas procesales, incluidas las de la acusación particular.

con datos personales, abarcando todo lo relacionado con su objeto social. Recopiló más de 300 archivos, "*bastantes miles de folios*" en palabras del perito, Sr. Passamar. Lo hizo de manera que pudiera dejar el menor rastro posible, cuando todavía estaba vigente su relación laboral, y toda esta información la transmitió a ex trabajadores de [redacted], y, a la mercantil a la que entró a trabajar el día después de haber extinguido su relación con la querellante, una sociedad de reciente constitución, con idéntico objeto social.

Acciones preventivas

- Reforzar seguridad en general
  - políticas internas
  - políticas dominio
  - firewall
  - antivirus, antimalware
  - formación (cultura de seguridad)
  - etc
- Forensics Readiness
- DLP (Data Loss Prevention)

Acciones reactivas

– Análisis forense informático

14

Caso 1

- Antecedentes
  - Recientemente **dos trabajadores** de una empresa del sector de alimentación han comunicado su **dimisión**
  - Uno de ellos es el **Responsable de Ventas** y **gestiona personalmente** una parte esencial del know-how de la empresa, **las fórmulas de los productos**
  - Al parecer, van a seguir en el sector y están tratando de llevarse a personal de la compañía
  - Se sospecha que han borrado información de las fórmulas de su ordenador. No están en el servidor

15

Objetivo

- localizar patrones de fuga y borrado de información

Fuentes de información

- Ordenador portátil y fijo del responsable de ventas y ordenador fijo de su compañero

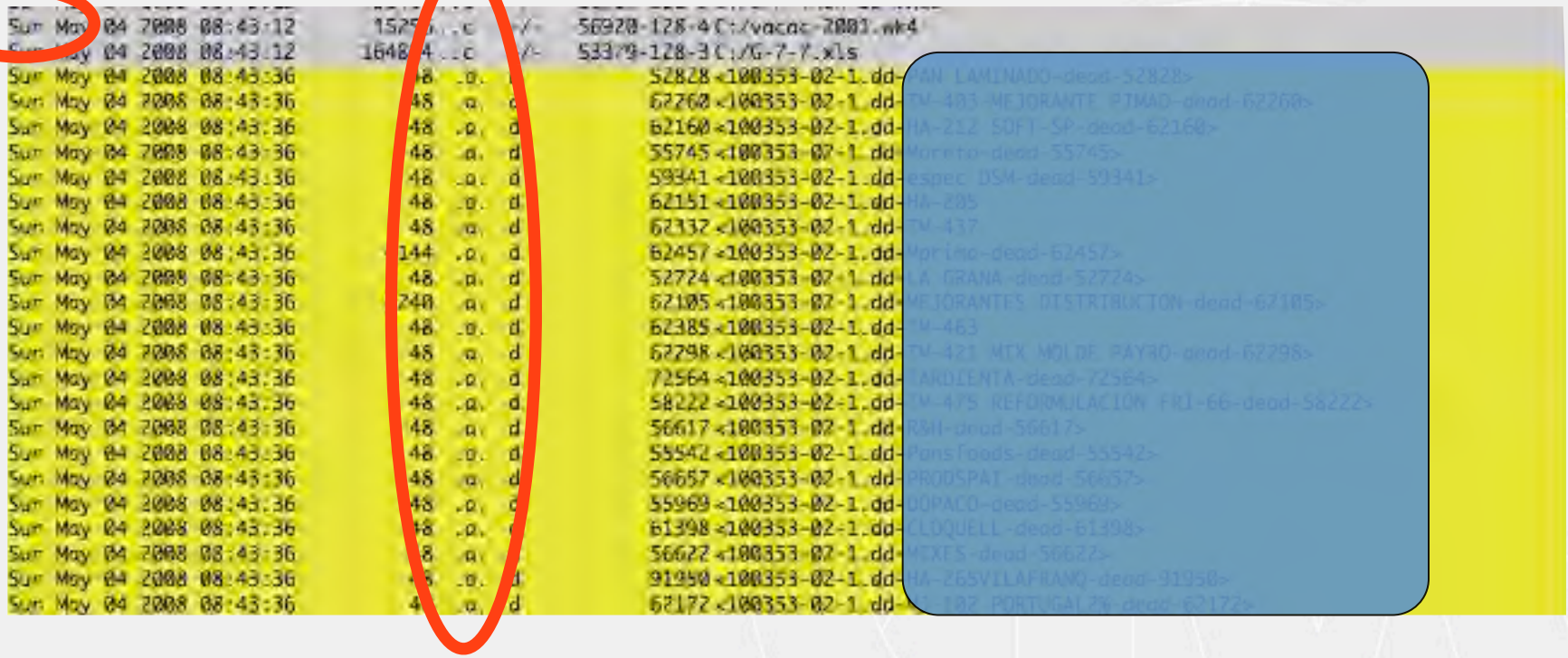
Nociones análisis forense

- Los ordenadores no disponen de un sistema de almacenamiento de todas las acciones realizadas
- Es preciso conocer como funcionan para buscar posibles rastros que ayuden a reconstruir los hechos ocurridos
- Los análisis forenses se basan en el estudio de:
  - líneas temporales
  - archivos recientes
  - registro sistema
  - búsquedas por palabras clave (keywords), etc

18

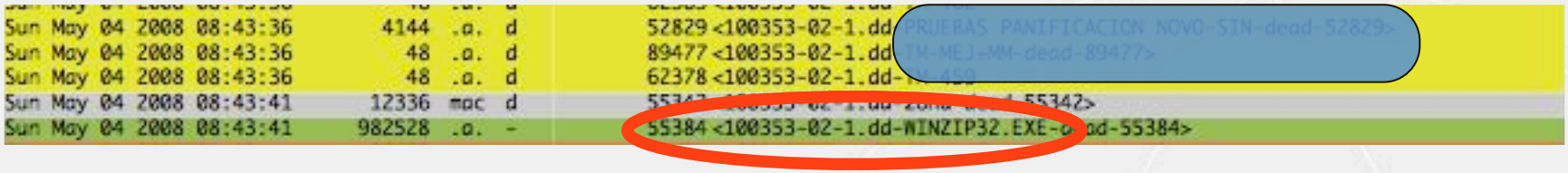
Análisis

- acceso masivo (domingo)



Análisis

- utilización de un compresor (winzip)



- Inserción dispositivo USB a las 9:53:
  - C:/WINDOWS/Media/Inserción de hardware de Windows XP.wav

Conclusiones

- El domingo 4 de mayo a las 8:43: se creó un fichero comprimido, conteniendo al menos trescientos (300) ficheros y doscientas (200) carpetas
- a continuación se conectó un dispositivo usb
- poco después se eliminaron los ficheros del ordenador

