PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

T E S I S

"ESTUDIO DE SOFTWARE LIBRE PARA REALIZAR EL ANÁLISIS FORENSE EN REDES DE COMPUTADORES PARA ENTIDADES ECUATORIANAS DEDICADAS A LA SEGURIDAD CIUDADANA"

PROAÑO FREIRE MARGOTH LUCILA

Trabajo previo a la obtención del Título de:

MAGISTER EN REDES DE COMUNICACIONES

Quito, Diciembre 2012

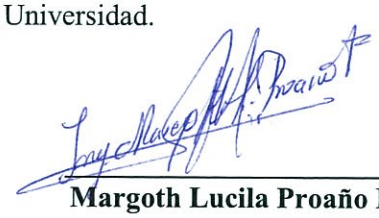
DECLARACIÓN Y AUTORIZACIÓN

Quito, 30 Noviembre del 2012

Yo, MARGOTH LUCILA PROAÑO FREIRE C.I. 0501213409, autora del trabajo de graduación intitulado: "ESTUDIO DE SOFTWARE LIBRE PARA REALIZAR EL ANÁLISIS FORENSE EN REDES DE COMPUTADORES PARA ENTIDADES ECUATORIANAS DEDICADAS A LA SEGURIDAD CIUDADANA", previa a la obtención del grado académico de Magister en Redes de Comunicaciones, en la Facultad de Ingeniería:

Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.



Margoth Lucila Proaño Freire

C.I. 0501213409

CERTIFICACIÓN

Certifico que el presente proyecto de tesis fue desarrollado por la Sra. Margoth Proaño, bajo mi supervisión.

_____

Máster Ricardo Ortega Ortega

Director de Tesis

AGRADECIMIENTO

Me siento profundamente agradecida y orgullosa de pertenecer a la Facultad de Ingeniería, Maestría de Redes y Comunicaciones de la Pontificia Universidad Católica del Ecuador, modelo de educación progresista que sigue alentando mis empeños.

Agradezco a mi tutor, el Señor Magister Ricardo Ortega, que con sabiduría y sagaces orientaciones me acompañó en la evolución del proyecto de tesis, hasta hacerla realidad.

Para dos personalidades singulares y brillantes profesores: el Señor Ph.D. Gustavo Chafla y el Señor Magister Javier Cóndor, que me honraron con su cátedra, su guía y revisión del proyecto, muchas gracias.

Y, una infinita gratitud para mi familia por su apoyo incondicional.

MARGOTH

DEDICATORIA

A mí querida hija Valeria, el mayor regalo de mi vida.

Gratitud eterna para mis padres Manuel e Inés, que me inculcaron fortaleza, fe y libertad para buscar mis metas.

Para mis afectuosos y brillantes hermanos: Susana, Hernán, Eduardo.

MARGOTH

ABSTRACT

"All warfares are based on deception."
—*Sun Tzu, the Art of War*

This document contains the results of investigation about computer forensics, network forensics and ethical hacking using free software intended for institutions related with customer security. These technical disciplines are intended to discover who, how, where and when was responsible for intrusion or security incident in a computer networks.

This work contains the results of a survey conducted to approximately 70 technicians and security officials. Regrettably, the results were almost useless due to the null or poor knowledge of computer forensics in Ecuador.

The author of this work hopes this situation will change in a near future and the computer forensics as long as the interest and dedication of security officials and computer technicians goes conducted to these disciplines.

This document contains a long list of free software that can help in some of the activities related to network forensics and ethical hacking [G11]. There is no program that can be named as "the best". There is no one that can be named as the unique. The preferences of the investigator, the variety of technologies involved in computer networks (wired, wireless, movil, Bluetooth) the variety of source and target environments (Linux, Windows, IOS, Android) the variety of devices involved are simply too many to name a program as "the best program for network forensics".

The technology evolves so rapidly that the best-suited programs for the job are rapidly pushed by the next generation of programs. Fortunately, there are so many programs in the free software category to make the correct election. This work answers with a loud YES to the question “is there a suitable free software program or programs in order to conduct network forensics or ethical hacking”.

