ABSTRACTO

El 11 de septiembre 2001 marcó un cambio en la opinión de la seguridad del ordenador. Siguiente a la devastación en NuevaYork, rumores emergieron de actividades terroristas en línea que implican la esteganografia, un método de secretamente ocultar mensajes dentro de imágenes. Esta tesis proporciona una breve descripción de la esteganografia electrónica a traves de imagenes e introduce nuevo material que cubre cómo la vigilancia hoy en dia y las técnicas y las herramientas de la detección se pueden utilizar contra ella en la red. Examina la anatomía de la red y de su subconjunto de multimedia, el World Wide Web, y explora una gama de acercamientos para detectar y para atacar esteganografia. Concluye con el diseño, el desarrollo, la prueba y la evaluación de una estrategia empleando un servidor de búsqueda para la interceptación, la recuperación, el análisis y la identificación de las imágenes electrónicas sospechadas de contener esteganografia.

RECONOCIMIENTOS

La producción de esta tesis ha sido de ninguna manera un asunto trivial. Éste es el producto de una comunidad de partidarios por este, mi esfuerzo.

Mis gracias van a mi esposa Elena e hijo Carlos por su paciencia y tolerancia de mi excedente académico este último año. Han adquirido la carga tanto como yo.

Mi supervisor, el Doctor Philip Nobles, acredito por su profundidad de conocimiento y por su experiencia en la comunicación escrita, permitiendo que mis ideas sean entregadas con eficacia en papel. Le agradezco su entusiasmo, estímulo, alabanza buena y aun mejor crítica.

Las gracias van también al cuerpo docente en RMCS para el talento y la experiencia enorme que exhibieron en entregar el material principal durante el curso enseñado y el personal técnico en el centro de informatica por permitir el acceso especial a la red para comprobar mis ideas.

CAPITULO 1 INTRODUCCION

Ocultado en los cuadros clasificados "XXX" en varios sitios pornographicos de la red y los comentarios fijados sobre salaa de charla sobre el deporte pueden existir los planos cifrados del proximo ataque terrorista contra los Estados Unidos o sus aliados. Suena exagerado, pero los funcionarios y los expertos de los EE.UU. dicen que es el método más último de comunicación utilizado por los seguidores de Osama Bin Laden en intento de adelantar a la ley. El Bin Laden, culpado por el bombardeo en 1998 de dos embajadas de los E.E.U.U. en África del este, y otros están ocultando mapas y las fotografías de las planos del terrorista y las instrucciones de la fijación para las actividades del terrorista en salas de charla sobre el deporte, los tablones de anuncios pornographicos y otros sitios de la red, los E.E.U.U. y agencias extranjeras dicen.

Artículos como éstos marcaron el principio de una ráfaga de la especulación y trajeron la atención del mundo al uso de la esteganografia. El mayor alambique era el impacto a venir de la devastación el 11 de septiembre de 2001 del centro de comercio mundial, el World Trade Center.

La red ha emergido como nueva forma de la caida muerta, un término de la manera en que los espías de la Guerra Fria se transmitían la información. Los mensajes son programas libres revueltos por claves que usan sobre la red que puede ocultar mapas y las fotografías en una imagen existente en sitios seleccionados de la red.

La comunicación electrónica ocultada es algo la inteligencia, la policia y las comunidades militares están encontrando difícil de supervisar o aún de detectar. Ocultan a los detalles operacionales y las planes futuros de terroristas en muchos casos en plena vista sobre el red. Solamente los miembros de las organizaciones del terrorista, sabiendo las señales ocultadas, pueden extraer la informacion.

Según funcionarios de los E.E.U.U., el Bin Laden comenzó usando el cifrado en 1996 pero aumentó recientemente su uso después de que fuera revelado que interceptaron sus llamadas telefónicas a traves de los satélites en Afganistán y siguieron sus actividades.

“Utilizaremos cualquier herramienta que podamos - correos electronicos y la red para facilitar el jihad contra los inquilinos (del israelí) y sus partidarios”, Ahmed Yassin, el fundador del grupo musulmán militante Hamas dijo en una entrevista en la tira de Gaza. “Tenemos nuestros mejores mentes dedicados a esto.”

CAPITULO 2 ESTEGANOGRAFIA

Este capítulo introduce al lector la definición y a la historia de la esteganografia, discutiendo su importancia a la tecnología de hoydia y a su renombre como herramienta de seguridad y de aislamiento.

2.1 La definición de la Esteganografia

La esteganografia, que significa literalmente "escritura cubierta", es el arte de la comunicación secreta. 'Steganos es griego por "cubierto" y "graphein" es griego por "escribir". Su propósito es ocultar la misma presencia de la comunicación en comparación con la criptografía cuyo intento es hacer que la comunicación sea no comprendida a quien no posea los claves correctos.

La esteganografia de la imagen se define como ocultar un mensaje secreto dentro de una imagen de una manera tal que otros no puedan discernir la presencia o el contenido del mensaje ocultado. Por ejemplo, un mensaje se puede ocultar dentro de una imagen cambiando los menos valores binarios significativos (LSB) para producir el mensaje.

Encajando un mensaje secreto en una imagen portadora, se obtiene una estego-imagen. Es importante que la estego-imagen no contenga ningun artefacto fácilmente perceptible debido al encaje del mensaje que se podría detectar por vigilancia electrónica. Uno podría utilizar esos artefactos para detectar las imágenes que contienen mensajes secretos. Una vez que se alcance esto, la herramienta esteganographica llega a ser inútil.

2.2 La historia de la Esteganografia

La esteganografia apareció antes de la criptografía. En 474 A.CC., el historiador griego Herodotus detalló cómo los paisanos intercambiaron lo que parecían tabletas en blanco de la cera. Por debajo de la cera, las bases de madera fueron rasguñadas con los mensajes secretos. Mientras que estuvo exiliado en Persia, Demeratus descubrió que Grecia estaba a punto de ser invadida y deseó transportar un mensaje de advertencia. Sin embargo, el su riesgo de descubrimiento era grande, así que él encubrió su mensaje escribiendo directamente en la madera y después cubriéndola con la cera. Las tabletas aparentemente en blanco entonces fueron transportadas a Sparta donde el mensaje fue destapado literalmente y sus aliados avisados con anticipacion.

Otro ejemplo es el del antiguo griego Histiaeus, que deseaba informar a sus aliados cuándo rebelar contra el enemigo. Para conseguir esto, él afeitó la cabeza de un criado en quien confiaba y después tatuaba un mensaje en su cabeza descabelluda. Después de espera una temporada para el pelo del esclavo creciera de nuevo, le enviaron a través del territorio enemigo a los aliados. Al observador, el esclavo aparecía ser un viajero inofensivo que pasaba por el área. Sin embargo, a su llegada, el

esclavo divulgó al líder de los aliados e indicó que su cabeza se debe afeitar, de tal modo revelando el mensaje.

Los tiempos recientes han rendido técnicas más avanzadas, tales como el uso de la tinta invisible, donde se escriben los mensajes usando las sustancias que luego desaparecen. El mensaje ocultado se revela más adelante usando calor o ciertas reacciones químicas. Otros métodos pueden emplear correspondencia rutinaria, tal como el uso de pinchazos en la vecindad de letras particulares al encanto fuera de un mensaje secreto. Los avances en fotografía produjeron el microfilm que fue utilizado para transmitir mensajes vía paloma portadora. Otros progresos en esta área mejoraron la película y las lentes que proporcionaron la capacidad de reducir el tamaño de mensajes secretos a un punto impreso. Los alemanes en la segunda guerra mundial utilizaron esta técnica, conocida como el microdot.

Con las comunicaciones de hoydia moviéndose cada vez más a los medios electrónicos, las señales digitales de la multimedia (típicamente audio, video, o aún las imágenes) se están utilizando como vehículos para la comunicación esteganographica.

2.3 La Esteganografia: Una Presencia Sólida en la Industria

La esteganografia electrónica es lejos de ser un capricho temporaneo. La esteganografia ha hecho la transición fácil de un arte antiguo a una de las herramientas más nuevas de seguridad en la red. Se ha establecido firmemente junto a criptografía como una medida agregada de seguridad y de aislamiento en muchos de los productos comerciales grandes de la seguridad.

El servidor de busqueda Google divulga 38.900 páginas de la red asociadas con el término "Esteganografia" mientras que el apéndice A enumera sobre 80 programas de esteganografia para nueve diversos sistemas operativos. La esteganografia es el foco de muchos de los grupos de investigación mas prestigiosos, incluyendo la investigación de Microsoft, el MIT y la universidad de Cambridge. El apéndice B enumera algunos de éstos.

Entre los academicos y los investigadores está la profesora Jessica Fridrich, profesora de la investigación en el departamento de la ingeniería eléctrica y de informatica en la universidad de Binghamton en Nueva York. La profesora Fridrich se especializa en la información oculta en imágenes digitales. Específicamente, esto implica el marcamiento para la autentificación y la detección del pisón robusto, esteganografia y el esteganalysis, análisis forense de imágenes digitales, proceso de imagen avanzado y las técnicas del cifrado, trabajando con un equipo de estudiantes graduados que se centran sobre todo en la investigación militar financiada por la fuerza aérea y otras agencias estatales.

Otro académico notable es profesor Hyoung Joong Kim del departamento de la ingeniería de control y de instrumentación de la universidad nacional de Kangwon, Corea. El profesor Kim está desarrollando software de multimedia para el contenido digital y la protección que emplea filigranas, el cifrado y los algoritmos del desciframiento, certificados, intercambio de claves y tecnologías de la gerencia, codificacion y algoritmos de descifro. stegano-l@excalibur.iks-jena.de es una lista del correo electronico de los profesionales de la esteganografia (el autor de la tesis es un miembro), donde los avances más últimos se discuten a menudo.

Este capítulo describe los varios métodos del esteganalisis y explica detalladamente el ataque estadístico como candidato conveniente a la automatización, incluyendo una descripción del cubo de color del RGB y de la codificación del los valores menos significativos (LSB).

3.1 Los Tipos De Ataques Contra La Esteganografia

El esteganalisis es la comparación entre el portador (cubierta), la estego-imagen y el mensaje ocultado. Los varios métodos de analizar estego-imagenes se llaman ataques e incluyen:

a. *estego-solo*, donde el atacante tiene acceso solamente a la estego-imagen,

b. *cubierta sabida*, donde el atacante tiene acceso solamente al portador,

c. *mensaje sabido*, donde el atacante tiene acceso solamente al mensaje,

d. *estego elegido*, donde el atacante tiene acceso a la estego-imagen y al estegoalgoritmo, y

e. *mensaje elegido*, donde el atacante genera una estego-imagen de un mensaje usando un algoritmo, buscando las firmas que le permitirán detectar otras estegoimagenes.

La tabla 1 ilustra esto más claramente.

El atacante emplea:	Cuando el atacante tiene acceso a:			
Ataque	Estego-imagen	Cubierta	Mensaje	Algoritmo
Estego-solo	✔			
Cubierta sabida		✔		
Mensaje sabido			✔	
Estego elegido	✔			✔
Mensaje elegido			✔	✔

Tabla 1. Estego-ataques

3.2 El ataque de Estego-Solo

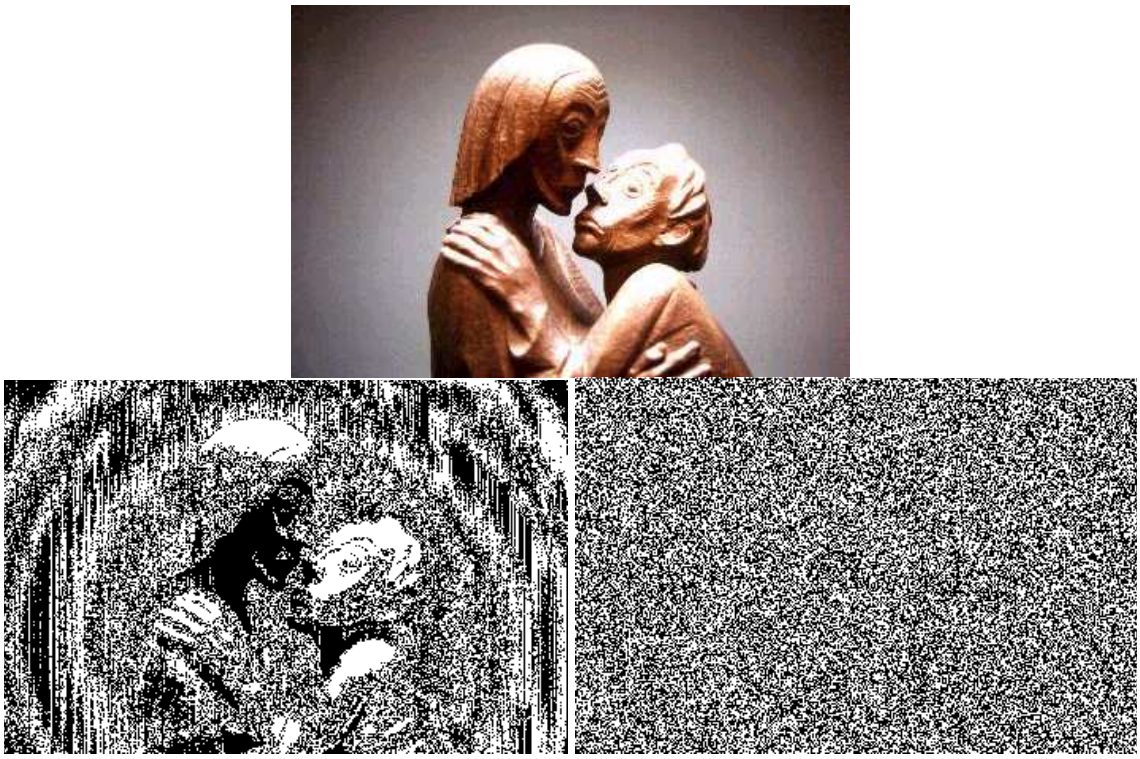
El ataque estego-solo es el ataque más importante contra sistemas esteganographicos porque ocurrirá con más frecuencia en la practica.

Los dos métodos principales desarrollados para determinar si cierto archivo de estego contiene datos ocultados son los ataques visuales, que confían en las capacidades del sistema visual humano, y los ataques estadísticos, que realizan pruebas estadísticas en el archivo del estego.

3.2.1 El ataque visual de Estego-Solo

El ataque visual de estego-solo es un ataque que explota la asunción de la mayoría de los autores de los programas de esteganografia que los LSBs de un archivo de la cubierta es al azar. Esto es hecha confiando en un ser humano a juzgar si una imagen presentada por un algoritmo de filtración contiene datos ocultados. El algoritmo de filtración quita las partes de la imagen que están cubriendo el mensaje. La salida del algoritmo de filtración es una imagen que consiste solamente en los valores binarios que potencialmente se habrían podido utilizar para encajar datos. La filtración de la imagen potencial del estego es dependiente en la función que originalmente encaja el mensaje oculto.

Esto demuestra similaridades al las tecnicas del espectro distribuido empleadas en la comuncación por radio, especialmente el encajar de la información en los LSBs, cuales valores esencialmente se pierden en el ruido de la imagen.



Cuadro 1. Das Weidersehen (arriba), LSB sin mensaje (izquierda), LSB con 1 octeto de mensaje (derecha)

El cuadro 1 ilustra cómo una tal herramienta, Steganos 1,5 de DEMCOM, aparece reescribir totalmente el plano de LSB para encajar incluso el pedazo más minúsculo de information. Sin embargo, este método particular de detectar la diferencia sigue siendo un ataque visual y por lo tanto requiere la interacción humana, hecha más difícil cuando las diferencias no están absolutamente como fáciles considerar.

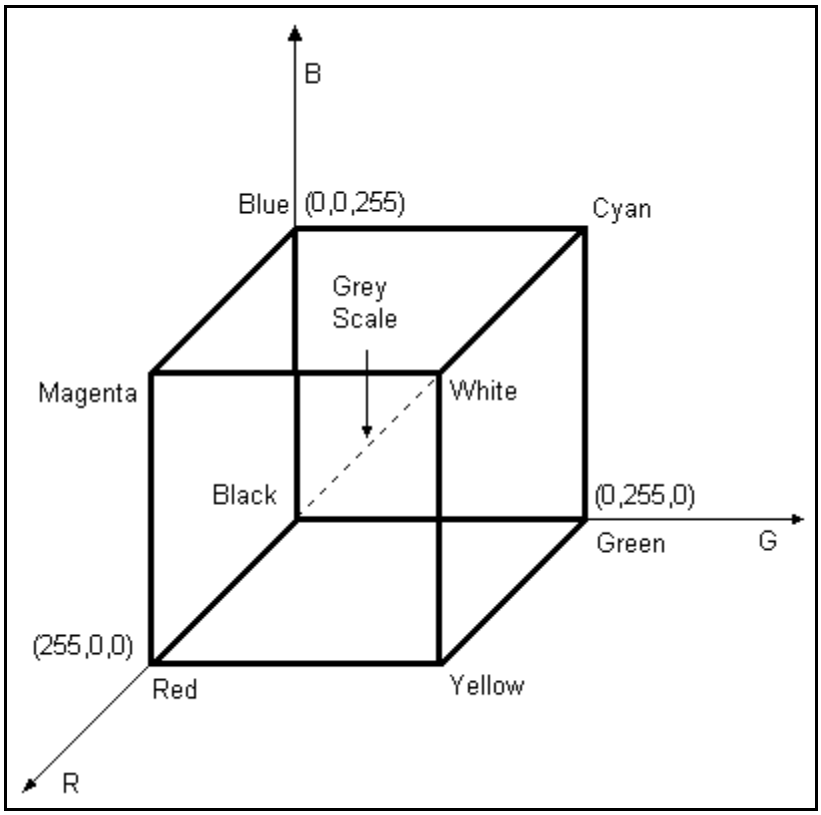
Considere que, en un ataque estego-solo, no tenemos acceso a la imagen limpia original del portador y que otros codificadores producen resultados muy diversos. A menos que poder emplear

algoritmos para examinar las características estadísticas del resultado, como ésas en el uso para el reconocimiento automático de la imagen, nuestro motor de búsqueda de esteganografia no es todavía una realidad.

3.2.2 El ataque estadístico de Estego-Solo

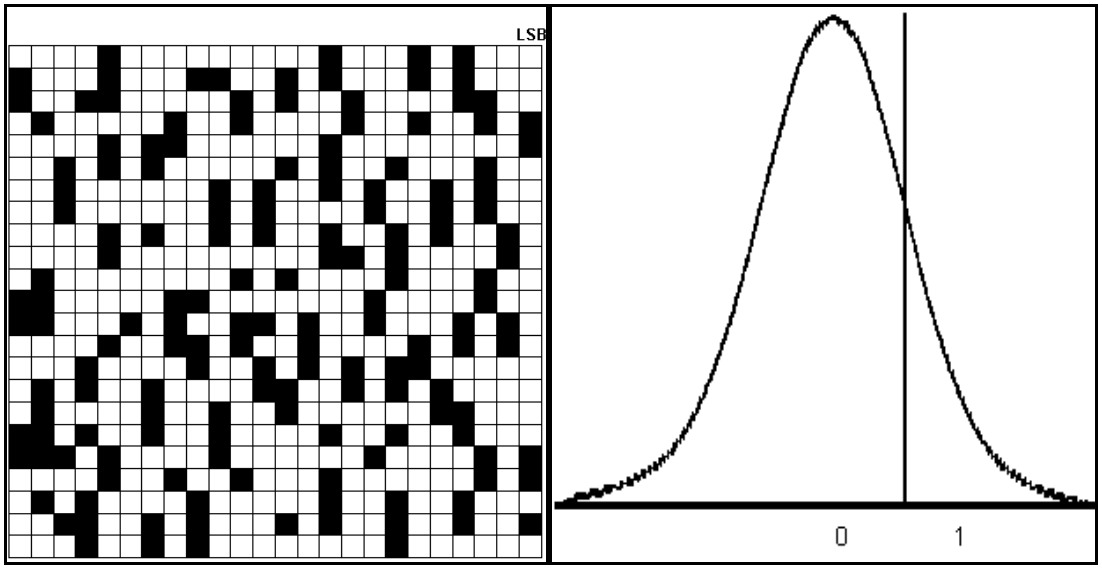
En contraste a los ataques de la representación visual, los ataques estadísticos explotan el hecho de que la mayoría de los programas de esteganografia tratan los LSBs del archivo de la cubierta y por lo tanto asumen que pueden sobreescribir estos valores con otros datos (el mensaje secreto cifrado). Sin embargo, como el ataque visual del cuadro 1 ha demostrado, los LSBs de una imagen no es random.

Cuando un programa esteganografico encaja un valor con sobreescribir el LSB de un pixel en el archivo de la cubierta, el valor del color de este pixel se cambia a un valor adyacente del color en la gama de colores (o en el cubo del RGB si el archivo de la cubierta es una imagen de verdadero-color). El volumen dentro del cubo del RGB, demostrado en el cuadro 2, representa todos los colores posibles identificados como combinación de rojo, verde y azul, cada uno con una intensidad a partir de 0 hasta 255.



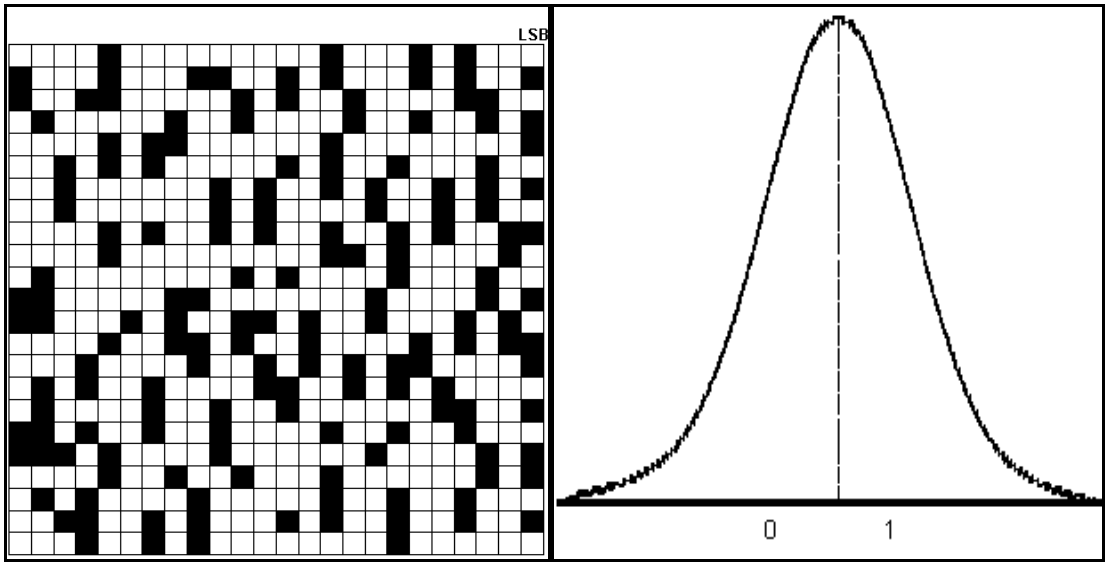
Cuadro 2. El cubo RGB

Considere dos valores adyacentes del color (par de valores, o PoV) donde los medios adyacentes son idénticos a excepción del LSB. Figura 3 y figura 4 son distribuciones de la demostración para las configuraciones de valores binarios dentro del plano de LSB de una imagen, de 0s demostrado en blanco y de 1s demostrado en negro.



Cuadro 3. La organizacion de LSB en una imagen normal de 24 valores de color – distribucion desigual

Al sobreescribir el LSBs de todas las ocurrencias de uno de estos valores del color con un valor del mensaje secreto, las frecuencias de estos valores de dos colores esencialmente serán iguales. Esto sucede porque los datos que son encajados se cifran y por lo tanto se distribuyen igualmente.



Cuadro 4. LSB representando datos encajados – distribucion igual

La esencia del ataque estadístico es medir cómo de cerca a idénticas las distribuciones de frecuencia del color del archivo potencial del estego están. Esto da lugar a una medida para la probabilidad de que el archivo analizado contenga un mensaje ocultado.

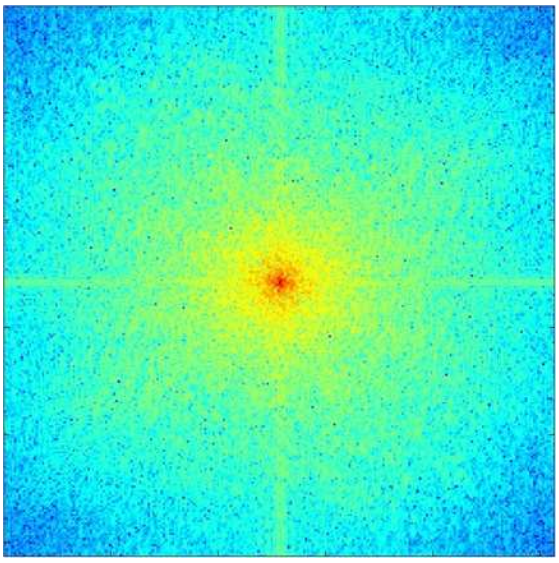
Se pone en ejecucion este ataque estadístico usando una prueba del chi-cuadrado. En pasos sucesivos, las áreas de aumento del archivo potencial de estego se analizan, comenzando con los primeros por ciento de se han analizado los datos, entonces los primeros dos por ciento de datos, etcétera hasta 100 por ciento de los datos.

La codificación de LSB es solamente uno de los métodos populares de ocultar la información. Otro es codificación del dominio de la frecuencia, demostrada en el cuadro 5, que inserta mensajes en

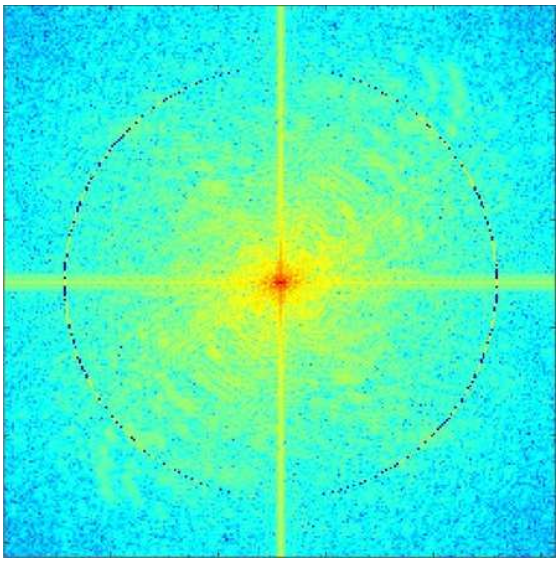
imágenes trabajando con el transforme Fourier rápido de 2 dimensiones (2-d FFT) de la imagen del portador. El 2-d FFT separa las frecuencias de la imagen en anillos centrados en un eje. Esos anillos más cercanos al eje representan las frecuencias bajas de la imagen, y ésos lejos representan las mas altas frecuencias. En el método de codificación del dominio de la frecuencia, el mensaje secreto se codifica en las frecuencias medias de la imagen. Esto se consigue convirtiendo el texto del mensaje a valores binarios y sobreponiendo estos valores en un anillo en la banda de frecuencia deseada en el 2-d FFT. Aunque el anillo de valores aparece oscuro y sobresaliente en el 2-d FFT, el efecto sobre la imagen sí mismo es muy leve. También, una imagen codificada con este método puede mejorar ruido, la compresión, la traducción, y la rotación, muco mas que las imágenes codificadas por el metodo LSB.

"Britney" antes del encajamiento de 2-D FFT

"Britney" despues del encajamiento de 2-D FFT



2-D FFT de "Britney"



2-D FFT encajado de datos

Cuadro 5. "Britney" antes y despues del encaje 2-D FFT

3.3 Otros Ataques

El análisis estadístico es el más prometedor de los análisis para el contenido esteganografico debido a su imparcialidad hacia cualquier sistema particular de la codificación. Sin embargo, muchos estegocodificadores no pueden ocultar su propia huella, su firma, con eficacia y puede ser encontrada bastante fácilmente si se sabe la firma. Entre éstos, algunos estegocodificadores para la protección de los derechos de autor están más interesados en la fabricación de la filigrana perceptible al algoritmo correcto de la detección que ocultándolo totalmente. Éstos dejan huellas características, como las firmas del virus, para dejarse encontrar por sus propios detectores. Tales empresas juzgan que es generalmente suficiente ocultar la filigrana del ladrón ocasional del derech de autor y dejarla visible al detector de los amos del los derechos por una firma tan distintiva.

CAPÍTULO 4 LA ANATOMÍA DEL INTERNET

Este capítulo proporciona una descripción del Internet, la red, como medio de comunicaciones, discutiendo el protocolo de transferencia de hypertext (HTTP), el trazo de la ruta, succionadores de paquete y los modelos de siete niveles del OSI y de TCP/IP.

