Forensia aplicaciones web

Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx

Forencia sobre correo electrónico

Correo electrónico

- *Kill Application* de Internet
- Inventado por Ray Tomlinson
- Protocolos y puertos
  - SMTP: 25
  - POP: 110
    - Poder administrar los correos sin tener que estar conectado
  - IMAP: 143
    - Necesario estar conectado a internet todo el tiempo.
- Estándares asociados
  - MIME
  - S/MIME
  - PGP

Lámina 3 Dr. Roberto Gómez C.

Entidades involucradas

- Agente de usuario
  - MUA
- Agente de transporte
  - MTA
- Agente de entrega
  - MDA

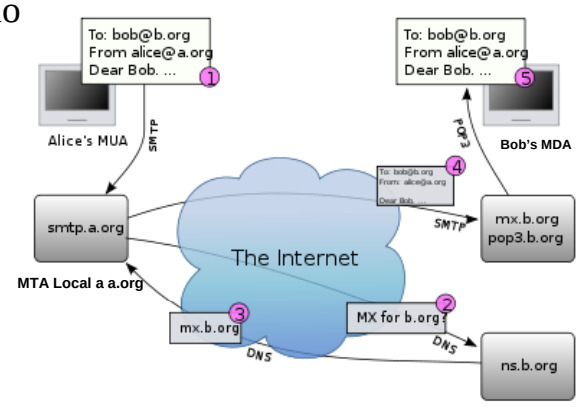
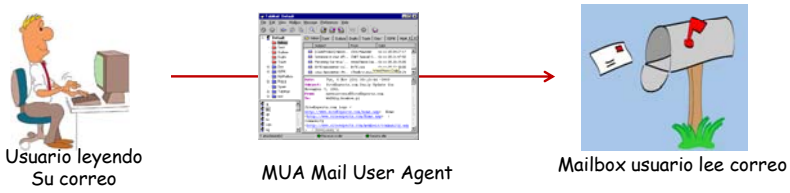


Lámina 4 Dr. Roberto Gómez C.

Lectura de correos electrónicos

- Acceso directo



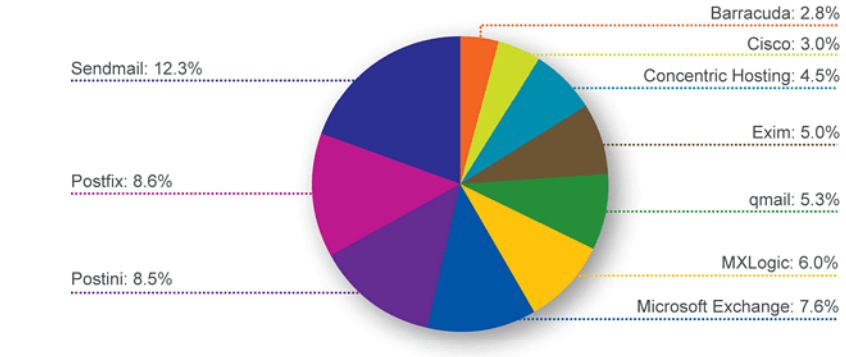
- Acceso remoto

Lámina 5 Dr. Roberto Gómez C.

Dispositivos móviles correo electrónico

Lámina 6 Dr. Roberto Gómez C.

Principales MTAs

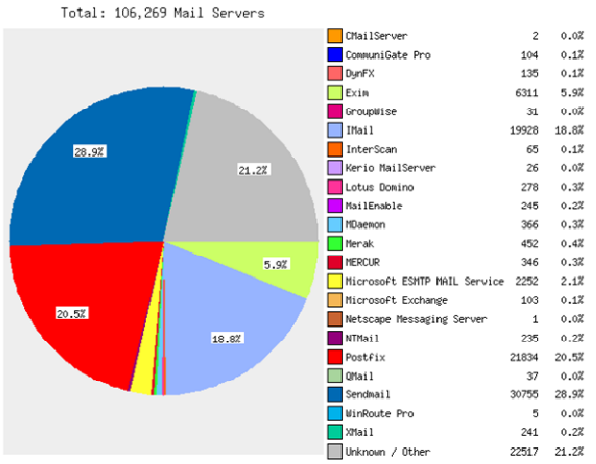


Fuente: Oreilly: http://www.oreillynet.com/pub/a/sysadmin/2007/01/05/fingerprinting-mail-servers.html

Lámina 7 Dr. Roberto Gómez C.

El mercado en el 2004

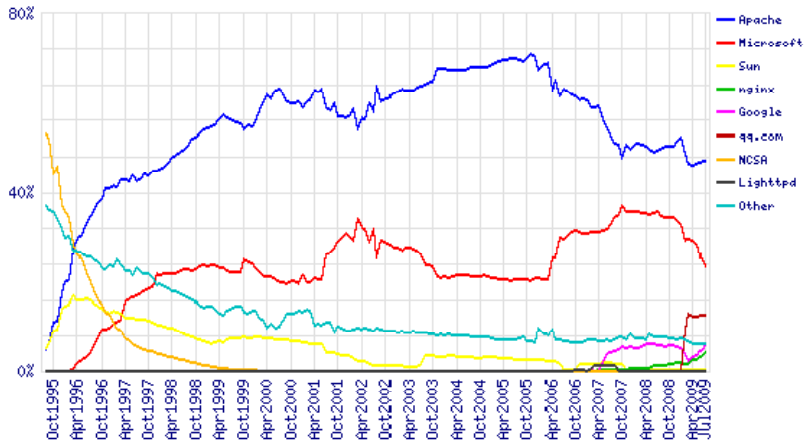
Sendmail	28.94
Postfix	20.55
Imail	18.75
Exim	5.94
:	:
Mic. ESMTP Mail Service	2.12
Microsoft Exchange	0.1
:	:
Otros	21.19



Fuente: http://www.falkotimme.com/projects/survey_smtp_032004.php

Lámina 8 Dr. Roberto Gómez C.

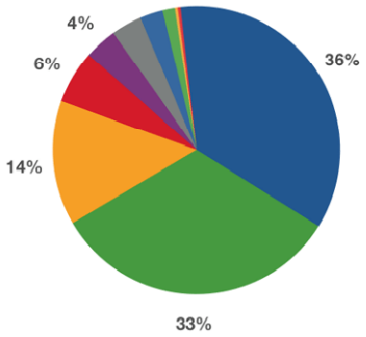
¿Y los servidores Web?



Fuente: Netcraft (http://news.netcraft.com)

Principales MUAs

Email client	Market share
Outlook	36%
Outlook 2003 and earlier	29%
Outlook 2007	7%
Hotmail	33%
Yahoo! Mail	14%
Gmail	6%
Apple Mail	4%
Windows Live Mail (Desktop)	3%
Thunderbird	2.4%
iPhone	1.3%
Lotus Notes	0.2%
AOL Mail	0.1%



Fuente: http://fingerprintapp.com/email-client-stats

Formatos de almacenamiento de correos electrónicos

Formato	Soportado por	Características
mbox	Thunderbird, Apple Mail	Todos los mensajes para un folder se encuentran dentro de un archivo lineal
mbx	Eudora	Igual que mbox, excepto que el status del mensaje es almacenado en un archivo externo.
maildir	qmail	Un archivo por directorio, tres directorios (new, cur, tmp) por folder.
pst	Microsoft	Personal Storage Table, Outlook almacena los mensajes, calendario y otros datos en archivos .pst o .osf (Off-line Storage Table). Los archivos .pst son usados para datos archivados y los .osf para disponibilidad de los dato sfuera de lína.

Ejemplo: La ubicación de los correos de Thunderbird en Windows:
C:\Documents and Settings\L00445569\Datos de programa\Thunderbird\Profiles\1mixdavl.default

Lámina 11 Dr. Roberto Gómez C.

Crecimiento del correo electrónico

- Usuarios consideran al correo electrónico en sus computadoras como una base de conocimiento histórico o para soportar decisiones pasadas o acciones tomadas.
- Los usuarios no cuentan con una guía/recomendación de cómo guardar, por lo que por default almacenan todo.
- Registros duplicados son almacenados como consecuencia de CCs e inundaciones de correo.
- Los usuarios reciben y almacenan mensajes de correo con anexos muy grandes.

Lámina 12 Dr. Roberto Gómez C.

Forencia en el correo electrónico

- Estudio de la fuente y contenido del correo electrónico como evidencia
  - Identificar el emisor y receptor de un mensaje, así como la fecha y hora a la que se envío el mensaje
  - En la mayor parte de los casos el correo es muy incriminatorio

Lámina 13 Dr. Roberto Gómez Cárdenas

Investigando crímenes y violaciones sobre correo electrónico

- Similar a otros tipos de investigación
- Objetivos
  - Encontrar quien esta detrás de un crimen
  - Recolectar evidencia
  - Presentar lo que se encontró
  - Construir un caso

Lámina 14 Dr. Roberto Gómez Cárdenas

Identificando crimenes de correo y violaciones

- Depende en la ciudad, estado o país
  - Spam
  - Siempre consultar con un abogado
- Se están volviendo comunes
- Ejemplos de crímenes que involucra correos electrónicos
  - Tráfico de narcóticos
  - Extorsión
  - Acoso sexual

Lámina 15 Dr. Roberto Gómez Cárdenas

Examinando mensajes de correo electrónico

- Acceder computadora víctima y retirar evidencia.
- Utilizar el cliente de correo electrónico de la víctima.
  - Encontrar y copiar evidencia en el correo electrónico.
  - Acceder material protegido o cifrado.
  - Imprimir correos electrónicos.
- Guiar a la víctima por teléfono.
  - Abrir y copiar correo electrónico incluyendo encabezados.
- Algunas veces se trata con correos borrados.