TABLA DE CONTENIDO

DECLARACIÓN Y AUTORIZACIÓN ..... **I**

CERTIFICACIÓN ..... **II**

AGRADECIMIENTO ..... **III**

DEDICATORIA ..... **IV**

ABSTRACT ..... **V**

TABLA DE CONTENIDO ..... **VII**

ÍNDICE DE GRÁFICOS ..... **XVI**

1. *GRÁFICOS GENERADOS EN LA TESIS* ..... *xvi*
2. *GRÁFICOS CON REFERENCIAS DE INTERNET* ..... *xviii*

ÍNDICE DE TABLAS ..... **XX**

1. *TABLAS GENERADAS EN LA TESIS* ..... *xx*
2. *TABLAS CON REFERENCIA DE INTERNET* ..... *xxii*

CAPÍTULO I: INTRODUCCIÓN ..... **- 1 -**

1.1 TEMA ..... - 1 -

1.2 JUSTIFICACIÓN ..... - 1 -

1.2.1 JUSTIFICACIÓN TECNOLÓGICA ..... - 1 -

1.2.2 JUSTIFICACIONES TEÓRICAS ..... - 2 -

1.2.3 ACTUALIDAD EN EL ECUADOR ..... - 3 -

1.2.4 VIABILIDAD Y OPORTUNIDAD ..... - 4 -

1.3 PLANTEAMIENTO DEL PROBLEMA ..... - 4 -

1.3.1 EL PROTOCOLO TCP/IP NO NACIÓ ORIENTADO A LA SEGURIDAD ..... - 4 -

1.3.2 LAS VULNERABILIDADES QUE SE DETECTAN CADA CIERTO TIEMPO ..... - 5 -

1.3.3 LOS ATAQUES Y CRÍMENES INFORMÁTICOS ..... - 7 -

1.3.4 NECESIDAD DE INVESTIGAR INCIDENTES ..... - 8 -

1.3.5 LAS RESPUESTAS QUE OFRECE LA INFORMÁTICA FORENSE ..... - 8 -

1.3.6 HERRAMIENTAS DE SOFTWARE LIBRE ..... - 9 -

1.3.7 LA PREGUNTA RECTORA DEL PROBLEMA QUE SE INVESTIGA ..... - 10 -

1.4 OBJETIVOS ..... - 11 -

1.4.1 OBJETIVO GENERAL ..... - 11 -

1.4.2 OBJETIVOS ESPECÍFICOS ..... *- 11 -*

1.5 MARCO TEÓRICO Y CONCEPTUAL DE LA INFORMÁTICA FORENSE ..... - 12 -

1.5.1 ANTECEDENTES EN EL MUNDO ..... *- 12 -*

1.5.2 ANTECEDENTES DE LA INFORMÁTICA FORENSE EN EL ECUADOR ..... *- 15 -*

1.5.3 ¿POR QUÉ ES ATRACTIVO EL DELITO INFORMÁTICO? ..... *- 16 -*

1.6 HIPÓTESIS O IDEA A DEFENDER ..... - 18 -

1.7 OPERACIONALIZACIÓN DE LA INVESTIGACIÓN ..... - 19 -

1.7.1 VARIABLES ..... *- 19 -*

1.7.2 DIMENSIONES ..... *- 19 -*

1.7.3 INDICADORES ..... *- 20 -*

1.8 PROCEDIMIENTO Y MARCO METODOLÓGICO ..... - 20 -

1.8.1 METODOLOGÍA ..... *- 20 -*

1.8.2 TÉCNICAS ..... *- 20 -*

1.8.3 UNIVERSO Y/O MUESTRA ..... *- 21 -*

CAPÍTULO II: LAS REDES Y EL ANÁLISIS FORENSE .....- 22 -

2.1 INTRODUCCIÓN ..... - 22 -

¿QUÉ ES LA FORENSIA EN REDES? ..... *- 23 -*

PARTICULARIDADES DE TCP/IP ..... *- 23 -*

NO EXISTE EL ANONIMATO 100% AL NAVEGAR POR INTERNET ..... *- 24 -*

TODO USUARIO RECIBE UNA IP PÚBLICA EXCLUSIVA O COMPARTIDA ..... *- 24 -*

LOGS Y REGISTROS DE ACCESOS [G29] ..... *- 29 -*

2.2 DISPONIBILIDAD DE INFORMACIÓN ACERCA DEL ANÁLISIS FORENSE ..... - 31 -

2.2.1 SITIOS WEB ESPECIALIZADOS EN SEGURIDAD ..... *- 31 -*

2.2.2 CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS ..... *- 34 -*

2.2.3 TIPOS DE INCIDENTES Y/O DELITOS INFORMÁTICOS ..... *- 34 -*

2.2.5 NAVEGACIÓN ANÓNIMA ..... *- 38 -*

2.3 ENCUESTA DE INCIDENTES DE SEGURIDAD ..... - 44 -

2.3.1 GRÁFICAS DE RESULTADOS ..... *- 44 -*

2.3.2 INTERPRETACIÓN DE LAS ENCUESTAS ..... *- 49 -*

2.4 VULNERABILIDADES IMPORTANTES DEL TCP/IP ..... - 50 -

2.4.1. LA MAYORÍA DE PROTOCOLOS DE TCP/IP NO SON CIFRADOS ..... - 50 -

2.4.2 UN GRUPO DE MÁQUINAS COMPARTEN LA MISMA ID DE RED..... - 50 -

2.4.3 TODO TRÁFICO DE TCP/IP DEBE PASAR POR UNA PUERTA DE ENLACE O SERVIDOR PROXY..... - 52 -

2.4.4 TODO EQUIPO NECESITA TENER ASIGNADO UN SERVIDOR DNS..... - 53 -

2.4.5 TODO EQUIPO NECESITA UNA DIRECCIÓN MAC..... - 53 -

2.5 VULNERABILIDADES DE PAQUETES Y PROGRAMAS POPULARES..... - 54 -

2.6 LA FORENSIA EN REDES..... - 55 -

¿QUÉ ES?..... - 55 -

¿CÓMO FUNCIONA?..... - 55 -

EL TIEMPO ES UN FACTOR IMPORTANTE..... - 56 -

2.7 EL DEBIDO PROCESO..... - 56 -

2.8 LA CADENA DE CUSTODIA..... - 59 -

2.9 LA EVIDENCIA DIGITAL. ..... - 60 -

2.10 LAS ETAPAS DEL ANÁLISIS FORENSE. ..... - 63 -

2.10.1 PLANIFICACIÓN ..... - 64 -

2.10.2 EJECUCIÓN ..... - 64 -

2.10.3 PRESENTACIÓN E INFORME ..... - 65 -

CAPÍTULO III: PROGRAMAS LIBRES PARA FORENSIA EN REDES .....- 67 -

3.1 INTRODUCCIÓN ..... - 67 -

3.2 ANÁLISIS DE ALTERNATIVAS ..... - 67 -

3.2.1 SUITS MULTIPROPÓSITO PARA INFORMÁTICA FORENSE ..... - 67 -

PROGRAMAS MULTIPROPÓSITO PARA INFORMÁTICA FORENSE ..... - 68 -

PRINCIPALES EMPRESAS DESARROLLADORAS DE SUITS DE PROGRAMAS PARA ANÁLISIS FORENSE..... - 70 -

3.2.2 PROGRAMAS PROPIETARIOS O CON MARCAS REGISTRADAS (™) ..... - 71 -

3.2.3 PROGRAMAS LIBRES..... - 73 -