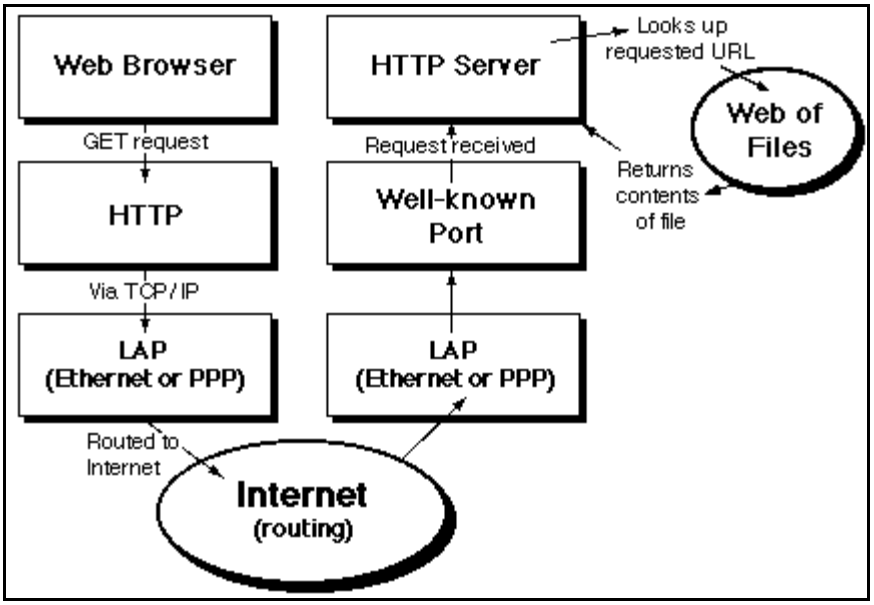
Para emprender la tarea ambiciosa de detectar esteganografia de la imagen basada en la red en una escala magnífica, una examinación de la estructura y el comportamiento de la red es vital. El Internet es un medio de comunicaciones que ha atravesado el globo desde sus principios tempranos como proyecto de investigación de la guerra fría para el departamento de defensa de los E.E.U.U. La estructura distribuida de la red, con su redundancia incorporada, es una defensa contra el muy temido ataque nuclear de la guerra fría en que le red cooperativa, como una tela de aranya, continuaría llevando comunicaciones incluso después de daño considerable y catastrófico a los nodos discretos dentro de ella.

Hoy, este régimen sin herarquia del establecimiento de una red ha facilitado la aparición del World Wide Web, de un hypertext y del subconjunto de los multimedia del Internet.

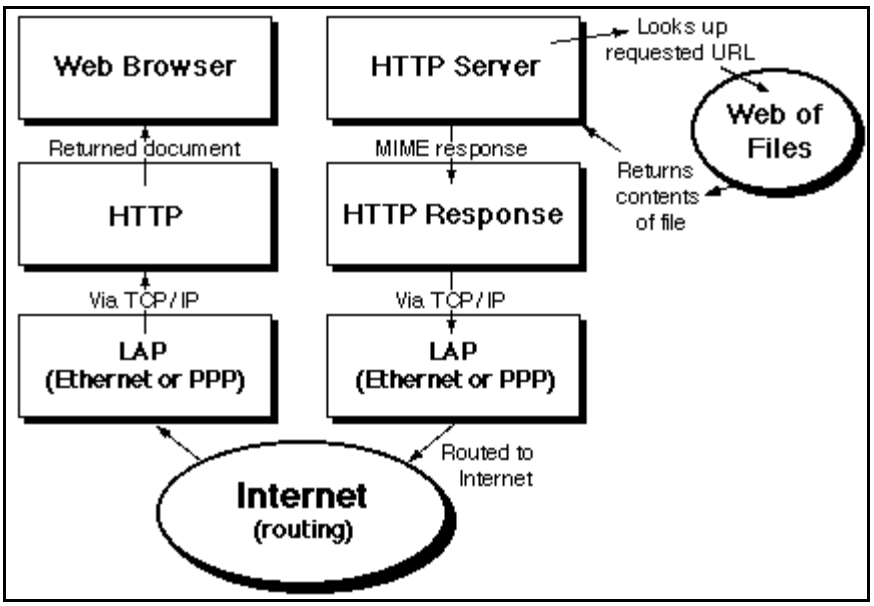
Una idea falsa popular de los no aficionados del World Wide Web es que los sitios de la red son estáticos y que los visitantes tropiezan contra la puerta de cada sitio que visitan, practicando el "surfing" sobre el mundo. Un concepto más exacto es el que podemos extrapolar del servidor , por el que el contenido de un sitio esté servido (entregado) a petición a cada usuario. Es más un caso del mundo viniendo al usuario como serie de transferencias directas.

4.1 El HTTP y el HTML

La mayoría extensa de imágenes están alcanzados vía un web browser, el más común siendo el Internet Explorer de Microsoft (IE). Los browsers son clientes del protocolo de transferencia de hypertext (HTTP) en comparación con los servidores del HTTP, que entregan el contenido de la red. Este protocolo se desarrolló de eso usado por los editores de periodicos mucho antes de que el World Wide Web existiera. Su desarrollo continuado ha permitido a la red entregar el texto, imágenes, el vídeo dinámico y el sonido, conocido popularmente como multimedia. Abrir una pagina Web usando un browser acciona una serie de peticiones de HTTP al servidor. El cuadro 6 demuestra cómo un pedido del browser por una pagina se maneja. El cuadro 7 es la misma visión para una respuesta.

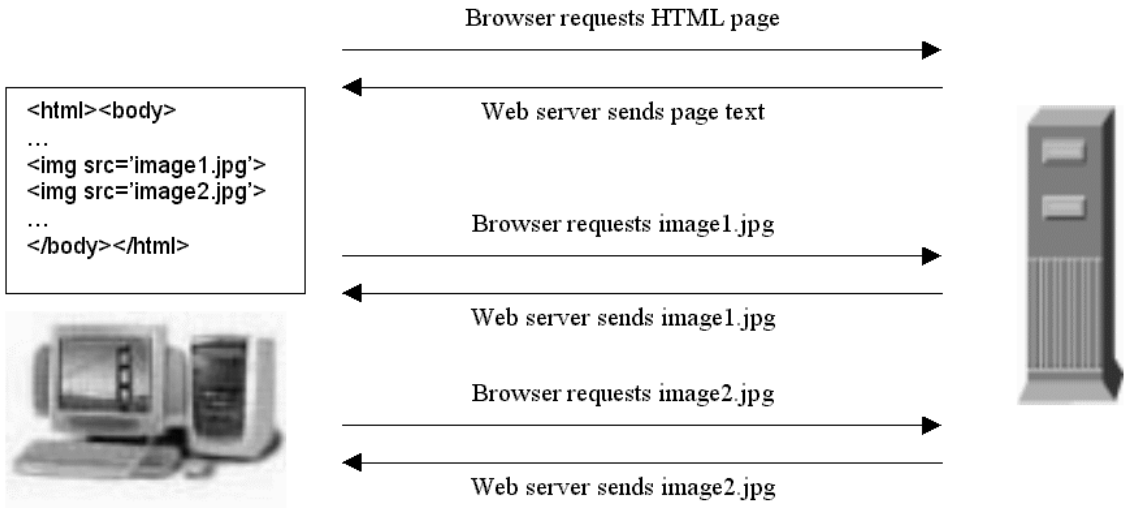


Cuadro 6. La peticion HTTP



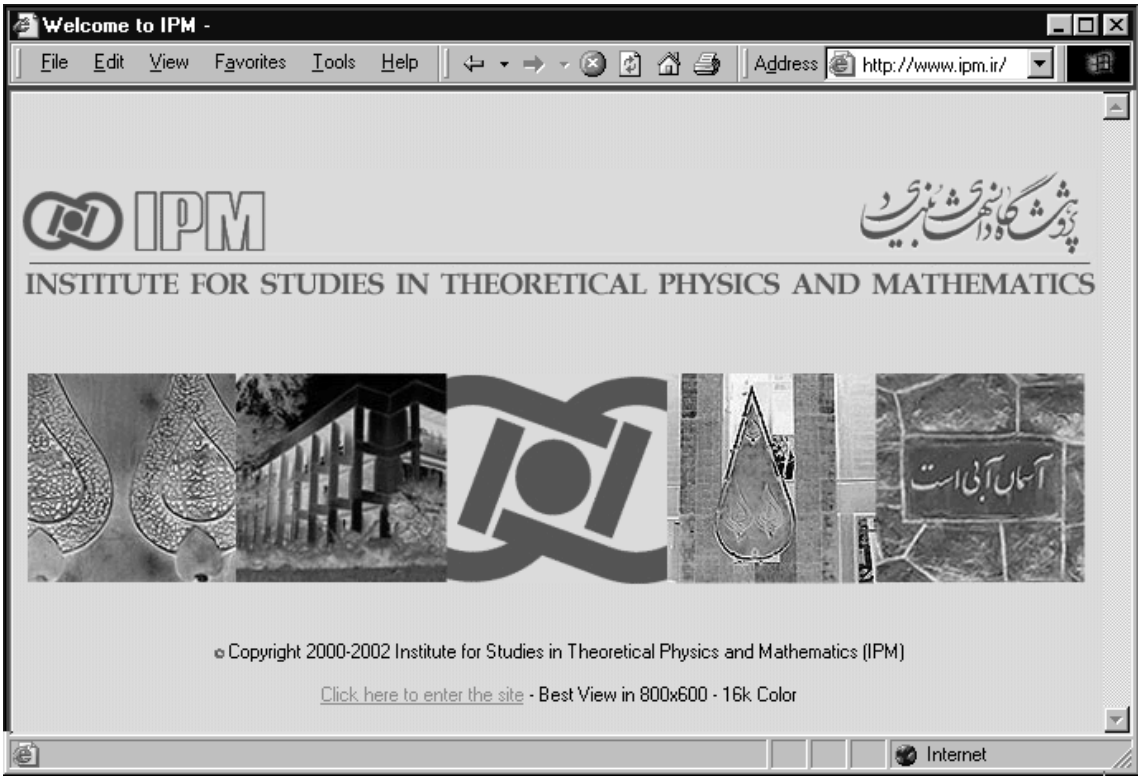
Cuadro 7. La respuesta HTTP

CONSIGUE es quizás la más usada de varios métodos por una petición, algunas otras siendo PRINCIPALES, el POSTE, PUESTO, la CANCELACIÓN y BUSQUEDADETEXTO . El cuadro 6 y el cuadro 7 son solos casos de una petición y de una respuesta. El cuadro 8 demuestra la secuencia de las peticiones requeridas para construir una pagina gráfica en el PC del usuario (cliente).



Cuadro 8. La petición de página con imagenes

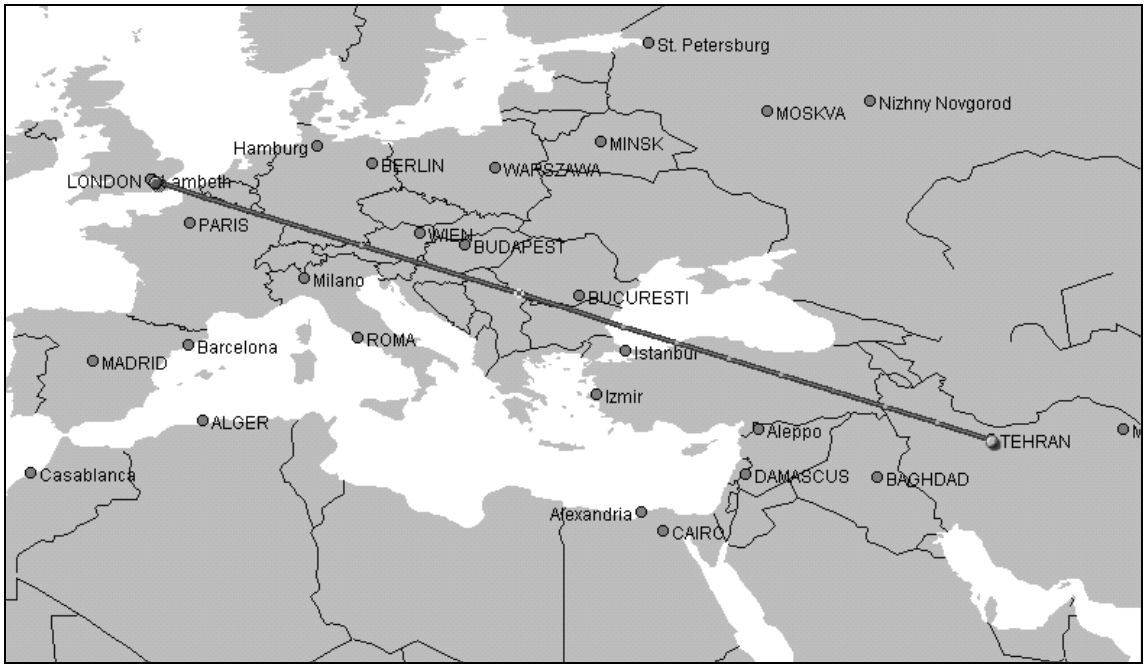
El Cuadro 9 es la vista de IE de la pagina para el instituto de estudios en la física y las matemáticas teóricas (www.ipm.ir), que administra autoridad nacional de *www.nic.ir*, del dominio de Iran y la entrada al resto del mundo.



Cuadro 9. La IPM autoridad de dominio de Iran

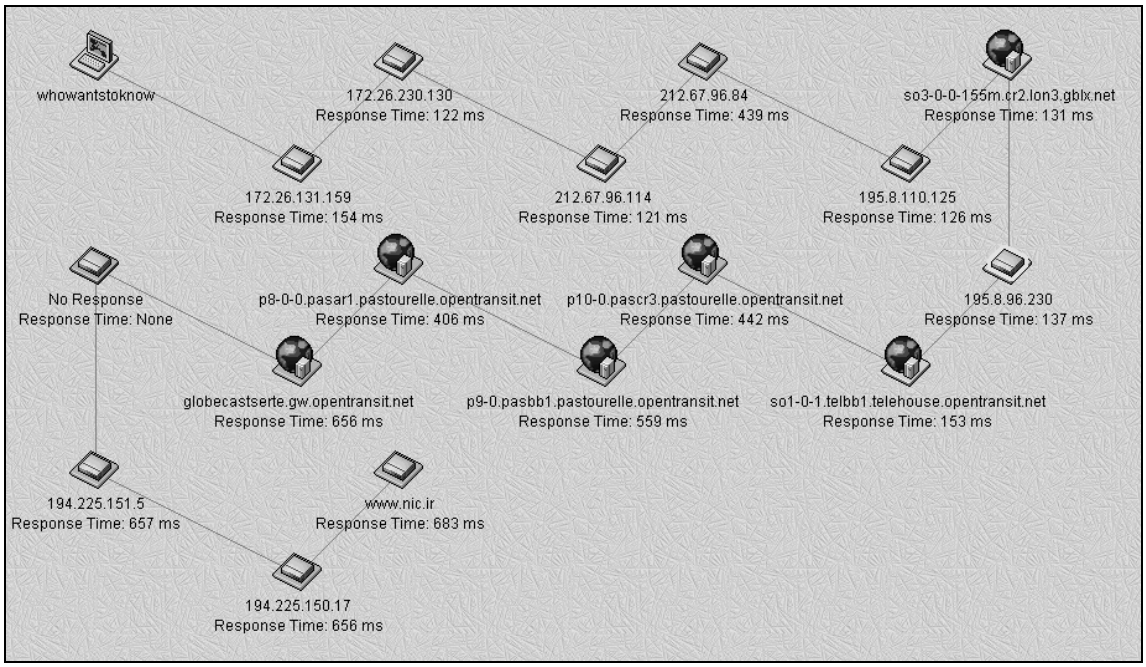
4.2 Calcando El Trafico De La Red

Para traer esta página, Internet Explorer envía un paquete del tipo http:request con una serie de servidores a través del mundo a Tehran, a la capital de Iran y al hogar del instituto (Afganistán puede haber sido una opción más tópica pero, a la hora de la escritura, todos los dominios de gov.af no se encontraban en línea. El único sitio disponible del "af" era www.pentium.af, que era en realidad un sitio de Intel basado en Los Ángeles!). Este traverso global se demuestra en el cuadro 10 como mapa de rastro.



Cuadro 10. Mapa de Traceroute desde Londres hasta Tehran

Aunque el mapa aparece demostrar una línea directa de Londres a Tehran, cuadro 11 de Traceroute demuestra que hay 15 rebajadoras y servidores implicados entre el PC del autor de la tesis (identificado como "quienquieresaberlo") y el servidor iraní (www.nic.ir)



Cuadro 11. Mapa de nodulos Londres a Tehran

El cuadro 12 enumera estos nodos, proporcionando el URL (localizador de recurso uniforme) vía el servidor de nobres de dominio (DNS) donde disponible. Un nodo, numerado 14, no respondió a la interrogacion del calcador para la identificación, el porque la respuesta "No" se demuestra. Esta lista demuestra que la trayectoria tomada por este rastro utilizó los nodos que pertenecían a la Autoridad de Internet de Numeros Asignados (IANA), a Onetel, Travesía Global Limitada (FGC), ISI (un portador de FGC), espina dorsal abierta del tránsito de Telecom de Francia, y el instituto.

#	IP Address	Name	RT (ms)	Network
1	213.78.109.69	whowantstoknow	0	-----
2	172.26.131.159	-----	125	IANA
3	172.26.230.130	-----	122	IANA
4	212.67.96.114	-----	121	UK-ONETEL-991117
5	212.67.96.84	-----	439	UK-ONETEL-991117
6	195.8.110.125	-----	126	UK-FGC-970319
7	195.8.96.206	so3-0-0-155m.cr2.lon3.gblx.net	131	UK-ISI-195-8-96
8	195.8.96.230	-----	137	UK-ISI-195-8-96
9	193.251.129.81	so1-0-1.telbb1.telehouse.opentransit.net	153	OPENTRANSIT-BACKBONE
10	193.251.241.178	p10-0.pascr3.pastourelle.opentransit.net	442	OPENTRANSIT-BACKBONE
11	193.251.241.161	p9-0.pasbb1.pastourelle.opentransit.net	559	OPENTRANSIT-BACKBONE
12	193.251.128.70	p8-0-0.pasar1.pastourelle.opentransit.net	406	OPENTRANSIT-BACKBONE
13	193.251.248.122	globecastserte.gw.opentransit.net	656	OPENTRANSIT-BACKBONE
14	-----	No Response	--	-----
15	194.225.151.5	-----	657	IRANET
16	194.225.150.17	-----	656	IRANET
17	194.225.70.96	www.nic.ir	683	IRANET

Cuadro 12. Lista de nodulos Londres a Tehran

#	IP Address	Name	RT (ms)	Network
1	213.78.109.69	whowantstoknow	0	-----
2	172.26.131.159	-----	127	IANA
3	172.26.230.138	-----	121	IANA
4	212.67.96.113	-----	125	UK-ONETEL-991117
5	212.67.96.83	-----	124	UK-ONETEL-991117
6	212.67.96.66	fe6-1-bdr2.onetel.net.uk	120	UK-ONETEL-991117
7	195.8.110.125	-----	127	UK-FGC-970319
8	195.8.96.206	so3-0-0-155m.cr2.lon3.gblx.net	125	UK-ISI-195-8-96
9	208.51.224.210	so2-0-0-2488m.cr1.pao2.gblx.net	252	Globalcrossing Internal
10	64.211.147.158	so0-0-0-622m.br4.pao2.gblx.net	259	GC Internal Department
11	208.50.13.230	-----	254	GC Internal
12	202.39.83.9	sj-c7r1.usa-sanjose.router.hinet.net	252	HINET-NET
13	210.65.161.2	tp-s2-c7e4r3.router.hinet.net	484	HINET-NET
14	211.22.33.14	tp-s2-c12r1.router.hinet.net	423	HINET-NET
15	168.95.207.1	tp-b-c6r5.router.hinet.net	594	Chunghwa Telecom Co., Ltd.
16	163.29.22.233	-----	1031	CHTD, Chunghwa Telecom Co.,Ltd.
17	210.69.250.38	-----	668	GSN-NET
18	210.69.250.57	-----	448	GSN-NET
19	163.29.22.137	-----	722	CHTD, Chunghwa Telecom Co.,Ltd.
20	211.79.170.250	-----	612	GSN-NET
21	211.79.170.8	www.gov.tw	577	GSN-NET

Cuadro 13. Lista de nodulos Londres a Taiwan

#	IP Address	Name	RT (ms)	Network
1	213.78.109.69	whowantstoknow	0	-----
2	172.26.131.159	-----	120	IANA
3	172.26.230.138	-----	122	IANA
4	212.67.96.113	-----	124	UK-ONETEL-991117
5	212.67.96.83	-----	128	UK-ONETEL-991117
6	212.67.96.66	fe6-1-bdr2.onetel.net.uk	120	UK-ONETEL-991117
7	195.8.110.125	-----	125	UK-FGC-970319
8	195.8.96.206	so3-0-0-155m.cr2.lon3.gblx.net	123	UK-ISI-195-8-96
9	206.132.249.170	pos1-0-622m.cr2.nyc2.gblx.net	190	Global Crossing
10	208.48.234.214	pos1-0-2488m.br2.nyc2.gblx.net	191	GC Internal Department
11	204.255.168.133	97.atm3-0.br2.nyc9.alter.net	194	UUNET Technologies, Inc.
12	152.63.22.226	0.so-6-1-0.xl1.nyc9.alter.net	190	UUNET-BACKBONE
13	152.63.0.173	0.so-4-0-0.tl1.nyc9.alter.net	212	UUNET-BACKBONE
14	152.63.10.78	0.so-1-1-0.tl1.sac1.alter.net	272	UUNET-BACKBONE
15	152.63.0.113	0.pos6-0.ir1.sac1.alter.net	252	UUNET-BACKBONE
16	137.39.31.189	so-7-0-0.ir1.sac2.alter.net	385	UUNET Technologies, Inc.
17	210.80.48.17	0.so-3-1-0.tr1.hkg2.alter.net	532	UUNET-ASPAC2
18	210.80.50.206	61.pos0-0-0.tg1.hkg2.alter.net	544	UUNET-ASPAC2
19	203.193.63.130	itsd-transit-hk-gw.customer.alter.net	--	UUNET-HK
20	-----	www.gov.hk	--	-----

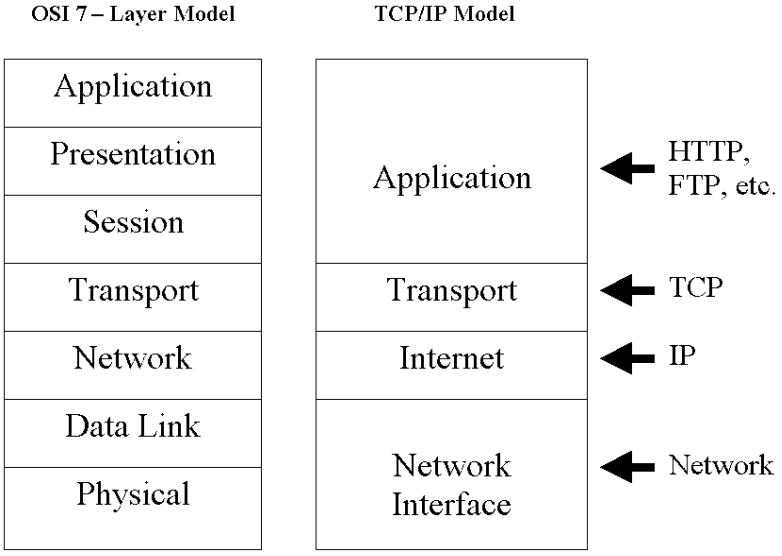
Cuadro 14. Lista de nodulos Londres a Hong Kong

Los cuadros 13 y 14 demuestran listas de los rastros a Taiwán y a Hong Kong respectivamente. Estos rastros todos demuestran una trayectoria común hasta e incluir la rebajadora de Global Crossing, ISI en el domicilio IP 195,8,110,125. Después de este nodo, las trayectorias divergen a sus destinaciones separadas. Esto sugiere que este nodo lleve mucho tráfico BRITÁNICO afuera y ofrezca un punto estratégico por el que el tráfico se pueda supervisar con eficacia. Identificar tal punto en cada de la mayoría de los principales servidores en el Reino Unido daría lugar a una frontera extremadamente eficaz de puntos de interceptación, una realidad no ignorada por las agencias tales como NTAC y Echelon.

Cuando el tráfico de la red incluye una imagen de JPG en una pagina, la evidencia de esta transacción aparecerá en las peticiones en pleno texto del HTTP: CONSIGUE. Un succionador de paquete puede filtrar para esta transacción particular.

4.2 Los Succionadores Y Los Paquetes

Conocidos más respetablemente como analizadores de la red o del paquete, succionadores funcionan a través de varias capas del modelo de siete niveles del OSI. Cada vez más, el renombre explosivo de la red como fuerza de la industria ha alcanzado este modelo con su propio, según lo ilustrado en el cuadro 15. Una implicación de los succionadores a través de muchas capas es necesaria porque, para detectar y analizar los paquetes en una red, debe poder no perder de vista los detalles de la fuente y de la destinación de paquetes en la capa más baja y descifrar el contenido de esos paquetes para volver a montar la información en las capas más altas. En este respeto, una examinación de una operación de los succionadores es ideal para ganar una buena comprensión de cómo los varios protocolos obran recíprocamente para efectuar la entrega de la información a través de la amplia gama de sistemas en uso.



Cuadro 15. Los Protocolos en los modelosOSI 7-Layer y TCP/IP

Para apreciar la necesidad para los succionadores para un conocimiento a todos niveles del modelo, considere que un peticion del browser por una imagen de JPG en una pagina deba ser:

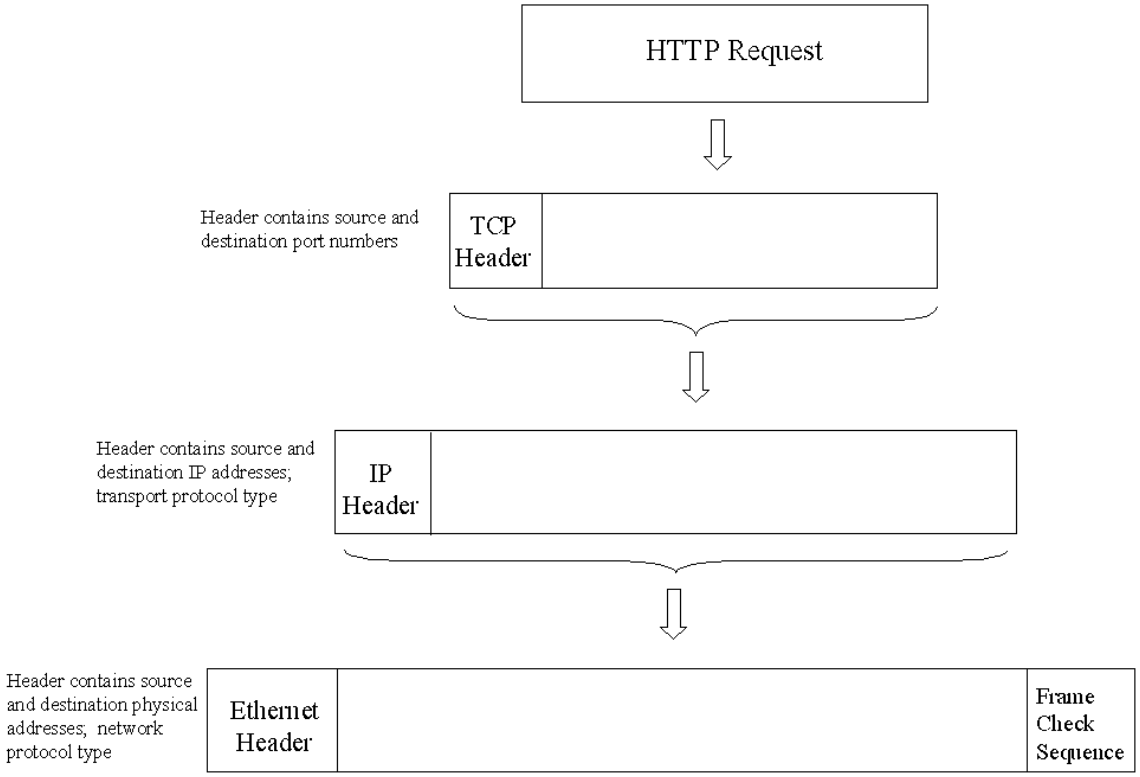
a. envuelto en un paquete del HTTP (protocolo de transferencia de hypertext) del tipo http:request;

b. entonces envuelto en un paquete del TCP (Transmission Control Protocol) junto con fuente y los números de acceso de la destinación. El TCP utiliza una estrategia de retransmisión para asegurarse de que los datos no serán perdidos en la transmisión;

c. entonces envuelta en un paquete del protocolo de IP(Internet) junto con direcciones del IP de la fuente y de la destinación y el protocolo de los packet?s mecanografía, y;

d. entonces finalmente envuelta en un paquete de Ethernet junto con las direcciones físicas de la fuente y de la destinación y el tipo del protocolo de red de los paquetes.

Cada capa contiene algo importante para el trazo y el análisis acertados del tráfico de la red. El cuadro 16 ilustra la naturaleza de esta estructura (envuelta) encapsulada.