Lámina 16 Dr. Roberto Gómez Cárdenas

Roles cliente y servidor en el correo electrónico

- Dos ambientes.
  - Internet.
  - LAN, MAN o WAN controlada.
- Arquitectura cliente/servidor.
  - El sistema operativo del servidor y el software de correo electrónico difieren de lo del cliente
- Cuentas protegidas.
  - Requiere una cuenta y una contraseña.

Lámina 17 Dr. Roberto Gómez Cárdenas

Roles cliente y servidor

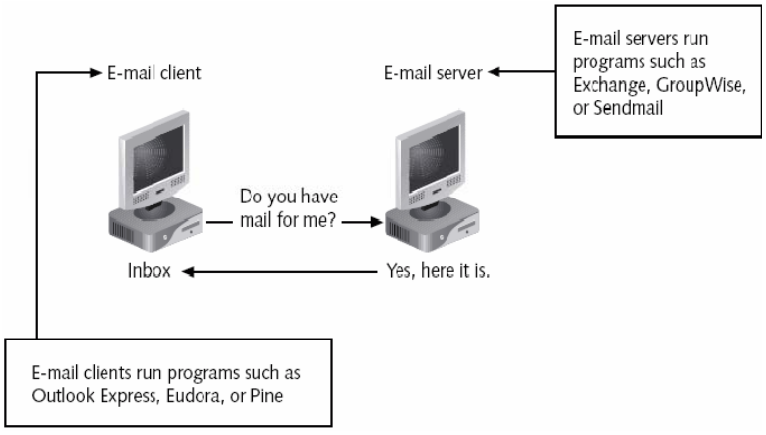


Lámina 18 Dr. Roberto Gómez Cárdenas

Las convenciones del nombre

- Corporativo
  - John.smith@somecompany.com
- Público
  - whatever@gmail.com
- Todo lo que sigue después de @ es un nombre de dominio.

Lámina 19 Dr. Roberto Gómez Cárdenas

Un poco de historia: origen @

- Conocida en español como "arroba" y en inglés como "at".
- La arroba era un equivalente del "ánfora", medida comercial utilizada por los navegantes venecianos,
  - documento del 4 de mayo de 1536, aparece con el nombre de "chiocciola" - caracol -,
  - era utilizado en todas las transacciones comerciales llevadas a cabo en el mundo hispanoárabe.
- La palabra "arroba" significa "un cuarto" en la lengua de Mahoma.

Lámina 20 Dr. Roberto Gómez Cárdenas

¿Y cómo llega @ a internet?

- Es una idea de Ray Tomlinson
  - ingeniero estadounidense y uno de los padres del Arpanet, el antecesor de Internet
- A principios de los 70, Tomlinson incorporó la arroba justo entre su nombre y el servidor que recibiría el mensaje.
- La arroba había sobrevivido en la tipografía anglosajona con el significado de "al precio de", de uso mercantil, y seguiía incorporada en los teclados de las computadoras y las máquinas de escribir de aquellos años.

Lámina 21 Dr. Roberto Gómez Cárdenas

Ejemplo cliente correo electrónico

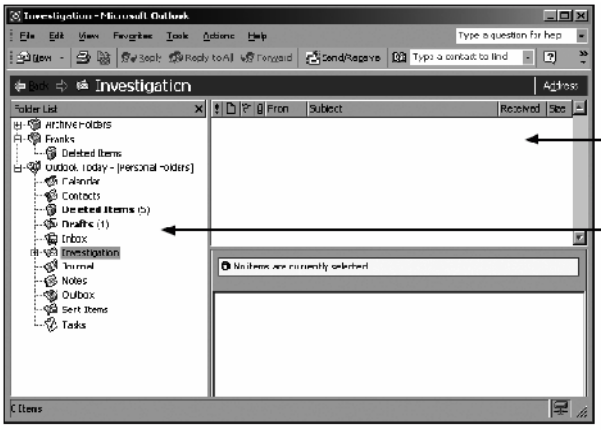


Lámina 22 Dr. Roberto Gómez Cárdenas

Estándar RFC

- RFC 2821
  - Simple Mail Transfer Protocol (SMTP): El objetivo del SMTP es transferir correo de forma eficiente y confiable. Es independiente del particular subtipo de transmisión y solo requiere un canal confiables de flujo de datos
  - Un correo de mensaje pasa a través de un número de hosts intermediarios en su recorrido del emisor al último receptor.
- RFC 2822
  - Internet Message Format: establece el formato de los mensajes.
  - Campos identificación: aunque opcional, cada mensaje debe contar con un campo de Message-ID
  - El campo proporciona identificador único del mensaje que hace referencia a una versión en particular de un mensaje en particular.
  - Debe ser legible por la máquina y no necesariamente con sentido para el ser humano.

Lámina 23 Dr. Roberto Gómez Cárdenas

Encabezados: El identificador único

- Message-ID
  - Compuesto por campos respetando la siguiente sintaxis:

    <date/time integer.unique_id-domain>
- Date/Time Integer
  - Puede contar con un formato para desplegar una fecha legible por el ser humano, pero usualmente es un string hexadecimal.
  - En sistemas Unix el hexadecimal representa el “número de microsegundos desde las 0:00:00 del 1 enero de 1970 (Greenwich Mean Time).

Lámina 24 Dr. Roberto Gómez Cárdenas

Encabezados

- unique_id-domain
  - Identificador único asignado en el proceso SMTP
  - Se añade el nombre del dominio para ayudar a asegurar que sea único a nivel global.
- ESMTP id
  - Identificador único asignado por cada intermediario o servidor gateway
  - Se trata de un string hexadecimal que es re-incializado cada día.
  - Se cuenta con un identificador que puede ser "resuelto" en una ventana de tiempo en un servidor en partícular.

Lámina 25 Dr. Roberto Gómez Cárdenas

Viendo encabezados correo electrónico

- Aprender como encontrar encabezados de correo electrónico
  - Clientes GUI
  - Clientes línea de comandos
  - Clientes basado en web
- Encabezados contiene información últil
  - Números de identificación únicos
  - Dirección IP del servidor emisor
  - Tiempo de envío

Lámina 26 Dr. Roberto Gómez Cárdenas

Los encabezados en correo electrónico en outlook

- Outlook
  - Abrir el cuadro de diálogo de Opciones Mensaje
  - Copiar los encabezados
  - Pegarlos en cualquier editor de texto.
- Outlook express
  - Abrir el cuadro de diálogo de Propiedades de Mensaje
  - Seleccionar Fuente Mensaje .
  - Copiar y pegar los encabezados en cualquier editor de texto