PROGRAMAS LIBRES SUITES (CONJUNTOS) INTEGRADOS ..... - 74 -

SOFTWARE LIBRE PARA FORENSIADE REDES Y ANÁLISIS DE INTERNET ..... - 75 -

PROGRAMAS LIBRES ANÁLISIS FORENSE EN COMPUTADORES INDIVIDUALES ..... - 77 -

SOFTWARE LIBRE PARA ANÁLISIS DE DISCOS E IMÁGENES DE DISCOS ..... - 79 -

PROGRAMAS LIBRES PARA ANÁLISIS DE CORREOS ELECTRÓNICOS..... - 80 -

SOFTWARE LIBRE PARA OBTENCIÓN DE INFORMACIÓN ..... *- 80 -*

SOFTWARE LIBRE PARA ANÁLISIS DE ARCHIVOS Y DATOS ..... *- 82 -*

PROGRAMAS PARA MAC OS ..... *- 85 -*

PROGRAMAS LIBRES PARA DISPOSITIVOS MÓVILES ..... *- 86 -*

PROGRAMAS LIBRES PARA VISUALIZAR ARCHIVOS ..... *- 86 -*

PROGRAMAS LIBRES PARA ANÁLISIS DE REGISTRO DE WINDOWS ..... *- 87 -*

PROGRAMAS LIBRES PARA ANÁLISIS DE APLICACIONES ..... *- 88 -*

3.2.4 PROGRAMAS EN AMBIENTE LIVE CDS ..... *- 88 -*

3.2.5 PROGRAMAS PARA AMBIENTE WINDOWS ..... *- 90 -*

3.3 PROGRAMAS Y HERRAMIENTAS DISPONIBLES PARA FORENSIA EN REDES ..... - 94 -

3.3.1 PLATAFORMA WINDOWS ..... *- 94 -*

3.3.2 LINUX/OPEN-SOURCE ..... *- 99 -*

ARP AND ETHERNET MAC TOOLS ..... *- 101 -*

CISCO ..... *- 101 -*

ICMP LAYER TESTS AND ATTACKS ..... *- 102 -*

IP LAYER TESTS ..... *- 102 -*

UDP LAYER TESTS ..... *- 102 -*

TCP LAYER ..... *- 103 -*

3.3.3 ANTIFORENSIC..... *- 104 -*

3.3.4 REGIONAL REGISTRIES..... *- 105 -*

CAPÍTULO IV: GUÍA RÁPIDA PARA FORENSIA EN REDES USANDO SOFTWARE LIBRE ..- 107 -

4.1 FINALIDAD DE LA GUÍA ..... - 107 -

4.2 CONSIDERACIONES..... - 107 -

4.3 GUÍA..... - 108 -

4.3.1 FASE 1: PLANIFICACIÓN..... *- 108 -*

4.3.2 FASE 2: EJECUCIÓN..... *- 110 -*

PROGRAMAS QUE PERMITEN OBTENER USUARIO Y CONTRASEÑA ..... *- 115 -*

4.3.3 FASE 3: PRESENTACIÓN DE RESULTADOS ..... *- 122 -*

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES.....- 123 -

5.1 CONCLUSIONES ..... - 123 -

5.1.1 RELACIONADAS CON LA SITUACIÓN ACTUAL DE LA INFORMÁTICA FORENSE - 123 -

5.1.2 RELACIONADAS CON PROGRAMAS DE SOFTWARE LIBRE PARA INFORMÁTICA FORENSE..... - 124 -

5.2 RECOMENDACIONES ..... - 125 -

5.2.1 PARA LOS OFICIALES DE SEGURIDAD ..... - 125 -

5.2.2 PARA LAS ENTIDADES E INSTITUCIONES ..... - 126 -

5.2.3 PARA EL PÚBLICO EN GENERAL..... - 126 -

CAPÍTULO VI: GLOSARIO..... - 128 -

CAPÍTULO VII: BIBLIOGRAFÍA ..... - 148 -

7.1. LIBROS. ..... - 148 -

7.2. DOCUMENTOS DIGITALES. ..... - 149 -

7.3 REFERENCIAS DE INTERNET. ..... - 151 -

ANEXO..... - 165 -

ANEXO 1 ..... - 166 -

ENCUESTA REALIZADA A TÉCNICOS Y OFICIALES DE SEGURIDAD..... - 166 -

ÍNDICE DE GRÁFICOS

1. GRÁFICOS GENERADOS EN LA TESIS

Gráfico A1: Comando linux –lastb. - 29 -

Gráfico A2: Comando linux – geoiplookup. - 30 -

Gráfico A3: Resultado de encuestas, según el género. - 44 -

Gráfico A4: Resultado de encuestas, según tamaño de la organización. - 45 -

Gráfico A5: Resultado de encuestas, según el nivel de dedicación a la seguridad ciudadana. - 45 -

Gráfico A6: Resultado de la pregunta: La informática forense se parece al hacking ético?. - 46 -

Gráfico A7: Resultado de la pregunta: Conoce usted los principios de la informática forense?. - 46 -

Gráfico A8: Resultado de la pregunta: Cuándo aplicaría su organización el análisis forense?. - 47 -

Gráfico A9: Medidas que su organización tomaría en una escena de un incidente informático. - 47 -

Gráfico A10: Resultado de la pregunta: ¿El principio de Locard es?. - 48 -

Gráfico A11: Resultado de la pregunta: En la organización sabemos lo que es el debido proceso. - 48 -

Gráfico A12: Resultado de las preguntas 14-20. - 49 -

Gráfico A13: Captura de pantalla de wireshark - 51 -

Gráfico A15: Reporte programa Angry IP Scanner. - 112 -

Gráfico A16: Reporte programa SharesEnum _____ *- 112 -*

2. GRÁFICOS CON REFERENCIAS DE INTERNET

Gráfico 01: Base de datos de vulnerabilidades. Ref. [1-01] _____ *- 4 -*

*Gráfico 02: Vulnerabilidades identificadas en el 2012, servidor apache. Ref. [1-02]*_____ *- 6 -*

Gráfico 03: Vulnerabilidades en el servidor Web TOMCAT año 2012. Ref. [1-02] _____ *- 6 -*

*Gráfico 04: Alertas publicadas por el ICI-CERT, Argentina. Ref. [1-03]*_____ *- 7 -*

Gráfico 05: Portada del Tratado de Los Venenos 1814. Ref. [1-04] _____ *- 12 -*

*Gráfico 06 : Triángulo del delito, se combina el motivo, la oportunidad y los medios. Ref. [R]*____ *- 18 -*