21

Caso 2

- Antecedentes
  - Un trabajador comienza a trabajar en el **departamento antifraude** de una gran compañía de venta por internet el día 2 de Noviembre
  - El día 8 de noviembre **no se presenta** en su puesto de trabajo y envía un correo electrónico alegando que por **motivos personales** renuncia a su posición actual y regresa a su país
  - Se sospecha que pueda haber sustraído información confidencial

Objetivo

- localizar patrones de fuga de información

Fuentes de información

- Ordenador portátil asignado al trabajador durante esos 6 días

24

Análisis

- **No** se observa utilización de dispositivos externos **USB**
- **No** se observa grabación de **CD/DVD**'s
- **No** accesos servicios externos: FTP, dropbox, etc
- Se detecta uso de cuenta de **gmail:**
  - actividad de GMail y navegador Firefox: ausencia de rastros locales

Análisis

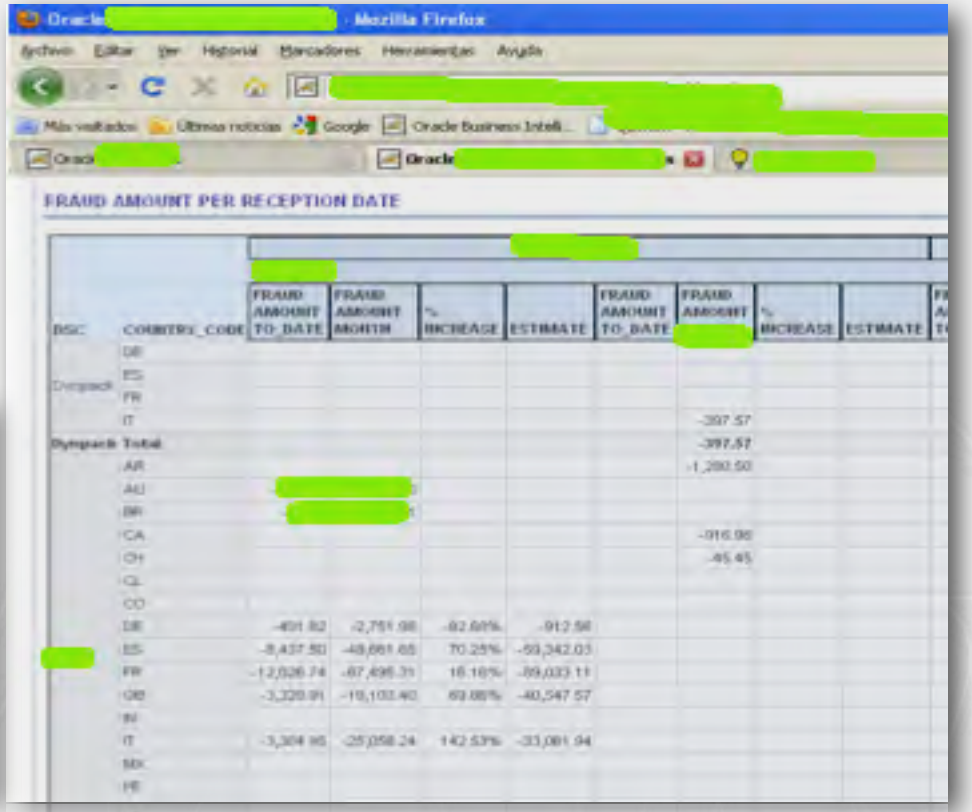
- Se estudia el histórico de la actividad de internet y se concatena con la actividad de disco (correlación de eventos)

		Actividad documentos		Navegación (Firefox)
Hora	Descripción	Nombre documento	Ruta	Título página
18:29:05	modificación del documento	Loss_forecast_ [redacted] onginal.xls	c:/Documents and Settings/mtoms/My Documents [redacted] /Fraud and Payments/Fraud Reports/	--
18:29:26	Redactar correo	--	--	Gmail - Compose Mail [redacted] @gmail.com
18:29:26	Bandeja de entrada	--	--	Gmail - Inbox (4722) - [redacted] @gmail.com
18:29:49	Borrador de correo	--	--	/mail/?shva=1#drafts/12c1d1 [redacted] e
18:30:27	creación del documento	Reports3.xlsx	C:/Documents and Settings/mtoms/My Documents [redacted] Fraud and Payments	--
18:30:26	Borrador de correo			/mail/?shva=1#drafts/12c1d16b [redacted] b
18:30:58	modificación del documento	Reports2.xlsx	C:/Documents and Settings/mtoms/My Document [redacted] ud and Payments	--
18:31:16	creación del documento	Reports1.xlsx	C:/Documents and Settings/mtoms/My Documents [redacted] /Fraud and Payments	--
18:31:34	Apertura del documento	Reports.xlsx	C:/Documents and Settings/mtoms/My Documents [redacted] /Fraud and Payments	--

Análisis

- Se recuperan archivos borrados de la papelera
- Se trata de capturas de pantalla de la aplicación anti-fraude

Análisis



Conclusiones

- Se han encontrado rastros del uso de una cuenta de GMail los días 4 y 5 de noviembre. El día 5 de noviembre, entre las 18:20 y las 18:36, se envían diversos correos electrónicos o se generan los borradores de los mismos
- Al mismo tiempo, entre las 18:21 y las 18:36, se crean un total de 6 documentos en formato Excel
- A las 18:32, desde el navegador utilizado para la consulta de la dirección de Gmail, se utiliza el cuadro de diálogo Abrir para uno o varios ficheros desde la carpeta `Mis Documentos \...\Fraud and Payments` del usuario
- Entre las 18:35 y las 18:36, se eliminan los referidos documentos de forma secuencial

29

Caso 3

- Antecedentes
  - Empresa en situación complicada y un ERE en negociación
  - Al comenzar las negociaciones el director de RRHH se percata de que todos los empleados están negociando muy bien y solicitan cifras cercanas al máximo previsto por la empresa
  - Se sospecha de filtraciones
  - El Director de RRHH, el CEO y los abogados externos son los únicos que han intercambiado esta información vía correo electrónico

30

Objetivo

- localizar patrones de fuga de información sin un sospechoso específico

31

Fuentes de información

- logs de los servidores de la empresa

Análisis

- Primer paso:
  - Verificar si los correos electrónicos pueden estar siendo intervenidos
  - Envío de correos electrónicos de trazabilidad
  - El abogado de la empresa envía a ambos directores un email con asunto: "actualización listado ERE" y un archivo excel adjunto.