Lámina 27 Dr. Roberto Gómez Cárdenas

Encabezado en Microsoft Outlook

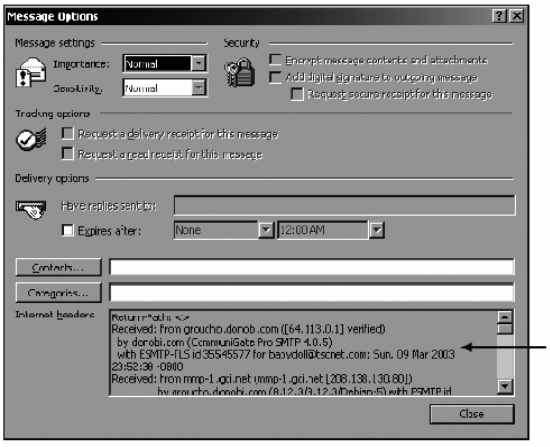


Lámina 28 Dr. Roberto Gómez Cárdenas

Encabezado en Microsoft Outlook Express

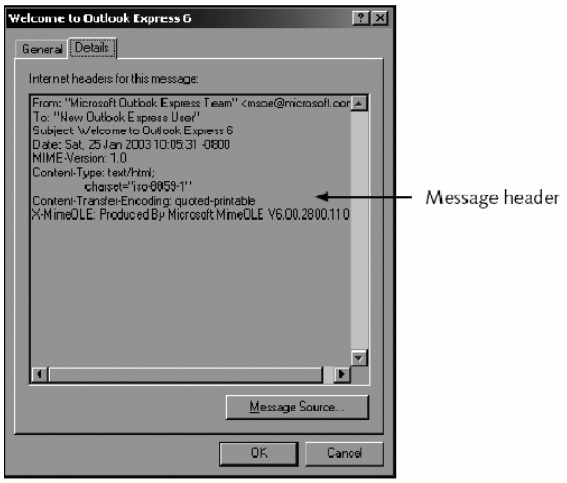


Lámina 29 Dr. Roberto Gómez Cárdenas

Detalle del encabezado en Outlook Express

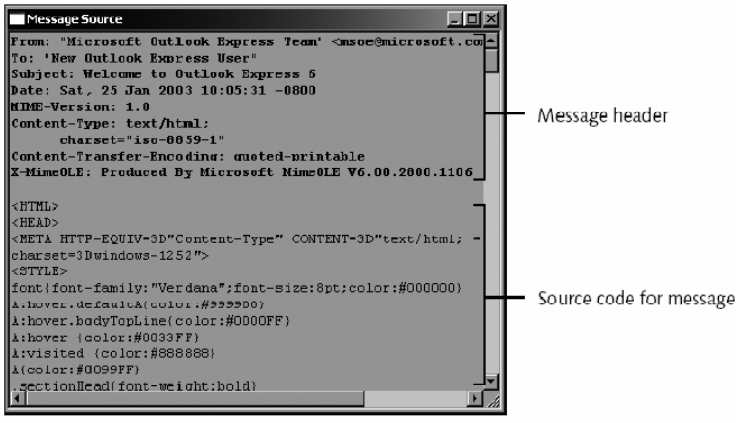


Lámina 30 Dr. Roberto Gómez Cárdenas

Viendo encabezado en Eudora

- Seleccionar boton BLAH BLAH BLAH
- Copiar y pegar el encabezado de correo

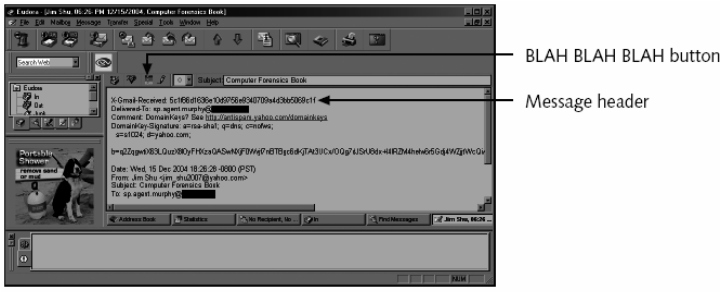


Lámina 31 Dr. Roberto Gómez Cárdenas

Viendo encabezado en Pine y ELM

- Verificar los encabezados completos

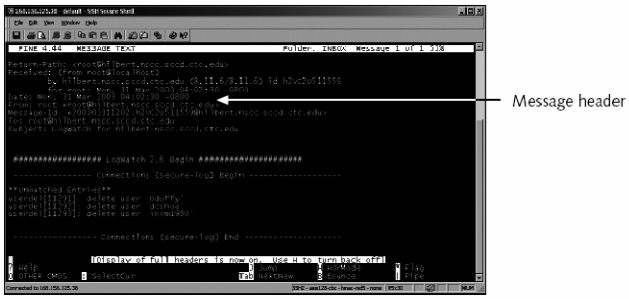
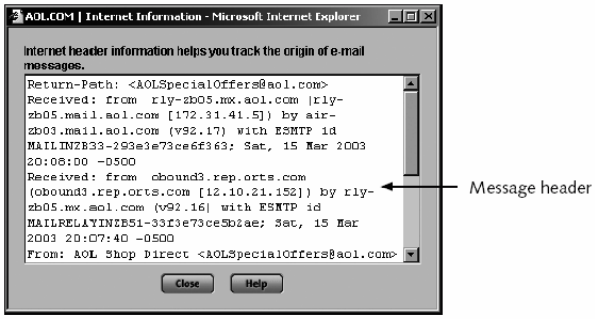


Lámina 32 Dr. Roberto Gómez Cárdenas

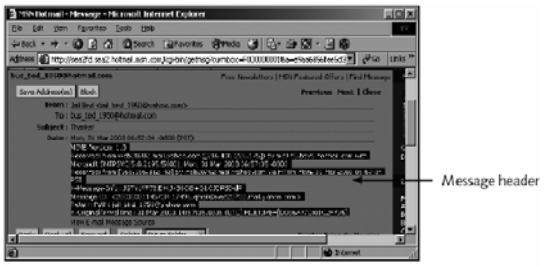
Encabezados AOL

- Abrir ventana diálogo de detalles de correo
- Copiar y pegar los encabezados



Encabezados hotmail

- En el menú seleccionar Options, Preferences.
- Seleccionar encabezados avanzado.
- Copiar y pegar encabezado.
- ingomla@hotmail,com



Encabezados Yahoo

- Seleccionar Mail Options.
- Seleccionar General Preferences y Show All headers en mensajes recibidos (incoming messages).

Encabezados gmail

Datos dentro del encabezado

1. Return de path
2. Direcciones de correo del recipiente
3. Tipo de servicio de envío de correo electrónico
4. Dirección IP de un servidor emisor
5. Nombre de un servidor de correo electrónico
6. Número único de mensaje
7. Fecha y tiempo en que el correo fue enviado
8. Información de los archivos anexos

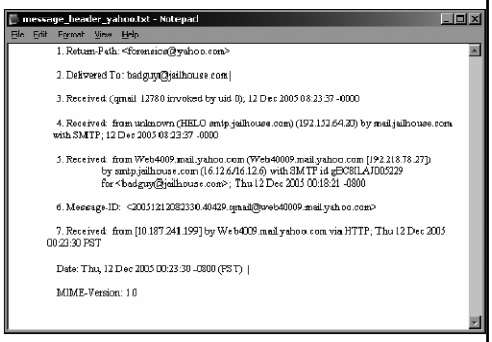


Lámina 37 Dr. Roberto Gómez Cárdenas

Examinando archivos adicionales de correo electrónico

- Los mensajes de correo electrónico son almacenados del lado del cliente o de
- Microsoft Outlook archivos .pst y .ost
- Libro direcciones personales
- Unix e-mail groups
  - Miembros leen los mismos mensajes
- Archivos y folder correo basados en web
  - Archivos de History, Cookies, Cache, Temp

Lámina 38 Dr. Roberto Gómez Cárdenas

Seguimiento de un mensaje de correo electrónico

- Contactar los responsables del envío del correo electrónico.
- Encontrar puntos de contacto de los nombres de domino.
  - www.arin.net
  - www.internic.com
  - www.freeality.com
  - www.google.com
- Encontrar información de contacto del sospechoso.
- Verificar lo encontrado contra las bitácoras de red.

Lámina 39 Dr. Roberto Gómez Cárdenas

Bitácoras rede relacionadas con correo electrónico

- Confirmar ruta de correo electrónico.
- Bitácoras ruteador.
  - Registrar todo el tráfico de entrada y salida.
  - Contar con reglas para permitir o filtrar tráfico.
- Bitácoras firewall.
  - Filtrar tráfico correo electrónico.
  - Verificar cuando el tráfico de correo pasó a través de este.
- Se puede utilizar cualquier editor de texto o herramientas especializadas.

Lámina 40 Dr. Roberto Gómez Cárdenas

Ejemplo bitácora firewall

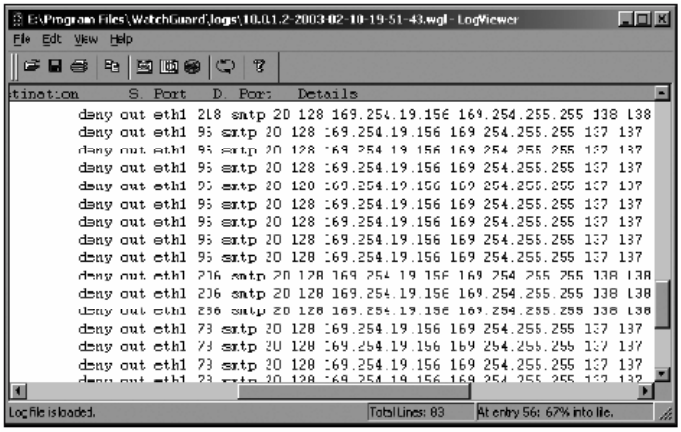


Lámina 41 Dr. Roberto Gómez Cárdenas

Los servidores de correo electrónico

- Computadora corriendo sistema operativo servidor y un paquete de correo electrónico.
- Almacenamiento de correo electrónico.
  - Bases de datos.
  - Archivos planos.
- Bitácoras.
  - Default o manual.
  - Continuo o circular.

Lámina 42 Dr. Roberto Gómez Cárdenas

Bitácoras y correo electrónico

- Información bitácoras.
  - Contenido del correo electrónico.
  - Enviando direcciones IP.
  - Fecha y hora de recepción y lectura.
  - Información específica del sistema.
- Contactar la red del sospechoso tan pronto como sea posible.
- Servidores pueden recuperar correos borrados.
  - Similar al borrado de archivos en un disco duro.

Lámina 43 Dr. Roberto Gómez Cárdenas

Ejemplo bitácora de un servidor de correo

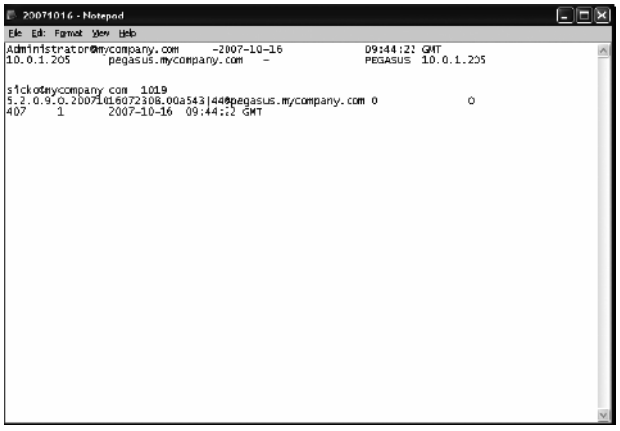


Lámina 44 Dr. Roberto Gómez Cárdenas

Examinando bitácoras servidores Unix

- /etc/sendmail.cf
  - Configuración información para correo electrónico
- /etc/syslog.conf
  - Especifica como y donde se almacenen las bitácoras relacionadas con Sendmail
- /var/log/maillog
  - Bitácoras comunicación SMTP y POP3
    - Dirección IP y estampilla de tiempo
- Mayor información
  - Páginas manual unix (comando man)