Gráfico 07: Información de ip real del host. Ref. [2-01] _____ *- 25 -*

*Gráfico 08: Información ubicación de host (MAC/IP) en el sitio iplookup . Ref. [2-02]*_____ *- 26 -*

*Gráfico 09: Geoip Tool en funcionamiento Ref. [2-03]*_____ *- 27 -*

Gráfico 10: Captura de pantalla de web con noticias de seguridad informática Ref. [2-04] _____ *- 31 -*

*Gráfico 11: Captura de pantalla: CERT- Carnegie Mellon University Ref. [2-05]*_____ *- 32 -*

Gráfico 12: Captura de pantalla: web de seguridad Ref. [2-06] _____ *- 33 -*

*Gráfico 13: Eventos de base de datos de vulnerabilidades open source (OSVDB). Ref [2-07]*_____ *- 33 -*

Gráfico 14: Tipos de incidentes y/o delitos informáticos. Ref. [X] _____ *- 35 -*

*Gráfico 15: Captura de pantalla de consola TOR. Ref. [2-08]*_____ *- 42 -*

Gráfico 16: Captura de pantalla de la configuración de TOR. Ref. [2-09]_____ - 43 -

Gráfico 17: Captura de pantalla del funcionamiento web con TOR habilitado. Ref. [2-10] _____ - 43 -

Gráfico 18: Direcciones IP servidores DNS fraudulentos (DNS Changer). Ref. [2-11] _____ - 53 -

Gráfico 19: Admisibilidad de la evidencia según Santiago Acurio (15/ 04/ 2010.) Ref. [R] _____ - 63 -

Gráfico 20: Metodología de Análisis Forense. Ref. [S]_____ - 64 -

Gráfico 21: Metodología tradicional para recolectar evidencias. Ref. [S] _____ - 65 -

Gráfico 22: Sitio del software propietario Access Data – FTK. Ref. [3-01]_____ - 72 -

Gráfico 23: Sitio del software propietrio EnCase Forensic Ref. [3-02] _____ - 72 -

ÍNDICE DE TABLAS

1. TABLAS GENERADAS EN LA TESIS

Tabla A01 : Suits y programas multipropósito para Informática Forense _____ *- 69 -*

*Tabla A02 : Principales empresas desarrolladoras de software para Informática Forense*_____ *- 71 -*

*Tabla A03 : Programas libres suites (conjuntos) integrados*_____ *- 75 -*

Tabla A04 : Software libre para forensia de redes y análisis de actividad en Internet _____ *- 77 -*

Tabla A05 : Programas libres para análisis forense en computadores individuales _____ *- 78 -*

Tabla A06 : Software libre para análisis de discos e imágenes de discos _____ *- 79 -*

Tabla A07 : Programas libres para análisis de correos electrónicos _____ *- 80 -*

Tabla A08 : Software libre para obtención de información _____ *- 82 -*

Tabla A09 : Software libre para análisis de archivos y datos _____ *- 84 -*

Tabla A10 : Programas para Mac OS _____ *- 85 -*

Tabla A11: Programas libres para Dispositivos Móviles _____ *- 86 -*

*Tabla A12: Programas libres para visualizar archivos*_____ *- 87 -*

Tabla A13 : Programas libres para análisis de registro de windows _____ *- 88 -*

*Tabla A14 : Programas libres para registro de windows*_____ *- 88 -*

Tabla A15: Programas libres en Lives CD _____ *- 90 -*

Tabla A16: Programas para ambiente windows _____ *- 93 -*

Tabla A17: Programas y herramientas disponibles para forensia en redes _____ *- 99 -*

Tabla A18: Programas linux/open-source _____ *- 100 -*

Tabla A19: Herramientas de Lìnea de comando _____ *- 101 -*

Tabla A20: Herramientas arp, ethernet y mac _____ *- 101 -*

Tabla A21: Herramienta CISCO _____ *- 101 -*

Tabla A22: Herramientas ICMP probadores de capas e incidentes. _____ *- 102 -*

Tabla A23: Herramientas de prueba para el protocolo IP _____ *- 102 -*

Tabla A24: Herramientas de prueba para el protocolo UDP _____ *- 103 -*

Tabla A25: Herramientas de prueba para el protocolo TCP _____ *- 103 -*

Tabla A27: Programas y herramientas antiforensic _____ *- 105 -*

Tabla A28: Programas y herramientas disponibles para forensia en redes _____ *- 106 -*

Tabla A29: Cuadro comparativo de programas que permiten obtener usuario y contraseña. __ *- 115 -*

2. TABLAS CON REFERENCIA DE INTERNET

Tabla 01 : Clasificación de los delitos informáticos según Naciones Unidas [Ref. W] _____ *- 38 -*

Tabla 02 : Libertades que garantiza el software libre. Ref. [3-100] _____ *- 73 -*

o

CAPÍTULO I: INTRODUCCIÓN

"Tienes que creer en ti mismo."
-Sun Tzu-, El Arte de la Guerra

1.1 TEMA

Estudio de software libre para realizar el análisis forense en redes de computadores para entidades ecuatorianas dedicadas a la seguridad ciudadana.

1.2 JUSTIFICACIÓN

Este proyecto se justifica por los siguientes motivos:

1.2.1 JUSTIFICACIÓN TECNOLÓGICA

- El gobierno ecuatoriano estableció, desde el 2008, como política para las entidades públicas, el uso obligatorio del software libre, negando la adquisición de software que no se ajuste al decreto 1014. El cambio ha sido progresivo pero constante. A esta fecha (2012) todas las entidades públicas tienen la obligación de analizar y utilizar alternativas de software libre.
- El software libre tiene apoyo a nivel mundial y su influencia sigue creciendo, por lo que es una alternativa técnicamente válida y viable.
- Los incidentes de seguridad informática, entendidos como ataques, intrusiones y alteraciones a los servidores y estaciones, se han vuelto demasiado frecuentes. Muchas veces estos incidentes pasan desapercibidos por la falta de técnicos y de herramientas que puedan identificar y mitigar los daños.