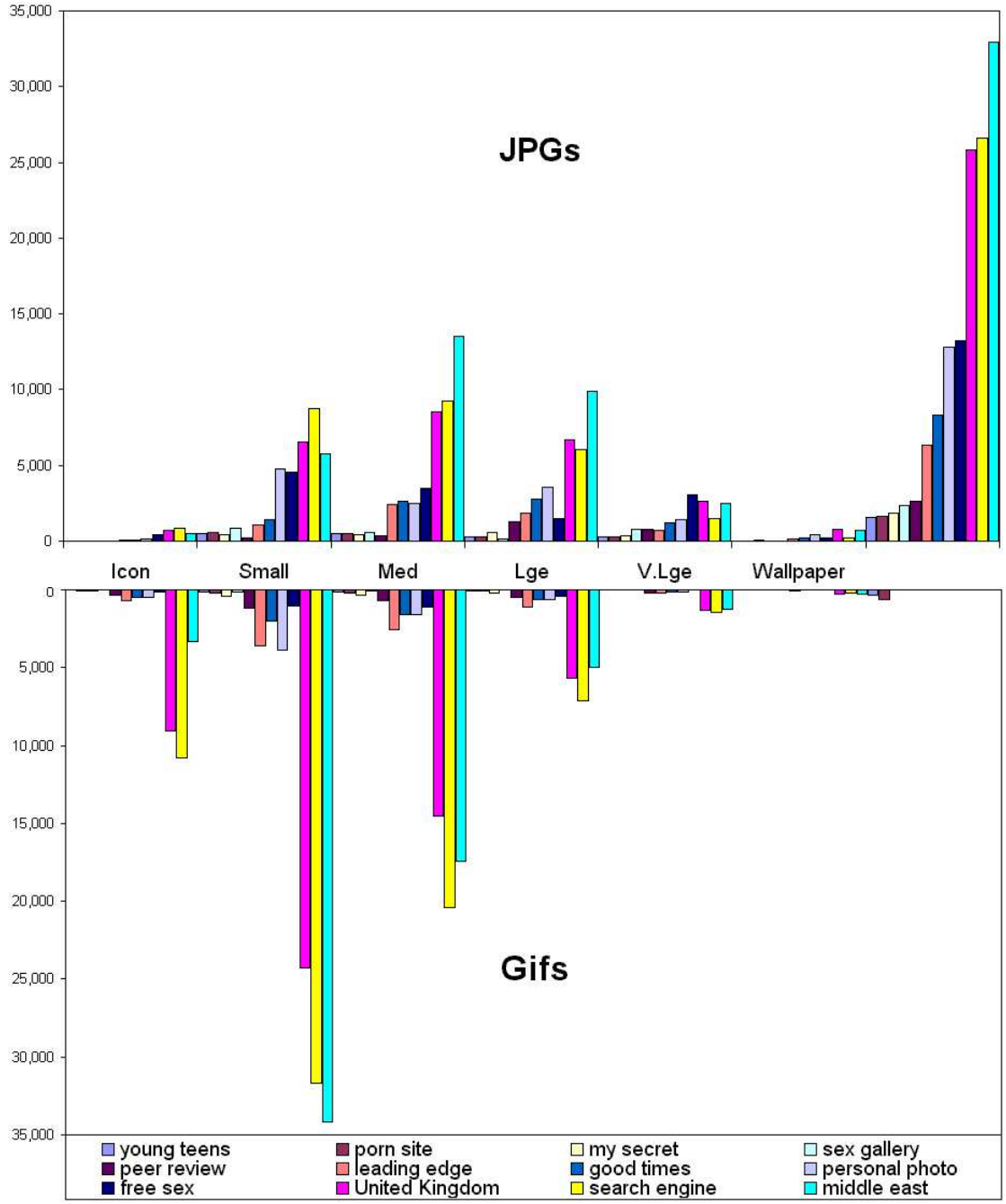


Cuadro 16. Encapsulacion multiple de protocolos

Este capítulo explora las estrategias para atacar la esteganografia, incluyendo la opción del formato de la imagen, una manera indistintamente de inhabilitar esteganografia usando un cortafuego y el uso de los motores de búsqueda y de las correas eslabonadas de la red.

5.1 ¿Por qué JPG?

Como la mayoría de los motores de búsqueda demuestran, los tipos lo más comúnmente posible usados del archivo de la imagen de la red son GIF y JPG. Para demostrar, el Google anuncia sobre 330 millones de imágenes en un índice, todas de forma GIF o JPG.



Cuadro 17. Resultados de busqueda de imagenes de Google

El cuadro 17, derivado de la búsqueda de Google, demuestra que los archivos del GIF, que se limitan a 256 colores, están utilizados sobre todo para (3.600 a 35.000 pixeles) las imágenes pequeñas de la red tales como botones, típicamente 1KB a 3KB de tamaño.

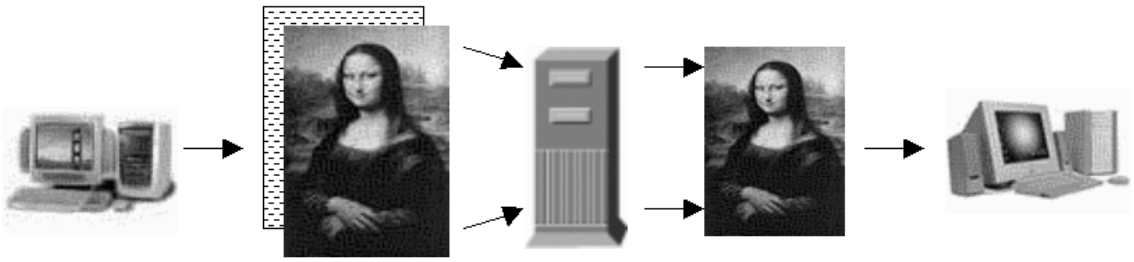
En contraste, las imágenes de JPG son capaces de color 24-bit (16,77 millones de colores) y son las más populares como (en el exceso de 480.000 pixeles) imágenes papel-clasificadas de la red tales como papeles pintados, salvapantallas y fotografías, típicamente 20KB a 1MB de tamaño.

Se preserva la calidad generalmente aceptable de la imagen al esteganograficamente encajar un máximo de el 15% del tamaño del archivo de la imagen cubierta. Estos tamaños del archivo limitan la cantidad de datos del mensaje en el GIF medio a no más de 150 a 450 octetos mientras que el JPG medio puede sostener con seguridad dondequiera de 3KB a 150KB.

5.2 Desabilitando la Esteganografia

Los archivos de Esteganografia que inhabilitan JPG son bien sabido para ser portadores eficientes de la información de la imagen, alcanzando a menudo aumentos de la compresión de el 90%, según comparaciones simples de JPGs y de sus imágenes equivalentes de BMP usando el Redactor de la Foto, un componente de Microsoft Windows. Sin embargo, este grado de compresión, que es imprescindible en la red, es realizable porque permite perdida, significando que hay pérdida (esperanzadamente imperceptible) de calidad del cuadro.

Esta compresión se alcanza parcialmente con la reducción del número de los colores usados,por ejemplo, de 16,77 millones a 256, permitiendo al formato comprimido de la imagen utilizar una gama de colores reducida de colores. Al corregir tal imagen incluso levemente cambiando el contraste o volviéndolo a clasificar según el tamaño, el archivo de JPG se reescribe con eficacia totalmente. En hacer así pues, el mensaje esteganograficamente ocultado y encajado delicadamente, generalmente dentro de los LSBs de la información de color se destruye fácilmente. Este resultado es verdad para el método de LSB empleado en la mayoría de los formatos de la imagen incluyendo BMP y GIF. Mientras que la esteganografia confía en no ser notada y por lo tanto espera evadir esta forma de ataque oculto, este método de encajar es vulnerable a la puesta en práctica de un estego-cortafuego como medida de seguridad, según lo ilustrado en el cuadro 18.



Cuadro 18. El Estego-Cotafuego

5.3 El Estego-Cortafuego

La modificación incluso leve del estego-cortafuego de la mayoría de los archivos de la imagen destruirá casi ciertamente cualquier esteganografia dentro de ellos, especialmente puesto que la mayoría de los de interés son de tipo JPG.

Por lo tanto, es absolutamente factible instalar un cortafuego que funciona una rutina simple que, por ejemplo, vuelva a clasificar según el tamaño todas las imágenes hasta el 95% de su tamaño original. Esto podía ser un fácil fija-y-olvida salvaguardia contra la mayoría de la esteganografia de la imagen a través del cortafuego elegido.

Sin embargo, el proceso de volver a clasificar según el tamaño cada imagen puede llegar a ser ineficaz para los volúmenes de tráfico grandes y puede ser indeseable. En ciertos foros legales y para las demandas de alta fidelidad tales como imágenes de diagnóstico médicas y forenses. La destrucción de cualquier huella de autor, para la protección del derecho, encajado en las imágenes es también indeseable.

Por otra parte, el cortafuego puede proteger solamente un solo punto de control con eficacia o supervisa una red pequeña con una sola conexión externa, no el mecanismo apropiado para tratar nuestra vigilancia en grande. Aunque los cortafuegos tienen tradicionalmente un alcance demasiado corto que se utilizará en un esquema de la vigilancia del Internet de la escala grande, vale el observar que:

a. supervisan el contenido actualmente alcanzado, no el que no se está leyendo, y

b. una red de varios cortafuegos con telecontrol a traves de agentes divulgados podría aumentar su alcance.

5.3 Motores de Busqueda

Un método más rápido, menos intruso y más de gran envergadura de localizar el contenido de la red es el uso de los motores de búsqueda. Éstos son sitios dedicados que consisten en las correas eslabonadas y las bases de datos puestas en un índice creadas para permitir que los usuarios localicen el contenido basado en las palabras claves o las fases, permitiendo respuestas a peticiones complicadas con el tipo y localización del archivo. Entre los mejores de éstos está Google (http://www.google.com), conocido por su velocidad, modernidad y flexibilidad. Al igual que dicho en su sitio, Google es particularmente bueno para la cobertura sobre 3 mil millones de páginas de la red y de 300.000 imágenes JPG y GIF.

Cuadro 19. Resultados de Google para "codo"

Como descripción de la disponibilidad y del funcionamiento del motor de búsqueda, los resultados de las listas de la tabla 2 de una gama de los motores de búsqueda populares para la búsqueda arbitraria, "codo", con la filtración ofensiva del contenido inhabilitada donde la opción fue ofrecida. Entre estos resultados está el punto interesante que aunque las imágenes incluidas en la búsqueda de FAST, ningunas de BMP fueron encontradas.

Los tipos disponibles de los criterios de selección del motor de búsqueda encontrados dan con las palabras de Google All/any, exigen frase, excluyen las palabras, tamaño de la imagen, JPG, GIF, B&W, color greyscale, completo, dominio JPG, palabras rápidas de la búsqueda All/any de los multimedia del GIF 22.400, frase exacta, JPG, GIF, BMP, B&W, color, gris, lineart JPG, fotos del GIF 12.050 Altavista, gráficos, Buttons/Banners, color, B&W, dominio, gama de la fecha, lengua JPG, palabras del GIF 2.861 MetaCrawler All/any, lengua, fecha, dominio JPG 164 ídem que ningunos JPG 100 no excitan ninguno la tabla 2 de JPG 100. Motores de búsqueda populares de la imagen: la palabra clave "codo"

Estos motores de búsqueda todos emplea mucho la misma estrategia de la búsqueda: el de las palabras claves de la indexación de direcciones del HTML PAGE en el cual las imágenes aparecen. De este modo, la importancia a la imagen es detectada por la asociación o el nombre de fichero sí

mismo del acoplamiento de la imagen. Esto significa invariable que el tema de la imagen nunca es examinado por el motor de búsqueda.

Importantemente, esto significa que el archivo sí mismo de la imagen nunca es examinado por este tipo de motor de búsqueda.

Poco se pregunta, después, que no hay motor de búsqueda público accesible dondequiera en el Internet capaz de la detección del contenido steganographic.

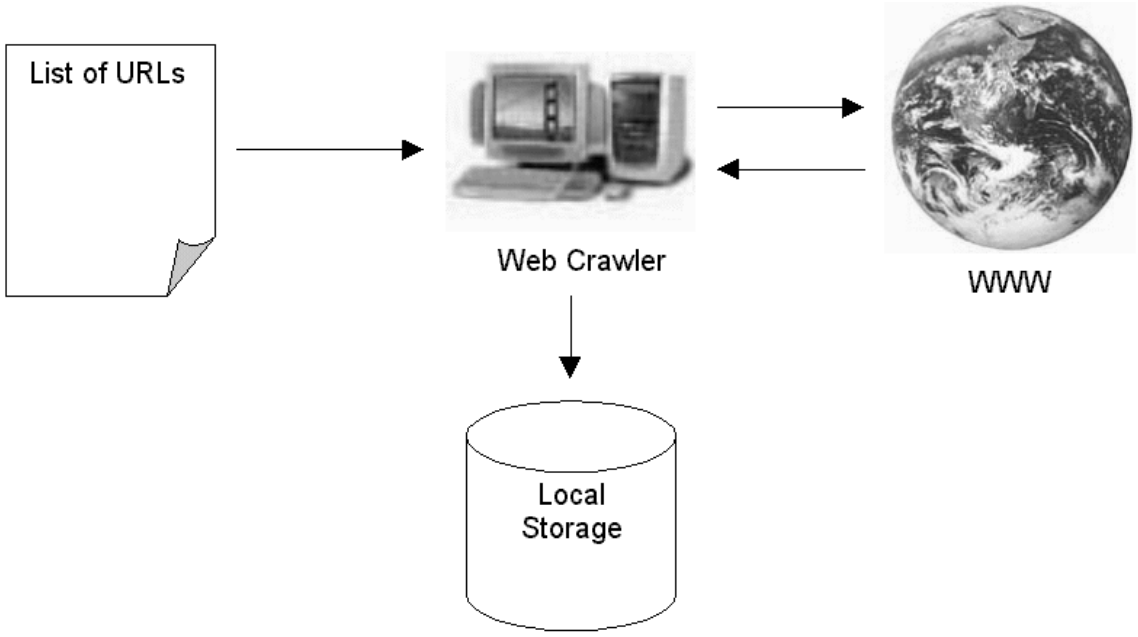
5.4 Las Correas Eslabonadas De Red, Las Arañas Y Los Bots

Las correas eslabonadas de red también se llaman Arañas (correas eslabonadas de red) y son un subconjunto de Bots (robotes).

Son utilizadas a menudo por las casas comerciales del E-mail surreptitiously para recolectar direcciones válidas del E-mail para aumentar sus bases de datos receptoras y empujar su publicidad a una audiencia más ancha en la forma de qué se llama el E-mail comercial no solicitado (los ECUS) o Spam. Las correas eslabonadas de red están también disponibles para el uso personal para ver fuera de línea contento de la red. Para este propósito, éstos a menudo se llaman los browsers fuera de línea. Una correa eslabonada de red puede explorar y descargar cualquier contenido publicado en un Web site navegando los acoplamientos encontrados en la página que comienza para ese sitio.

Una convención seguida voluntariamente por algunas correas eslabonadas es la de la comprobación para saber si hay la existencia del archivo robots.txt del texto en el directorio de raíz de los sitios de la red. Un administrador del la pagina puede desear que solamente las correas eslabonadas enumeradas dentro de este archivo se les permita poner en un índice el sitio. La objeción principal es la del abuso de anchura de banda durante el proceso de arrastre. Sin embargo, la mayoría de las correas eslabonadas tienen la opción de desatender este archivo, dejando al administrador de la pagina impotente para pararlas.

El oler para los HTTP CONSIGUE pedidos por una imagen de JPG es un proceso en tiempo real. Una vez que cada petición sea detectada por el succionador, se registra esto y el oler continúa. El valor de una correa eslabonada de red para la solución presentada en esta tesis es que las peticiones registradas se deben leer juntas con las destinaciónes, las cuales se alcanzan por la correa eslabonada para recolectar esas imágenes para el análisis.



Cuadro 20. La operacion de la correa eslabonada

En este papel, la correa eslabonada está actuando a nombre del sistema propuesto como el browser automatizado, trayendo todas las imágenes requeridas para el análisis. El cuadro 21 demuestra cómo una correa eslabonada de red toma una lista de URLs y alcanza cada uno de éstos a través de una conexión abierta del Internet para tener acceso a cualesquiera páginas e imagen disponibles que se encontrarán.

5.6 Enangostando La Búsqueda

Consideremos qué características de cualquier mensaje secreto proporcionan su valor. Con excepción de la robustez de los mecanismos de codificación empleados, su éxito debe ser medido por lo que aquí se ha llamado su:

a. calidad de entrega, y

b. calidad de cubierta.

La calidad de la entrega puede ser buscada proporcionando el mismo mensaje en el múltiplo las localizaciones altamente visibles y accesibles y/o vía medios múltiples del transporte.

Los mensajes secretos son esencialmente de breve duración y servicio poco propósito después de la entrega. Un peligro muy verdadero a su cubierta es su restante expuesto más de largo que necesita ser. La calidad de la cubierta, por lo tanto, incluye el retiro o la destrucción del mensaje una vez que se haya recibido, como en los metodos tradicionales de los espias que queman o tragan del medio del mensaje.

Estas dos características trabajan a menudo cara a cara y el método de la entrega secreta entonces es determinado por un compromiso entre las dos. la esteganografia red-basado de la imagen, como método de entrega, se emplea lo más mejor posible cerca:

a. que promovía la calidad de la entrega por su presencia en sitios fácilmente accesibles de la red, y

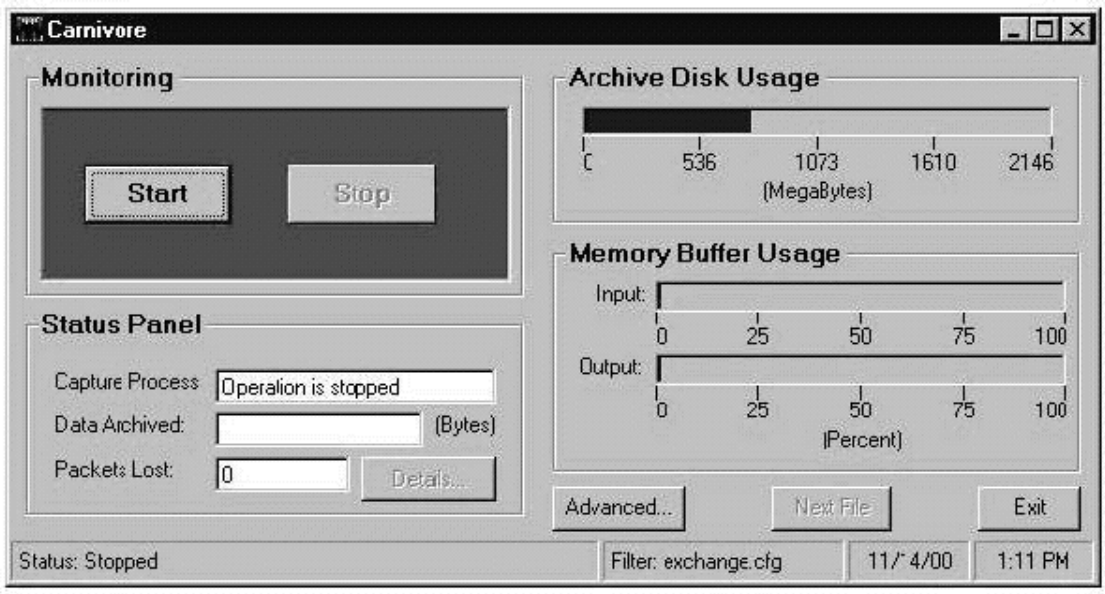
b. accesible restante solamente hasta que el mensaje se ha recibido.

Para emplear los datos tradicionales que minan con resultados existentes de los motores de búsqueda esencialmente en una búsqueda oculta laboriosa. Dado las características esperadas de esteganografia red-basado, un aumento en gran medida más respetable en búsqueda y la eficacia de la detección es el reconocimiento que estas imágenes secretas no existirían ordinariamente afuera de su periodo de entrega prevista. Esto significa que la estrategia ideal de la búsqueda para esta forma de esteganografia es detectar las imágenes mientras que existen. Para llevar este razonamiento a su conclusión, estas imágenes existen solamente para su transmisión y es entonces que deben ser detectadas.

Este capítulo examina la evidencia de cuatro ejemplos de estrategias, tres en uso por la comunidad de la inteligencia y uno por una empresa comercial. Cada ejemplo demuestra la importancia de la esteganografia como un dispositivo de seguridad y arma de la guerra electrónica.

6.1 El Carnívoro

El Carnívoro del FBI es así nombrado porque mastica todos los datos que vienen a través de cierta red de datos pero solamente se come la información permitida por orden judicial. Básicamente, el carnívoro es un monitor usado en el Internet. Una foto del interfaz del Carnivoro se demuestra en el cuadro 22. Según Marcus Thomas, el jefe sección de la cybertecnología FBI, 'Carnívoro consiste de una computadora portátil de Windows NT o de Windows 2000 sin apilado de TCP/IP y con 128 megabytes de memoria, de un Pentium III, de entre 4 y 18 gigabytes de espacio de disco, y de una unidad de Jazz de 2G para la collection de evidencia.



Cuadro 21. El interfaz básico del Carnívoro

Utiliza un programa del succionador de paquete, escrito como los plugins de C++ (véase el cuadro 23) al EtherPeek, un producto similar a Ethereal, y selecciona los datos que desea por dentro de la red local del proveedor.

Un dispositivo de la autentificación del hardware se utiliza para controlar el acceso a la caja (medida de prevención de que el proveedor tenga acceso al dispositivo sin dejar muestras visibles del daño). Una interfaz de red de Shomiti o de NetOptics se utiliza como dispositivo de aislamiento de la red. Esto evita que la caja transmita incluso si un hacker pudiera alcanzar adentro de alguna manera.

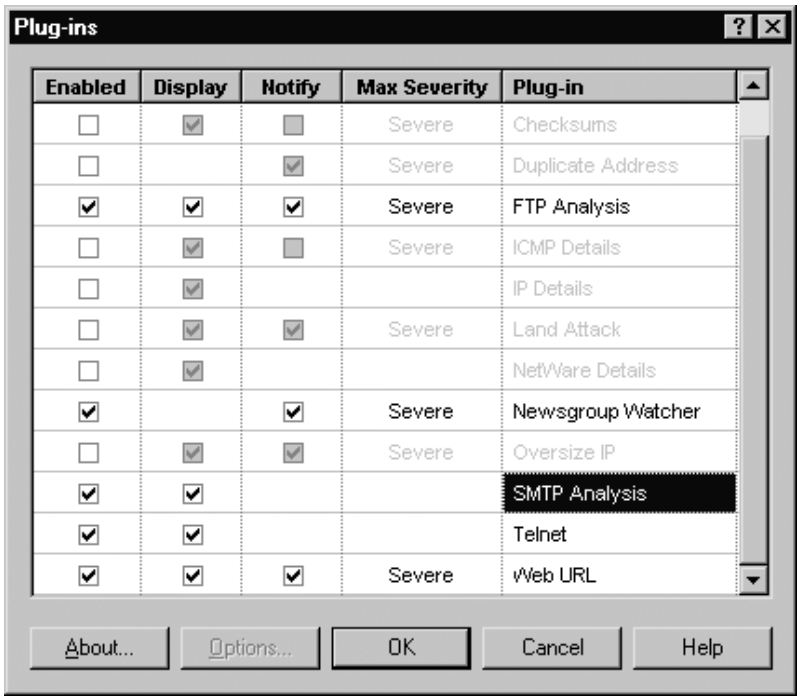


Figure 22. La adición de plugins al Etherpeek del Carnívoro

Carnívoro requiere la ayuda del proveedor para localizar y conectar con eficacia con un punto conveniente en la espina dorsal del proveedor. Se sabe que es capaz de examinar los protocolos siguientes:

- IP (IP ADDRESS) de from/to
- ftp (nombres de fichero de los registros transferidos)
- NNTP/Usenet (los registros tienen acceso a los newsgroup)
- smtp (correos electronicos de los registros accionados cerca o a la dirección del correo)
- HTTP (registros URLs)
- IRC (filtro portuario)

Se considera que la mensajería inmediata (filtro portuario) del Carnivoro, el modo de operación, parece ser el texto del correo sin la capacidad de a mirar mas adentro del correo o un domicilio IP pre-seleccionado. Un problema con este acercamiento es que el correo de un grupo terrorista no será etiquetado como tal (los remailers anónimos, por ejemplo las redes del Cyberpunk y de Mixmaster anonimizan con eficacia cualquier correo), así todo el correo en el Internet tendría que ser buscado.

Otro es que la comunicación secreta es no más larga probablemente estar en el texto del E-mail. Como con imágenes de JPG, éstos serían llevados adentro como accesorio. El Carnívoro, si no está ya, tendrá que ser mejorado para poder examinar los accesorios y discernir si un accesorio contiene un archivo encajado. Si el Carnívoro encuentra un archivo encajado, tendrá que abrirlo para leerlo, o aún para analizarlo.

6.2 NTAC

El Acto de la Regulación del Acto de los Poderes Investigatorios (RIPA), efectivo el 5 de octubre de 2000, dio a la secretaría casera británica poderes sin par de la interceptación y de la vigilancia. La policía y los servicios de seguridad británicos tienen poderes arrebatadoras a la vigilancia de tráfico de correo electronico y el uso de la red. Esta facilidad total de la vigilancia se llama el Centro Nacional de la Asistencia Técnica (NTAC), conocida antes como el Centro de la Asistencia Técnica del Gobierno (GTAC).

NTAC se prepone depender eventualmente de una red polémica de cajas negras, instaladas en redes de Internet y la alimentación directa en jefaturas en el domicilio de MI5 en la Casa de Thamesis, Millbank, en Londres, donde el centro será basado, demostrado en el cuadro 24.

Cuadro 23. La Casa de Thamesis

La idea de tales cajas causó ultraje cuando fue sugerido. Por lo tanto, a pesar de ser incluido en el RIPA, no se le exigido a ningun proveedor todavía por el gobierno el instalar tal sistema de la vigilancia.

Bajo una de las provisiones del RIPA, si piden un de funcionario de la compañía la entrega de una llave de cifrado al gobierno, la ley le prohibe al individuo el decirselo a cualquier persona, incluyendo su patrón o cualquier persona en la compañía. Las consecuencias de esta comunicacion prohibida, pues se sabe, podría dejar una compañía internacional totalmente inconsciente que sus datos asumidos seguros pueden estar bajo investigación del MI5. Ésos que violan la ley pueden encontrarse con hasta cinco años de carcel.

Los funcionarios ahora admiten que una legislación secundaria es necesaria antes de que se pueda instalar las cajas negras en los proveedores. Incluso entonces, el proveedor (el RIPA refiere a un Proveedor de Servicios de Comunicación, CSP, sugiriendo un alcance más amplio de la industria) tendrá recurso a un cuerpo independiente si se siente que es demasiado costoso, que podría resultar un retraso significativo. Sin tales cajas, será imposible que NTAC ponga sus manos en la red de communications.

En la conducta de la investigación de este curso sobre las operaciones de NTAC, el autor de la tesis eestabelció contacto con el Ministerio del Interior, de el cual NTAC es una unidad, y recibió la correspondencia, unida en el apéndice C, del Principal Guardia Auxiliar Ian Humphreys, jefe de NTAC. Sr. Humphreys tensiona en su correspondencia que NTAC no estaría implicado en la vigilancia del alto volumen dada las pautas terminantes del Government. El paso siguiente aparece en el bosquejo más último del RIPA, ofrecido amablemente como referencia por Sr. Humphreys, sugiriendo que la cobertura amplia es una prioridad:

'El gobierno reconoce las preocupaciones de los CSP por costes resultando de las obligaciones en la orden del bosquejo. La sección 14(2) pone un deber en la secretaria del estado para asegurarse de que los arreglos están en vigor para asegurar que esos CSP reciben una contribución justa por los costes incurridos como consecuencia de la imposición de las obligaciones en la orden del bosquejo y de la aplicación de las autorizaciones de la interceptación.

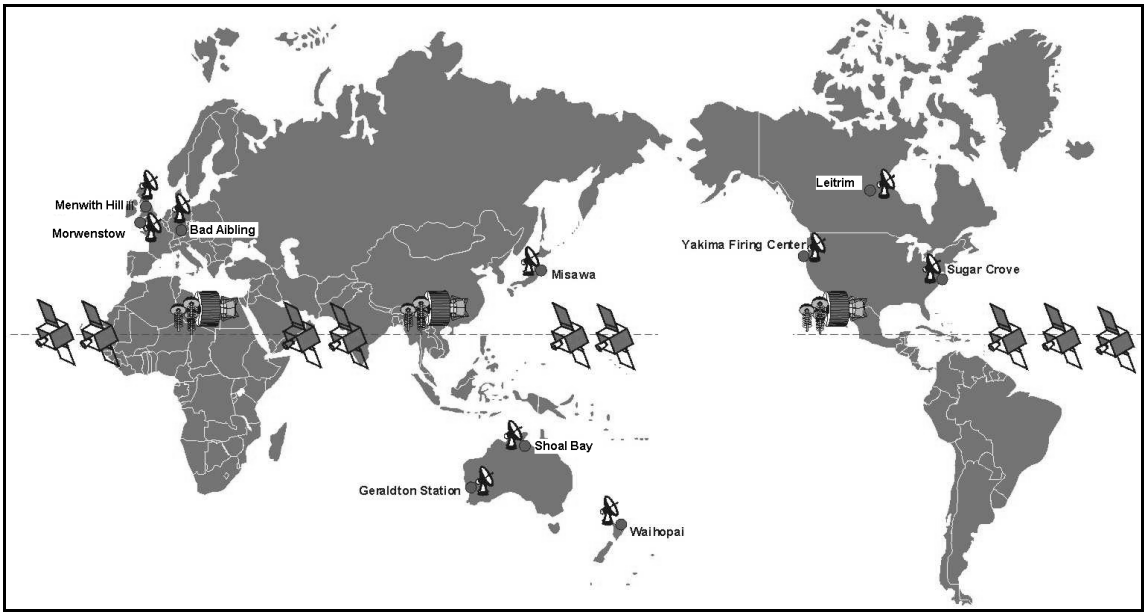
"A traves de las agencias de interceptacion, el gobierno tiene acuerdos en lugar con todos los CSPs que proporcionan actualmente la interceptación y paga actualmente una contribución substancial a los costes. El año pasado, CSPs recibieron en exceso de £14 millónes del gobierno. El dinero es principalmente para pagar los costes de dar efecto a las autorizaciones de la interceptación, pero también se utiliza para asistir con el mantenimiento de una capacidad de interceptación."

Claramente, las capacidades de la interceptación de NTAC son una realidad. Más allá de este hecho, puede haber poca más información disponible. Las palabras de despedida de Sr. Humphreys eran:

'Dado el fondo de nuestro trabajo, dudo que yo podría proveer a usted cualquier más información en el futuro."