Lámina 45 Dr. Roberto Gómez Cárdenas

Ejemplo syslog

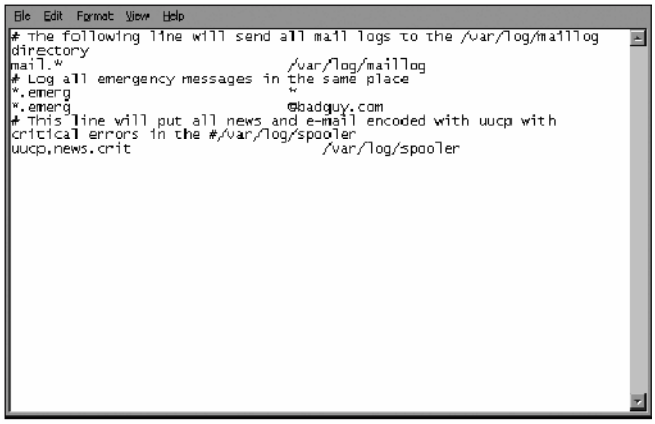


Lámina 46 Dr. Roberto Gómez Cárdenas

Ejemplo bitácora de correo con información POP3

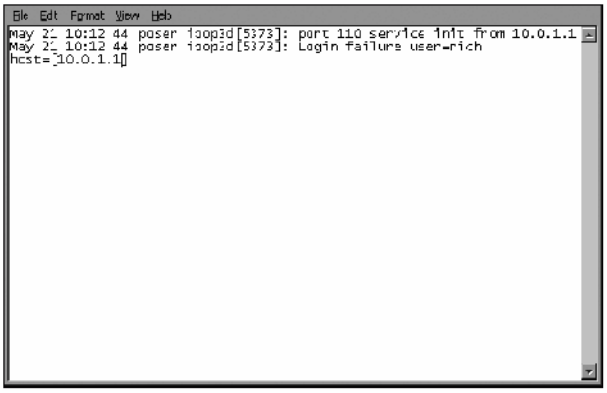


Lámina 47 Dr. Roberto Gómez Cárdenas

Bitácoras Servidor Correo Microsoft

- Microsoft Exchange Server (Exchange)
  - Utiliza una base de datos.
  - Basado en Microsoft Extensible Storage Engine.
- Archivos almacenamiento de información.
  - Archivos base datos *.edb
    - Responsable para información MAPI
  - Archivos base datos *.stm
    - Responsable para información no MAPI

Lámina 48 Dr. Roberto Gómez Cárdenas

Bitácoras Servidor Correo Microsoft

- Bitácoras transacción .
  - Seguimiento de las bases de datos de los correos.
- Checkpoints
  - Seguimiento de bitácoras de transacción
- Archivos temporales
- Bitácoras comunicación correo electrónico
  - RES#.log
- Seguimiento .log
  - Seguimiento mensajes

Lámina 49 Dr. Roberto Gómez Cárdenas

Ejemplo bitácora seguimiento de mensaje en modo verbose

Lámina 50 Dr. Roberto Gómez Cárdenas

Examinando servidor correos Microsoft

- Problemas o bitácoras diagnostico
  - Eventos bitácras
  - Utilizar Windows Event Viewer
  - Abrir cuadro diálogo Event Properties para más detalles acerca de un evento

Lámina 51 Dr. Roberto Gómez Cárdenas

Herramientas especializadas para forencia de correo electrónico

- AccessData's FTK
- EnCase
- FINALeMAIL
- Sawmill-GroupWise
- DBXtract
- MailBag
- Assitant
- Paraben

Lámina 52 Dr. Roberto Gómez Cárdenas

Y que hacen las herramientas

- Las herramientas permiten encontrar
  - Archivos bases datos
  - Archivos correo personales
  - Archivos de almacenamiento fuera de línea
- Ventaja
  - No es necesario conocer como funcionan los servidores de correo y los clientes

Lámina 53 Dr. Roberto Gómez Cárdenas

Ejemplo

caso

Lámina 54 Dr. Roberto Gómez Cárdenas

Caso: los hechos

- Correo relacionado con un pleito legal por $20 millones de dólares proclamaba venir del CEO de "Tech.com" a un corredor de bolsa.
- El mensajes prometía recompensas garantizadas en la siguiente ronda de fondeo del corredor.
- Tech.com indico que el correo era falso.
- La firma legal de Tech.com contrata a alguien para investigar la validez del mensaje.
- Se obtuvieron imágenes del CEO en su oficina y en su hogar. Se copiaron las cintas de respaldo de servidor de correo de su sitio de almacenamiento.

Lámina 55 Dr. Roberto Gómez Cárdenas

Caso: buscando en Tech.com

- Se buscaron todos los discos duros y respaldos de servidores de correo del mensaje cuestionado. La búsqueda no revelo ningún rastro del mensaje.
- Las estampillas de tiempo y los identificadores de mensajes se compararon con las bitácoras de los servidores, se encontró que el mensaje cuestionado no había atravesado ningún servidor de correo o webmail en el tiempo indicado por la estampilla de tiempo del mensaje.
- Basado en lo anterior se procedió a examinar las computadoras del corredor de bolsa.

Lámina 56 Dr. Roberto Gómez Cárdenas

Caso: buscando en el corredor

- Corredor se negó a que se obtuvieran imágenes de su sistema.
- Abogado del corredor fue una corte estatal para solicitar un nuevo examen.
- El nuevo examen reveló pruebas de la alteración del encabezado del mensaje para crear el correo cuestionado..

Lámina 57 Dr. Roberto Gómez Cárdenas

String del Message-ID auténtico

- Message ID
  - 3989F5A3.87BDEEE2@tech.com
- Convirtiendo la primera parte que corresponde a la fecha:
  - 3989F5A3 = hexadecimal
  - 965342627 = decimal
  - Con la ayuda de un script de tiempo de unix se puede deducir que la fecha es
    - Aug 3, 2000 18:43
    - Fecha y hora: +1 hora desfasamiento con respecto a bitácoras

Lámina 58 Dr. Roberto Gómez Cárdenas

String del Message-ID sospechoso

- Message ID
  - 3989e793.87BDEEE2@tech.com
- Convirtiendo la primera parte que corresponde a la fecha:
  - 3989E793 = hexadecimal
  - 965339027 = decimal
  - Con la ayuda de un script de tiempo de unix se puede deducir que la fecha es
    - Aug 3, 2000 17:43
    - Fecha y hora coinciden con bitácoras

Lámina 59 Dr. Roberto Gómez Cárdenas

Encabezado seguimiento

```
Return-Path: CEO Good_Guy@tech.com
Received:  from mail.tech.com (mail.tech.com [201.10.20.152])
           by hedgefund.fund.com (8.11.0/8.11.0) ESMTP id
             e73MfZ331592; Thu, 3 Aug 2000 15:45:31 -0400
Received:  from webmail.tech.com (webmail.tech.com
           [10.27.30.190]) by mail.tech.com (Switch-2.0.1/Switch-
           2.0.1) ESMTP id e73MfW903843; Thu, 3 Aug 2000
           14:41:32 -0500
Received:  from tech.com (ostrich.tech.com [10.27.20.190])
           by webmail.tech.com (8.8.8+Sun/8.8.8)  with ESMTP
           id RAA01318; Thu, 3 Aug 2000 14:41:31 -0500
content-class: urn:content-classes:message
Subject: Warrants on $25 Million Funding
Date: Thu, 3 Aug 2000 14:43:47 -0500
MIME-Version: 1.0
Content-Type: application/ms-tnef;
      name="winmail.dat"
Content-Transfer-Encoding: binary
Message-ID: <3989e793.87BDEEE2@tech.com>
X-MS-Has-Attach:
X-MS-TNEF-Correlator: <3989e793.87BDEEE2@tech.com>
Thread-Topic: Warrants on $25 Million Funding
Thread-Index: AcHatCZUSkaLe0ajEdaelQACpYcy8A==
From: "CEO Good_Guy@tech.com" <ceo_good_guy@tech.com >
To: "Bad_Guy_Broker" <bad_guy@fund.com>
```

Lámina 60 Dr. Roberto Gómez Cárdenas

Bitácoras servidores

webmail@tech.com

Typical logs kept for a week or less and then new log spawned.

syslog. = 7/30 – 8/4 (current period)
syslog.0 = 7/23 – 7/30
syslog.1 = 7/16 – 7/23
syslog.2 = 7/09 – 7/16
syslog.3 = 7/02 – 7/09
syslog.4 = 6/25 – 7/02
syslog.5 = 6/18 – 6/25
syslog.6 = 6/11 – 6/18
syslog.7 = 6/04 – 6/11