Análisis


INTRUSO EXTERNO
El destinatario del correo abre el correo pero no el archivo adjunto
Receptor
Servidor Correo de la empresa
Posible INTRUSO con acceso al servidor o conocimiento de credenciales de alguna de las cuentas de correo
INTRUSO INTERNO
Internet
Posible INTRUSO con acceso al servidor o conocimiento de credenciales de alguna de las cuentas de correo
Si el INTRUSO abre el correo INCIDE tendrá constancia de ello y podrá estudiar la dirección IP, fecha, hora, etc.
EMPRESA
SERVIDOR INCIDE
Email con archivo adjunto especialmente configurado
Emisor
SISTEMA DE MONITORIZACIÓN de correos electrónicos que permite controlar la apertura de los mismos

34

Análisis

- Verificada la apertura de correos electrónicos por terceros ajenos a la comunicación original, una de las aperturas es interna, desde dentro de la empresa, la otra es externa, una IP dinámica que no aporta por el momento más información.
- Para la lectura se utiliza el OWA (outlook web app)

35

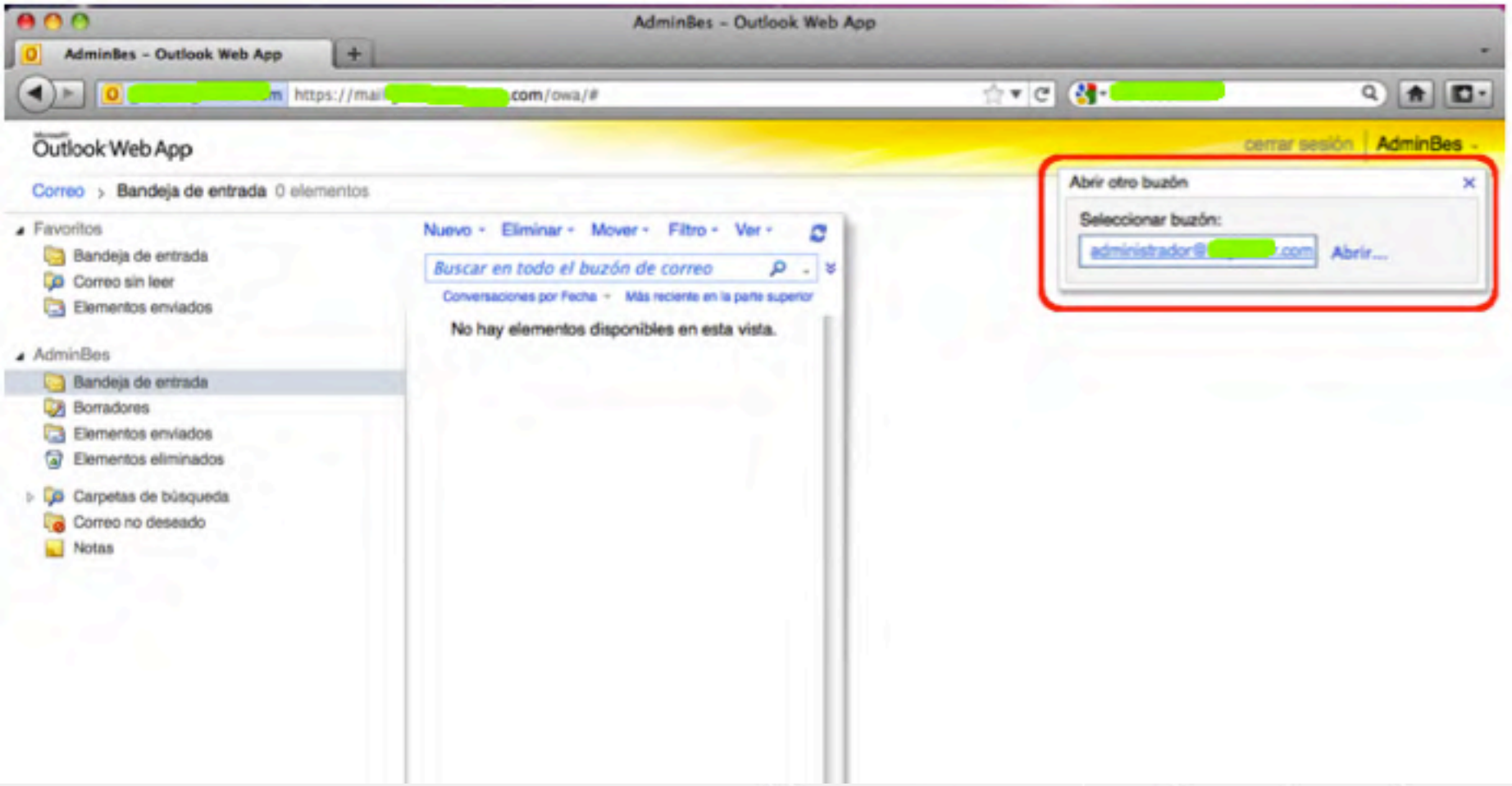
Análisis

- ¿Cómo acceden sin las contraseñas a los buzones de los usuarios? No ha habido reset de contraseñas y están sincronizadas con el AD (Active Directory)
- Análisis logs OWA
  - Logins usuario Adminbes del servidor de Blackberry en el OWA !!!