- Las entidades dedicadas a brindar seguridad ciudadana, especialmente la policía y los servicios de inteligencia, se han convertido en blanco frecuente de estos incidentes.
- Es prioritario que exista un estudio serio, preciso y actualizado de las alternativas de software libre para realizar análisis forense en redes, detección de vulnerabilidades, rastreo de incidentes, y en general el uso de técnicas que permitan identificar qué, quién, cuándo, cómo y con qué medios logró ingresar al sistema de una entidad pública dedicada a la defensa y seguridad ciudadana.
- Las entidades dedicadas a la seguridad deben atender pedidos de análisis forense en redes de terceros que han sufrido incidentes; por consiguiente, no sólo deben conocer sus propios sistemas sino, además, conocer sistemas de terceros.
- Es indiscutible que existen soluciones tecnológicas libres orientadas a la seguridad que pueden considerarse alternativas a las soluciones tecnológicas de seguridad propietarias.

1.2.2 JUSTIFICACIONES TEÓRICAS

- El protocolo TCP/IP [G04] tiene varias vulnerabilidades [G05] perfectamente identificadas y documentadas pero que, muchas veces, no son tomadas en cuenta por los responsables de los centros de cómputo, razón por la que abundan los incidentes [G41] de seguridad informática [G45].
- La informática forense [G02] y la forensia en redes (network forensics [G07]) son una rama del conocimiento que está perfectamente identificada y sistematizada; sin embargo, la mayoría de programas utilizados por las empresas y entidades dedicadas

a estas actividades son de carácter comercial, haciéndose necesario un estudio de las alternativas en software libre [G03].

- En informática forense [G02] y en el análisis forense de redes [G01], es tan importante el resultado como el procedimiento que se siguió para obtener el resultado. Por esto es fundamental que el analista de seguridad conozca la forma correcta de ejecutar los procedimientos de análisis forense.
- Existen numerosos programas, basados principalmente en Linux, que permiten realizar el análisis forense pero la mayoría de ellos tienen mala fama por el uso indebido que les dan los hackers [G26] y los atacantes. Sin embargo, también pueden tener usos legítimos para proteger redes y para realizar el análisis forense.

1.2.3 ACTUALIDAD EN EL ECUADOR

- Las entidades ecuatorianas dedicadas a la seguridad se han convertido involuntariamente en un blanco de ataques de hackers e incidentes de seguridad. La seguridad de la información [G45] no se obtiene con sólo comprar un programa. Esta situación se agrava ya que la mayoría de entidades públicas tienen prohibido comprar y usar programas comerciales. Un estudio de las alternativas de software libre es urgente.
- La autora de este proyecto labora en una entidad pública dedicada a la seguridad, que por políticas institucionales debe mantenerse en reserva. Por consiguiente, la autora de este trabajo conoce las necesidades y requerimientos de este tipo de entidades dedicadas a la seguridad ciudadana.
- Este trabajo busca beneficiar de todas las entidades ecuatorianas dedicadas a la seguridad e inteligencia.

- Muchos programas incluidos en CDs o colecciones de “hacking” o “de seguridad” son intrusiones a la privacidad, por lo cual se hace necesario un estudio serio acerca de estos programas con el fin de evitar caer en actividades ilegales.

1.2.4 VIABILIDAD Y OPORTUNIDAD

- El tema es oportuno, factible y viable ya que existen los conocimientos, el tiempo y los recursos propios para realizar este trabajo. Además, el software libre está disponible en internet y representaría un ahorro de costos.