Lámina 61 Dr. Roberto Gómez Cárdenas

Análisis bitácoras servidor webmail@tech.com

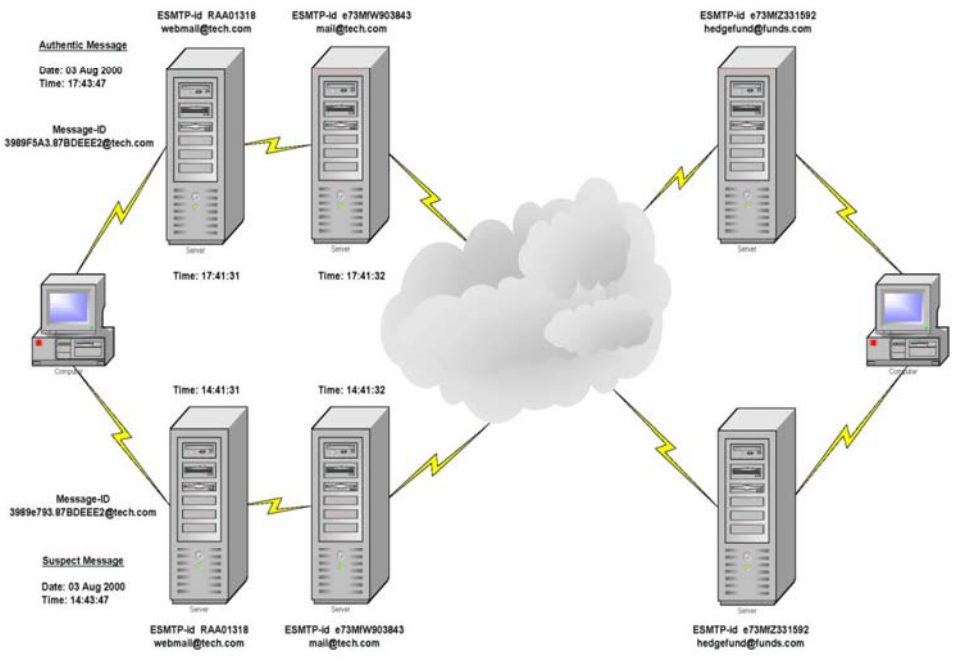
- Haciendo coincidir estampillas tiempo del encabezado y ids del ESMTP revelaron que RAA01318 fue entregado a las 17:41:31 al mensaje autentico.
- Comparado la estampilla 14:41:31 del mensaje sospechoso con la bitácora reveló que el servidor estaba asignando identificadores ESMTP con “OAA” no “RRA” como se encuentra representado en el encabezado.

Lámina 62 Dr. Roberto Gómez Cárdenas

Análisis bitácoras servidor webmail@tech.com

- Análisis bitácoras confirmaron que el mensaje sospechoso no era autentico.
- Haciendo coincidir estampillas e identificadores ESMTP revelaron que el autentico identificador de mensaje fue cargado a las 17:41:32 y se le asigno el id ESMTP e73MfW903843 cuando fue enviado al sevidor hedgefund@fund.com y se le asignó un nuevo ESMTP id: e73MfZ331592.
- Comparando estampilla 14:41:32 del mensaje sospechoso con la bitácora revelo que no hubo mensajes durante una hora durante dicha ventana de tiempo.

Lámina 63 Dr. Roberto Gómez Cárdenas



Email Spoofs

Received: from tht.com (wfarwell.ne.mediaone.net
[24.128.21.184])by chmls06.mediaone.net
(8.11.1/8.11.1) with ESMTP id f1RC2GK11063;
Tue, 27 Feb 2001 07:02:16 -0500 (EST)

From: Robert Lovett [Bob_Lovett@tht.com]
Sent: Thursday, August 03, 2000 8:03 AM
To: Bill Farwell [wfarwell@ix.netcom.com]; r.lovett@tht.com
Subject: Email Spoof

Bob,

This is one way to spoof email.

Bill

~~~~~~

William L. Farwell, CFE, SCERS
Senior Manager
Computer Forensic Specialist

Deloitte & Touche LLP
Forensic Investigative Services
200 Berkeley Street
Boston, MA 02116

617.437.3956 Voice
617.437.5956 Direct Fax
617.437.3849 Lab
617.839.1998 Mobile
mailto:wfarwell@deloitte.com

~~~~~~

Lámina 65 Dr. Roberto Gómez Cárdenas

Referencias

- Leyendo los encabezados de correo electrónico
  - http://www.stopspam.org/email/headers.html
- Como interpretar los encabezados de los correos electrónicos
  - http://help.mindspring.com/docs/006/emailheaders
- Como puedo lograr que un programa de correo revele el mensaje completo y sin modificar
  - http://www.spamcop.net/fom-serve/cache/19.html

Lámina 66 Dr. Roberto Gómez Cárdenas

Forensia Web

Forencia web

- Proceso de reunir junto donde y cuando un usuario ha estado en internet
  - p.e. Scott Peterson, Muchael Jackson
- ¿Porqué?
  - Pornografia infantil
  - Fraude tarjeta bancaria
  - Robo de identidad
  - Espionaje industrial

Tipos de ataques

- Clientes
  - Penetración perimetral
  - Fraude tarjeta bancaria/robo identidad
- Servidores web
  - Acceso a información crítica (p.e. bases datos de clientes)
  - Software troyano

Lámina 69 Dr. Roberto Gómez Cárdenas

Browsers web

- Los principales
  - Internet Explorer
  - Firefox/Mozilla/Netscape
- Otros
  - Safari
  - Opera
  - Konqueror
  - Galeon
  - Chrome
  - links/lynx








Lámina 70 Dr. Roberto Gómez Cárdenas

links/lynx

- Lynx
  - Browser tipo texto para WWW.
- Comando links
  - Browser en modo carácter estilo lynx

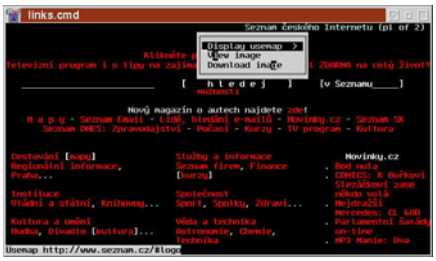


Lámina 71 Dr. Roberto Gómez Cárdenas

Internet explorer

- Información cache
  - C:\Documents and Settings\john\Local Settings\Temporary Internet Files\Content.IE5\
- Historial
  - C:\Documents and Settings\john\Local Settings\History\History.IE5\
- Cookies
  - C:\Documents and Settings\john\Cookies\
- Archivo
  - Index.dat

Lámina 72 Dr. Roberto Gómez Cárdenas

Firefox Mozilla Netscape

- Archivos ubicados en directorio
  - \Documents and Settings\<user name>\Application Data\Mozilla\Firefox\Profiles\<random text>\history.dat
- Mozilla/Netscape
  - \Documents and Settings\<user name>\Application Data\Mozilla\Profiles\<profile name>\<random text>\history.dat

Lámina 73 Dr. Roberto Gómez Cárdenas

Herramientas análisis forense en web

- Pasco
- Web Historian
- IE History
- IEHistoryView v1.35
- FTK Forensic Tool Kit

Lámina 74 Dr. Roberto Gómez Cárdenas

La herramienta Pasco

- Pasco: palabra latina para Browse.
- Herramienta línea comandos que correo en Unix o Windows y puede reconstruir las estructuras internas de archivos Index.dat de Internet Explorer
- Acepta un archivo Index.dat, reconstruye los datos y entrega la información en un formato delimitado por texto.
- Formato útil cuando es necesario importar los datos a una hoja de cálculo como Excel.

Lámina 75 Dr. Roberto Gómez Cárdenas

Datos almacenados en el archivo Index.dat

- El registro tipo
  - Pasco establece que la actividad es un URL, que ha sido accedido a través de un browser o un sitio web que redirigió el browser del usuario a otro sitio.
- The URL
  - El sitio web actual que el usuario visitó.
- Modified Time
  - El último momento en tiempo que el sitio web fue modificado.
- Access Time
  - El momento en tiempo que el usuario accedió al sitio web.
- Filename
  - El nombre del archivo local que contiene una copia del URL listado.
- Directory
  - El directorio local donde puede encontrar el archivo local del punto anterior.
- HTTP Headers
  - Los encabezados HTTP que el usurio accedió al URL

Lámina 76 Dr. Roberto Gómez Cárdenas

Ejemplo Pasco

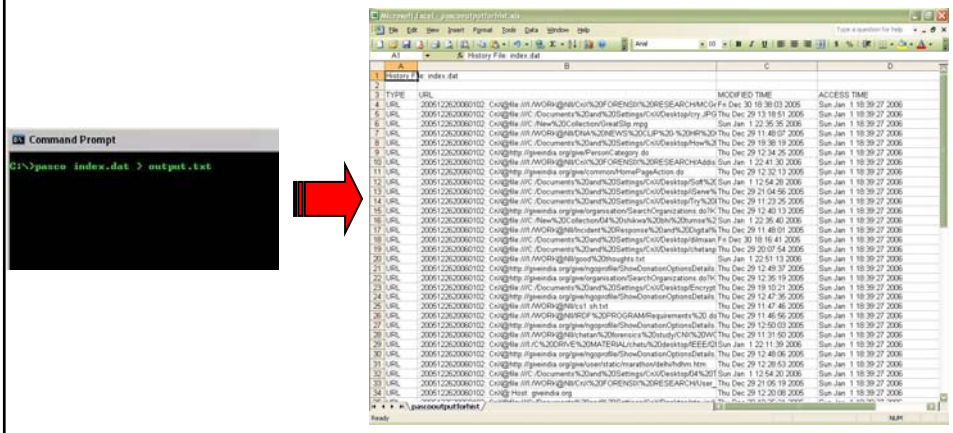


Lámina 77 Dr. Roberto Gómez Cárdenas

Últimos comentarios Pasco

- Para cada renglón en la hoja de cálculo puede retribuir el archivo listado en el “Filename”
- Pasco trabaja bien con archivos de actividades de IE no reconstruye actividad web de otros buscadores (browsers) como Firefox/Mozilla/Netscape
- Pagina descarga
  - http://sourceforge.net/project/showfiles.php?group_id=78332

Lámina 78 Dr. Roberto Gómez Cárdenas

Web Historian

- Herramienta free diseñada por Red Cliff.
- Posee la habilidad de recorrer una estructura del directorio y de identificar los archivos de actividad de internet de los siguientes buscadores (browsers)
  - Internet Explorer
  - Mozilla
  - Firefox
  - Netscape
  - Safari (Apple OS X)
  - Opera