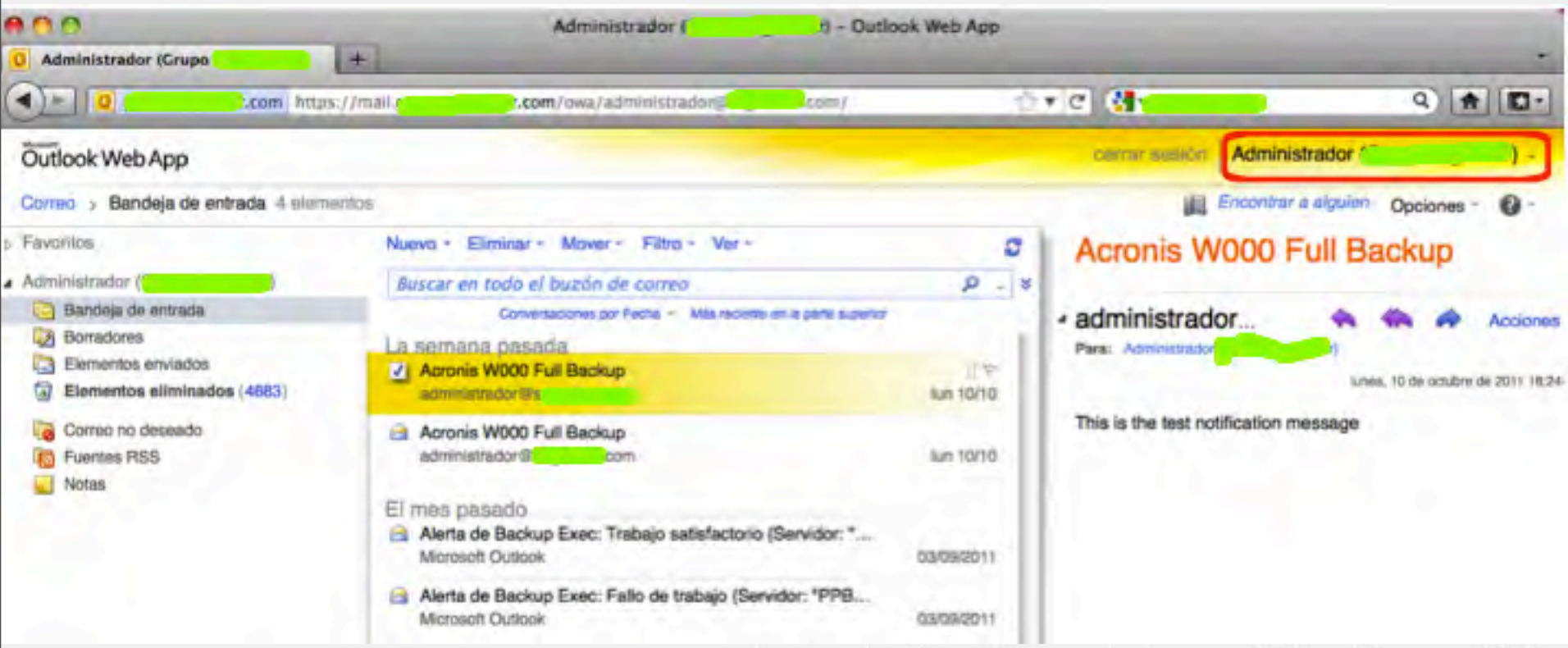
Análisis


Outlook Web App
Seguridad (mostrar explicación)
Equipo público o compartido
Equipo privado
Advertencia: al seleccionar esta opción declara que el equipo cumple con la directiva de seguridad de su organización.
Usar Outlook Web App Light
Dominio\nombre de usuario:
\Administrador
Contraseña:
Iniciar sesión
Conectado a Microsoft Exchange
Protegido por Microsoft Forefront Threat Management Gateway
© 2009 Microsoft Corporation. Reservados todos los derechos.

Análisis

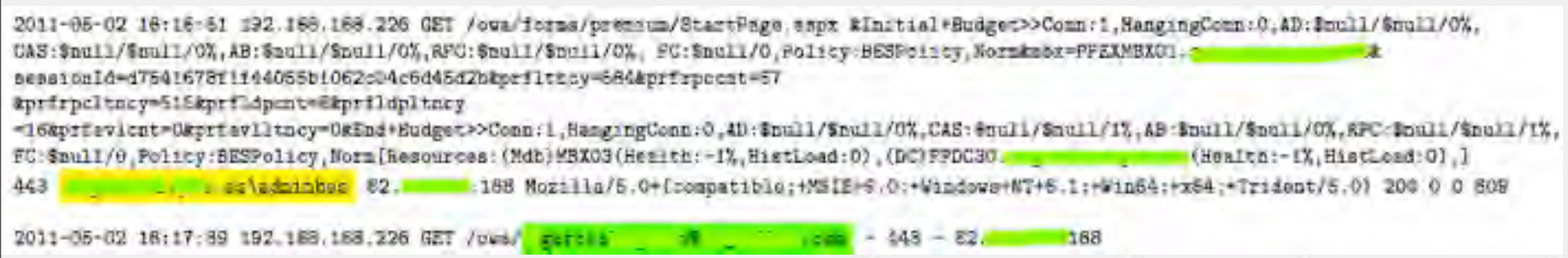

AdminBes – Outlook Web App
AdminBes – Outlook Web App
https://mai[redacted].com/owa/#
Outlook Web App
cerrar sesión
AdminBes
Correo › Bandeja de entrada 0 elementos
Favoritos
Bandeja de entrada
Correo sin leer
Elementos enviados
AdminBes
Bandeja de entrada
Borradores
Elementos enviados
Elementos eliminados
Carpetas de búsqueda
Correo no deseado
Notas
Nuevo
Eliminar
Mover
Filtro
Ver
Buscar en todo el buzón de correo
Conversaciones por Fecha
Más reciente en la parte superior
No hay elementos disponibles en esta vista.
Abrir otro buzón
Seleccionar buzón:
administrador@[redacted].com
Abrir...

Análisis


Administrador ( ) - Outlook Web App
Administrador (Grupo
.com https://mail .com/owa/administrador .com/
Outlook Web App
cerrar sesión
Administrador ( )
Correo › Bandeja de entrada 4 elementos
Encontrar a alguien
Opciones
Favoritos
Administrador ( )
Bandeja de entrada
Borradores
Elementos enviados
Elementos eliminados (4883)
Correo no deseado
Fuentes RSS
Notas
Nuevo
Eliminar
Mover
Filtro
Ver
Buscar en todo el buzón de correo
Conversaciones por Fecha
Más reciente en la parte superior
La semana pasada
Acronis W000 Full Backup
lun 10/10
Acronis W000 Full Backup
lun 10/10
El mes pasado
Alerta de Backup Exec: Trabajo satisfactorio (Servidor: "...
Microsoft Outlook
03/09/2011
Alerta de Backup Exec: Fallo de trabajo (Servidor: "PPB...
Microsoft Outlook
03/09/2011
Acronis W000 Full Backup
administrador...
Acciones
Para:
lunes, 10 de octubre de 2011 18:24
This is the test notification message

39

Análisis


2011-05-02 16:16:51 192.168.168.226 GET /owa/forms/premium/StartPage.aspx &Initial+Budget>>Conn:1,HangingConn:0,AD:$null/$null/0%,
CAS:$null/$null/0%,AB:$null/$null/0%,RPC:$null/$null/0%, FC:$null/0,Policy:BESPolicy,Norm&nbr=PFEXMBX01.
sessionId=d754!678f!f44065b1062c04c6d45d2b&prfltncy=684&prfrpcnt=57
&prfrpcltncy=515&prfldpcnt=6&prfldpltncy
=16&prfevicnt=0&prfevlltncy=0&End+Budget>>Conn:1,HangingConn:0,AD:$null/$null/0%,CAS:$null/$null/1%,AB:$null/$null/0%,RPC:$null/$null/1%,
FC:$null/0,Policy:BESPolicy,Norm[Resources:(Mdb)MBX03(Health:-1%,HistLoad:0),(DC)FPDC30
(Health:-1%,HistLoad:0),]
443 es\adminbus 82. :168 Mozilla/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;+Win64;+x64;+Trident/5.0) 200 0 0 609
2011-05-02 16:17:39 192.168.168.226 GET /owa/ - 443 - 82. 168