1.3 PLANTEAMIENTO DEL PROBLEMA

1.3.1 EL PROTOCOLO TCP/IP NO NACIÓ ORIENTADO A LA SEGURIDAD

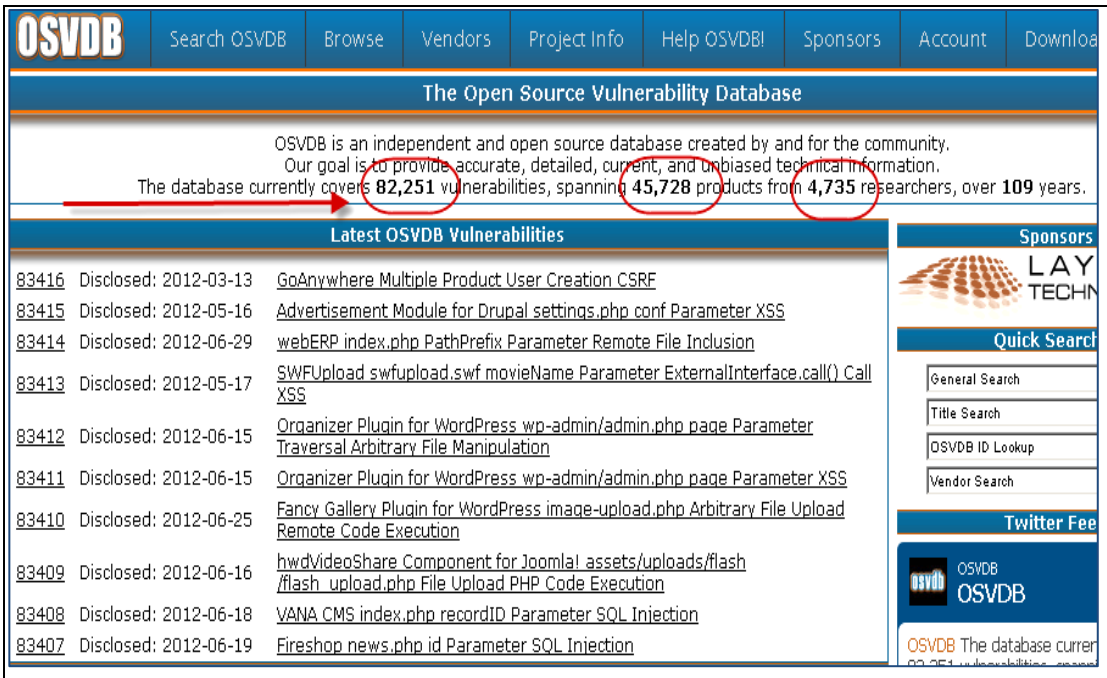


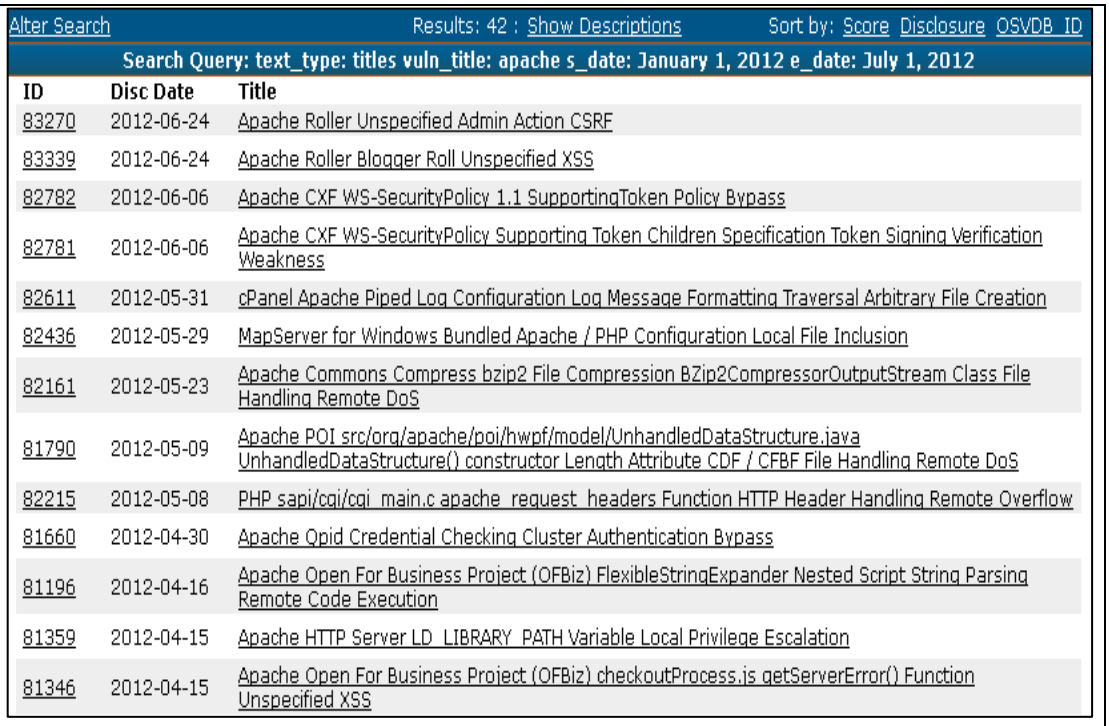
Gráfico 01: Base de datos de vulnerabilidades. Ref. [1-01]

El protocolo TCP/IP [G36] sobre el cual se fundamentan las redes actuales, es un protocolo que no fue diseñado con la seguridad en mente. Si bien es cierto que existen maneras de asegurar una red TCP/IP, éstas no siempre son tomadas en cuenta por los responsables de la infraestructura tecnológica, sea por desconocimiento, por costos, o simplemente porque el avance tecnológico y las malas intenciones de los atacantes superan la dedicación normal de los responsables.

1.3.2 LAS VULNERABILIDADES QUE SE DETECTAN CADA CIERTO TIEMPO

La Base de Datos Abierta de Vulnerabilidades (OSVDB) [G46] contiene (Junio 2012) un listado de 82252 vulnerabilidades que abarcan 45728 productos, de 4735 investigadores durante 109 años. Allí se pueden encontrar fallas, por ejemplo, de Firefox (mozilla), Apache, Sendmail, Named, Joomla y otros programas de uso popular, arrojando decenas de vulnerabilidades aportadas por grupos y proyectos como CERT [G14], Nessus, Snort, Bugtraq, Microsoft Security Bulletin, Nikto, Exploit Database y otra docena de sitios especializados en seguridad. Como ejemplo, en el año 2012 el servidor web Apache reporta 42 vulnerabilidades.

De esta pequeña muestra de vulnerabilidades, se puede concluir que los programas más populares -comerciales y libres-: Apache, Tomcat, Google Chrome, Firefox, Java, Joomla, Wordpress; contienen vulnerabilidades que podrían comprometer la seguridad de la información y del público en general.

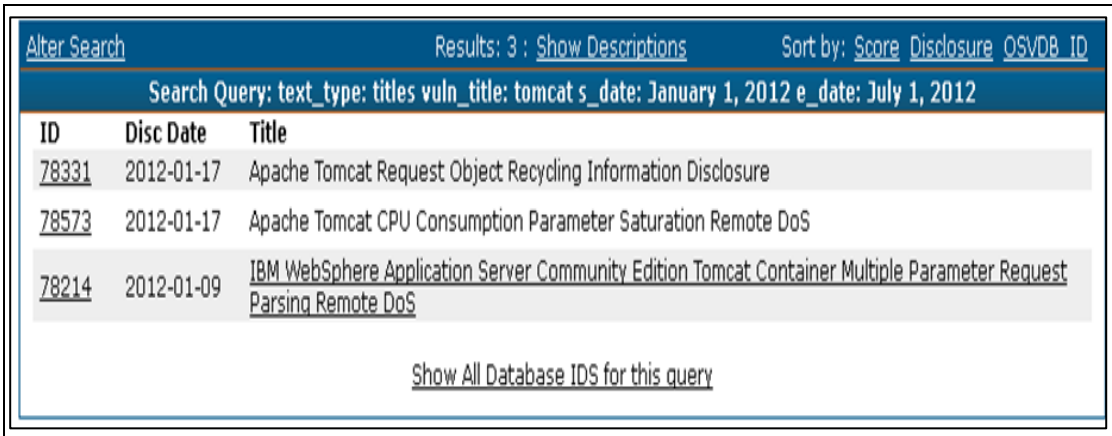


Alter Search — Results: 42 : Show Descriptions — Sort by: Score Disclosure OSVDB ID

Search Query: text_type: titles vuln_title: apache s_date: January 1, 2012 e_date: July 1, 2012