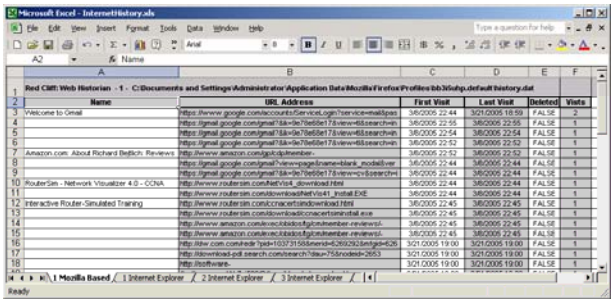
Lámina 79 Dr. Roberto Gómez Cárdenas

Salida

- Investigador no necesita memorizar las rutas para archivos de actividad en Internet para cada buscador
- Tiene la habilidad de reconstruir datos en los siguientes formatos
  - Native Excel Spreadsheet
  - HTML
  - Delimited Text File

Lámina 80 Dr. Roberto Gómez Cárdenas

Algunas imágenes web historian



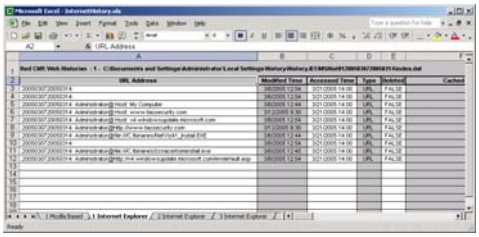


Lámina 81 Dr. Roberto Gómez Cárdenas

IE History

- Una de las primeras herramientas comerciales para reconstrucción de actividades web.
- Aplicación Windows que abre diferentes tipos de archivos de historiales de web browsers incluyendo IE, Firefox, Netscape, Mozilla.
- Herramienta ligera que facilmente puede exportar historial web a hojas de calculo y archivos delimitados por texto.

Lámina 82 Dr. Roberto Gómez Cárdenas

Características extras

- Una vez analizada la información en el archivo Index.dat, ofrece algunas funcionalidades que simplifica su análisis.
- Por ejemplo es posible seleccionar un URL y abrir un web browser y visitar el sitio que el usuario visitó.
  - Sin embargo no se liga la actividad web a los archivos cache
  - se esta viendo una copia viva del sitio web
  - Posible que se este viendo una vista diferente a la que el usuario tenía cuando visito el sitio web

Lámina 83 Dr. Roberto Gómez Cárdenas

IEHistoryView v1.35

- http://www.nirsoft.net/utils/iehv.html

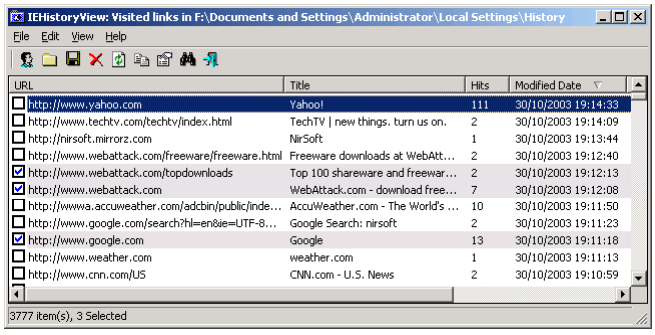


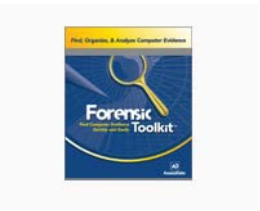
Lámina 84 Dr. Roberto Gómez Cárdenas

FTK Forensic Tool Kit

- Combina la funcionalidad de todas las herramientas presentadas.
- Reconocida como una de las mejores por su facilidad de uso.
- Posible ver las paginas en el caché y verlas en una interfaz estilo web browser.
- Reconstruye las páginas muy bien.
- Desventaja
  - Después seleccionar archivo Index.dat los datos son presentados en un formato difícil de usar.
  - Cada instancia de actividad es presentada de forma separada y no se puede seleccionar ninguna de la información.
  - El importar los datos a una hoja de calculo es casi imposible

Lámina 85 Dr. Roberto Gómez Cárdenas

Snapshot FTK



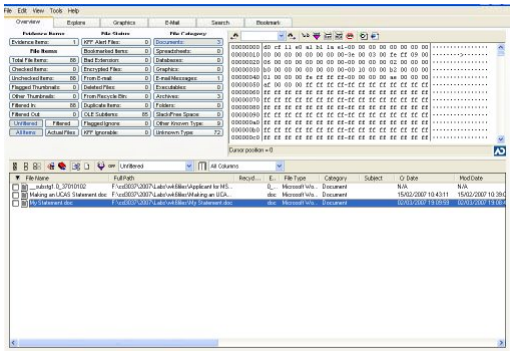
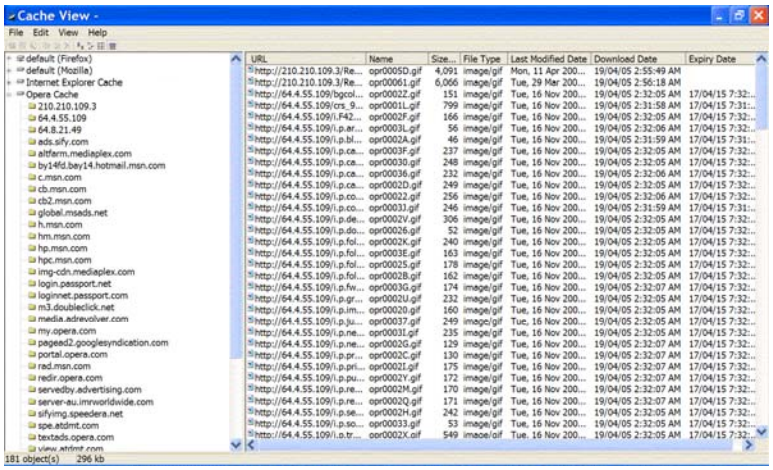


Lámina 86 Dr. Roberto Gómez Cárdenas

Cache view

- Proporciona acceso a los archivo cache de varios tipos de browsers
- Proporciona
  - URL de la página
  - Nombre del cache almacenado en el sistema local
  - Tamaño del archivo
  - Tipo del archivo
  - Ultima fecha de modificación
  - Fecha de “download” y su expiración (si aplica)

Ejemplo Cache View



Caso

- 8:25pm del 18 marzo 2005
  - Senior Associate intenta subir un documento a un servidor de almacenamiento
  - Obtiene mensaje error:

    "You have reached the storage limit.
    Please call your system administrator"

  - Usuario llama al adminstrador (Pepito) y el buzon de voz le indica que esta de vacaciones en el periodo 7 al 21 marzo del 2005
- Investigación interna revela que 500GB de MP3, software pirata y peliculas recien salidas se encuentran en el sistema bajo el profle de Pepito
- Se contrata firma para investigar que paso.

Lámina 89 Dr. Roberto Gómez Cárdenas

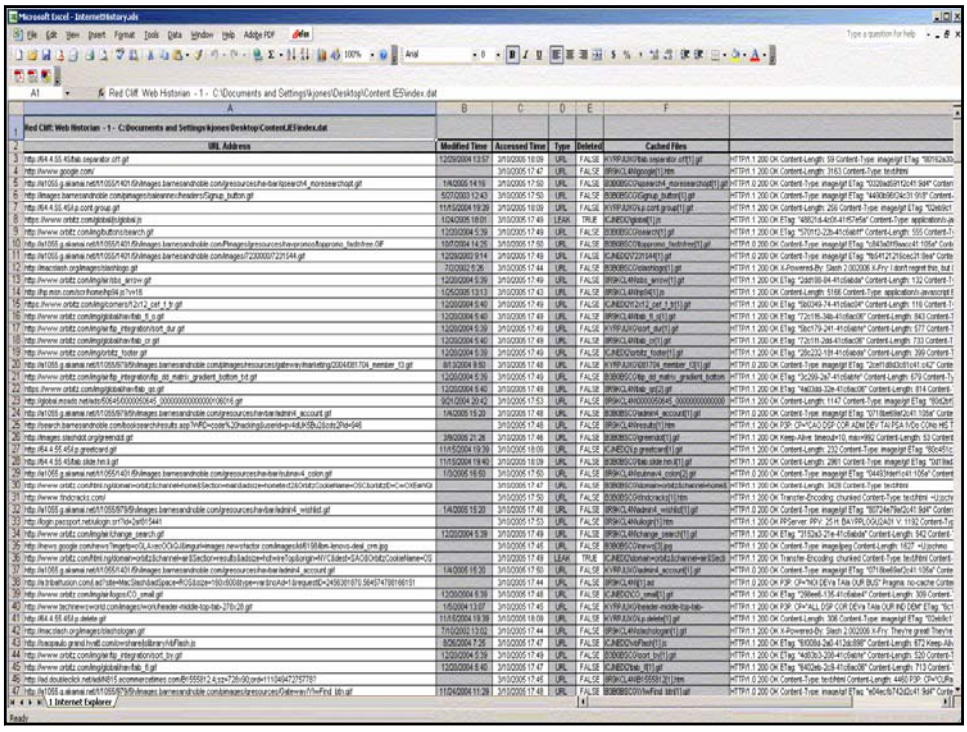
La investigación

- Reconstruir la actividad de web browsing para establecer la relación del ataque con Pepito.
- Uso de herramientas comerciales y de software libre.