Análisis

Fecha	Dirección IP	ISP	Ciudad	País
2011-01-02	79 [redacted] 6	Telefonica de España	[redacted]	ES
2011-01-03	21 [redacted] 241	Telefonica de España	Madrid	ES
2011-01-04	21 [redacted] 241	Telefonica de España	Madrid	ES
2011-01-10	21 [redacted] 241	Telefonica de España	Madrid	ES
2011-01-11	21 [redacted] 241	Telefonica de España	Madrid	ES
2011-01-19	21 [redacted] 241	Telefonica de España	Madrid	ES
2011-01-29	88 [redacted]	Telefonica de España	Madrid	ES
2011-02-02	80 [redacted] 57	Telefonica de España	[redacted]	ES
2011-02-02	88 [redacted]	Telefonica de España	Madrid	ES
2011-03-29	21 [redacted] 85	ONO	Madrid	ES
2011-05-02	82 [redacted] 68	ONO	[redacted]	ES
2011-06-15	21 [redacted] 0	ONO	Madrid	ES
2011-06-29	88 [redacted] 0	Telefonica de España	[redacted]	ES
2011-07-04	88 [redacted] 0	Telefonica de España	[redacted]	ES
2011-07-28	80 [redacted] 22	Telefonica de España	Madrid	ES
2011-07-28	88 [redacted] 16	Telefonica de España	Madrid	ES
2011-08-17	88 [redacted] 30	Telefonica de España	Madrid	ES
2011-08-23	88 [redacted] 30	Telefonica de España	Madrid	ES
2011-09-03	83 [redacted] 9	Telefonica de España	[redacted]	ES
2011-09-04	88 [redacted]	Telefonica de España	Madrid	ES
2011-09-22	82 [redacted] 22	ONO	Madrid	ES
2011-09-24	82 [redacted] 68	ONO	[redacted]	ES
2011-09-30	82 [redacted] 68	ONO	[redacted]	ES
2011-10-01	82 [redacted] 68	ONO	[redacted]	ES
2011-10-02	82 [redacted] 68	ONO	[redacted]	ES
2011-10-02	90 [redacted] 5	Uni2	Madrid	ES

41

Análisis

Nº accesos total	buzón de correo
18	monica[redacted]
12	lmar[redacted]
11	[redacted]
7	[redacted]
6	[redacted]
6	[redacted]
6	[redacted]
5	[redacted]
5	[redacted]

Conclusiones

- Los correos de trazabilidad demostraron accesos a los buzones de CEO y Dir. RRHH por parte de terceros
- El análisis de logs ha demostrado accesos mediante un procedimiento poco convencional a los buzones de muchos más usuarios
- Es necesario solicitar requerimientos a los Proveedores de Servicio para identificar a los posibles autores (direcciones IP)
- Otras pruebas adicionales:
  - Análisis vulneración intimidad (¿qué se ha accedido exactamente?)
  - Forense PC's
  - Empresa: metodología trabajo IT, incidencias

43

Metodología y buenas prácticas forenses

- Reglas de los NO:
  - NO encender el ordenador (de nuevo) ya que puede sobrescribir sus datos y perder indicios
  - NO acceder al ordenador del empleado aunque el informático le diga que no se puede detectar (SE DETECTA)
  - NO hacer búsquedas
  - NO intentar recuperar archivos

Metodología y buenas prácticas forenses

- Pasos a seguir tras un incidente:
  - Por parte de la **empresa**:
    - Política de uso de sistemas que incluya auditoria (firmada por el trabajador)
    - Indagar solo en los sistemas comunes (SAP, Proxy, logs (con cuidado), etc.)
    - Anotar todo el histórico de sospechas, fechas y detalles
    - Ser prudente (minimizar el número de informados)
    - Llamar a su abogado

Metodología y buenas prácticas forenses

- Pasos a seguir tras un incidente:
  - Por parte del **abogado**:
    - Consultar lo antes posible a expertos en prueba electrónica para:
      - Aseguramiento/Evitar pérdida y/o conseguir más indicios
      - Estrategia correcta (experiencia acumulada)
      - Valor probatorio
    - No solo en casos en los que se evidencia un incidente informático, en todos en los que haya involucrados correos electrónicos, necesidad de acceso a equipos informáticos, etc

Metodología y buenas prácticas forenses

- ¿Que haremos nosotros?
  - Reunión/Comité crisis --> estrategia
  - Información de contexto
  - Identificación fuentes de información
    - ordenadores
    - servidores
    - dispositivos usb
    - teléfonos móviles
  - Preservación de la información
    - cadena de custodia: copia espejo

Metodología y buenas prácticas forenses

Metodología y buenas prácticas forenses

- Actuaciones **in-situ:**
  - Solo para casos muy concretos:
    - Tiempo muy limitado / exceso de información
    - Procesos forenses son largos y complejos
    - Presión
    - Imprecisión
    - Sesgo
    - Falta objetividad
    - Falta herramientas

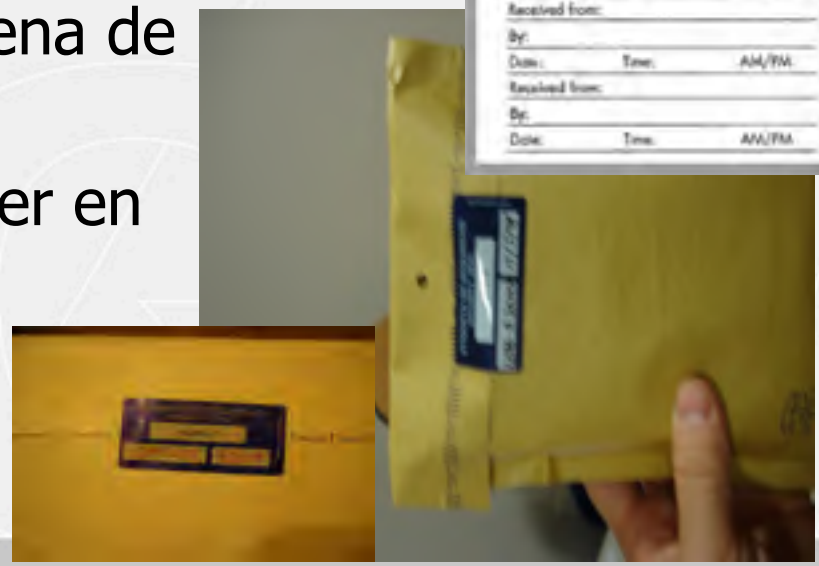
49

Metodología y buenas prácticas forenses

- Cadena de custodia:
  - **copia espejo/copia forense**, aunque exista protocolo interno y la Tribunal Supremo 26 Septiembre 2007, se recomienda:
    - Ante notario (presencia y depósito)
    - Presencia trabajador/Notificación al trabajador
    - Representante de los trabajadores
    - En horario laboral
    - Actas de testigos
    - Hash criptográfico

Metodología y buenas prácticas forenses

- Cadena de custodia:
  - **copia espejo/copia forense**
    - Cerrar un sobre con disco duro
    - Etiqueta de seguridad
    - Reflejar información cadena de custodia
    - Entregar a notario o meter en caja fuerte