ID	Disc Date	Title
83270	2012-06-24	Apache Roller Unspecified Admin Action CSRF
83339	2012-06-24	Apache Roller Blogger Roll Unspecified XSS
82782	2012-06-06	Apache CXF WS-SecurityPolicy 1.1 SupportingToken Policy Bypass
82781	2012-06-06	Apache CXF WS-SecurityPolicy Supporting Token Children Specification Token Signing Verification Weakness
82611	2012-05-31	cPanel Apache Piped Log Configuration Log Message Formatting Traversal Arbitrary File Creation
82436	2012-05-29	MapServer for Windows Bundled Apache / PHP Configuration Local File Inclusion
82161	2012-05-23	Apache Commons Compress bzip2 File Compression BZip2CompressorOutputStream Class File Handling Remote DoS
81790	2012-05-09	Apache POI src/org/apache/poi/hwpf/model/UnhandledDataStructure.java UnhandledDataStructure() constructor Length Attribute CDF / CFBF File Handling Remote DoS
82215	2012-05-08	PHP sapi/cgi/cgi_main.c apache_request_headers Function HTTP Header Handling Remote Overflow
81660	2012-04-30	Apache Qpid Credential Checking Cluster Authentication Bypass
81196	2012-04-16	Apache Open For Business Project (OFBiz) FlexibleStringExpander Nested Script String Parsing Remote Code Execution
81359	2012-04-15	Apache HTTP Server LD_LIBRARY_PATH Variable Local Privilege Escalation
81346	2012-04-15	Apache Open For Business Project (OFBiz) checkoutProcess.js getServerError() Function Unspecified XSS

Gráfico 02: Vulnerabilidades identificadas en el 2012, servidor apache. Ref. [1-02]



Alter Search — Results: 3 : Show Descriptions — Sort by: Score Disclosure OSVDB ID

Search Query: text_type: titles vuln_title: tomcat s_date: January 1, 2012 e_date: July 1, 2012

ID	Disc Date	Title
78331	2012-01-17	Apache Tomcat Request Object Recycling Information Disclosure
78573	2012-01-17	Apache Tomcat CPU Consumption Parameter Saturation Remote DoS
78214	2012-01-09	IBM WebSphere Application Server Community Edition Tomcat Container Multiple Parameter Request Parsing Remote DoS

Show All Database IDS for this query

Gráfico 03: Vulnerabilidades en el servidor Web TOMCAT año 2012. Ref. [1-02]

Gráfico 04: Alertas publicadas por el ICI-CERT, Argentina. Ref. [1-03]

1.3.3 LOS ATAQUES Y CRÍMENES INFORMÁTICOS

Los intrusos, llamados hackers [G26], crackers [G27], atacantes, delincuentes, fanáticos o curiosos, están mejor informados que los responsables de seguridades. Estos disponen de mejores herramientas y mejores conocimientos para aprovechar estas vulnerabilidades y para descubrir nuevas formas de quebrar las seguridades; como consecuencia que cada vez son más frecuentes las páginas web caídas, alteradas o "hackeadas", así como los servidores

invadidos, secuestrados o fuera de servicio. En la misma base de datos OSVDB se pueden apreciar los "exploits" [G35], que son los programas que se aprovechan de ciertas vulnerabilidades.

1.3.4 NECESIDAD DE INVESTIGAR INCIDENTES

El caso Wikileaks [G47], de mucha actualidad y publicidad en estos días, demuestra que ningún país del mundo y ninguna entidad está exenta de incidentes de seguridad, sean de sustracción de información o, peor aún, de alteración de información. No se ha sabido de un análisis forense a los computadores o redes de donde se tomó la información que ahora se publica en Wikileaks. Este es un tema pendiente que merece investigación y análisis para buscar un remedio y una sanción en los casos aplicables. En el Ecuador, nadie ha realizado un análisis serio del caso para determinar si los sistemas informáticos ecuatorianos sufren de las mismas vulnerabilidades aprovechadas por Wikileaks o, al menos, si sufren de las vulnerabilidades publicadas en OSVDB y otros. Tampoco se conoce que el Ecuador esté asociado, participe o colabore con los grupos CSIRT [G15], o equivalentes, que permiten afrontar rápidamente incidentes de seguridad. En resumen, en el Ecuador poco se ha hecho para prevenir esta situación.

1.3.5 LAS RESPUESTAS QUE OFRECE LA INFORMÁTICA FORENSE

La informática forense, forensia en redes y el análisis forense, con sus parientes hacking ético [G28] y otras, son las disciplinas técnico – científicas que permiten determinar qué ocurrió, cuándo ocurrió, desde dónde provino el incidente y sobre todo permite mitigar los riesgos de que vuelva a ocurrir el incidente. La informática forense, a diferencia de la auditoría informática -Normas de seguridad informática ISO 2700[G33], es correctivo y

permite solucionar el problema y perseguir a los responsables, evitando que vuelva a producirse el incidente.

Una filtración de información, por leve que sea, o la alteración de información de una entidad dedicada a recopilar, almacenar y analizar información sensible de ciudadanos, sería catastrófica.

La informática forense, el análisis forense y forensia en redes, hacen uso de muchas herramientas destinadas a realizar hacking, pero se diferencian del hacking ético en muchos aspectos. El objetivo forense es determinar la oportunidad, el motivo y los medios que usaron los culpables, con la finalidad de aplicar la ley y evitar incidentes futuros, mientras que el hacking ético se queda en una simple curiosidad o en un informe de vulnerabilidades. El análisis forense tiene el deber de ir mucho más allá: prevenir hechos futuros y corregir los efectos.

1.3.6 HERRAMIENTAS DE SOFTWARE LIBRE

Entonces se hace necesario un estudio actual que, usando software libre[G03], permita identificar las vulnerabilidades de un sistema informático en red, que presente guías y herramientas para cubrir dichas vulnerabilidades y, sobre todo, que permita realizar el análisis de aquellos sistemas que han sido vulnerados para plantear correctivos y tomar medidas preventivas.

En el mercado existen soluciones de seguridad de tipo comercial, que debido al decreto 1014 de uso del software libre, están fuera del alcance del sector público ecuatoriano. Son pocas las entidades públicas que pueden adquirir ENCASE, FORENSIC TOOLKIT, HELIX,

SHADOW COPY y otras soluciones privadas que son usadas por los especialistas forenses a nivel mundial.