Quizás los proveedores que son financiados por la contribución de NTAC se juran a una medida igual de secreto: el correo del autor, titulado 'Estudio sobre información buscada en conexion con NTAC/Echelon" a una docena de los proveedores más grandes del Reino Unido ha pasado totalmente sin respuesta.

6.3 Echelon



Cuadro 24. La cubertura global de Echelon

Características atribuidas al sistema echelon:

El sistema conocido como Echelon es un sistema de interceptación que diferencia de otros sistemas de la inteligencia en que posee dos características que lo hagan absolutamente inusual:

La primera tal característica atribuida a él es la capacidad de realizar vigilancia casi total. Las estaciones del receptor y los satélites basados en los satélites del espía en detalle se alegan para darle la capacidad de interceptar cualquier teléfono, fax, mensaje del Internet o del E-mail enviado por el individuo y de examinar así su contenido.

La segunda característica inusual del Echelon es dicho ser que el sistema funciona por todo el mundo en base de la cooperación proporcionada a sus capacidades entre varios estados (el Reino Unido, los E.E.U.U., Canadá, Australia y Nueva Zelanda), dándola valor agregado en la comparación a los sistemas nacionales: los estados que participan en el Echelon (estados del Echelon) pueden poner sus sistemas de interceptación a disposición de los otros, compartiendo el coste y haciendo uso común de la información que resulta.

Este tipo de cooperación internacional es esencial en el detalle para la interceptación mundial de comunicaciones basadas en satélites, puesto que solamente de esta manera es posible asegurarse de comunicaciones internacionales de que ambos lados de un diálogo puedan ser interceptados. Está claro que, en vista de su tamaño, una estación receptora de satélites no se puede establecer en territorio de un estado sin su conocimiento. El acuerdo mutuo y la cooperación proporcionada entre varios estados en diversas partes del mundo es esencial.

El Echelon es una red mundial de la vigilancia que se ha rumoreado existir desde 1990. Prueba que el sistema del Echelon funcionaba fue encontrada en documentos del gobierno de los E.E.U.U. en 1998 y 1999. El especialista doctor Jeff Richelson de la inteligencia de los E.E.U.U., del Archivo de

la Seguridad Nacional, de Washington D.C, utilizó el Acto de la Libertad de Información para obtener una serie de documentos nuevos de la marina y de la fuerza aérea de los E.E.U.U. que confirmaron la existencia, la escala y la extensión continuada del sistema del Echelon. Los documentos identificaron cinco sitios como parte del sistema que recogía la información de los satélites de comunicaciones.

La primera estación que se confirma como parte de Echelon era Sugar Groves en Virginia del Oeste en los E.E.U.U. Según los documentos oficiales, la misión de este sitio es vigilar consumidores directos del equipo de comunicaciones basadas en los satélites Comsat... que esto es alcanzado proporcionando a un cuadro entrenado de los operadores de sistema de la colección, de los analistas y de los encargados...

En 1990, la fotografía por satélite demostró que habían cuatro antenas en la estación del campo de la Sugar Groves. En 1998, una visita de tierra de un equipo de TV reveló que éstas se habían ampliado a nueve. Todas estaban dirigidas hacia los satélites sobre el Océano Atlántico, proporcionando comunicaciones a y desde las Américas así como Europa y África.

Los documentos también identifican cuatro otras bases de la inteligencia que eran parte de la red del Echelon antes de 1995. Éstos eran Yakima, Sabana Seca en Puerto Rico, Guam, y Misawa, Japón.

En 1997, British Telecom reveló la información detallada sobre los cables altos de la anchura de banda que fueron cabidos en la colina de Menwith, la base de alianza-supervisión de R.U./E.E.U.U. en Yorkshire. Se había instalado tres cables de fibra óptica digitales capaces de llevar 100.000 conversaciones de teléfono simultáneamente.

Cuadro 25. El sitio de Echelon en Menwith Hill

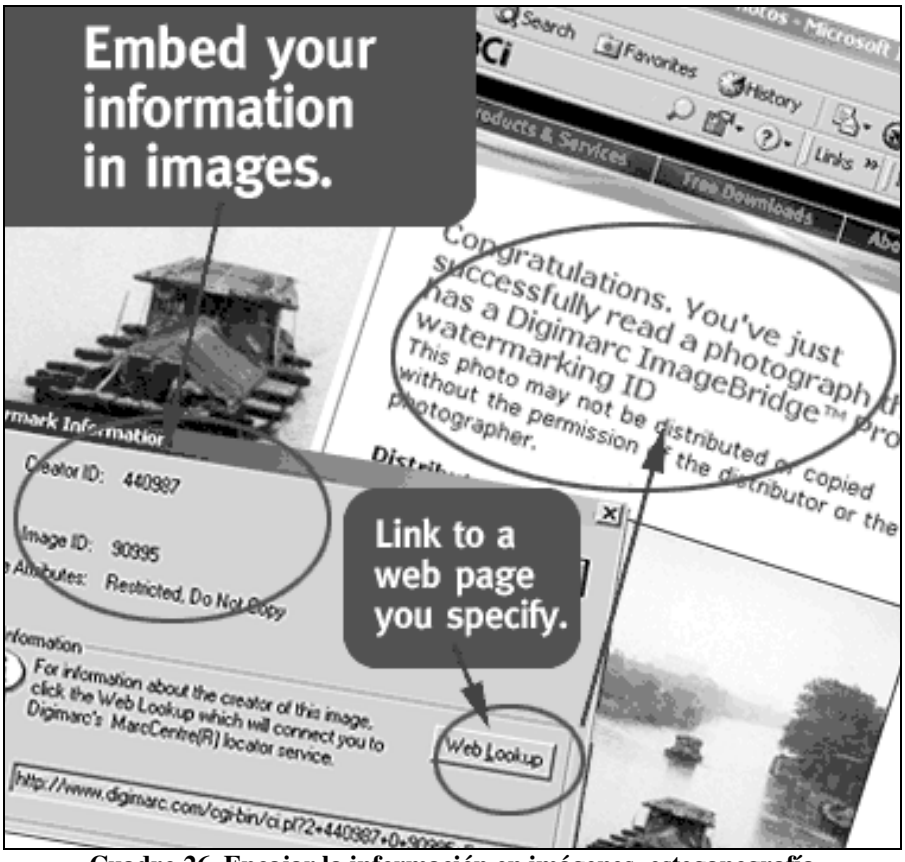
En noviembre de 1999, el BBC publicó un artículo que dijo que el gobierno australiano había confirmado la existencia del Echelon. El senador Bill Blick, inspector-general de inteligencia y

seguridad de Australia, dijo a BBC que la Directorado de Señales de Defensa (DSD) forma parte de Echelon. La existencia de los sistemas discretos tales como Carnívoro y NTAC entre otros, probablemente bajo sistemas paraguas tal como Echelon, demuestra que la vigilancia se ha madurado a una capacidad de traer cualquier forma de comunicación dentro de su alcance fácil. Esto puede sugerir que el potencial para la esteganografia, cuya hipótesis primaria es que funciona en plena vista del enemigo, es más fuerte hoy que nunca.

6.4 MarcSpider de Digimarc

Digimarc es una compañía que se especializa en imágenes para la protección de los derechos del autor.

La tecnología que sigue de la imagen de MarcSpider combinada con alimentaciones de los datos de los monitores de la correa eslabonada de la red de Digimarc dan por resultado una cobertura de más de 50 millones de imágenes al mes. MarcSpider arrastra las áreas públicas más frecuentadas del World Wide Web en busca de imágenes ImageBridge de Digimarc y detalles marcados por la huella indicando cuando y donde se encuentran las imágenes mientras que mantienen un archivo de las imágenes encontradas, investigable por fecha.



Cuadro 26. Encajar la información en imágenes -esteganografía

La muy detallada pagina de web de Digimarc describe su uso de huellas como los medios imperceptibles de proteger imágenes de sus clientes contra la piratería, a través del encajamiento de

su información en los imágenes. Éste es uso claro de la esteganografia, aunque el término no aparece en ninguna parte en su sitio (http://www.digimarc.com). Sus servicios cubren audio y vídeo así como imágenes.

CAPÍTULO 7 EL MOTOR DE BÚSQUEDA CONTRATERRORISTA DE ESTEGANOGRAFIA: UN ACERCAMIENTO PRO-ACTIVO

Este capítulo presenta una solución al combate del problema de la esteganografia en las manos de un terrorista y justifica su diseño por referencia a la investigación emprendida. Cada componente del sistema se describe detalladamente y cada uno de los modos de operación se explica.

7.1 Una Mejor Manera

Una intensiva evaluation de los resultados de la investigación demostró que ni los motores de búsqueda convencionales ni los cortafuegos convencionales solamente están diseñados para satisfacer los requisitos para detectar esteganografia de imágenes basados en la red.

El tamaño y el índice de crecimiento escarpados del Internet hace arquitecturas convencionales del motor de búsqueda inadecuadas, dado la naturaleza de la comunicación esteganografica. Mientras que las estimaciones varían considerablemente de fuente a la fuente, aproximadamente 81 páginas nuevas de la red aparecen cada segundo en el Internet.

Según el Generador de la Estadística Irresponsable del Internet, antes del 1 de agosto de 2002 habrán 3.008.622.746 personas usando el Internet. Esto representa a 50,14 % de la población del mundo. El generador se titula "irresponsible" porque el autor admite abiertamente la dificultad de hacer valoraciones sobre el tamaño del Internet, dado su independencia de arquitectura y de la gerencia.

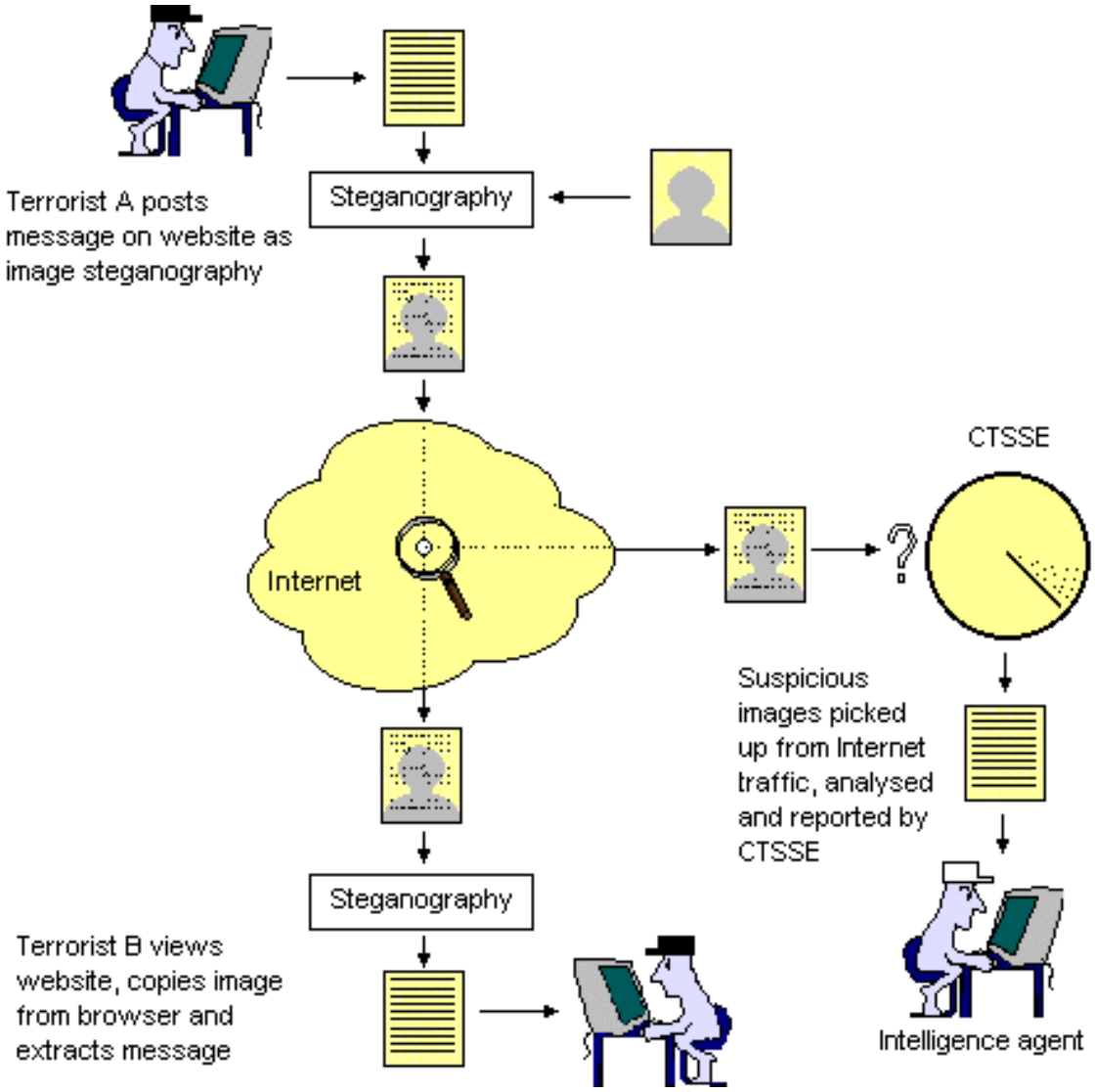
La obligacion inescapable del esteganografo de transmitir el mensaje se debe considerar como la debilidad más grande del medio y por lo tanto la fuerza más grande de la solución ideal. El Motor de Búsqueda Contraterrorista de Esteganografia (CTSSE) demuestra un paso significativo hacia este ideal con éxito, combinando las mejores características de una gama de software de Internet y de redes.

Los componentes de software de esta tesis de MESE MSc, diseñados todo para la operación discreta e independiente, han sido seleccionados, adaptados y coordinados por el software escrito como parte de esta tesis para producir una solución basada en PC capaz del control desatendido y continuo, del análisis y de la divulgación de la esteganografia de imágen basada en la red. El CTSSE es capaz de dos modos de operación:

a. Tiro singular: El operador funciona un archivo de hornada para producir un caso del análisis de un conclusión del registro del succionador en la producción de la página de los resultados de CTSSE, y

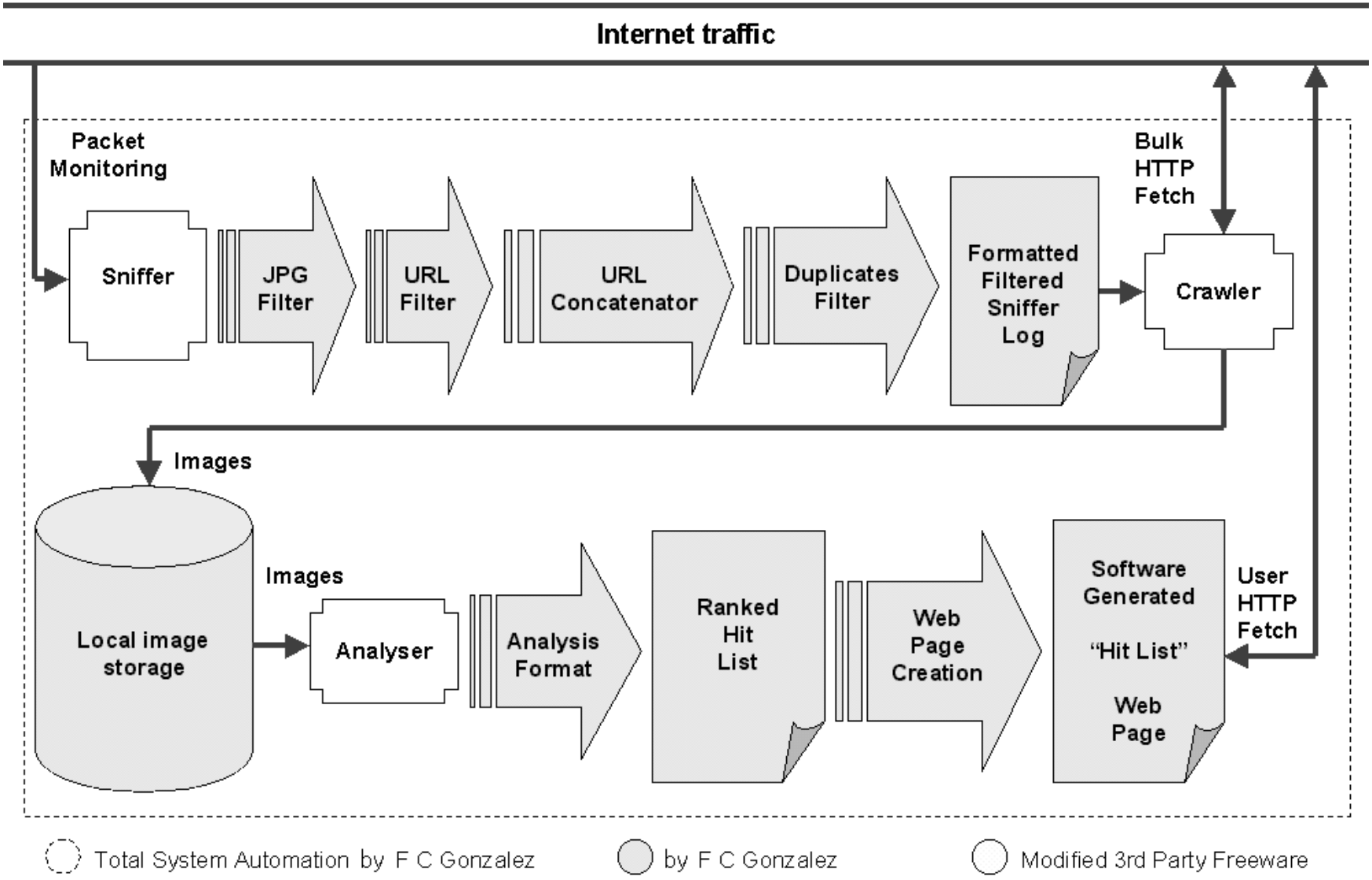
b. Continuo: El operador golpea una combinación de la Alt-llave para comenzar el ciclo de la operación del CTSSE, automatizada completamente de oler inicial a la página final de los resultados, con este ciclo ocurriendo continuamente en una frecuencia seleccionable. El éxito de este diseño, centrado en un protocolo y un tipo de portador, señala la oportunidad para utilizar "plug-ins", ser adaptado y agregado para ensanchar su alcance eficaz.

El cuadro 28 demuestra donde el CTSSE se ajusta en el esquema de la vigilancia.



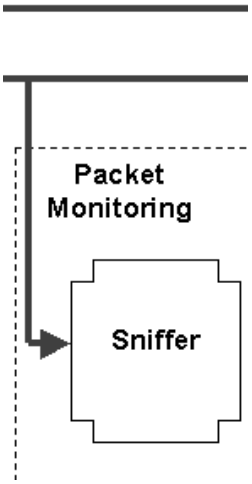
Cuadro 27. Interceptando esteganografía de imagen.

Todo el software escrito expreso para esta tesis, software de base, se ha documentado completamente en el apéndice D. Los diagramas de lógica se proporcionan en el apéndice E. Figure 29 es una descripción funcional del CTSSE, demostrando la secuencia de eventos y el papel de cada componente. Los componentes sombreados fueron creados para esta tesis por el autor. La discusión siguiente sobre cada componente se relaciona con este diagrama de la descripción y se puede seguir por las imágenes proporcionadas como cabezas de párrafo.



CuaCuadro 28. El motor de busqueda contraterrorista de esteganografía

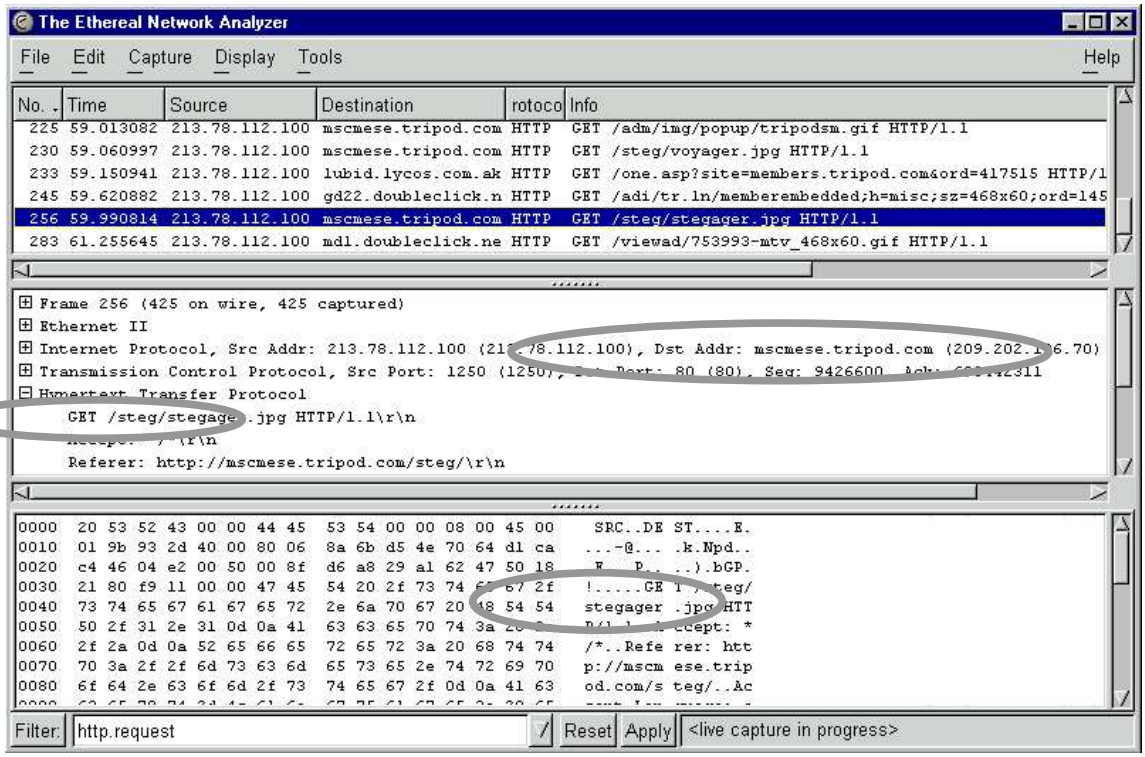
7.2 El Succionador De Paquetes



El cuadro 30 demuestra el succionador de paquete seleccionado para esta tesis, Ethereal, en el proceso de registrar peticiones del HTTP incluyendo una para una imagen llamada *stegager.jpg* de *mscmese.tripod.com/steg/* cuyo domicilio es *209.202.196.701*.

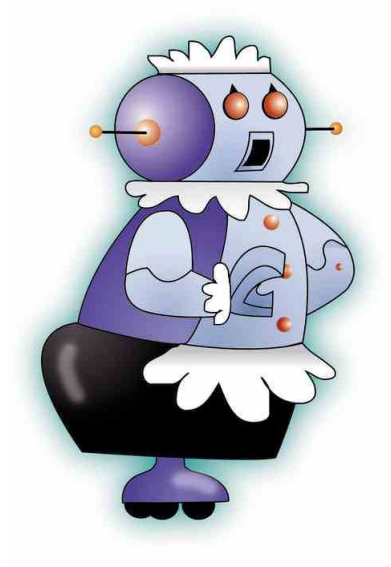
La ventana superior demuestra los paquetes, uno por la línea, mientras que la ventana media demuestra el detalle de un paquete seleccionado, dividida en las secciones separadas de la estructura del paquete: El capítulo, Ethernet II, el IP, el TCP, y el HTTP. De interés particular para nuestro CTSSE es la dirección de destinación del paquete de la petición (la cabazera IP) y del nombre de fichero que es solicitado (la cabezera HTTP).

La ventana inferior exhibe la misma información que la ventana media pero sin la estructura demostrada, y en hexadecimal y texto. Observe que es la petición y no la respuesta que se graba.



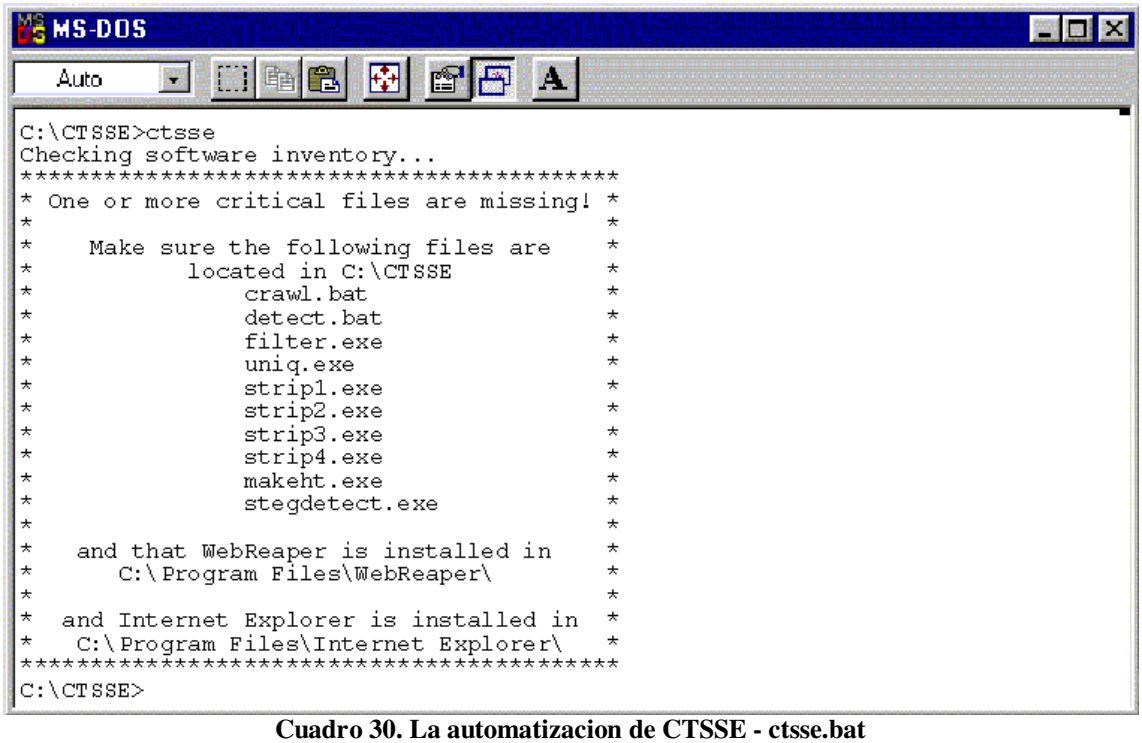
Cuadro 29. El succionador de paquetes Ethereal

7.3 Automatización De La Economía Doméstica



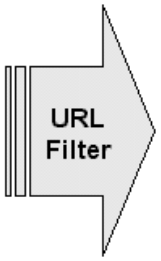
Agradable como pueda aparecer "automatizar la economía doméstica", no es absolutamente tan entretenido como la historieta famosa de la criada mecánica Rosie de los Jetsons. Sin embargo, una de sus punterías es ser suficientemente informativa al usuario. La economía doméstica se refiere, entre otras cosas, a la tarea de los programadores del software de asegurarse de que el software producido no funcione fuera de su intentado enviro o pierda control ni llegue a ser confuso cuando su ambiente cambie. Las cosas tales como la dirección de excepción y la divulgación del nivel de error son útiles, no solamente al usuario del extremo después de la entrega, pero a la ayuda en el mantenimiento del software que puede seguir.

En última instancia, es un aspecto del buen prácticante y el CTSSE incorpora esto en la forma de inventario del software (donde se buscan todos los archivos requeridos antes de que la operación se permita comenzar) y error del archivo de la entrada-salida (I/O) que divulga por los varios componentes ejecutables escritos para esta tesis. El cuadro 31 demuestra la respuesta del programa cuando cualquier archivo requerido falta de su localización prevista.



Cuadro 30. La automatizacion de CTSSE - ctsse.bat

7.4 Analizando El Registro Del Succionador



El cuadro 32 es el detalle completo de apenas un paquete interceptado por el succionador de paquete del CTSSE. Típicamente, los millares serían registrados en cuestión de minutos en el fichero de diario que se utilizará por el CTSSE. De estos expedientes, el software extrae automáticamente apenas la línea que contiene la dirección de destinación del IP (circundada). Esto da lugar a la salida que se asemeja a eso en el cuadro 31. Observe el entrelazamiento de las direcciones de destinación del paquete, demostrando que dos browsers funcionaban simultáneamente al recolectar la muestra demostrada.