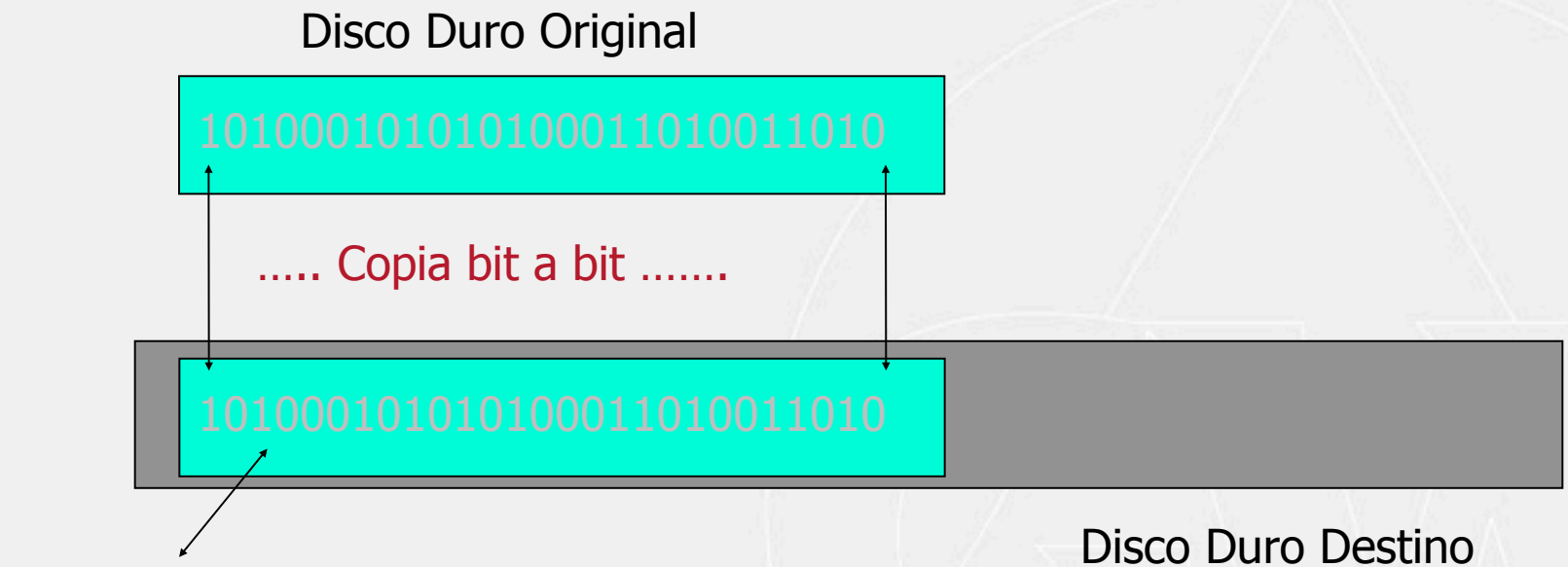
51

Metodología y buenas prácticas forenses

- **Copia espejo/copia forense/copia ciega/copia bit a bit**:
  - Es una copia BIT a BIT de TODA la información contenida en un medio de almacenamiento de información (generalmente un disco duro)

Metodología y buenas prácticas forenses

- **Copia espejo**



-No es una copia a nivel de Archivos ni de sistema operativo

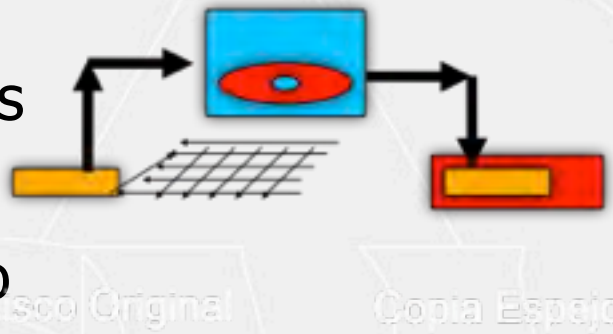
53

Metodología y buenas prácticas forenses

- Métodos de copia
  - **Hardware de copiado:**
    - Sencillo de entender por los profanos
    - Método muy visual
    - Fácil de utilizar
    - Problema: No siempre es posible extraer el disco duro de un dispositivo

Metodología y buenas prácticas forenses

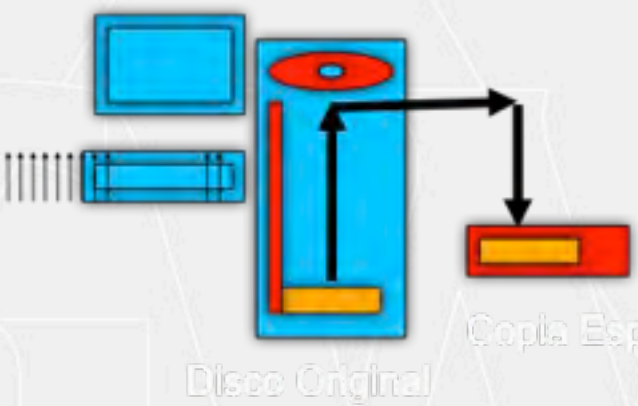
- Métodos de copia
  - **Copiado disco a disco desde PC Alternativo**
    - Posible entender por los profanos
    - Método visual
    - Garantía del software de copiado
    - (Puede entregarse el CD-ROM)
    - Difícil de realizar (expertos)
    - Problema: No siempre es posible extraer el disco duro de un dispositivo



55

Metodología y buenas prácticas forenses

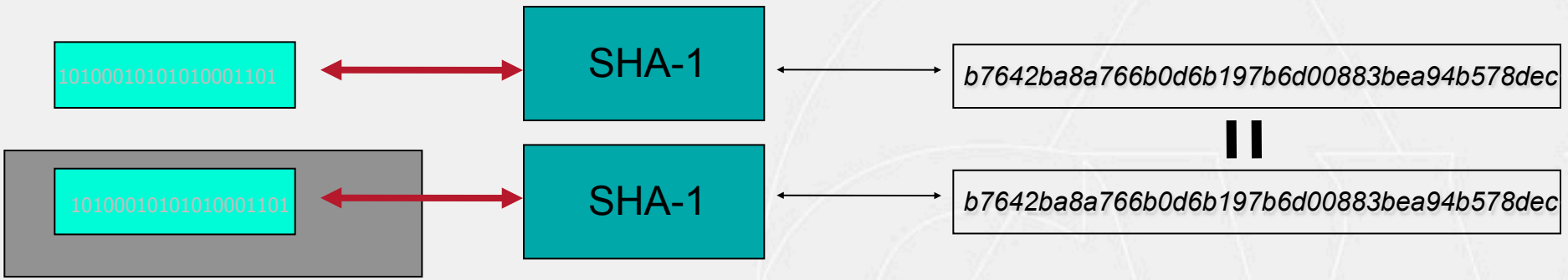
- Métodos de copia
  - **Copia del disco desde el mismo PC Objetivo**
    - No es necesario abrir y extraer disco
    - Garantía del software de copiado.
    - Puede entregarse el CD-ROM
    - Muy poco visual
    - Difícil de realizar (expertos)