Lámina 90 Dr. Roberto Gómez Cárdenas

Usando Pasco

- Con Pasco se puede revisar las sitios web que visitó.
- Solo se presenta la actividad relevante a la investigación.
- La salida se presenta a continuación.

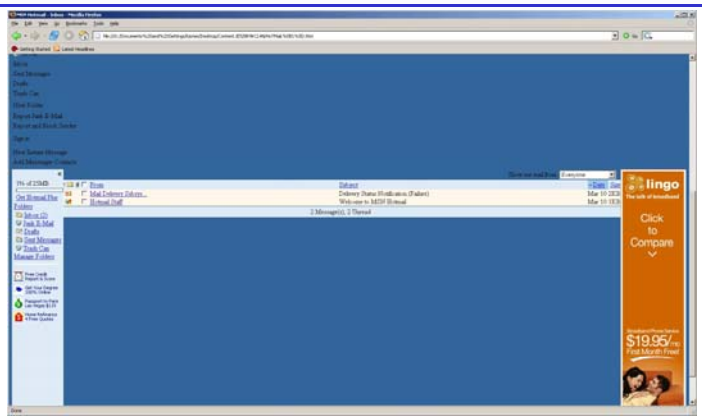


Paginas visitada por Pepito

- Pepito visitó Hotmail.com
- Esta visita creo el archivo 8R9KCL4N\HoTMaiL[1].htm en el directorio caché.
- El abrir dicho archivo da como resultado la página visitada.

Lámina 93 Dr. Roberto Gómez Cárdenas

La pagina visitada



- Se aprecia que la cuenta de Hotmail de Pepito es JoeSchmo1980@hotmail.com
- También se puede ver que no tenía ningún correo interesante en el tiempo en que accedió a la página.

Lámina 94 Dr. Roberto Gómez Cárdenas

Otra página visitada por Pepito

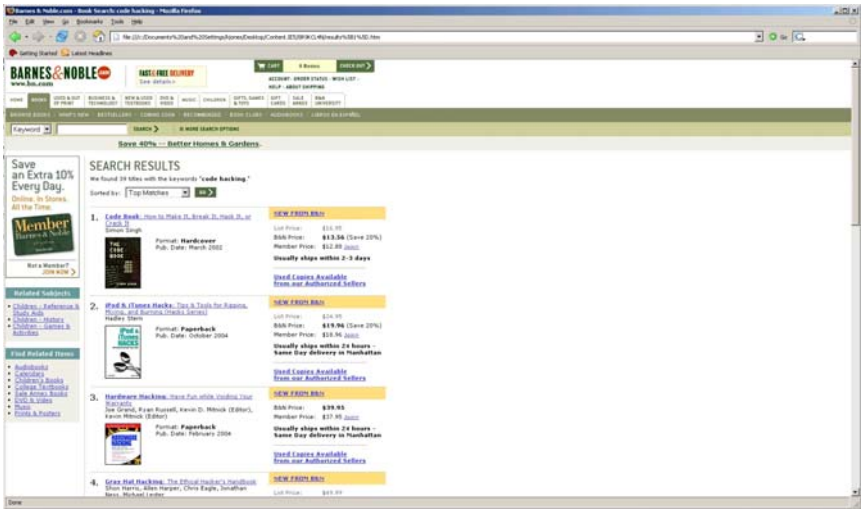


Lámina 95 Dr. Roberto Gómez Cárdenas

Actividad en el web de Pepito

- Visita página Barnes and Noble revela que Pepito estaba interesado en libros relacionados con hacking y cracking
- Otras instancias de búsqueda de Pepito indican que también busco material similar en sitios relacionados con hacking.
- Visitas a otros sitios indican que busco por cracks para Docustodian
  - La aplicación que fue saturada con material no autorizado.

Lámina 96 Dr. Roberto Gómez Cárdenas

Pepito buscando por números de serie

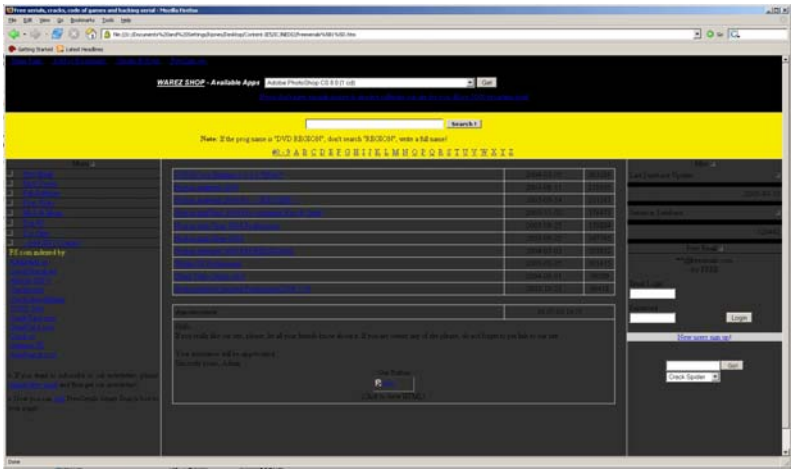


Lámina 97 Dr. Roberto Gómez Cárdenas

Busquedas en Google de Pepito

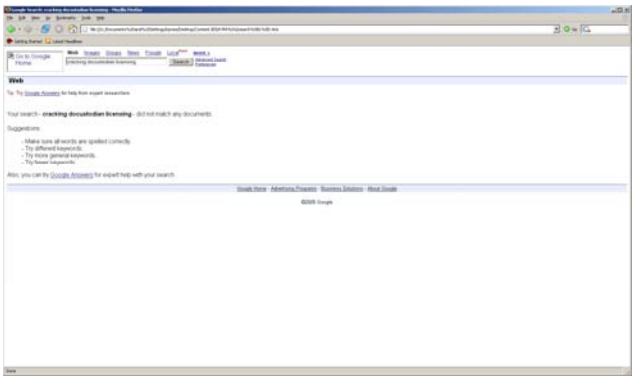


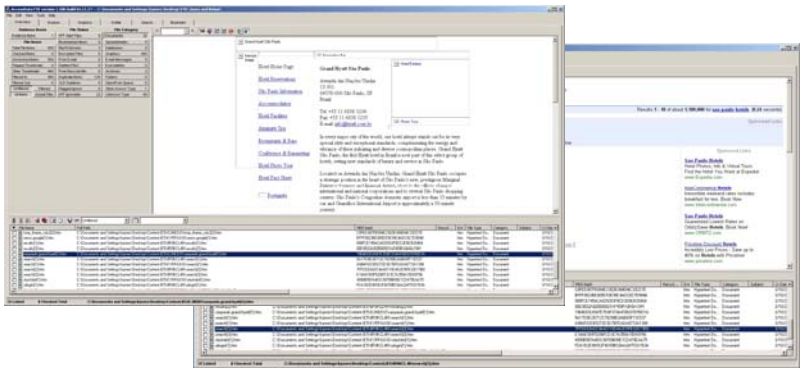
Lámina 98 Dr. Roberto Gómez Cárdenas

Deducciones

- Pepito interesado en información para “crackear” Docustodian.
- Tiempo que los sitios web fueron visitado
  - Aproximadamente 5:50:58 el 10 marzo del 2005
- Pepito estaba de vacaciones a esa fecha y hora.
- Muy poco probable que Pepito hiciera eso desde la playa de Acapulco.

Lámina 99 Dr. Roberto Gómez Cárdenas

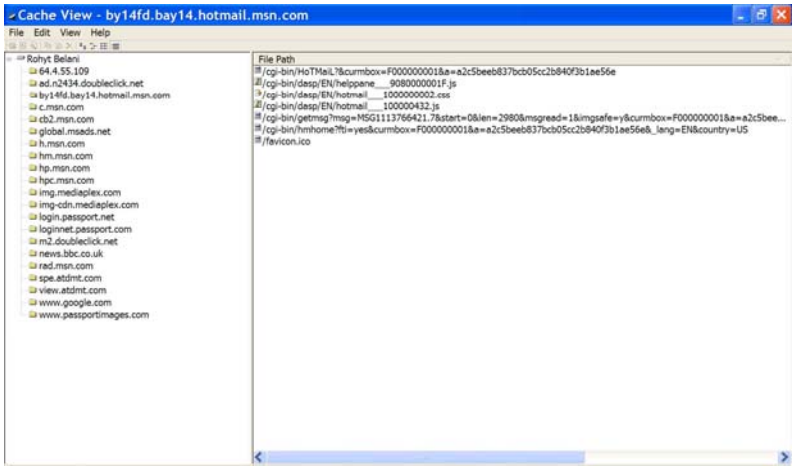
Usando FTK para analizar páginas visitadas por Pepito



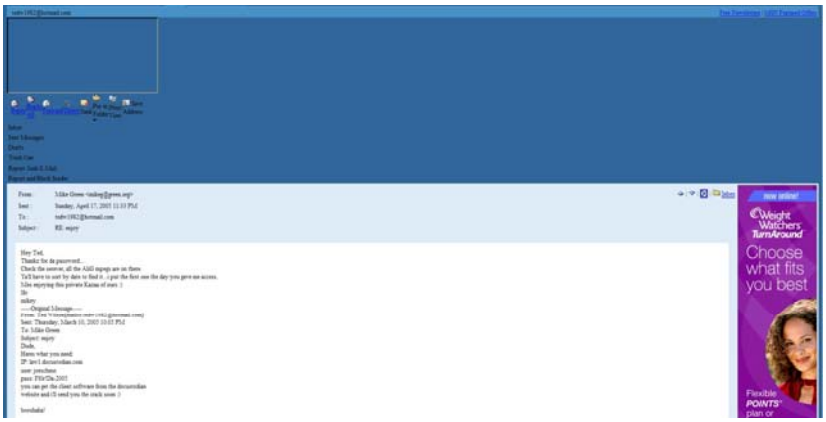
- Páginas de hoteles en Sao Paulo.
- Pepito de vacaciones en Acapulco, por lo que es poco probable que sea responsable de esta actividad.