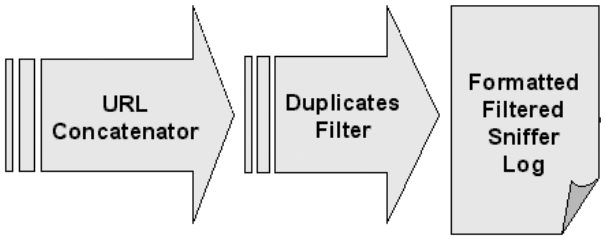
```
Frame 1600 (341 on wire, 341 captured)
    Arrival Time: Jun  9, 2002 11:34:21.007894000
    Time delta from previous packet: 0.366954000 seconds
    Time relative to first packet: 349.611781000 seconds
    Frame Number: 1600
    Packet Length: 341 bytes
    Capture Length: 341 bytes
Ethernet II
    Destination: 20:53:52:43:00:00 (20:53:52:43:00:00)
    Source: 44:45:53:54:00:00 (friaco.onetel.net.uk)
    Type: IP (0x0800)
Internet Protocol, Src Addr: friaco.onetel.net.uk (213.78.112.100), Dst Addr: a33.g.akamai.net (212.187.244.17)
    Version: 4
    Header length: 20 bytes
    Differentiated Services: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 327
    Identification: 0x3134
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0xb9fc (correct)
    Source: friaco.onetel.net.uk (213.78.112.100)
    Destination: a33.g.akamai.net (212.187.244.17)
Transmission Control Protocol, Src Port: 1349 (1349), Dst Port: 80 (80), Seq: 12747735, Ack: 4226462337
    Source port: 1349 (1349)
    Destination port: 80 (80)
    Sequence number: 12747735
    Next sequence number: 12748022
    Acknowledgement number: 4226462337
    Header length: 20 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 8576
    Checksum: 0x911b (correct)
Hypertext Transfer Protocol
    GET /hq/lab/carnivore/images/carnivore.jpg HTTP/1.1\r\n
    Accept: */*\r\n
    Referer: http://www.fbi.gov/hq/lab/carnivore/carnivore.htm\r\n
    Accept-Language: en-au\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)\r\n
    Host: www.fbi.gov\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

Cuadro 31. Producto detallado del succionador para un paquete

```
Internet Protocol, Src Addr: onetel.net.uk (213.78.112.100), Dst Addr: www.google.com (216.239.37.101)
Internet Protocol, Src Addr: onetel.net.uk (213.78.112.100), Dst Addr: www.tripod.com (209.202.196.70)
Internet Protocol, Src Addr: onetel.net.uk (213.78.112.100), Dst Addr: www.google.com (216.239.37.101)
Internet Protocol, Src Addr: onetel.net.uk (213.78.112.100), Dst Addr: gd22.click.net (206.65.183.80)
.                                                                                                    .
.                                                                                                    .
Internet Protocol, Src Addr: onetel.net.uk (213.78.112.100), Dst Addr: www.tripod.com (209.202.196.70)
Internet Protocol, Src Addr: onetel.net.uk (213.78.112.100), Dst Addr: a111.akamai.net (212.187.244.8)
Internet Protocol, Src Addr: onetel.net.uk (213.78.112.100), Dst Addr: a33.akamai.net (212.187.244.17)
Internet Protocol, Src Addr: onetel.net.uk (213.78.112.100), Dst Addr: a33.akamai.net (212.187.244.17)
```

Cuadro 32. Primer instante de filtracion para URLs

7.5 El Ajuste De Formato Y La Filtracion De Urls Duplicados



La tabla 3 ilustra el sistema siguiente de procesos que pelan lejos todos menos el ultimo domicilio IP acorchetado de cada línea, representando el domiciolio IP donde las imágenes de JPG pueden ser encontradas (la columna 1).

Esto se hace guardando solamente ese texto en el cual aparezca y después del ultimo soporte izquierdo en cada línea.

La longitud imprevisible del domicilio IP hizo este el método preferido del análisis. Para producir un formato conveniente para la correa eslabonada de red al uso como archivo de comando, la transformación posterior se requiere también para quitar los soportes (columna 2).

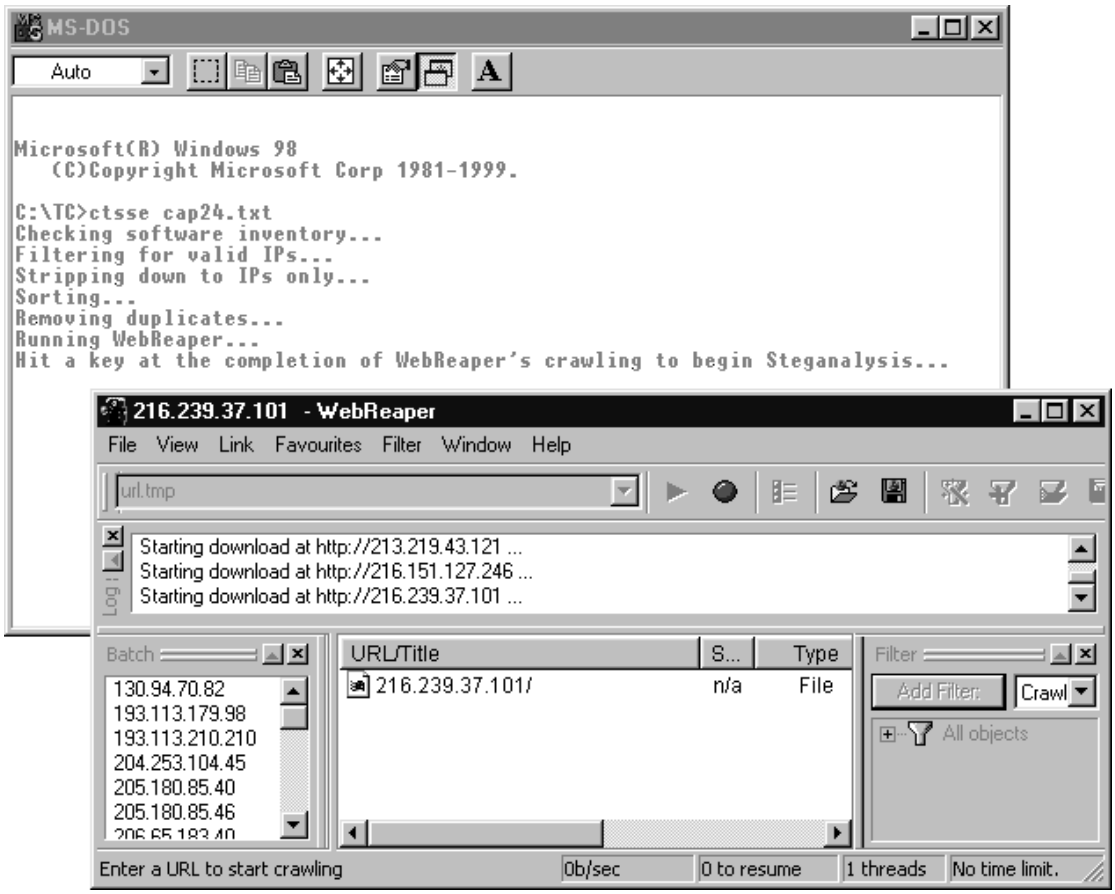
La repetición ocurre debido a los alcances múltiples al mismo lugar de web, tal como la página web sí misma y las muchas imágenes que puede contener. Esta repetición se elimina en el último de estos procesos (columna 3).

Column 1	Column 2	Column 3
(216.239.37.101)	216.239.37.101	216.239.37.101
(209.202.196.70)	209.202.196.70	209.202.196.70
(206.65.183.80)	206.65.183.80	206.65.183.80
(209.202.196.70)	209.202.196.70	64.220.205.140
(64.220.205.140)	64.220.205.140	193.113.210.210
(216.239.37.101)	216.239.37.101	193.113.179.98
(193.113.210.210)	193.113.210.210	64.246.24.94
(193.113.179.98)	193.113.179.98	205.180.85.40
(64.246.24.94)	64.246.24.94	205.180.85.46
(205.180.85.40)	205.180.85.40	
(64.246.24.94)	64.246.24.94	
(205.180.85.46)	205.180.85.46	
(64.246.24.94)	64.246.24.94	

Tabla 2. Formateando y filtrando duplicados

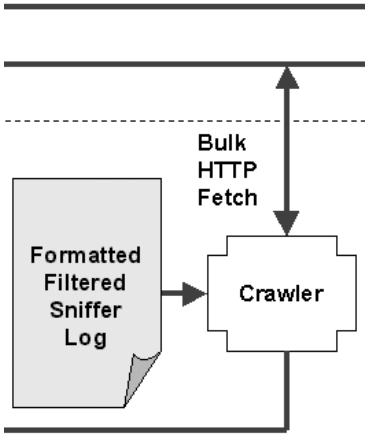
7.6 Interaccion Con El Usuario

Dentro de algunos segundos, según lo demostrado en el cuadro 34, el programa espera para coordinar con el usuario el tiempo en que WebReaper termina su eslabonación.



Cuadro 33. La automizacion de CTSSE – invocando la correa eslabonada y esperando su conclusion

7.7 La Correa Eslabonada De Red

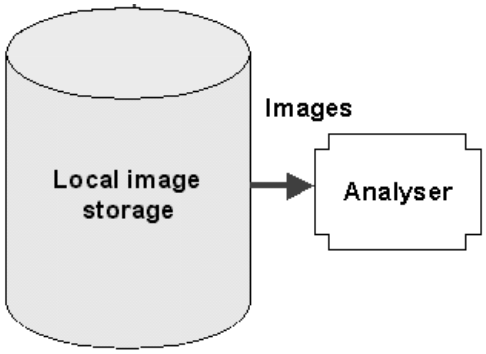


La correa eslabonada de red de CTSSE, *WebReaper*, utiliza *url.tmp* como archivo de comando, cuyo contenido es visible en la ventana izquierda baja del cuadro 35. La correa eslabonada de red se ha configurado para descargar solamente esos archivos con una extensión de JPG, como es visto por el filtro que fija en la ventana derecha baja.

La correa eslabonada de red también asiste participando en una forma de la tarifa falsa constante del alarmar (CFAR), un mecanismo por el que los resultados de los sistémas no estén permitidos saturarse, usado comúnmente en sistémas de RADAR. La correa eslabonada de red puede hacer esto aceptando límites máximos y mínimos del tamaño del archivo así como límites en la duración y la anchura de

banda de transferencias directas. Este arreglo de CFAR se puede ampliar fácilmente para excluir ciertos sitios, dominios o gamas del domicilio IP.

Cuadro 34. WebReaper en accion



A la terminación de la actividad de WebCrawler, típicamente un minuto, el usuario entonces golpea una tecla (cuando en la operación monoestable) para permitir que el CTSSE reasuma el proceso, invocando el esteganalisis, priorizacion de resultados y el resto de la automatización que culmina en los resultados en una página HTML.

7.8 El Esteganalizador

El esteganalizador de CTSSE, StegDetect, se utiliza típicamente como herramienta independiente para detectar el contenido esteganográfico de imágenes. Es capaz de detectar varios diversos métodos esteganográficos para encajar la información ocultada en imágenes del JPEG. Al momento, los esquemas perceptibles son:

i. JSteg,

ii. JPHide (Unix y Windows)

iii. Secretos Invisibles,

iv. Supere en el Acierto 01.3b,

v. F5 (análisis de cabecera),

vi. AppendX, y

vii. Camuflaje.

El CTSSE coordina la entrega al esteganalizador de un listado del directorio de todas las imágenes de JPG recolectadas por la correa eslabonada de red en carpetas de almacenaje local. Cada línea de este listado se asemejará a lo siguiente:

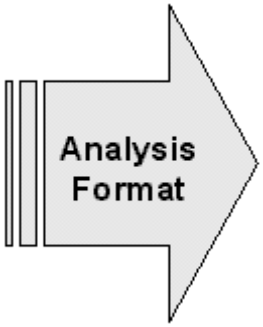
```
C:/Windows/Desktop/Reaped Sites/209.165.20.107/photos/mydog.jpg
```

El CTSSE utiliza estas líneas para localizar y analizar cada localización del archivo de la imagen al esteganalizador para realizar la estego-prueba extensa para medir y divulgar la probabilidad de la presencia de esteganografia, produciendo un archivo de salida cuya línea correspondiente a la de arriba podría ser:

```
C:/Windows/Desktop/Reaped Sites/209.165.20.107/photos/mydog.jpg : jsteg(***)
```

La porción " : jsteg(***)" es agregada por el esteganalizador si el codificador usado se sospecha de ser JSteg y la probabilidad de esteganografia es alta (3 de 3).

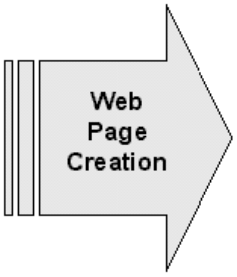
StegDetect funciona desde la línea de comando (una "cubierta" de Windows es incluido pero, aunque es bonita, ofrece mucha menos potencia y facilidad de automatización!). Entre los interruptores aceptados por StegDetect está -sN donde s representa sensibilidad y N es un valor de la coma flotante entre 0,1 y 10,0. Esto permite al CTSSE otro punto de control para CFAR, templado actualmente a mano dentro de detect.bat pero incorporado fácilmente para la automatización con alguna programación adicional.



Para ajustar a formato los resultados del esteganalizador para la presentación del HTML, Strip4.exe elimina los primeros 32 caracteres y los resultados son clasificados reutilizando el mismo Filter.exe usado originalmente para el archivo de la captura, sólo ahora se utiliza tres veces en sucesión para producir 1.tmp, 2.tmp y 3.tmp, cada archivo constitiendo de lineas con ese número de asteriscos.

El CTSSE copia éstos a un archivo de texto en orden reversa usando el comando de la copia del DOS, produciendo una lista alineada de encuentros como lo siguiente. Observe que la correa eslabonada de red podía utilizar operaciones de búsqueda del DNS para proporcionar los domicilios de las páginas en ambos formatos:

```
209.165.20.107/photos/mydog.jpg : jsteg(***)
198.48.120.189/images/mycat.jpg: jphide( ***)
www.funnyguy.com/photos/mycar.jpg : invisible[50](**)
134.64.450.70/family.jpg : outguess(old)(*)
```

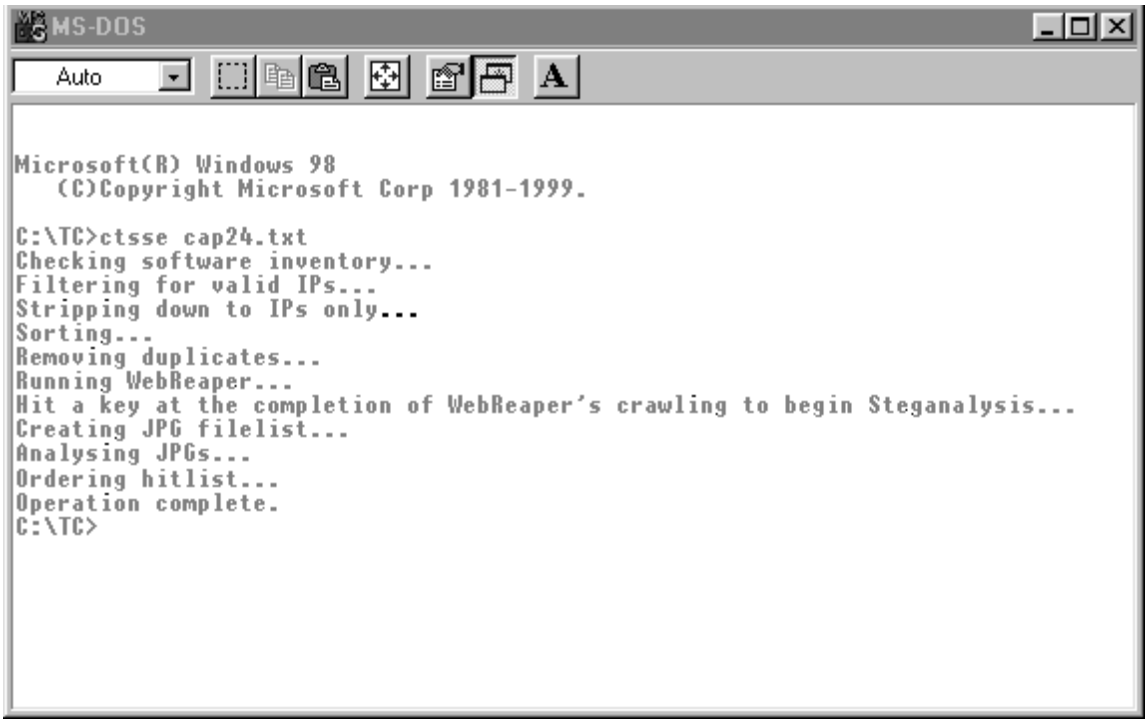


El CTSSE entonces invoca *MakeHT.exe* para tomar esta información y construir dinámicamente una página web por el que la porción del domicilio de estas líneas esté leída y convertida en el formato siguiente del hyperlink del HTML:

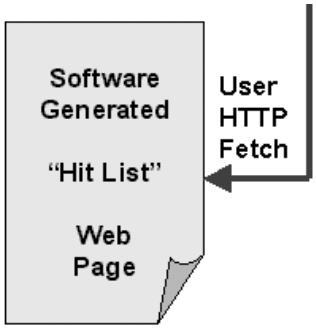
<a href='http://209.165.20.107/photos/mydog.jpg'

target='top'>209.165.20.107/photos/mydog.jpg: jsteg(***)

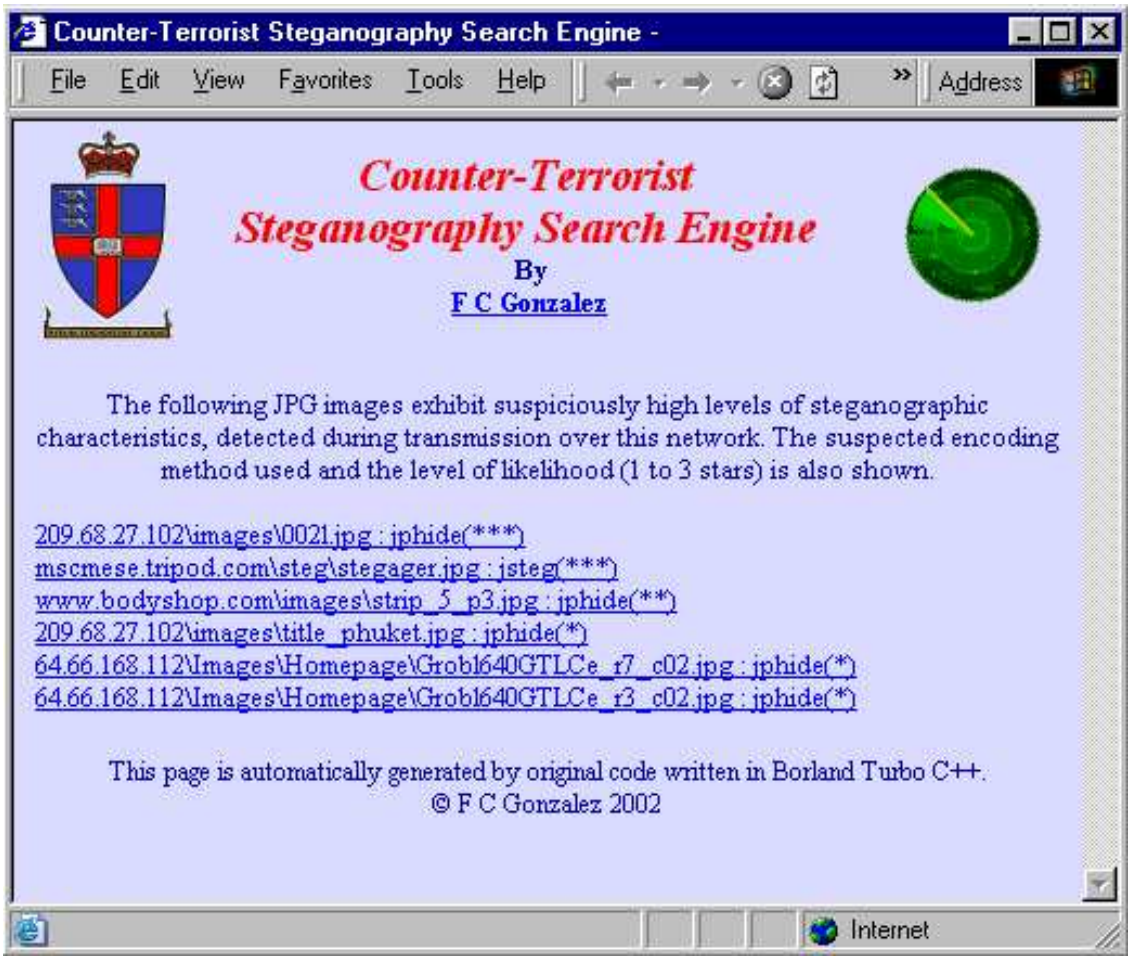
Note que la etiqueta al principio sirve para cerrar el hyperlink anterior, de tal modo simplificando la tarea del formato. El principio y las partes periféricas de la página de resultados codificadas con anticipación se agregan alrededor de este sistema de hyperlinks para producir el producto acabado. La salida en la caja del DOS en el cuadro 36 demuestra el progreso del CTSSE y también incluye los avisos del esteganalizador con respecto a archivos malformados o no-obedientes de JPG si se encuentran cualesquiera.



Cuadro 35. Todos los procesos de CTSSE completados



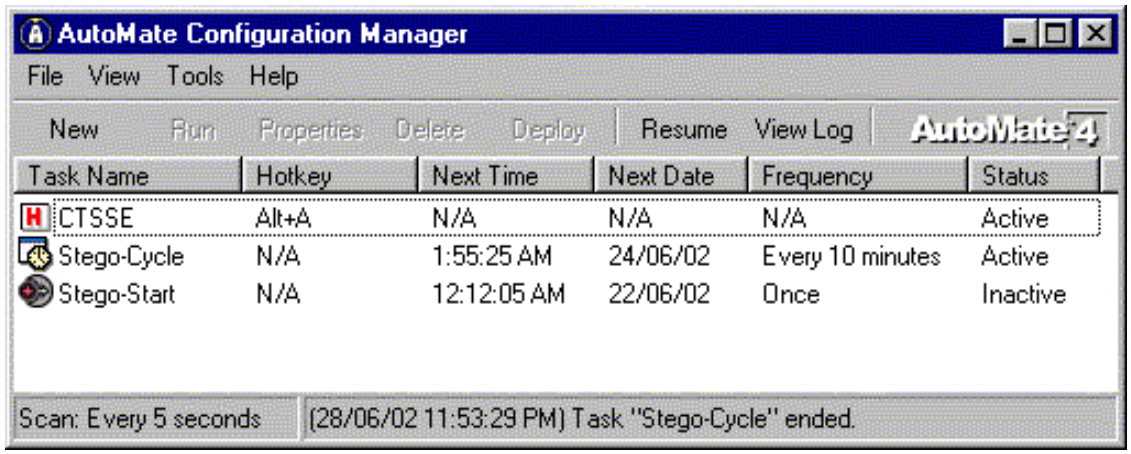
A la vez que todos los procesos de CTSSE terminan en la ventana del DOS, el browser, Internet Explorer, se invoca automáticamente, según lo demostrado en el cuadro 37, para proveer al usuario los resultados del motor de búsqueda.



Cuadro 36. La automizacion de CTSSE – resultados al usuario

7.9 La Operación Continua

Los procesos descritos hasta este punto entregan una solución automatizada que implica el análisis del fichero de diario del sniffer y la creación de una página de los resultados de HTML como salida del análisis. Esto sin embargo representa apenas un caso de la operación y el usuario debe poner en marcha otra vez el proceso para repetir el análisis, quizás de un registro más nuevo de tráfico. La introducción de un planificador para proporcionar el funcionamiento completo y sin atención se juzga de mérito a pesar de el desafío de las cargas variables del tráfico, requiriendo cuidadosamente previsto el retraso entre las tareas individuales dentro del horario.



Cuadro 37. El planificador de CTSSE - Automate

La automatización ya en el lugar para la operación monoestable se acomoda por el abastecimiento de golpes de teclado escritos de una manera que mímica una interacción del usuario. El cuadro 38 demuestra el planificador seleccionado, Automate, con las escrituras funcionando ya en mediados de ciclo. El escritura para la operación de AutoMate está en el apéndice F. Para la claridad, la escritura para cada tarea se presenta aquí en la tabla 4.

Task	Trigger	Script
CTSSE	Hotkey (Alt-A)	`STARTTASK: 0,0,"Stego-Start",0` `STARTTASK: 0,0,"Stego-Cycle",0`

Stego-Start	Once only	`START: "C:\Program Files\Ethereal\Ethereal.exe","",0,"",0,1,0,""`
		`SEND:1,"50",{TAB}{TAB}{TAB}{TAB}{TAB}{TAB}{TAB}{TAB}{SPACE}{TAB}`
		`{TAB}{TAB}{SPACE}~%cs{TAB}{TAB}{TAB}{TAB}{TAB}{TAB}{TAB}`
		`cap.txt~`
		`START: "C:\Program Files\Internet Explorer\Iexplore.exe",`
		`"C:\CTSSE\Hits.htm",0,"",0,1,0,""`

Stego-Cycle	Every 10 mins	`FOCUS: "The Ethereal Network Analyzer",1,0,0`
		`SEND: 1,"50",%fp{TAB}{TAB}{TAB}{TAB}C:\ctsse\cap.txt~`
		`PAUSE: 30 seconds`
		`START: "C:\CTSSE\ctsse.bat","cap.txt",0,"",0,1,0,""`
		`PAUSE: 1 minute`
		`CLOSEWIND: " - WebReaper",0,0,0`
		`FOCUS: "CRAWL",0,0,0`
		`SEND: 1,"50",{SPACE}`
		`PAUSE: 5 minutes`
		`FOCUS: "Counter-Terrorist Steganography Search Engine - ",0,0,0`
		`SEND: 1,"50",{F5}`

Tabla 3. Tareas planificadas para operacion continua

El papel de la primera tarea, *CTSSE*, es simplemente poner en marcha las otras dos en la secuencia correcta, como resultado de golpear la combinación de tecla Alt-A (para completamente automático).

Stego-Start invoca el succionador, Ethereal, genera un archivo inicial de la captura, cap.txt, e invoca el IE para abrir la página de los resultados, Hits.htm.

Stego-Cycle funciona cada 10 minutos, (aunque todos los períodos son completamente configurables) y maneja el bulto de la automatización así como algunas sincronizaciones críticas.

Su papel es:

a. enfocar en la ventana del sniffer,

b. hacer salir los 10 minutos más recientes de oler a cap.txt,

c. esperar de 30 segundos a tener en cuenta la escritura de los registros grandes de las capturas,

d. comenzar ctsse.bat para la automatización monoestable,

e. da un plazo de 3 minutos para que correa eslabonada, WebReaper, recolecte las imágenes de sitios del blanco,

f. cerrar la correa eslabonada después de este período,

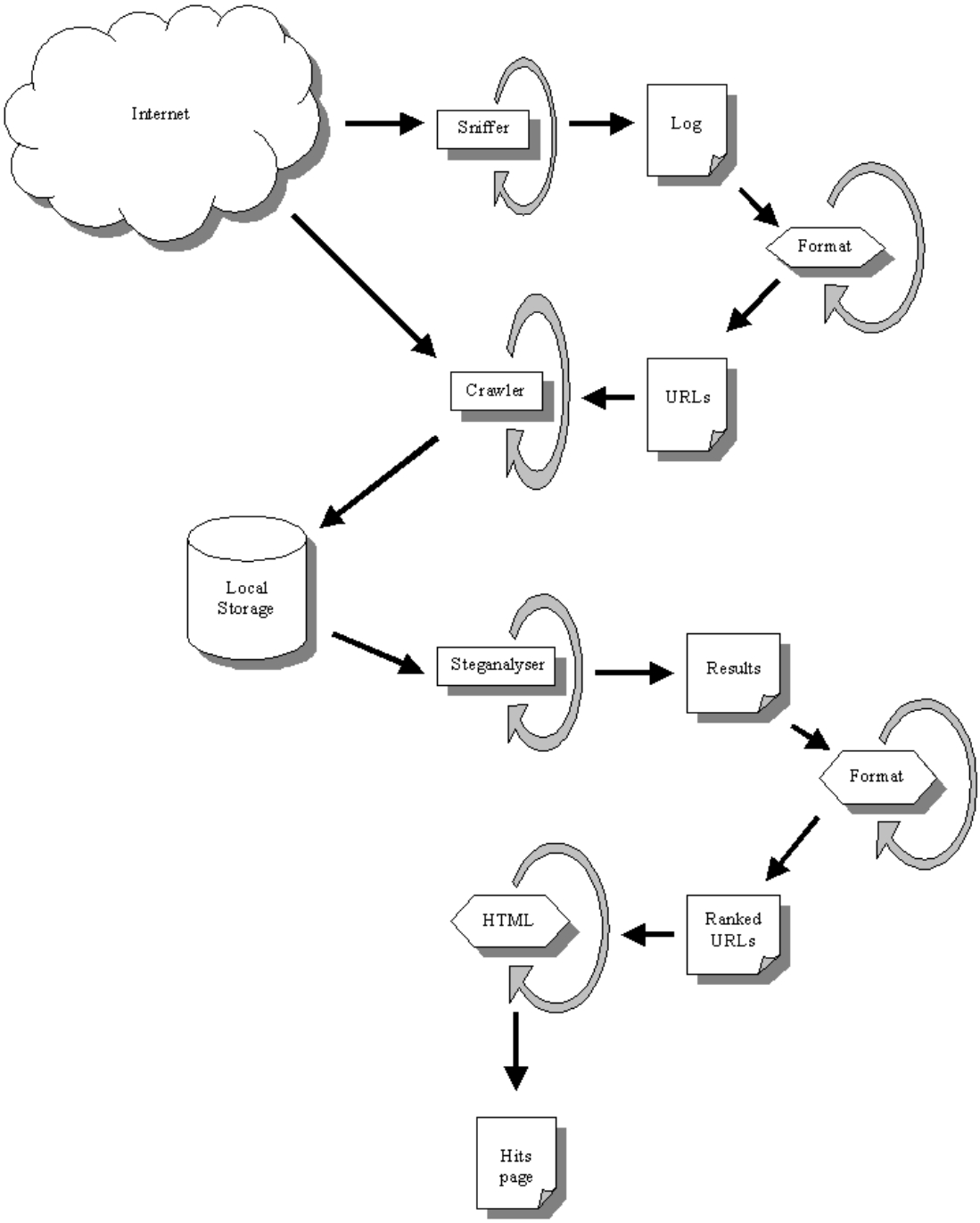
g. enfocar en la ventana del DOS de ctsse.bat, titulada ‘CRAWL’,

h. enviar el golpe de teclado del ESPACIADOR para permitir que el esteganalzador comience,

i. esperar 3 minutos para que el esteganalizador termine, y

j. enfocar en la ventana de IE de Hits.htm y restaurarla con el golpe de teclado F5.

Aunque la escritura para la automatización de ciclo total es breve según lo visto en la tabla 4, la dificultad de la visualización exige un diagrama, en el cuadro 39, para resumir esta operación continua.



Cuadro 38. Automatizacion completa de CTSSE: Modo Continuo

CAPÍTULO 8 RESULTADOS

Este capítulo examina los resultados del funcionamiento de pruebas contra el sistema diseñado para esta tesis. Los resultados de la prueba, presentados en tablas y graficamente en los apéndices G y H respectivamente, se discuten, y se evalúa el funcionamiento del sistema.

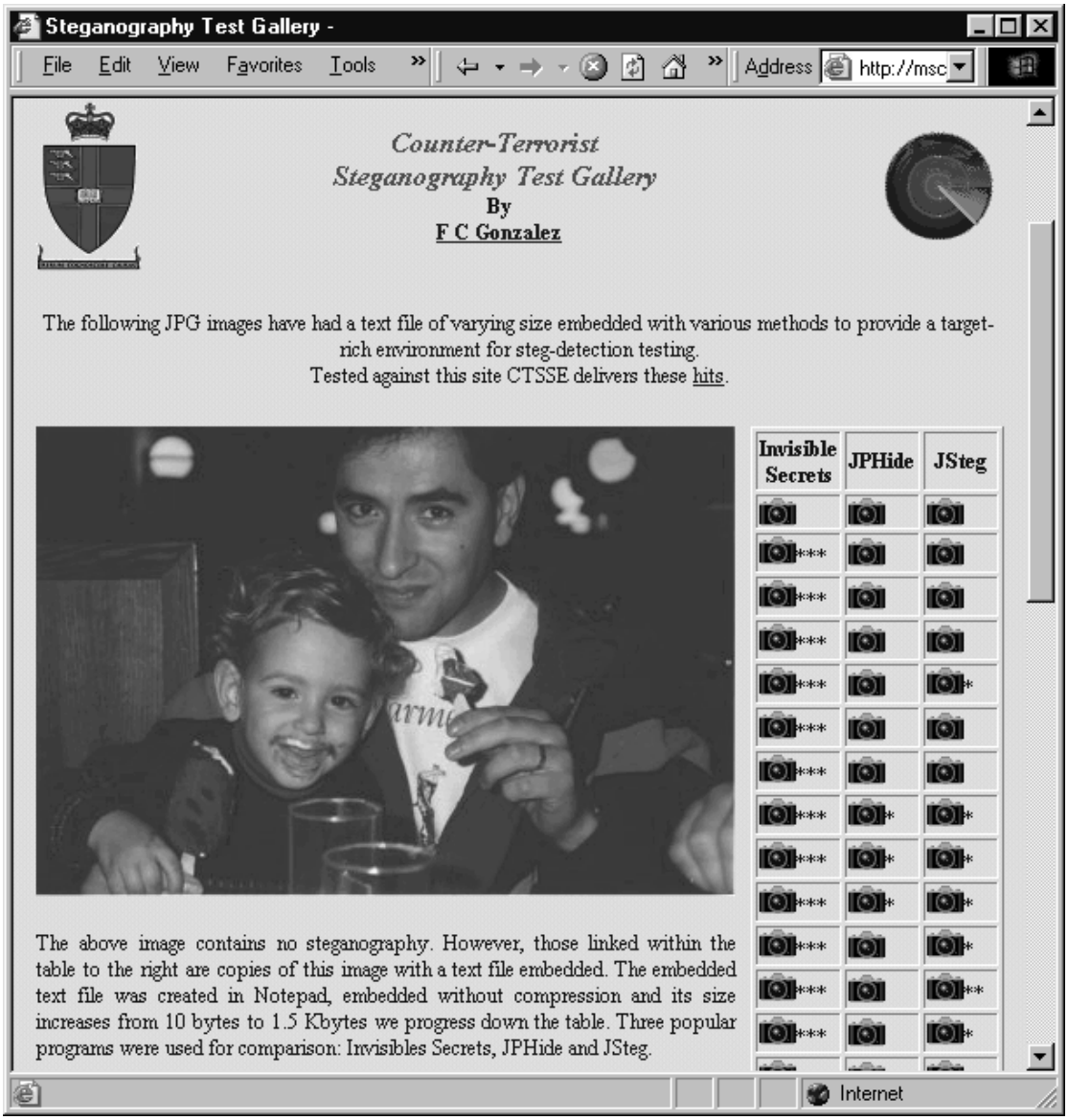
8.1 La métrica del Sistema

El CTSSE ocupa el espacio siguiente:

Programa	**Espacio**	**Comentario**
La base de CTSSE	700K	Agrega 50% tamaño de captura para archivos *.tmp
Ethereal	16.8M	Agrega varios MBytes para las grandes capturas
WebReaper	980K	Agrega tamaño del los imágenes descargados
StegDetect	6.15M	Instalación grande del interfaz gráfico no utilizado
AutoMate	10M	La adición de archivos de escritura es insignificante
Total	**34.63M**	Tamaño de IE, Windows 98 no contado

8.2 Los Datos de Prueba

Para verificar capacidades de CTSSE, la Galería de la Prueba de Esteganografia fue creadas en http://mscmese.tripod.com/steg/gallery/. Esto consiste en varias versiones de la misma imagen de JPG sometida a varios grados de la estego-inserción de un archivo de texto usando una gama de codificadores.



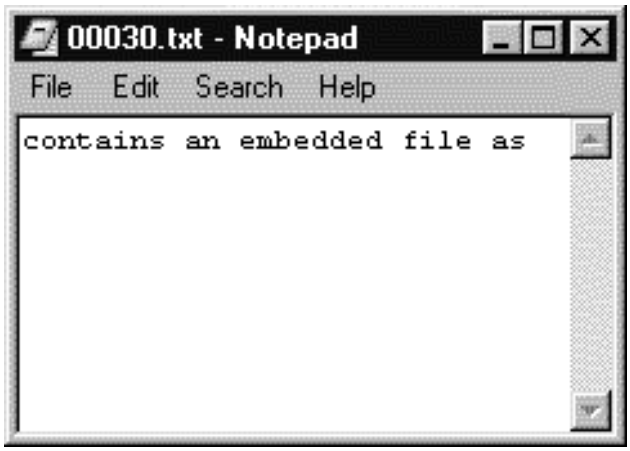
Cuadro 39. La galería de prueba de esteganografía

8.2.1 El portador

El archivo de la imagen del tema de prueba, demostrado en el cuadro 40, era una fotografía verdadera de color (24-valores), 400 pixeles de par en par y 269 pixeles altos. Esto produce una imagen cruda de 322.800 octetos (3 valores del RGB por pixel por la altura por la anchura) mientras que su tamaño como archivo de JPG es 17.683 octetos. Esto demuestra una compresión eficaz de JPG de la imagen al cerca de 18% de su tamaño original.

8.2.2 El Mensaje

Un archivo de texto conteniendo fragmentos de este documento de la tesis fue creado para actuar como el mensaje de la prueba, extendiéndose de tamaño a partir de 10 octetos a 1.500 octetos. Pruebas preliminarias demostraron que, para el tamaño de la imagen usado, esta gama era suficiente para ejercitar los codificadores a sus capacidades máximas y extraer resultados significativos.



Cuadro 40. 30 octetos de mensaje

8.2.3 Los Codificadores

Tres codificadores fueron utilizados, principalmente porque fueron enumerados como perceptibles por *StegDetect* y estaban libremente disponibles, por lo menos sobre una base de ensayo. Éstos eran *Secretos Invisibles*, *JPHide* y *JSteg*.

8.2.4 Los Ajustes De La Detección

La sensibilidad del análisis era variable como valor punto flotante desde 0,1 a 10. Las pruebas fueron funcionadas en 6 niveles de la sensibilidad: 0,1, 0,3, 0,5, 1,0, 2,0 y 3,0.

8.3 Resultados

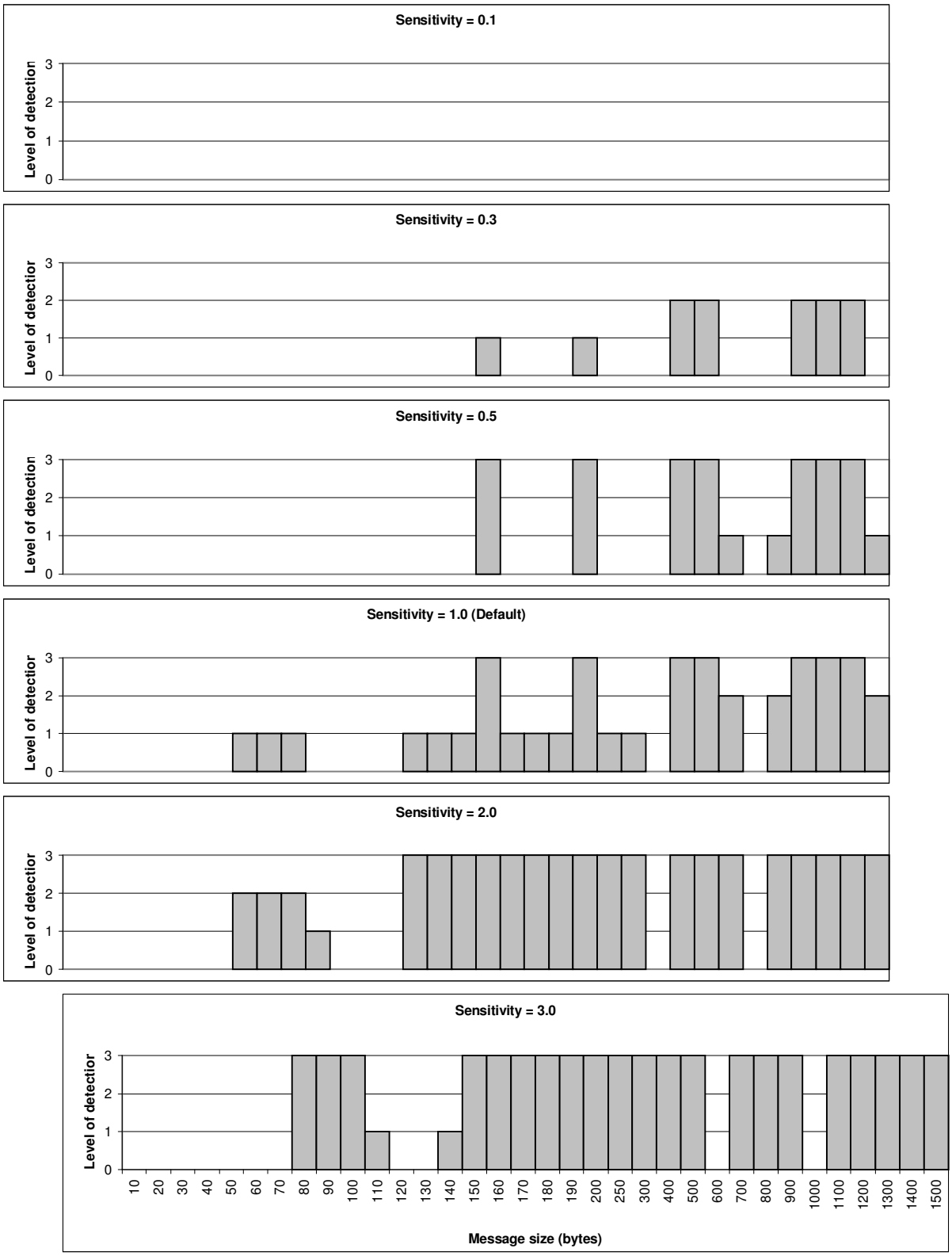
El funcionamiento de cada codificador ofreció diversos resultados llamativos:

a. Secretos Invisibles era perceptible sin importar la sensibilidad para todos los tamaños incluyendo el más pequeño, 10 octetos del mensaje.

b. la detectabilidad de JPHide aumentó constantemente con tamaño y sensibilidad del mensaje.

c. la detectabilidad de JSteg aumentó constantemente con tamaño del mensaje sin importar la sensibilidad.

Un resumen completo de resultados se enumera en el apéndice G. Para ilustrar las diferencias entre los codificadores, cuadros 42, 43 y 44 se incluyen aquí.



Cuadro 41. JPHide: visible con aumentacion constante

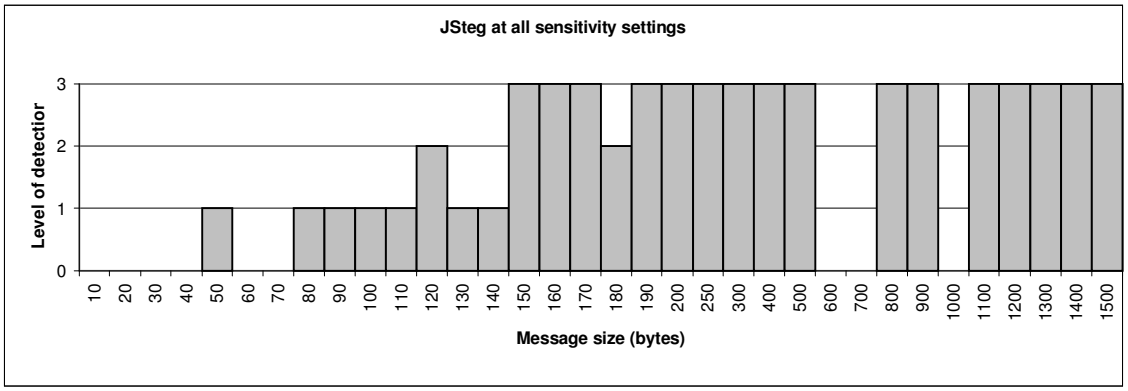


Figure 42. JSteg a todos niveles de sensibilidad

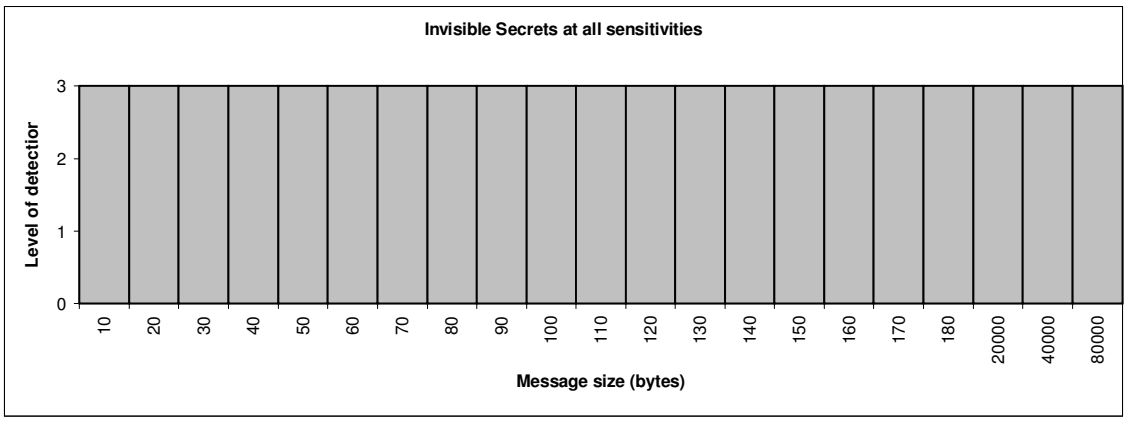


Figure 43. Secretos Invisibles: lejos de ser invisible!

JPHide y JSteg producen una medida de la desigualdad, más evidente de las muescas que corresponden a un tamaño encajado del mensaje de 600 octetos y 1000 octetos. Ésto se piensa ser una característica de esta combinación particular del mensaje sin comprimir y el imagen de cubierta.

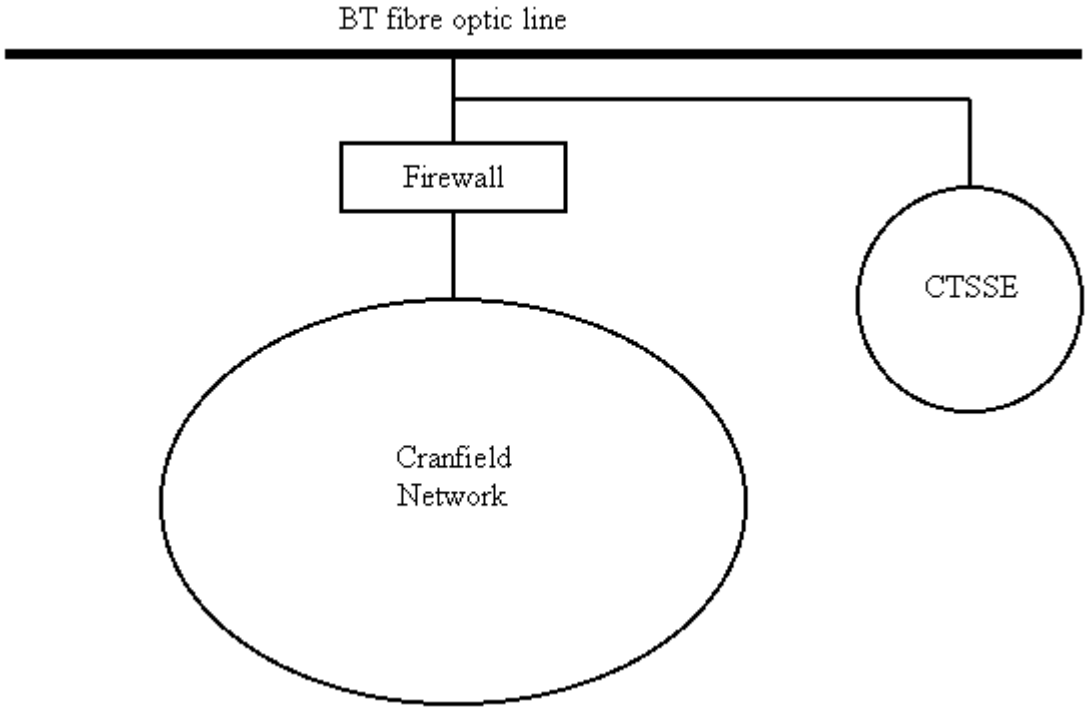
Las pruebas preliminares fueron funcionadas con una gama de diversas imágenes de cubierta, demostrando que estas muescas se podrían considerar una forma de ruido estadístico del muestreo, y confirmando que la tendencia está generalmente para la mayor visibilidad con mayor tamaño del mensaje.

Dado los resultados antedichos, y el hecho de que el golpe más común (y por lo tanto probablemente la alarma falsa más común) era del tipo JPHide, este codificador se recomienda sobre los otros. Irónicamente, Secretos Invisibles es muy lejos de invisible al CTSSE. Puede o puede no tener cifrado fuerte como virtud, aunque este punto está más allá del alcance de este asunto puesto que no se relaciona terminantemente con la esteganografia por la definición. Sin embargo, como una herramienta de la esteganografia él ha fallado en la primera prueba: el seguir ocultado.

8.4 La Prueba de la Anchura Alta de Banda

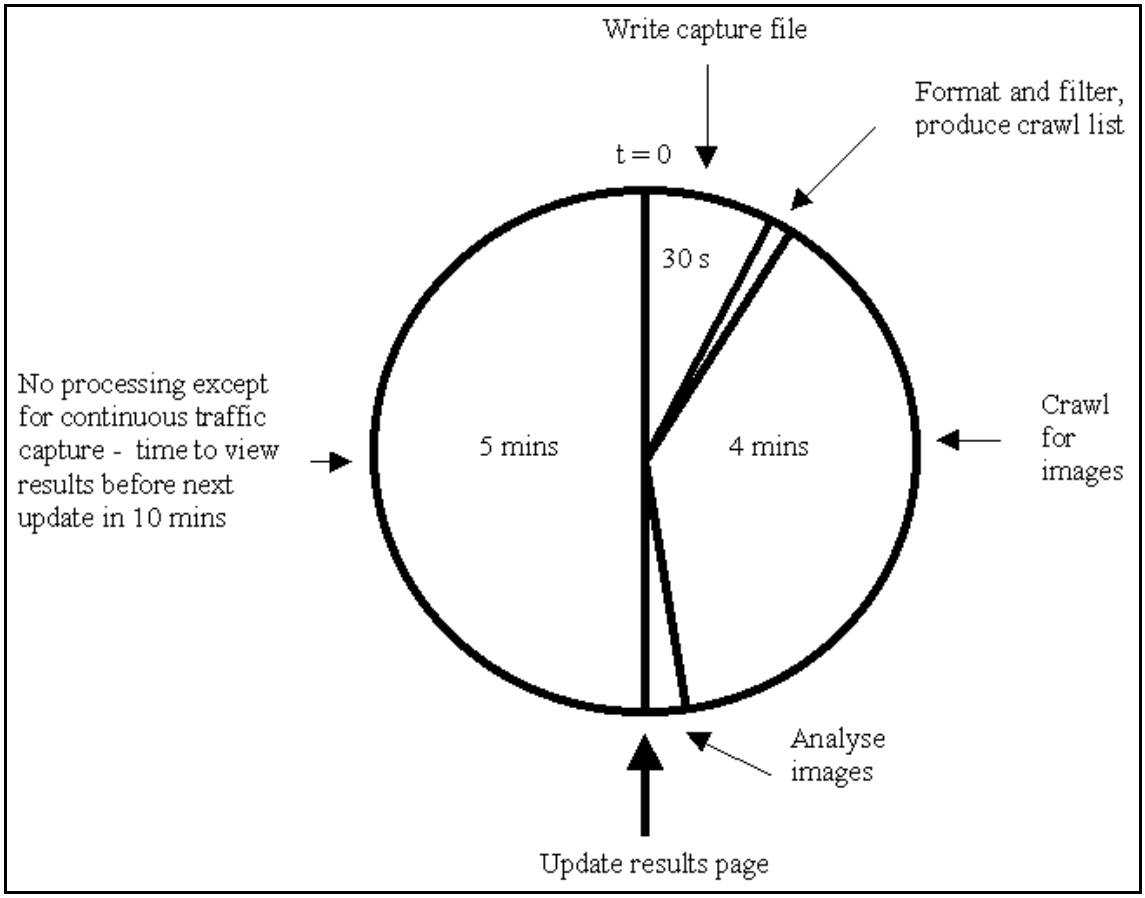
8.4.1 La Captura de Cranfield

El autor fue dado una oportunidad rara de conectar el CTSSE con el acoplamiento fibroóptico de alta capacidad de British Telecom (BT) justo fuera del cortafuego en el centro de informática de Cranfield University a aproximadamente las 3 de la tarde un jueves. El significado de esto es que los datos capturados en esta conexión son representantes del tráfico del Internet a través del Reino Unido, no limitado apenas al tráfico que entra o que se va vía el cortafuego. Una analogía apropiada puede ser una de asomar sobre Swindon y de mirar todo el tráfico de vehículo en el autopista M4 así como eso que entra en y que deja Swindon. El cuadro 45 ilustra este arreglo.



Cuadro 44. La captura de Cranfield

El tiempo disponible para esta prueba era extremadamente limitado. Una tentativa fue hecha de funcionar el CTSSE en modo continuo pero la cantidad de tráfico expuesta al CTSSE era tan grande que el proceso de escribir el archivo de la captura al disco era más largo que anticipado. Esto requirió cambiar el tiempo para escribir el archivo de captura a algo en la vecindad de 3 minutos más bien que los 30 segundos originalmente considerados adecuados (véase la tabla 4). Esto tenía un efecto de la continuación de requerir que la sincronización de los procedimientos del formato y de filtrado esté ajustada por consiguiente, dejando mucho menos tiempo que el adecuado para arrastrar la red. Este efecto de conexión en cascada significó que era necesario ajustar la duración del ciclo entero a base de la observación de cada duración discreta de los procesos. Más bien que utilizar el tiempo limitado disponible para ajustar éstos con el ensayo y el error, el autor consideraba más sabio utilizar la oportunidad de capturar tanto tráfico como sea posible para un análisis más tarde.



Cuadro 45. El previsto ciclo de 10 minutos para el modo continuo

Esto no se debe necesariamente considerar una falta de la automatización en modo continuo, puesto que la automatización todavía funcionaba y ha funcionado ya perfectamente con cargas más ligeras de tráfico. Sin embargo, en el centro de informática, el análisis y los procesos de la presentación fallaron en sincronizar con el proceso de la captura, significando que las actualizaciones a la página de los resultados no representaron los 10 minutos completos de tráfico o, aún peor, los procesos de formatear causaban de vez en cuando violaciones de compartimiento con la aún no terminada escritura del archivo de la captura.

En resumen, el plazo dado para escribir el archivo de la captura al disco fue subestimado, requiriendo que este parámetro específico esté ajustado en la escritura de la automatización.

Para tomar la mayor ventaja del tiempo que seguía habiendo de esta oportunidad, el CTSSE entonces fue funcionado en modo monoestable para capturar aproximadamente 20 minutos de tráfico HTTP GET de petición en forma de un archivo de texto de 240Megaoctetas. El inesperado tamaño grande del archivo hizo necesario la transferencia a un nodo de red alterno y el archivo de la captura fue escrito eventualmente a disco compacto (CD). En una tentativa de examinar el contenido del archivo de captura a este punto, el archivo resultó demasiado grande para que Ethereal (el programa que lo creó), Libreta, WordPad o Word lo lean en un sistema de Windows.

Sin embargo, el software de base de CTSSE, diseñado alrededor del concepto de usar la sola corriente de entrada y salida para eliminar restricciones del tamaño del archivo y de los recursos, podía producir una lista de los archivos para el esteganalisis en el plazo de 12 segundos en un Pentium III con 64Megaoctetas de la memoria de acceso al azar (RAM), el mismo PC que no podía abrir el archivo de otra manera. Ésta era una ventaja agradable de las eficacias de recursos derivado del acercamiento adoptado para la programación de base, el de construir un ejecutable simple para cada tarea discreta. Este mismo PC, situado en la sala de clase de MESE para presentar conferencias, fue utilizado para todas las medidas subsecuentes.

La etapa siguiente del ciclo de operación de CTSSE era arrastrarse la red usando esta lista nuevamente creada de aproximadamente 1.000 localizaciones de imagenes. Templando la correa eslabonada de red para que la velocidad óptima descargue solamente los archivos especificados de la imagen (límite de la profundidad del arrastre de 0) las imágenes fueron descargadas adentro apenas bajo 4 minutos, usando la anchura de banda disponible en el campo de Shrivenham. ¡El mismo proceso procurado en la casa del autor en una conexión de 44KBPS (mil valores por segundo) todavía no fue terminado y fue abandonado después de 4 horas!

El ciclo completo de análisis de fin-de-captura hasta la presentación de los resultados analizados,ilustrados en el cuadro 47, fue alcanzado en los 5 minutos escritos como plazo para la operación continua. Esto demuestra que el único parámetro que requiere el ajuste acertado para la operación continua es el plazo para escribir el archivo muy grande de captura al disco, una plazo que será enteramente dependiente en la cantidad de tráfico del HTTP:REQUEST interceptado. El plazo tomado para arrastrarse a terminar, aunque es adecuado en este ensayo, puede también cambiar. Sin embargo, la correa eslabonada de red puede aceptar un límite de tiempo para su arrastre, un límite que no era posible fijar para la escritura real del archivo de la captura.

8.4.2 Resultados Verdaderos

La captura del tráfico británico del Internet proporcionó una penetración rara y fascinadora en los hábitos de hojear del público británico. Observe que el CTSSE registra las localizaciones de las imágenes solicitadas y de ninguna manera identifica la persona que hace la petición. El apéndice J enumera las localizaciones de la imagen detalladamente e incluye los resultados de la prueba para la gama completa del nivel de la sensibilidad del esteganalisis del 1 hasta el 10, ampliando grandemente la resolución original de la graduación de los esteganalyizadores de solamente una, dos o tres estrellas. El cuadro 47 demuestra los resultados de esta captura con la sensibilidad de 1, revelando entre otras cosas el alto nivel del interés que el público británico tiene en Elizabeth Hurley, por lo menos para los 20 minutos examinados.

8.4.3 Las lecciones aprendidas

La experiencia era instructiva en destacar una característica opcional importante de la operación de Ethereal, la de emplear un almacenador intermediario de tipo anillo para capturar tráfico. El manual de Ethereal explica que, usando esta opción del almacenador intermediario de anillo, un usuario puede fijar un criterio que especifique cuando Ethereal escribe a un archivo de captura. El criterio puede ser cualquiera de:

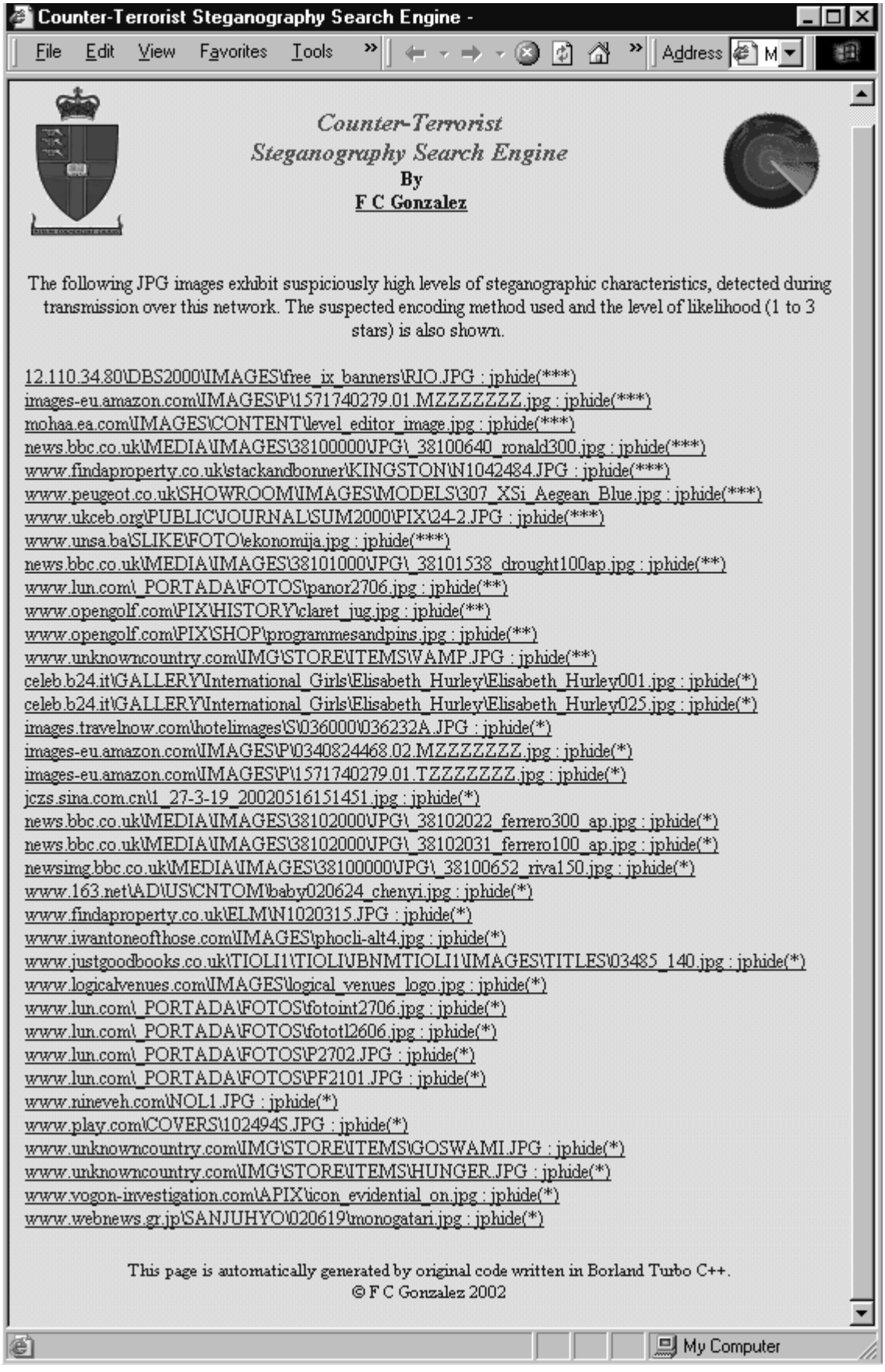
a. duración: parar de escribir a un archivo de captura después de un número especificado de segundos, o

b. tamaño de archivo: parar de escribir a un archivo de captura después de que alcance un tamaño especificado en kilooctetas.

Cualquiera de estos criterios habría sido una mejora extensa sobre la tentativa de predecir la cantidad de tráfico encontrada, inevitablemente imprevisible.

Ironicamente, puesto que esta característica trabaja con Windows NT pero se inhabilita en Windows 98, había oportunidad escasa de tomar la ventaja completa de ella.

Otro factor importante es que, debido a la dificultad de transportar el archivo grande de la captura, casi había caducado una semana antes de que la recuperación y el análisis de la imagen fueran hechos. Esto habría podido degradar el valor de los resultados, dado que la ventaja dominante de CTSSE sobre otras estrategias de la búsqueda es la interceptación en tiempo real de las imágenes sospechadas.



Cuadro 46. Producto de CTSSE para la captura de Cranfield

CAPÍTULO 9 LA CONCLUSIÓN

Este capítulo repasa las punterías y los logros de la tesis comparando la estrategia y el resultado del desarrollo. La flexibilidad y la adaptabilidad del diseño se explica y las oportunidades dentro del diseño para la innovación futura se exploran, incluyendo una lista de otras recomendaciones.

9.1 La Estrategia De Desarrollo

Para establecer una investigacion para esta tesis, varias partes importantes requirió la atención cercana. La primera pregunta hecha era porqué un motor de búsqueda de Esteganografia era juzgado deseable. Esto fue contestada por los miembros militares en el personal de la inteligencia de la defensa (DIS), el abastecedor principal de la inteligencia estratégica de la defensa al ministerio de la defensa. Según DIS, la dificultad principal con la detección de la comunicación secreta es la masa escarpada de los datos que se examinarán. "Estrechando el campo" fue sugerido como quizás el paso más importante hacia el éxito.

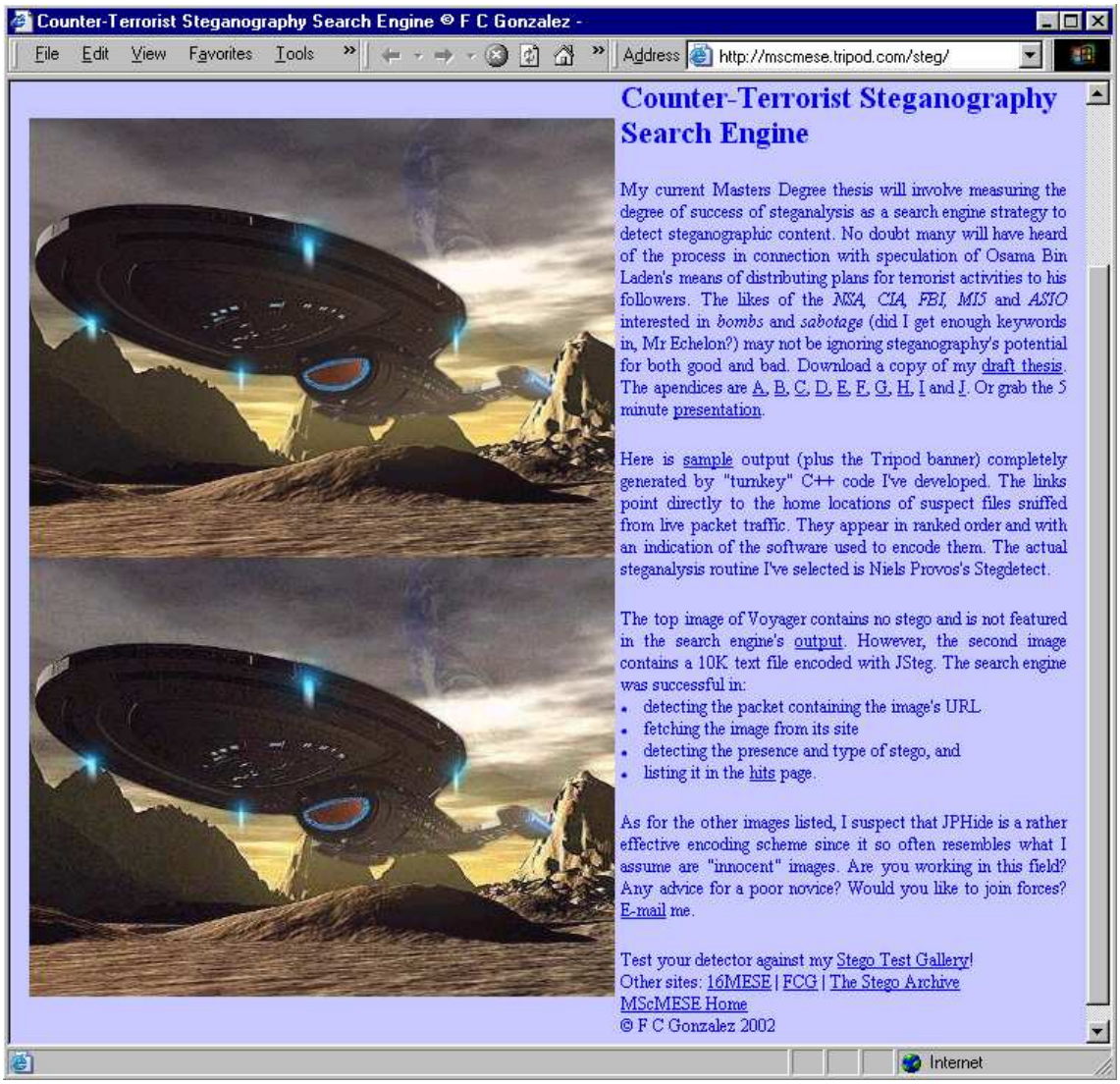
Era necesario investigar la naturaleza y el comportamiento de la esteganografia basada en la red para explorar sus debilidades potenciales. Como un medio dependiente pesadamente en un sistema de comunicación público, el motor de búsqueda existente y las estrategias de la vigilancia fueron examinados para su conveniencia como armazones de la detección.

Una vez que esta etapa fuera alcanzada, era necesario innovar una nueva estrategia que empleaba el mejor de los métodos existentes cuando sea apropiado. Esta nueva estrategia combinó el pensamiento innovador con una gama de las herramientas especializadas del software de una manera que nunca había sido hecho antes.

Porque la esteganografia existe en muchas formas, esta tesis requirió la selección de un medio eficiente y probable para la distribución de la esteganografia. Para limitar el desarrollo a el de un prueba-de-concepto sin duplicación de trabajo, un solo formato de archivo y un solo protocolo fueron seleccionados para ser supervisados.

Habiendo hecho cuidadosa evaluación y selección de componentes de software, el diseño y la construcción de los programas de interacción fue hecho para coordinar y controlar los varios componentes.

Con un sistema completo trabajando suavemente, el requisito siguiente era la creación de los datos de prueba y el desarrollo de los resultados significativos de la prueba. Los datos de prueba fueron cargados sobre una pagina fabricada para la tesis (http://mscmese.tripod.com/steg/) según lo demostrado en el cuadro 48 (este sitio ahora contiene los documentos de la tesis, la presentación, acoplamientos de interés, la galería de la prueba y los resultados de prueba publicados).



Cuadro 47. La página web de la tesis

9.2 El Resultado Del Desarrollo

El más notable de los resultados del desarrollo es que el CTSSE comprueba con éxito el concepto de una herramienta que intercepte la esteganografia de imagen ocultado en la red. La característica que distingue primariamente el CTSSE contra otras estrategias de la búsqueda es que alcanza este "Estrechar el campo", interceptando el domicilio del imagen en el momento que está en tránsito a través del Internet, discutible un salto astronómico en eficacia sobre otras estrategias.

Otras características del CTSSE son:

a. El sistema fue diseñado y construido sin coste financial. Todo el software, enumerado en el apéndice I, era freeware, shareware o escrito por el autor de la tesis.

b. El analizador de paquetes (succionador), Ethereal, fue seleccionado por su excelente estabilidad y capacidad para las cargas de circulación densa.

c. La correa eslabonada de red, WebReaper, fue seleccionada por sus opciones de filtración, estabilidad de programa y empleo fácil y detallado.

d. El esteganalizador, StegDetect, fue seleccionado por su capacidad de aceptar una lista de archivos de imágenes candidatos como parámetro de la entrada de la línea de comando y para su amplio espectro de la detección de siete diversos esquemas de codificación.

e. En armonía con el familiar e intuitivo aspecto del motor de búsqueda, un constructor del HTML para crear una página de resultados basada en la red era escrito como ejecutable en el idioma C++. Esto hace los resultados automáticamente examinables a través del Internet, si se desea.

f. El sistema puede funcionar en modos monoestable y continuo, teniendo en cuenta para que un registro particular de la captura sea analizado o la operación desatendida y/o alejada, respectivamente. Para este propósito (y porque el planificador de Windows es espantosamente inadecuado), Automate fue instalado y la automatización necesaria fue programada en el.

g. El uso de executables discretos, escritos en C++, permite al sistema ser extremadamente robusto, particularmente al manejar ficheros de diario grandes de haber grabado una circulación densa. Cada ejecutable se diseñó para trabajar con una sola corriente de entrada y salida, eliminando el problema de ficheros temporales o de la asignación de la memoria virtual que se puede esperar de un programa escrito para funcionar de otra manera.

9.3 El Desarrollo Adicional

Este asunto tiene el potencial para el desarrollo adicional en un ambiente donde el tema se está desarrollando rápidamente. El CTSSE ha utilizado una combinación de software de tercera persona libre ligado junto con manipulación de archivos en C++, la manipulación de datos y la automatización escrita para desarrollar una herramienta de prueba-de-concepto. Las áreas siguientes se juzgan dignas de la nueva visita para la mejora adicional:

9.3.1 Desarrollo Del Sistema

Dos opciones necesitan la consideración particular con respecto a la automatización total del sistema:

a. desarrollar y hacer funcionar el sistema entero en un PC de UNIX o de Windows NT, de tal modo haciendo uso la opción del almacenador intermediario de anillo de Ethereal y permitiendo que el sistema haga frente a las cargas variables, y/o

b. habiendo comprobado el concepto, diseñar un nuevo sistema en el local sin una confianza pesada en las herramientas de los terceros. Un reajuste completo para substituir las herramientas de los terceros sería un ejercicio intensivo del diseño del software que puede requerir a un equipo de

estudiantes y del personal y, mientras que es de mérito para un MSc o un PhD en informática, podría ser visto como demasiado intensivo para una tesis de la ingeniería de sistemas.

El refinamiento continuo del sistema existente, con su arquitectura abierta basada en bloques de edificación relativamente simples, puede ser más satisfecho a la disciplina de la ingeniería de sistemas y al horario relativamente breve de la tesis del MSc. Hay ventajas inherentes en adoptar software de los terceros en que está desarrollado y probado generalmente sobre una sección representativa grande de ambientes y de circunstancias para el momento en que se haga disponible.

9.3.2 Selección de Software de Terceros / Desarrollo de Análisis Interno

StegDetect es ambos muy capaz y simple de utilizar y realiza todo el esteganalisis dentro del CTSSE. Sin embargo, segun los estegocodificadores nuevos aparecen en el mercado, el CTSSE necesita mantener su importancia y eficacia empleando una gama de esteganalizadores para ensanchar su espectro de detección. Por lo tanto, cualquier otro esteganalizador nuevo o existente se debe repasar y considerar para la inclusión en los reajustes futuros del CTSSE como biblioteca de "plug-ins". Esto se puede también combinar con el diseño interno de los algoritmos de detección donde no están convenientes o disponibles del dominio public.

Los nuevos algoritmos se pueden agregar en secuencia dentro del archivo de hornada detect.bat sin ninguna necesidad de modificar el software de base.

9.3.3 Una Resolución Más Alta de Graduación

Haciendo uso del ajuste de sensibilidad del analizador, el autor podía desarrollar una resolución más alta de los resultados para la prueba de la alta anchura de banda que la ofrecida por cualquier sola graduación. Dado que la duración de análisis para las capturas hasta muy grandes era solamente algunos segundos, puede ser de mérito introducir esta resolución más alta reajustando el software de base para funcionar una serie de pruebas a través de la gama entera de la sensibilidad y compilando los resultados finales como la suma de éstos, de la misma manera que se demuestra en el apéndice J.

9.3.4 La selección del medio del portador

Esta tesis, como prueba-de-concepto en funcionamiento, se ha concentrado en el formato de imágen conveniente más popular, el JPG, transmitido vía el protocolo más popular, HTTP. Otros formatos de archivo dignos de la investigación incluyen:

a. Otras imagenes, por ejemplo el GIF, PNG25 y BMP,

b. películas tales como películas Audio Video de Interpolación (AVI), películas Apple QuickTime (MOV) y archivos del Grupo de Expertos de la Película (MPG/MPEG),

c. sonido y música tal como formas de onda de Microsoft (WAV), archivos de la Voz de Creative (VOC) y archivos MPEG-1 Audio de la Capa 3 (MP3), y

d. los documentos tales como texto (TXT), Word de Microsoft (DOC) y los Documentos Portátiles del Acróbata (PDF).

Estos nuevos formatos de archivo pueden ser incluidos cambiando los casos actuales de "JPG" dentro de los ajustes de filtro del eslabonador y dentro del archivo de hornada detect.bat, otra vez sin ninguna necesidad de modificar el software de base.

Otros protocolos dignos de escrutinio adicional incluyen:

a. Simple Mail Transfer Protocol (SMTP),

b. File Transfer Protocol (FTP), y

c. emuladores terminales tales como Telnet.

Estos protocolos se pueden acomodar dentro del CTSSE modificando casos de "HTTP" dentro de los ajustes de la detección de Ethereal, de nuevo sin cualquier necesidad de modificar el software de base.

El CTSSE se ha diseñado del principio para ser tan flexible y acomodado de nuevos requisitos de la búsqueda como sea posible.

9.3.5 Incorporando Desciframiento

Una extensión natural para el CTSSE puede ser la adición del ataque del diccionario, utilizando la agrieta a fuerza bruta de contraseña contra esas imágenes sospechadas de esteganografia. StegDetect incluye StegBreak, escrito expresamente para este propósito. Se sugiere esto como un punto excelente de el cual comenzar este desarrollo.

9.4 El Resumen

La investigación, el análisis y la discusión presentada aquí culmina en una conclusión. El Motor de Búsqueda Contraterrorista de Esteganografia se ha comprobado como idea, como sistema de trabajo y como nuevo y fascinador asunto de investigación y de desarrollo, evolucionando constantemente con la tecnología que utiliza y mereciendo atención en el futuro.

REFERENCIAS

1 Kelly, J., Grupos Del?Terror Ocultan Detrás Del Cifrado De la Red?, Los E.E.U.U. Hoy, El 2 De Mayo 2001 http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm

2 Venzke, B., De Grupos Del?Terror Ocultan Detrás Del Cifrado De la Red?, Los E.E.U.U. hoy, 2 de mayo 2001 http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm

3 Rivest, R. de L.?Chaffing y aventando: Secreto sin el cifrado?, El laboratorio del MIT para la informática, 22 estropea 1998

4 ?Histories de Herodotus?, S. de 440BC

5 Singh, Libro Del Código Del?The: La evolución del secreto de la reina de Maria de Scots a la criptografía del quántum?, Doubleday, 1999

6 Johnson, el N. F. y Jajodia, S.?Steganalysis de imágenes crearon con el software actual de Esteganografia?, Céntrese para el sistema de información seguro, universidad del masón de George, http://isse.gmu.edu/~csis

7 Hetzl, S., encuesta sobre el?A de Esteganografia?, http://steghide.sourceforge.net/esteganografia/survey/node5.html, El 8 De Enero 2002

8 Se maravillan, L., Boncelet, G., Retter, C., Imagen Esteganografia Del Espectro Del?Spread?, Transacciones de IEEE en el proceso de imagen, vol. 8, no 8, agosto 1999

9 Westfeld, dr A.?Attacks en Esteganografia?, Universidad técnica de Dresden, http://wwwrn.inf.tu-dresden.de/~westfeld/attacks.html

10 Hetzl, S., encuesta sobre el?A de Esteganografia?, experimentación del dominio de http://steghide.sourceforge.net/esteganografia/survey /, el 8 de enero 2002

11 los muchachos del nPhaze, del?Frequency?, http://wwwdsp. rice.edu/courses/elec301/Projects01/steganosaurus/

12 Peines, G., Analizador De Red?Ethereal?, el?Google de http://www.ethereal.com

13 Avanzó búsqueda de la imagen?, Google, http://www.google.com/advanced_image_search?hl=en

14 Kawaguchi, E., principio del?The de la segmentación de la complejidad del Pedacito-Plano basaron Esteganografia?, Instituto de Kyushu de la tecnología, http://www.know.comp.kyutech.ac.jp/BPCSe/BPCSe-principle.html, 28 de oct 2001

15 Graham, R., seguridad del?With y justicia para todos?, DevTalk, Septiembre 2001

16 Rohde, L., Ley Del E-mail de?UK Alcanza los E.E.U.U.?, Infoworld, el 1 de sept. 2000 centro neto excesivo de Snooping de

17 ?Questions?, BBC noticia, del 6 el parlamento?European

18 de de junio 2002 divulga sobre la existencia del ECHELON?, El 18 De Mayo 2001

19 Barry, R. Y Campbell, D.?Echelon: Prueba de su existencia?, Noticias De ZDNetUK, El 29 De De junio 2000

20 Digimarc Corporation, Corporación Del?Digimarc: El Revelador Principal Del Watermarking Digital?, http://www.digimarc.com

21 Bradley, P.?The avanzó el manual de Searcher?s del Internet?, Asociación que publica, 2002

22 Orenstein, R., el generador irresponsable de la estadística del Internet, Anamorph, http://www.anamorph.com/docs/cgi/all.cgi

23 Skolnik, M.?Introduction de la biblioteca a los sistemas del RADAR?, McGraw-Colina, segunda Edition, 1981, pp 392-395

24 Provos, N., detección del?Esteganografia con StegDetect?, gráficos portables de la red de http://www.outguess.com

25 (png), formato de la imagen de Turbo-Studly del?A con la compresión de Lossless?, http://www.libpng.org/pub/png/

Apéndice A: Un Catálogo Software De Esteganografia Del Freeware

Blindside del (http://www.blindside.co.uk). Blindside es una utilidad de la comando-li' nea que oculta archivos en BMP y tiene cifrado opcional. También disponible están Linux, el HP, Solaris, y las versiones de AIX, con el GUI ventana-basado prometido pronto.

Freeware de los secretos de BMP (http://www.pworlds.com/products/i_secrets.html). Los secretos de BMP son un producto BMP-basado del stego para Windows con un interfaz decente y una capacidad que oculta muy grande (el ~65% del archivo del portador). Incluye el cifrado y la capacidad incorporados de ocultar datos dentro de las subzonas específicas de la imagen.

Freeware del camuflaje (http://www.camouflagesoftware.co.uk/). El camuflaje es un programa basado Windows interesante que permite que usted oculte archivos revolviéndolos y después uniéndolos al extremo del archivo de su opción. El archivo camuflado después parece y se comporta un archivo normal y se puede almacenar o emailed sin la atracción de la atención. Trabaja para bonito mucho cualquier tipo del archivo. La protección de contraseña es incluida. El archivo ocultado puede ser detectado examinando a los datos crudos del archivo y viendo que el archivo

ocultado se ha agregado después de los datos normales del portador, pero éste aparecerá solamente como guirigay puesto que se cifran los datos. No es la forma más segura de esteganografia, pero qué carece en fuerza es compensa en ser discreto usando los archivos rutinarios (es decir palabra doc.).

Freeware del contrabando (http://www.biol.rug.nl/hens/j/contrabd.exe). Éste es un programa basado Windows que encaja y extrae cualquier archivo concebible en 24-bit BMPs e incluye código de fuente. Edición del infierno del contrabando (http://www.biol.rug.nl/hens/j/che_xmas-beta.zip). Esto es un programa basado BMP del stego con el cifrado fuerte construido adentro. Tiene un programa de la disposición y un interfaz utilizador agradables y está libre. ¿Todavía está en beta, pero solamente adentro de modo que carezca helpfiles? fácil utilizar.

Freeware del mensajero v1.0a (http://pages.prodigy.net/robyn.wilson/courier.zip).

Tecnologías de DataMark (http://www.datamark-tech.com/products/products.htm) Commercialware. DataMark Techologies tiene cuatro productos del stego que oculten la información en formatos de BMP, de JPG, del GIF, de TGA, de TIF, del png, de MIDI, de WAV, de AVI, y del MPEG. - StegComm para la comunicación confidencial de los multimedia, - StegMark para el watermarking digital de los medios de la memoria numérica, - StegSafe para la memoria numérica y el acoplamiento, y - StegSign para las transacciones del e-comercio.

Freeware de D.P.T. (Herramientas) De la Aislamiento De Datos (http://www.xsâll.nl/~bernard/home_e.html). DPT tiene cifrado fuerte con esteganografia opcional de BMP. Los datos esconden (http://hosted.barrysworld.net/minimice/Body/Programs/ds_info.html) Shareware $25, ocultan archivos en BMP o archivos de base de datos y vienen con la protección de contraseña. (http://members.tripod.com/~Nikola_Injac/stegano/) freeware C.C.-Steganograph. Por Nikola Injac, éste es un pequeño, fácil utilizar el programa DOS-basado del stego que oculta datos en imagen de PCX archiva.

Freeware del sobre del cuadro Digital (http://www.know.comp.kyutech.ac.jp/BPCSe/Dpenve/DPENVe-home.html). DPE es un programa de Windows 95/98/NT basado en la técnica de BPCS-Steganographic que fue inventada por Eiji Kawaguchi en 1997. Es un programa BMP-basado del stego que puede ocultar una cantidad increíble de datos en un solo archivo, a menudo 50-100% de la imagen originial sin cambiar el tamaño del archivo. Éste es la primera vez que el grupo de BPCS ha lanzado el codificador (con el decodificador) y debido a las preocupaciones de la seguridad, el exe expirará en abril de 2002. Encaje IFF24 y encaje 256V, (http://us.aminet.net/pub/aminet/util/crypt/) freeware, los datos de la piel en IFF24 y 256 imágenes del color, respectivamente.

El freeware vacío de Pic (http://www.crtelco.com/~robertw/), proporciona esteganografia GIF-basado simple. Cifre Pic (ftp://ftp.elet.polimi.it/mirror/Winsite/win95/miscutil/encpic13.exe) Shareware $10. Con cifre Pic, usted puede ocultar datos en 24 imágenes del pedacito BMP. Tiene ventaja agregada del cifrado de datos de ofrecimiento vía el algoritmo de BlowFish. Versión francesa también disponible.

Freeware de EZStego (http://www.stego.com/). EZStego es un uso GIF-basado del stego de Romana Machado, el autor de Stego para el mac. Tiene funciones steganographic similares como su precursor Mac-basado, pero se escribe en la lengua plataforma-independiente de Java en lugar de otro.

Freeware De FatMacPGP 2,6,3 (ftp://ftp.euro.net/d6/pgp/OLD/mac/Fatmacpgp263v16.sea.hqx). FatMacPGP 2,6,3 es la versión más reciente de MacPGP optimizada para PowerMacs. Tiene una opción de Stealth que pele toda la información de jefe que identifica a la licencia solamente los datos cifrados en un formato conveniente para el uso steganographic.

Freeware de FFEncode (http://www.rugeley.demon.co.uk/security/ffencode.zip). Éste es un pequeño programa interesante del DOS que oculta un archivo en un archivo del texto usando un código Morse de caracteres NULOS. Desempaquete el archivo del cierre relámpago y mecanografíe FFENCODE o FFDECODE en el aviso del DOS para los parámetros simples de la línea de comando. GIF-él-Para arriba (http://crypto.radiusnet.net/archive/steanography/gif-it-up/) freeware v1.0. Éste es un programa basado Windows 95 del stego que oculta datos en archivos del GIF. Tiene un interfaz que mira profesional e incluye un programa pulido de la instalación y una opción del cifrado de datos.

Freeware de Gifshuffle (http://www.darkside.com.au/gifshuffle/). Gifshuffle es un programa de la comando-li' nea-solamente para Windows que encubra mensajes en imágenes del GIF mezclando el colourmap. El cuadro sigue siendo visiblemente intacto, sólo la orden del color dentro de la gama de colores se cambia. Trabaja con todas las imágenes del GIF, incluyendo ésos con la transparencia y la animación, y además proporciona la compresión y el cifrado del mensaje encubierto.

Freeware de GZSteg (http://linkbeat.com/files/). GZSteg oculta datos en archivos comprimidos GZip y fue compilado para el DOS por Preston Wilson.

Freeware de Hide4PGP v2.0 (http://www.heinz-repp.onlinehome.de/Hide4PGP.htm). Hide4PGP v2.0 de Heinz Repp es un programa steganographic de la comando-li' nea para Windows, el DOS, OS/2, y Linux que oculte datos dentro de archivos de BMP, de WAV, y de VOC. Se diseña para ser utilizado con el PGP y Stealth, pero también trabaja bien como independiente programa. La versión 2,0 tiene varias nuevas características, incluyendo un nuevo formato del stego que sea mucho más

robusto contra conversiones del formato - solamente los formatos de la compresión del lossy soltarán los datos ocultados. La fuente también se incluye y debe compilar en cualquier plataforma sin problemas importantes. Piel y freeware de la búsqueda v4.1b (ftp://ftp.ntua.gr/pub/crypt/esteganografia/hdsk41.zip). Las manos proporcionan los datos hiding/seeking usando archivos de la imagen del GIF. Estos programas del DOS toman los datos, generalmente texto, incluyendo el texto cifrado, y los ocultan en un archivo del GIF.

Hide and Seek v5.0, freeware (http://www.rugeley.demon.co.uk/security/hdsk50.zip). La versión más última de la Hide and Seek se ha reajustado totalmente. Sigue siendo un programa basado DOS, pero ahora incluye un interfaz utilizador (no más de operaciones de la línea de comando) para ocultar el Info en archivos del GIF. Oculte y busque para Win95 (ftp://ftp.hacktic.nl/pub/crypto/incoming/hideseek95.zip) Shareware $15.

HSWin95 es un programa BMP-basado dla esteganografia de Colin Moroney, el autor de las versiones del DOS de la piel y de la búsqueda. Esta versión es una considerable intensifica de sus esfuerzos anteriores. Su interfaz que mira profesional hace fácil utilizar. Las opciones del archivo y el método del cifrado del jefe del blowfish que limpian son primas agregadas.

Oculte en freeware del cuadro 2,0 (http://www.brasil.terravista.pt/Jenipabu/2571/e_hip.htm), es un Win9x pequeño, fácil de utilizar o programa del stego del DOS con el cifrado del blowfish que oculta datos en imágenes de BMP.

In Plain Sight, freeware (http://www.9-yards.com/software.html), es la esteganografia de BMP con la protección de contraseña. En el cuadro (http://www.intar.com/ITP/itpinfo.htm) Shareware $25. ITP es un programa del stego de Windows 95-based que oculta datos en imágenes de BMP. Ofrece llaves únicas múltiples así que usted puede cifrar los datos previstos para los recipientes múltiples en el mismo archivo. Tiene un interfaz de la fricción y de la gota y puede generar una imagen fractal al azar para utilizar como imagen del recipiente, si está necesitado.

El freeware invisible del cifrado (IVE) (http://www.fitin.com/), es un pequeño programa steganographic fresco que trabaja en GIFs en páginas de la red. Después de chascar 3 veces en la imagen cifrada sospechada en el browser del Internet, un contraseña-password-textbox aparece. Después de incorporar la contraseña correcta las ventanas ocultadas de text/message aparecen. Una Java pequeña el applet incluido preve el acceso público y el desciframiento en línea de los browsers estándares de WWW en todas las plataformas. IVE es fácil de dirigir y el explicar del uno mismo. Versión Bandera-libre (libre) invisible $19,95 de Sponsorware de los secretos (http://www.innovatools.com/software/isecrets/). ES es un pedazo interesante de software en que es el primer software bandera-apoyado del stego que ha aparecido. Como tal, usted tiene estar en la red para utilizar lo (así que las banderas puede cargar). Usted puede pagar un honorario modesto

($19,95) para perder el ads, que pueden estar bien digno de él pues hay un número de características de mérito en este software. Éstos incluyen JPG, BMP y el png que oculta, el cifrado fuerte, la ayuda del ftp, el archivo de la temperatura que limpia, y la generación falsa del mensaje. También se incluye la capacidad de agregar los módulos adicionales del archivo del cifrado y de la imagen.

Los secretos invisibles 3 (http://www.neobytesolutions.com/invsecr/index.htm) Shareware $34,95, cifran y ocultan archivos en el JPEG, el png, BMP, el HTML y WAV. También proporciona el cifrado fuerte (Blowfish, Twofish, RC4, Cast128, y GOST), una desfibradora, y un encargado y un generador de la contraseña. Interconecta agradable con el explorador de Windows vía menús sensibles al contexto del derecho-tecleo.

JP Hide and Seek, freeware (http://linux01.gwdg.de/~alatham/stego.html). JPHS es un programa del stego de Win95/98/NT con un GUI de los ninguno-volantes que oculte datos en el formato siempre popular de la imagen de JPG. Hay porciones de versiones de los programas similares disponibles en el Internet pero JPHIDE y JPSEEK son algo especiales. El objetivo de diseño no era simplemente ocultar un archivo pero hacer algo esto de una manera tal que sea imposible probar que el archivo del anfitrión contiene un archivo ocultado. Dado una imagen visual típica, una tarifa baja de la inserción (debajo del 5%) y la ausencia del archivo original, no es posible concluir con ninguna certeza de mérito que el archivo del anfitrión contiene datos insertados. Mientras que el porcentaje de la inserción aumenta la naturaleza estadística de los coeficientes del JPEG diferencia de "normal" hasta el punto de levante la suspicacia. Sobre el 15% los efectos comienzan a llegar a ser visibles al ojo desnudo. Por supuesto algunas imágenes están mucho mejor que otras cuando están utilizadas un archivo del anfitrión - el un montón de detalle fino es bueno. Un cielo azul despejado sobre un paraíso cubierto nieve del esquí es malo. Una cascada en un bosque es probablemente ideal. Su tamaño pequeño es una prima importante como él fácilmente los ajustes en un disco. Utiliza el cifrado también, pero no menciona qué tipo. DOS y versión de Linux también disponible.

Freeware de JSteg (http://linkbeat.com/files/). Por Derek Upham, esto oculta datos dentro del formato popular de JPG. Por favor la nota, JSteg no lee directamente archivos del JPEG como entrada. Antes de ocultar los datos en un JPG archivan, usted necesitarán excepto que archivo en el formato de TGA (targa). Después de que los datos sean stego' d en la imagen, el archivo de salida que resulta estará en el formato de JPG, con todas las ventajas de la compresión que JPG exige. Previamente solamente disponible para Unix, Preston Wilson y Randall Williams han sido bastante bueno compilar esta versión del DOS para su placer del stego. Si usted planea funcionar esto bajo DOS pelado (no una cáscara del DOS de Windows), después descargue este archivo de la ayuda.

Jsteg Shell v2.0, Freeware (http://members.tripod.com/esteganografia/stego/jstegshella.zip). JSteg Shell es un interfaz de Win95/98/NT (no Win2000) para funcionar DOS de JSteg, un programa por

Derek Upham que oculte datos en el formato siempre popular de la imagen de JPG. Incluye 40 el encrytion del pedacito RC4, determinación de la cantidad de datos que un JPG puede ocultar de antemano, y las opciones seleccionables por el usuario de JPG (grado del IE de la compresión). La cáscara de JSteg tiene un pulido, fácil utilizar el interfaz que hace con el DOS de JSteg un broche de presión. La cáscara de Jsteg viene con los executables del DOS, y el instalador toma el cuidado de todos los detalles de la disposición.

Freeware de JSteg (http://us.aminet.net/pub/aminet/util/crypt/jstegbin.lha). Versión de Amiga del programa popular del DOS de la línea de comando para ocultar archivos en JPGs. MandelSteg (http://www.sevenlocks.com/steganog/MandelSteg1.0.tar.gz) es un programa basado GIF del stego.

Freeware mímico de las funciones (http://www.nic.funet.fi/pub/crypt/old/mimic/MimicTR.sit.hqx). Las funciones mímicas son un programa basado texto pseudo-random del stego que utiliza el grammer libre del contexto para ocultar datos. Usando los diccionarios customizable, uno puede ocultar cualquier archivo con el texto que ése suena como Shakespeare, Fables de Aesop, u otros estilos interesantes.

Freeware de MP3Stego (http://www.cl.cam.ac.uk/~fapp2/esteganografia/mp3stego/). MP3Stego tiene versiones del GUI y de la comando-li' nea que oculten la información en los archivos MP3, que son las pistas de sonidos del archivo de WAV se comprimen que usando el formato audio de la capa III del MPEG. Ofrecen el sonido de la calidad de near-CD en un cociente de la compresión de 11 a 1 (128 kilobites por segundo). MP3Stego ocultará la información en los archivos MP3 durante el proceso de la compresión. Los datos primero se comprimen, se cifran y después se ocultan en la corriente del pedacito MP3. Aunque MP3Stego se ha escrito con usos steganographic en mente pudo utilícese como un sistema de la marca del copyright para MP3 archiva (débil pero aún mucho mejor que la bandera del copyright del MPEG definida por el estándar). Cualquieres uncompress de la lata del opositor la corriente y los recompress del pedacito él; ¿esto suprimirá la información ocultada? ¿éste es realmente el único ataque que sabemos todavía? pero a expensas de pérdida severa de la calidad. MP3Stego está disponible pues los executables de Windows 95/98/NT y código de fuente de Linux/Unix (encontrado en el archivo del cierre relámpago).