56

Metodología y buenas prácticas forenses

- HASH criptográfico
  - Integridad de la información adquirida



Metodología y buenas prácticas forenses

- Análisis
  - Alcance --> ¿PODEMOS ANALIZARLO TODO?
    - Ejemplo:Disco Duro 100 GB
    - 1 Página WORD aprox. 400 palabras, 3000 caracteres, 3Kb
    - lectura media: 0,3 páginas/ minuto100.000.000.000 / 3000 = 33MM Páginas
    - 634 años para una persona a razón de 8 horas al día

58

Metodología y buenas prácticas forenses

- Como debe ser la prueba:
  - Lícita
  - Necesaria
  - Idónea
  - **Proporcional**

Metodología y buenas prácticas forenses

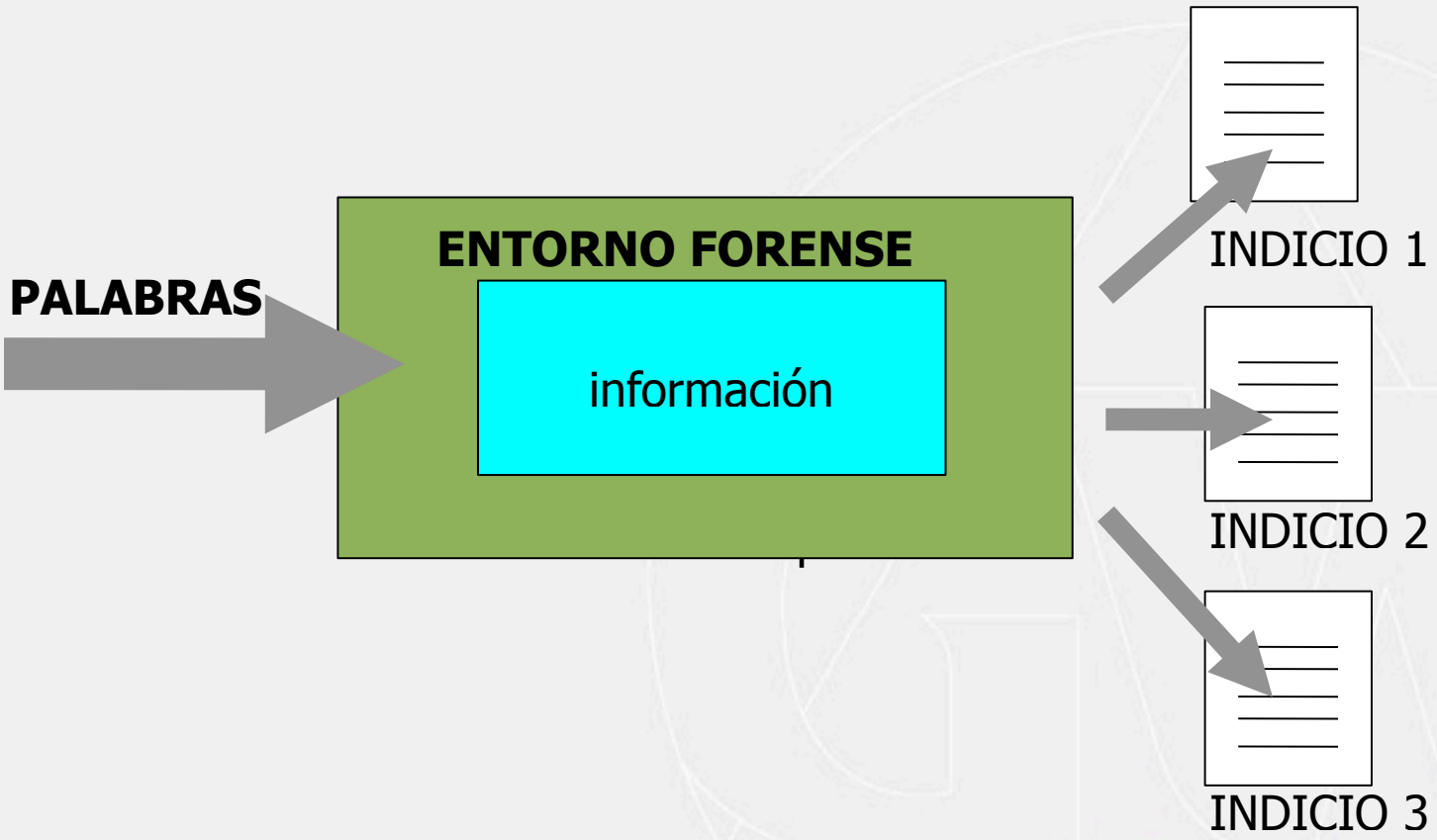
- Procedimientos técnicos forenses
  - Timeline. Actividad del ordenador
  - Timeline hechos (línea temporal de sucesos)
  - Logs (registros del sistema)
  - Recuperación datos
  - Dispositivos HW conectados
  - Navegación
  - Historial
  - Temporales
  - …

Metodología y buenas prácticas forenses

- Procedimientos búsqueda y revisión de información
  - **Búsquedas ciegas**
  - **Heurística**

Metodología y buenas prácticas forenses

- Búsquedas ciegas por palabras clave:



62

Metodología y buenas prácticas forenses

- Búsquedas ciegas por palabras clave:

1 2 3 4 5	En un lugar de la Manc0101101010101010101010111111111010101ha [2], de cuyosdfhldfkghkldhjwrgirtky3p 45kyqt69876pyhethl0101101010101010101010111111111010101muw5thlla de algo más vaca que carnero, salpi có n las más noches [5], duelos y queb0101101010101010101010111111111010101rantos los sábados [6], lantejas los viernes [7], algún palomino d0101101010101010101010111111111010101e añadidura los domingos [8], consumían las tres partes de su hsdfgawemñ ropghaeropvthkkwrterghtrjdetgjdor y amigo de la caza. Quieren decir que tenía el sobrenombre de «Quijada», o «Quesada», que en esdgsdfhdfjyghjsto hay alguna diferencia en los autores que deste caso escriben, aunque por conjeturas verisímiles [*]se 0101101010101010101010111111111010101deja entender que se llamaba «Quijana» [*][16]. Pero esto importa poco a nuestro cuento: basta que en la narración dél no se salga un punto de la verdad.asgsdh sghhstrbvqyw45yc4w 576457878k9mnbu v65we 45yvc34qt6w45yub57jws45 pepe@hotmail.com 834058234058230458erwerwerwer oc01010101010010101001 010101010 10101000000000000000000000101011010 10101010101010111111 11110101010110asdñfjjqcgmex

Palabras Clave

El software forense nos indica si la palabra clave localizada corresponde a un fichero, si está borrado o es un rastro que queda por el disco

Metodología y buenas prácticas forenses

- Búsqueda forense: (Búsqueda extendida)
  - Ficheros Ofimáticos
  - Ficheros PDF
  - Correo corporativo
  - Ficheros comprimidos
  - Registro sistema
  - …