Lámina 100 Dr. Roberto Gómez Cárdenas

Usando cache view para reconstruir el cache de Firefox de la máquina de Pepito



Reconstruyendo lo visto por Pepito



Observaciones de la última página

- Se puede ver que el correo reside en el inbox de Hotmail del usuario *tedw1982@hotmail.com*.
- Contenido del correo relacionado con el caso.
- Indica que Ted Wilson, el propietario de *tedw1982@hotmail.com* envió un correo a Mike Green con las credenciales de Pepito.
- Tambien le indica que el cliente de Docustodian necesita un crack que enviara pronto.
- Correo enviado el 10 marzo 2005 a las 10:05PM

Lámina 103 Dr. Roberto Gómez Cárdenas

¿Cómo gano Ted acceso al sistema de Pepito?

- Conversaciones con el personal indican que Ted era un empleado interno que cubría a Pepito cuando este se iba de vacaciones.
- También se encontró un archivo llamada licensecrack.jave en el directorio

  C:\windows\system32\temp\temp\temp\

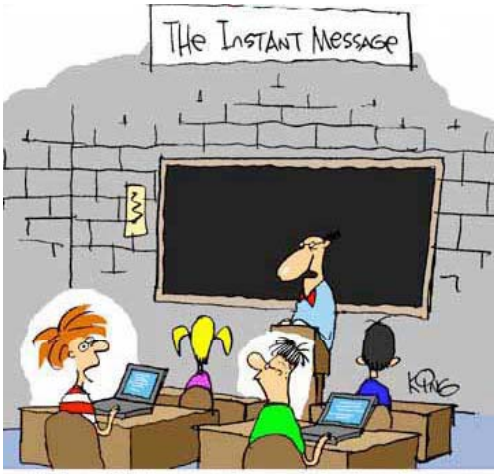
- El archivo tenía como tiempo de último acceso 11 marzo 2005 07:32PM

Lámina 104 Dr. Roberto Gómez Cárdenas

Contenido archivo encontrado

```
/*
 * This program should be run on the same LAN
 * as the Docustodian client machine.
 * Modify the hosts file on the client machine accordingly.
 * It tricks the client in believing that it has a valid license
 * to access the server
 * Author: Ted Wilson
 */


import java.net.*;
import java.io.*;
import java.io.ByteArrayOutputStream;


public class License
{
        static DatagramSocket   sock;           // socket
        static DatagramPacket   opkt;           // communications packet
        static DatagramPacket   ipkt;           // communications packet
        static InetAddress      clientIP;                       // IP address of client
        static String   msg;                    // message sent and received
        static byte[]   inbuf;                  // input message buffer
        static final int port = 4760;           // port number to use
        static byte[] temp;
        static String[] hex ;
        static int port1;

        public static void main (String[] args)
        {
        // create the input packet

                hex = new String[3];
                hex[0] = "e3e075cd5a946d70cbb3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e
3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3e3ea4213";
                hex[1] = "d2d719c58e69159f46fad2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2
d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d2d6022a";
                hex[2] = "c1c0fc1b57c5bffcaa45c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1
c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1c1";
```


Forencia en IM



"How did they get through boring lectures back in the days of paper? I can IM and it looks just like note-taking!"

Lámina 107 Dr. Roberto Gómez Cárdenas

Mensajería instantanea

- En el registro y bajo el directorio Documents & Settings de cada usuario es posible encontrar
  - Últimos logins, screen names, permisos para compartir archivos, listas de amigos, contraseñas, archivos compartidos/bajados, uso del chat room, mensajes archivados, etc…
- Muchas de estas opciones deben ser activadas por el usuario intencionalmente.
- Cualquier fecha y hora recuperadas pueden ayudar para reconstruir la actividad del usuario.

Lámina 108 Dr. Roberto Gómez Cárdenas

Peer to Peer

- Kazaa
  - Programa para compartir
  - La instalación por default para el usuario es compartir archivos (se crea folder Shared Folder)
- Otros programas para compartir
  - Limewire, Bearshare, edonkey2000, etc
- Usuarios pueden compartir archivos/programas sospechosos, sin saberlo, si todos los defaults son aceptados durante la instalación de la aplicación

Lámina 109 Dr. Roberto Gómez Cárdenas

¿Por que nos interesa?

Autor: **anonimo** Fecha: **13/03/2006**
Tema: **induccion al suicidio y necesito recuperar conversaciones del msn como pruebas**

me gustaria que me aclarasen una duda que tengo respecto al caso de mi hija, acusada de induccion al suicidio.
como todo esto llegara a juicio,mi hija debera presentar las pruebas de que el xico le decia x el messenger que estaba harto de vivir x los maltratos de sus padres y la bebida. estas conversaciones son muy importantes y mi hija las elimino y no tiene nada de ellas, xq en el caso de que el xico negase que lo maltratasen las conversaciones serian una prueba. lo e hablado con mi abogado y esta de acuerdo pero mi duda es la siguiente:
en el servidor del messenger guardan las conversaciones durante un año, si el juicio sale dentro de otro año ya no habra dichas conversaciones, xq el servidor las habra eliminado.mi abogado me dice que esto lo tiene que autorizar el juez y que el caso esta en diligencias previas. que quiere decir diligencias previas? si el juez tarda en dar la autorizacion que podra hacer mi hija sino tiene pruebas?quiere decir que aunque no se celebre el juicio hasta dentro de 1 o 2 años podra conseguir las conversaciones antes? como va todo esto?que tendra que hacer mi abogado?es que cuando hablo con el son tantas las preguntas y el miedo a lo que me diga que me quedo en blanco.nunca e tenido una denuncia y ... se que me direis que lo consulte con mi abogado y lo exc, solo quiero que me lo expliqealguien que entiendade internet y leyes. me pasao x este foro xq la señorita ana fernandez que hasta ahora es la que me aconsejaba y me tranquilizaba me a dixo que pregunte aqui.no pretendo recuperar las conversaciones de mi pc sino del servidor, atraves del juez o de mi abogado. si no entendeis os digo donde espuesto el caso entero y ya vais cogiendole el hilo xq es muy complicado, largo y delicado.
un saludo.
gracias

Lámina 110 Dr. Roberto Gómez Cárdenas

Como funciona

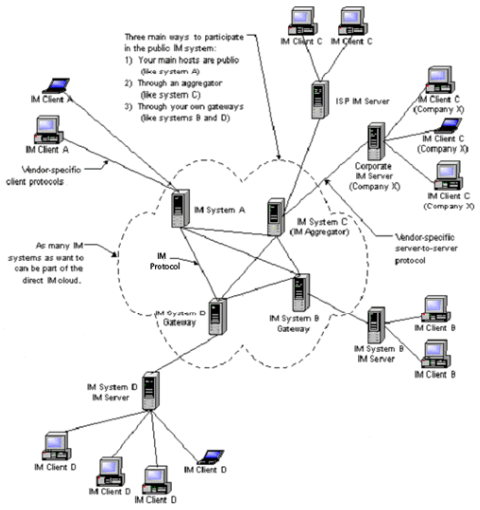


Lámina 111 Dr. Roberto Gómez Cárdenas

Clientes favoritos

- AIM (53 millones)
- Jabber
- Ebuddy
- MSN
- Yahoo
- QQ
- Sametime
- Skype
- Xfire
- Gadu-Gadu
- ICQ
- Paltalk
- Mxit
- PSYC
- Meebo
- IMVU (1 millón)

Lámina 112 Dr. Roberto Gómez Cárdenas

Algunas herramientas

- Paraben's Chat Examiner
- SmartButler
- Belkasoft ICQ History Extractor
- Belkasoft Forensic IM Extractor
- Advanced Instant Messengers Password Recovery

Lámina 113 Dr. Roberto Gómez Cárdenas

Screenshot

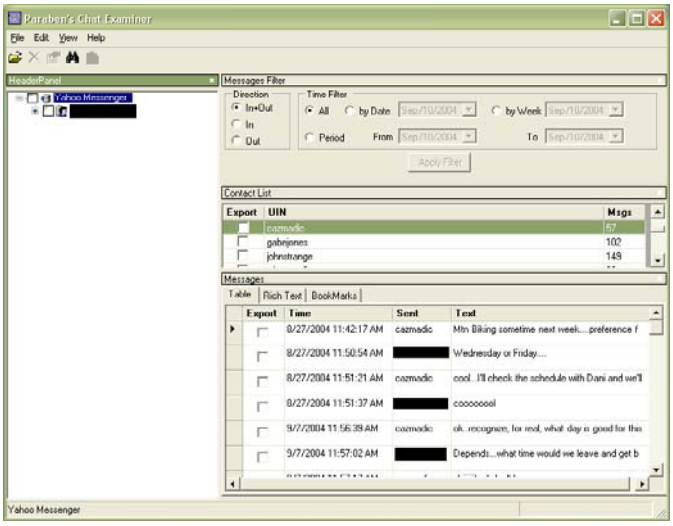


Lámina 114 Dr. Roberto Gómez Cárdenas


Forensia aplicaciones web
Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx
Lámina 115
Dr. Roberto Gómez Cárdenas