Nicetext (http://www.ctgi.net/nicetext/) es un stego basado texto pseudo-random usando el grammer context-free y diccionarios customizable supera en el acierto v0.2 (http://www.outguess.org) es una herramienta steganographic universal que permite la inserción de la información ocultada en los pedacitos redundantes de las fuentes de datos. La naturaleza de la fuente de datos es inaplicable a la base de supera en el acierto. El programa confía en los tratantes específicos de los datos que extraerán pedacitos redundantes y los escribirán detrás después de la modificación. ¿En esta versión

se apoyan los formatos de la imagen de PNM y del JPEG? el único producto del stego de JPG imperceptible por Stegdetect (véase abajo).

Freeware Paranoico (ftp://ftp.hacktic.nl/pub/crypto/macintosh/Paranoid1.1.hqx). El paranoico es sobre todo un programa del cifrado que permite que usted cifre archivos con IDEA, el DES triple, y un algoritmo escrito por el autor Nathan Mariels. Es un programa dla esteganografia en que permite que usted oculte archivos en sonidos. Viene con la función que limpia del archivo incorporado.

PGMStealth
(ftp://ftp.ntua.gr/pub/crypt/mirrors/idea.sec.dsi.unimi.it/rpub.cl.msu.edu/crypt/other/PG
M.stealth.c.gz) oculta datos en imágenes greyscale de PGM.

Freeware PGPn123 (http://www.pobox.com/~alpha1). PGPn123 es sobre todo un programa de la cáscara del sujetapapeles del PGP "Windows" que hace con el PGP para Eudora, el agente, o el correo de Pegasus muy fácil. La versión más última incluye una opción dla esteganografia se ponga en ejecucio' n que después de que el mensaje sea PGP cifrado. El algoritmo se basa en el programa de Texto, haciendo parecer cifrado de los archivos del texto algo entre los libs enojados y la mala poesía.

Freeware De Piilo (ftp://ftp.ntua.gr/pub/crypt/esteganografia/piilo061195.tar.gz). Oculta datos en imágenes greyscale de PGM.

Freeware Bastante bueno Del Sobre v1.0 (http://www.rugeley.demon.co.uk/security/pge10.zip). El sobre bastante bueno (PGE) es un programa basado DOS que oculta un mensaje en otro archivo por el método muy simple de añadir el mensaje al archivo, y después adición de un octeto 4 poco número endian que señale al comienzo del mensaje. Un programa UNPGE del compañero recupera el mensaje. PGE se puede utilizar con los archivos gráficos (GIF y JPG) o cualquier otro archivo binario, incluyendo archivos de COM y de EXE.

Freeware Bastante bueno Del Sobre v2.0 (http://members.tripod.com/~afn21533/pge20.zip). El sobre bastante bueno v2.0 es un programa del stego que oculta datos en virtualmente cualquier archivo. La versión 2 incluye un nuevo programa, PGECLEAR, para automatizar el claro del uso posterior del sobre.

Freeware grande del fabricante del juego del SAM (http://www.scramdisk.clara.net/play/playmaker.html). El fabricante grande del juego de Sams es un programa basado Windows que convierte el texto arbitrario a un juego de diversión. Es solamente práctico para los mensajes pequeños, si no la salida "juego" es absolutamente grande.

Freeware de Scramdisk (http://www.scramdisk.clara.net/). Scramdisk es Windows 95/98 programa basado del cifrado del disco que permita la creación y el uso de impulsiones cifradas virtuales.

Éstos se pueden crear en un archivo del envase en un disco duro ajustado a formato GORDO, en una partición vacía, o almacenar en los pedacitos bajos de un archivo audio de WAV (que le haga esteganografia). Tiene un interfaz pulido y viene con un número de algoritmos estándares del cifrado de la ' industria ' , incluyendo Triple-DES, IDEA, MISTY1, Blowfish, TÉ, y cuadrado. Está también disponible como EXE basado francés.

Freeware de Scytale (http://scytale.rever.fr/main.html). Scytale es un programa de la cáscara del PGP que tiene la característica agregada de datos que ocultan en imágenes de PCX. Otras fuerzas del programa incluyen un limpiador incorporado y las capacidades y él del modo tratamiento por lotes está disponibles en 16 y 32 versiones del pedacito.

Freeware de SGPO (http://glu.freeservers.com/sgpo.htm). SGPO (SteganoGifPalatteOrder) es un programa basado v1.1 de Java con un interfaz agradable que oculte mensajes en imágenes del GIF mezclando el colourmap. El cuadro sigue siendo visiblemente intacto; solamente la orden del color dentro de la gama de colores se cambia. S-Mail (http://www.privacysoftware.com/) Shareware v1.3 $195 - v1.4 $695 (alta seguridad). El s-Mail es un programa del stego que funciona bajo todas las versiones de Windows y del DOS que cifrado fuerte y compresión de las aplicaciones para ocultar archivos en archivos de EXE y del DLL. ¡Sí, usted puede ocultar archivos dentro de programas de funcionamiento completos! Tiene un interfaz utilizador agradable y toma medidas de asegurarse de que su esquema que oculta no es detectado por los exploradores del patrón o de la secuencia de la identificación.

Freeware de la nieve (http://www.darkside.com.au/snow/index.html). La nieve es un programa basado texto del stego por Matthew Kwan que encubra mensajes en archivos del texto por las lengüetas y los espacios de la adición en el extremo de líneas. Las lengüetas y los espacios son invisibles a la mayoría de los espectadores del texto, por lo tanto a la naturaleza steganographic de este esquema de codificación. La nieve incluye una función de la compresión para no prohibirle al stego más información en un archivo dado y tiene algunas funciones crypto básicas vía el algoritmo del HIELO. Compruebe fuera del homepage para saber si hay DOS, Java applet de Java, y versiones del código de fuente.

Esconder-él freeware v1.1 (http://www.smalleranimals.com/stash.htm). Esconda es un programa basado 95/98/NT simple del stego de Windows que permitirá que usted oculte y que extraiga cualquier fichero de datos dentro de un archivo perfectamente normal de BMP, del GIF, del tiff, del png o de PCX. No aparece tener ninguna características adicional del cifrado.

Freeware de Stealth (http://www.radiusnet.net/crypto/archive/pgp/pgp_stealth/). Stealth es un filtro simple para el PGP que pela toda la información de jefe que identifica a la licencia solamente los datos cifrados en un formato conveniente para el uso steganographic. Es decir, los datos se pueden

ocultar en imágenes, archivos audio, archivos del texto, archivos del cad, y/o cualquier otro tipo del archivo que pueda contener datos al azar, después enviar a otra persona que pueda recuperar los datos del archivo, de los jefes de la fijación, y del decrypt del PGP él. Stealthencrypt (http://www.stealthencrypt.com/) Commercialware.

Stealthencrypt es parte de la habitación de la seguridad del Internet que ofrece esteganografia de BMP y de TIF y utiliza el cifrado triple del DES y de Blowfish. El software está disponible en los E.E.U.U. y el Canadá en los almacenes del software tales como CompUSA, mejor compra, Walmart, y blanco.

Freeware de Steganos v1.4 (ftp://ftp.ntua.gr/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/steganos.zip). ¡Steganos es un pequeño, fácil utilizar programa basado DOS del stego por Fabian Hansmann que oculte datos dentro de BMP, de VOC, de WAV e incluso de archivos de ASCII!

Habitación de la seguridad de Steganos 3 (http://www.steganos.com/) Shareware/Commercialware $49,95 (mejora $29,95). La habitación de la seguridad de Steganos 3 es una completa, fácil utilizar habitación de la seguridad que utiliza el encyption fuerte y técnicas steganographic para ocultar datos en archivos del gráfico y del sonido. También se incluye la caja fuerte (encryptor de la impulsión), el destructor del rastro del Internet, la desfibradora del archivo, el cifrado del E-mail, al encargado de la contraseña y la fijación de el ordenador. Disponible en las versiones inglesas, alemanas, italianas, francesas, y españolas, Steganos apenas guarda el conseguir mejor.

Freeware de Steganosaurus (ftp://ftp.ntua.gr/pub/crypt/esteganografia/stego.shar.gz). Un texto basó programa del stego.

Freeware de Stegdetect (XSteg) (http://www.outguess.org/detection.php). Stegdetect es una herramienta automatizada para detectar el contenido steganographic en imágenes. Es capaz de detectar varios diversos métodos steganographic para encajar la información ocultada en imágenes del JPEG. Actualmente, los esquemas perceptibles son JSTEG, JPHIDE (Unix y Windows), secretos invisibles, y superan en el acierto 01.3b.

Freeware de StegFS (http://www.mcdonald.org.uk/StegFS/). Un sistema de ficheros steganographic para Linux.

Steghide 0,3, freeware del lanzamiento 1 (http://www.crosswinds.net/~shetzl/steghide/index.html). Steghide, por Stefan Hetzl, es un uso de la comando-li' nea que ofrece datos que ocultan en los archivos de BMP, de WAV y del AU, cifrado de Blowfish, 128 hashing del pedacito MD5 de passphrases a las llaves de Blowfish y distribución pseudo-random de pedacitos ocultados en los

datos del envase. Steghide se escribe en ANSI C así que el código de fuente debe compilar en muchos sistemas. Los binaries de Precompiled están disponibles para Windows y Linux.

Stego (ftp://ftp.ntua.gr/pub/crypt/mirrors/utopia.hacktic.nl/crypto/MAC/Stego1a2.sit.hqx) Shareware $15. Stego es una herramienta dla esteganografia que le permite encajar datos en archivos del formato de Macintosh PICT, sin cambiar el aspecto o el tamaño. Así, Stego se puede utilizar como "sobre" para ocultar un fichero de datos previamente cifrado en un archivo de PICT, haciéndolo mucho menos probablemente que se detectará (disponible como a binhexed el archivo del Stuffit).

Freeware de StegoDos (ftp://ftp.ntua.gr/pub/crypt/esteganografia/stegodos.zip). Este codificador basado DOS del cuadro consiste en un grupo de programas diseñados le dejó capturar un cuadro, codificar un mensaje en él, y exhibirlo para poderlo capturar otra vez en otro formato con un programa de tercera persona, después lo recobre y descifre el mensaje puesto previamente dentro de él.

Freeware de Stego Wav (ftp://ftp.externet.hu/pub/mirror/sac/sound/stegowav.zip). Escrito por Peter Heist, Stego Wav es un programa basado del stego de Java 1,0 que oculta datos en archivos 16-bit de WAV.

Freeware De StegoWav (http://www.geocities.com/SiliconValley/9210/stegowav.zip). StegoWav oculta datos en archivo de WAV y ha agregado el cifrado.

Freeware de StegParty (http://www.fasterlight.com/hugg/projects/stegparty.html). A textbased el stego que utilizaba cambios pequeños en el deletreo y puntuación.

Freeware de Stella (http://www.stella-esteganografia.de/). Stella es un programa del stego de la Java-base que utiliza dos técnicas del stego del differenct para ocultar datos en formatos del archivo de GIF/BMP/JPG. Tiene cifrado dominante privado y puede ocultar mensajes de la trampa también.

Freeware de StirMark (http://www.cl.cam.ac.uk/~fapp2/software/StirMark_3_1_79.zip) y de UnZign (http://www.cl.cam.ac.uk/users/fapp2/software/unZign12.zip). Stirmark y UnZign son los programas de la comando-li' nea que quitan la información del copyright y del stego' d de archivos. Como muchos otros programas que se rompen estableció mecanismos de la seguridad, estos programas se piensan demostrar la debilidad en algoritmos actuales de modo que motiven a las compañías para desarrollar tecnologías más robustas del watermarking y dla esteganografia.

Freeware De los Taburetes 4 (ftp://ftp.ntua.gr/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/s-tools4.zip). Los taburetes v4 son una herramienta basada 95/NT excelente dla esteganografia de Windows que oculta archivos en los archivos de BMP, del GIF, de WAV y el espacio inusitado en diskettes. Los taburetes v4 tienen un número de nuevas mejoras sobre la versión anterior.

Freeware de TCP/IP (http://www.psionic.com/papers/covert/covert.tcp.tar.gz). Datos de Conceales dentro de los jefes de la habitación del protocolo de TCP/IP.

TextHide (http://www.texthide.com) Demo/Commercialware libre $39 (Lite) 89,50 (favorable). SubiText (Texthide) es un programa interesante que cambia sutil características del texto, tales como tiempo de la narración, perspectiva, y reemplazos del sinónimo de la sola palabra para ocultar datos dentro de cualquier texto archiva. Por ejemplo, "las impulsiones auto ayunan en un camino deslizadizo sobre la colina" en lugar de otro se convierten "sobre la cuesta que el coche viaja rápidamente en una calle hielo-cubierta." SubiText utiliza el cifrado fuerte (Twofish y RSA) para cubrir sus pistas. El programa El GUI se escribe actualmente en alemán, haciendo su uso un pedacito desafiador para este usuario no de habla alemana.

Freeware de Textego (http://www.soltec.net/~huson/atextego.lha). Textego, para el Amiga, es basado en el programa de Texto por Kevin Maher (véase abajo) con algunas mejoras agregadas.

Freeware de Texto (http://linkbeat.com/files/). Texto es un programa dla esteganografia del texto que transforma uuencoded o los datos del PGP ASCII-armoured en oraciones inglesas. Los archivos del texto de Texto parecen algo entre los libs enojados y la mala poesía y deben estar bastante cercanos al inglés normal conseguir más allá de exploradores simple-importados del correo. Criptografía visual (http://www.shareware.dabsol.co.uk/) Shareware. Oculta datos en dos imágenes transparentes y revela los datos cuando se apilan las dos imágenes. Cifrado visual (VE) (http://www.fitin.com/) Shareware $40. El cifrado visual es el hermano más sofisticado de IVE (arriba) puede cifrar imágenes del GIF Y los textos ocultados para el acceso público y el desciframiento en línea. Las huéspedes en línea pueden incorporar una contraseña en el área del GIF. Si es aceptable, el GIF total incluyendo ventana adicional del mensaje aparece. VE es la herramienta para asegurar partes de las imágenes del GIF que contienen bosquejos, fórmulas, o noticias importantes. wbStego 4,1 (http://wbstego.wbailer.com/) Shareware $20.

Esteganografia de BMP, de TXT, de HTML/XML, y del pdf para Windows. Incluye un interfaz práctico del mago, un motor (más rápido) nuevo, la ayuda del passphrase a 2 GB, el cifrado incorporado, y la generación de la llave. Nuevo a esta versión es un "encargado del copyright Info" para agregar la información de la profesión de escritor a los archivos, aunque la aplicabilidad legal de esta característica es incierta. La versión inglesa y alemana está disponible.

Freeware De Wnstorm (ftp://ftp.ntua.gr/pub/crypt/esteganografia/wns210.zip). Wnstorm (tormenta blanca del ruido) es una paquete de software de la criptografía y dla esteganografia que usted puede utilizar para cifrar y para ocultar archivos dentro de imágenes de PCX.

APÉNDICE B: ACTIVIDADES de INVESTIGACIÓN

La investigación relacionada con la esteganografia de Microsoft tiene varios grupos el trabajar en tecnologías digitales del watermarking incluyendo el watermarking de los modelos 3D, el watermarking de la imagen, y la evaluación de las técnicas del watermarking.

AT&T está funcionando un proyecto del watermarking del texto que emplea el espaciamiento de línea y asegura la distribución.

El centro de Fraunhofer para la investigación en los gráficos de el ordenador, los E.E.U.U., tiene un proyecto sobre watermarking audio.

El École Polytechnique Fédérale (escuela politécnica federal) de Lausanne, señal de Laboratoire de Traitement du (laboratorio de investigación de la señal), Suiza, ha desarrollado el watermarking JK_PGS llamado software.

El Institut Eurécom, Francia, tiene una imagen y un grupo activos del vídeo para las comunicaciones de los multiMedia.

I.N.R.I.A. Rocquencourt, Francia, publica documentos con respecto a la información fractal numérica que encaja técnicas en el projet Fractales.

El Instituto de Tecnología de Massachusetts, laboratorios de los medios, los E.E.U.U., recibe el homepage el ocultar de datos que presenta muchas técnicas el ocultar de datos (para la imagen, el audio y el texto).

PixelTag (Joshua Smith y Barrett Comiskey) permite que algunos valores de la información del copyright sean encajados imperceptiblemente en imágenes y otros medios. La técnica se basa en la modulación y la información que ocultan en imágenes, un papel presentado en el primer taller internacional sobre ocultar de la información.

El grupo seguro y altamente disponible del establecimiento de una red, departamento de la informática, universidad de la ingeniería, universidad de estado de Carolina del norte, los E.E.U.U., está funcionando un proyecto sobre la protección de la seguridad y del copyright para MPEG2.

La tecnología de seguridad para los gráficos y los sistemas de comunicación es un grupo de interés especial dado al desarrollo de los mecanismos de la seguridad y los protocolos adaptados a las particularidades de los multimedia comunicación y cooperación, incluyendo el control de acceso para los sistemas de radiodifusión de los multimedia (Pagar-TV, Vi' deo-en-exige, etc), la protección del copyright y la gerencia para los datos de los multimedia, el uso de la voz y del reconocimiento de la cara para la autentificación, y los servicios de seguridad para los sistemas del hypermedia.

TALISMAN (que remontaba fue autor de las derechas servicios de etiquetado y supervisando de la imagen la red de acceso) apunta proveer de abastecedores de servicio europeos de la unión un

mecanismo estándar del copyright para proteger sus productos digitales contra piratería comercial de la escala grande y el copiado ilegal. Un problema que no ha encontrado una solución con todo es el que esta' de cómo a realice la protección del copyright para los datos digital almacenados.

Université Catholique (universidad católica) de Louvain, Laboratoire de Télécommunications et Télédétection (las telecomunicaciones y laboratorio del teledetection), Bélgica, lleva a cabo presentaciones regulares de su proyecto de ACCOPI (control de acceso y protección de COpyright para las imágenes).

Université de Genève, centro Universitaire D' informatique, grupo de la visión, Suiza, está desarrollando los mecanismos de la protección del copyright para las imágenes y los videos, implicando en las filigranas digitales particulares ocultadas en las imágenes empleando el software de KryPict.

La universidad de Minnesota, los E.E.U.U., ha desarrollado multi-escala a grupo del proceso de señal.

La universidad de Vigo, España, se especializa en el análisis teórico y estadístico de los algoritmos del watermarking.

APÉNDICE I: Los componentes del SOFTWARE CTSSE de los TERCEROS

El software siguiente fueron incorporados en el CTSSE como componentes funcionales. Las descripciones son de sus websites respectivos: (freeware) Ethereal, Gerald Combs, http://www.ethereal.com/ethereal es un analizador libre del protocolo de red para Unix y Windows. Permite que usted examine datos de una red viva o de un archivo de la captura en disco. Usted puede hojear recíprocamente los datos de la captura, el resumen que ve y la información del detalle para cada paquete. Etéreo tiene varias características de gran alcance, incluyendo una lengua rica del filtro de la exhibición y la capacidad de visión la corriente reconstruida de una sesión del TCP.

La marca Otway, http://www.webreaper.net/WebReaper de WebReaper (freeware) es correa eslabonada o la araña de red, que puede trabajar su manera a través de un website, descargando las páginas, cuadros y se opone que encuentra para poderlas ver localmente, sin necesitar ser conectado con el Internet. Los sitios se pueden ahorrar localmente como website lleno-fully-browsable que se pueda ver con cualquier browser (tal como Internet Explorer, Netscape, ópera, etc), o pueden ser ahorrados en el escondrijo del Internet Explorer y ser vistos usando el modo fuera de línea de IE?s como si usted ' d resaca la mano?by de los sitios?.

StegDetect (freeware) Niels Provos, http://www.webreaper.net/Stegdetect es una herramienta automatizada para detectar el contenido steganographic en imágenes. Es capaz de detectar varios diversos métodos steganographic para encajar la información ocultada en imágenes del JPEG.

Automate 4 (el ensayo 30-day) Unisyn, http://www.unisyn.com/automatícelo es una herramienta del software para Windows que permita a usuarios manejar tareas repetidoras por costumbre fácilmente constructivo. Automate permite a usuarios construir tareas automatizadas con la ayuda de un mago y de un constructor intuitivo de la tarea de la arrastrar-y-gota.

Las herramientas para el desarrollo de CTSSE

Las siguientes herramientas de software fueron utilizadas para generar la software interna de base:

Borland Turbo C++ V1.01 (ahora freeware) Borland, http://community.borland.com/lanzado en 1991, éste era el primer recopilador de Borland?s que apoyó la lengua de C++. Se conforma con la especificación de AT&T?s 2,0 y las herramientas de la línea del ambiente y de comando del desarrollo funcionadas bajo DOS o en una ventana del DOS.

En la producción de la galería de prueba de CTSSE el software siguiente fue utilizada para generar imágenes de prueba:

Los secretos invisibles 2002 (Shareware) Neobyte, http://www.neobytesolutions.com/secretos invisibles 2002 cifran no solamente sus datos y archivos para la caja fuerte que guarda o para la transferencia segura a través de la red, también los oculta en los lugares que en la superficie aparecen totalmente inocentes, por ejemplo archivos del cuadro o del sonido, o la red pagina. Estos tipos de archivos son un disfraz perfecto para information.It sensible proporcionan el cifrado fuerte en la forma de Blowfish (usado en la prueba), de Twofish, de RC4, de Cast128, y de GOST. Incluye una desfibradora, un encargado de la contraseña y el generador. Interconecta agradable con el explorador de Windows vía menús sensibles al contexto del derecho-tecleo.

JP Hide and Seek, freeware (http://linux01.gwdg.de/~alatham/stego.html). JPHS es un programa del stego de Win95/98/NT con un GUI de los ninguno-volantes que oculte datos en el formato siempre popular de la imagen de JPG. JPHIDE y JPSEEK son algo especiales. El objetivo de diseño no era simplemente ocultar un archivo pero hacer algo esto de una manera tal que sea imposible probar que el archivo del anfitrión contiene un archivo ocultado. Dado una imagen visual típica, una tarifa baja de la inserción (debajo del 5%) y la ausencia del archivo original, no es posible concluir con ninguna certeza de mérito que el archivo del anfitrión contiene datos insertados. Mientras que el porcentaje de la inserción aumenta la naturaleza estadística de los coeficientes del JPEG diferencia de "normal" hasta el punto de levante la suspicacia. Sobre el 15% los efectos comienzan a llegar a ser visibles al ojo desnudo. Por supuesto algunas imágenes están mucho mejor que otras cuando están utilizadas pues un archivo del anfitrión - el un montón de detalle fino es bueno. Un cielo azul despejado sobre un paraíso cubierto nieve del esquí es malo. Una cascada en un bosque es probablemente ideal. Su tamaño pequeño es una prima importante como él fácilmente ajustes en un

disco. Utiliza el cifrado también, pero no menciona qué tipo. DOS y versión de Linux también disponible.

Jsteg Shell v2.0, Freeware (http://members.tripod.com/steganography/stego/jstegshella.zip). JSteg Shell es un interfaz de Win95/98/NT (no Win2000) para funcionar Jsteg del DOS, un programa por Derek Upham que oculte datos en el formato popular de imagen JPG. Incluye encrytion de 40 valores RC4, determinación de la cantidad de datos que un JPG puede ocultar de antemano, y las opciones seleccionables por el usuario de JPG (grado del IE de la compresión). JSteg Shell tiene un pulido y fácil de utilizar interfaz que hace con el JSteg de DOS un broche de presión. JSteg Shell viene con los executables del DOS, y el instalador toma el cuidado de todos los detalles de la disposición.