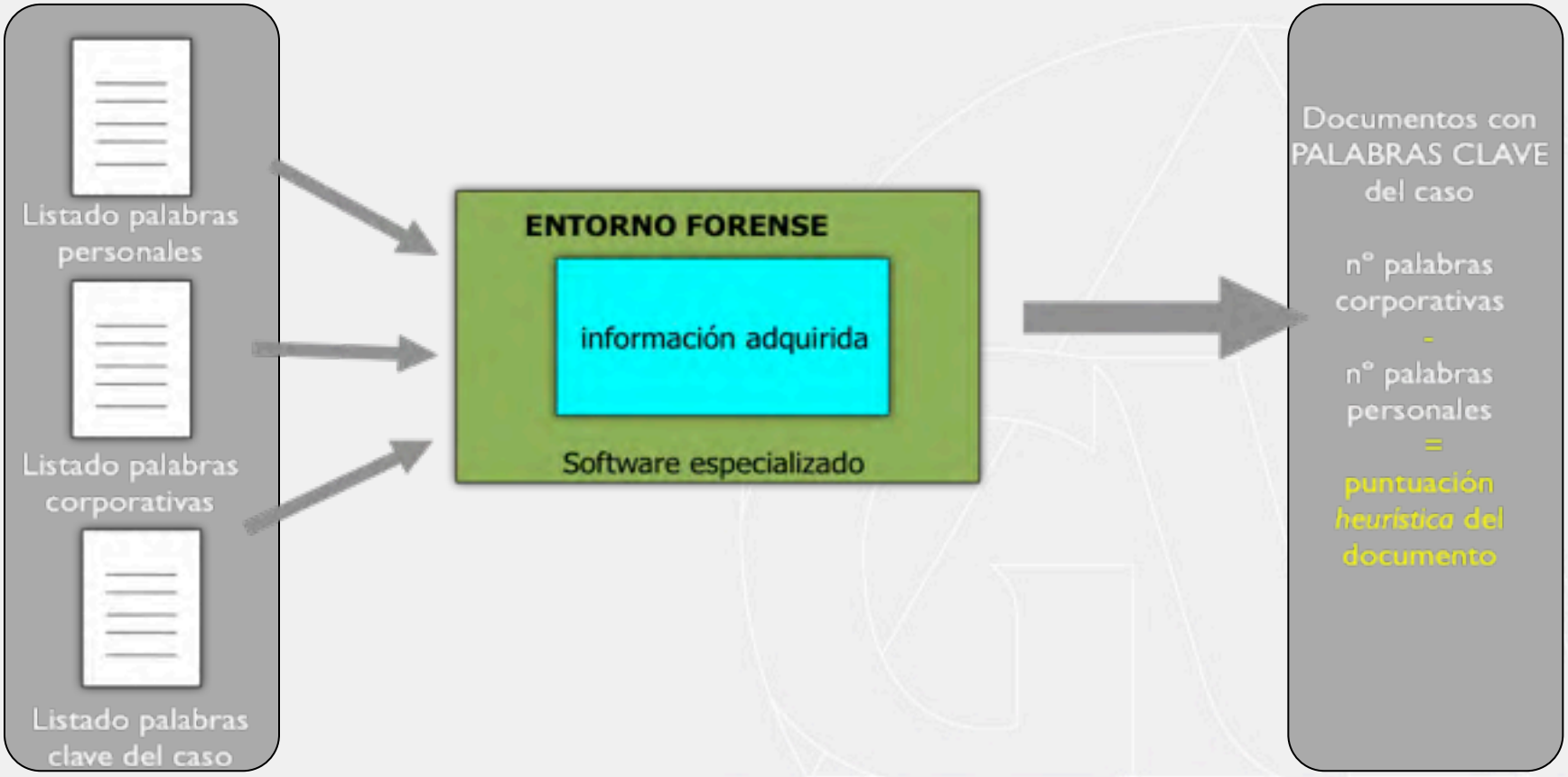
64

Metodología y buenas prácticas forenses

- **Sentencia 164/08 Audiencia Provincial de Barcelona**
  - "Y a la vista de ello argumentábamos que en este caso no era posible apreciar una vulneración de este derecho constitucional porque el perito informático no había interferido ningún proceso de comunicación ajeno. El perito lo que hizo fue una **búsqueda ciega** a través de una herramienta informática (...),que no conlleva la lectura de toda la información para detectar lo relevante para la empresa, sino la utilización de **palabras clave** que solo permiten rescatar lo que interesa, si es que no hubiera sido borrado en la reinstalación. El borrado usual (pues existen otros de bajo nivel que sí eliminan la información), no hace desaparecer los datos, sino que elimina las entradas de los mismos y hace imposible acceder a ellos: al romperse el código de entrada en sistema binario, los datos permanecen, pero confundidos e indistinguibles en una enorme cantidad de ceros y unos, de modo que el programa empleado pretende detectar los patrones binarios de ciertas palabras, y una vez detectados, reinterpretar por encima y por debajo hasta reconstruir un texto.

Metodología y buenas prácticas forenses

- Heurística



Metodología y buenas prácticas forenses

P.total	Referencia del correo	P. total	P. corporativa	P. personal	Palabras profesionales	Palabras personales
-23	100410-501	Puntuación total=-23	Puntuación corporativa=0	Puntuación personal=23		amor:2;invitacion:1;miembro:1;miembros:1;mujer:2;novia:1;novio:1;pareja:3;pop:1;reino:2;romance:1;santa:4;santo:2;titulo:1;
0	100410-101	Puntuación total=0	Puntuación corporativa=2	Puntuación personal=2	informe:1;tanque:1;	videos:2;
2	100410-088	Puntuación total=2	Puntuación corporativa=2	Puntuación personal=0	informe:1;tanque:1;	
0	100410-001	Puntuación total=0	Puntuación corporativa=0	Puntuación personal=0		
-8	100410-055	Puntuación total=-8	Puntuación corporativa=4	Puntuación personal=12	oferta:1;mercado:1;solicitud:1;metros:1	amigo:1;culo:4;hand:1;legal:1;libres:1;mano:3;manos:1;
-2	100410-807	Puntuación total=-2	Puntuación corporativa=6	Puntuación personal=8	oferta:3;mercado:1;solicitud:1;presupuesto:1	amigos:2;deseado:1;hand:1;legal:1;mano:3
-9	100410-019	Puntuación total=-9	Puntuación corporativa=3	Puntuación personal=12	mercado:1;meter:2	atentado:1;blancos:1;deportes:1;entertainment:1;entretenimiento:1;huelga:1;meter:2;muerta:1;muertos:1;mujer:1;negros:1;

67

Contacto

- ¿Preguntas?

INCIDE – Investigación Digital

Passeig Sant Gervasi, 10 ent. 3ª

08021 **Barcelona**

info@incide.es

http://www.incide.es

http://www.twitter.com/1NC1D3

http://www.atrapadosporlosbits.com

http://www.youtube.com/incidetube

Companies > INCIDE - Investigación Digital

Tel./Fax. +34 932 546 277 / +34 932 546 314