En este documento se describen varias soluciones de software libre, pero todos comparten algunos inconvenientes: la falta de difusión, la falta de capacitación, la falta de documentación específica, la falta de integración (se necesita dominar varias herramientas) y especialmente la falta de enfoque hacía un problema concreto.

Muchas de estas "soluciones" libres son CDs o DVDs que incluyen colecciones de miles de programas con distintos fines, especialmente el hackeo y exploits [G35] de sistemas. Por lo tanto, cuando alguien coloca uno de estos CDs o DVDs en un computador los antivirus [G48] activan sus mensajes de alerta. Esto desmotiva al investigador y plantean la duda de si la herramienta debe ser retirada de inmediato o continuar con su aplicación y "afrontar las consecuencias". Muchos de los mensajes de alerta, en estos casos, son simples falsos positivos [G49], pero otros pueden ser reales y perjudiciales si no conocemos el origen del CD o DVD. Por consiguiente, se hace necesario un estudio serio que apunte al conocimiento especializado, encaminado a un uso serio, profesional y apegado a la legalidad de estos programas.

1.3.7 LA PREGUNTA RECTORA DEL PROBLEMA QUE SE INVESTIGA

Entonces, el problema de investigación de este trabajo tiene esta pregunta rectora:

¿CUÁLES SON LOS PROGRAMAS DE SOFTWARE LIBRE QUE PERMITEN REALIZAR EL ANÁLISIS FORENSE DE INCIDENTES DE SEGURIDAD RELACIONADOS CON ENTIDADES DEDICADAS A LA INTELIGENCIA Y SEGURIDAD CIUDADANA EN EL ECUADOR?

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Realizar un estudio de los programas de software libre que permitan ejecutar el análisis forense de incidentes de seguridad, especialmente, en entidades ecuatorianas dedicadas a inteligencia y seguridad pública.

1.4.2 OBJETIVOS ESPECÍFICOS

- Investigar las vulnerabilidades del protocolo TCP/IP, sobre todo los denominados "agujeros de seguridad" y los "exploits" que permiten a un atacante ingresar y/o alterar un sistema de cómputo.
- Investigar los programas de software libre que permiten identificar y prevenir las vulnerabilidades.
- Investigar los programas de software libre que permitan realizar el monitoreo, seguimiento y rastreo de atacantes o intrusos a través de una red.
- Investigar los programas de software libre que permitan crear "honeypots" o "honeynets" esto es, trampas de miel para despistar a los atacantes.
- Elaborar conclusiones y recomendaciones.

1.5 MARCO TEÓRICO Y CONCEPTUAL DE LA INFORMÁTICA FORENSE

1.5.1 ANTECEDENTES EN EL MUNDO

La informática forense tiene sus raíces en la investigación forense. Ya en 1814, el químico y profesor español Manuel Orfila publicó el Tratado de los Venenos donde se documentaba la detección de distintas sustancias toxicas.

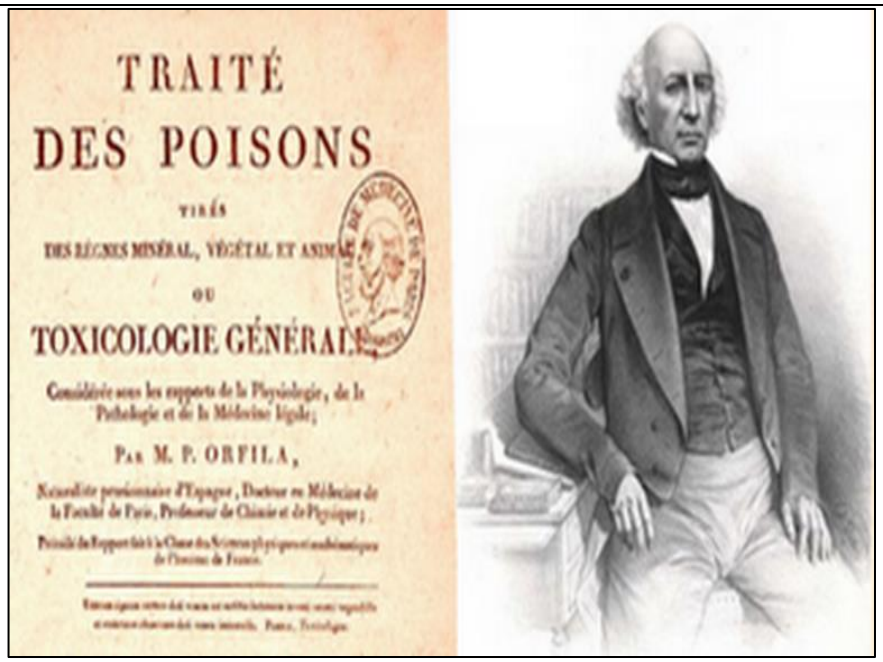


Gráfico 05: Portada del Tratado de Los Venenos 1814. Ref. [1-04]

La informática forense, como disciplina reconocida, aplicada a los computadores, nace en la década de 1970 cuando el FBI [G50] emite las primeras recomendaciones para el análisis de computadores y para el manejo de la evidencia digital [G32].

En 1978, Florida reconoce los crímenes de sistemas informáticos en el "Computer Crimes Act", en casos de sabotaje, copyright, modificación de datos y ataques similares [G17].

En 1981, aparece el programa Copy II PC de Central Point Software. Este fue el primer programa "forense" que se usó para la copia exacta de disquetes, que generalmente estaban protegidos para evitar copias piratas. El producto sería integrado posteriormente en las "Pc Tools". La compañía PCTOOLS fue un éxito y será comprada por Symantec en 1994.

COPYII PC pasó a ser una herramienta con dos fines diferentes por ser usado tanto por los investigadores forenses como por "infractores" o "piratas". Desde entonces esta característica acompaña a los programas forenses. La instrumento forense, entonces, es neutral y puede ser usado para el bien -investigación forense- o para el mal -hacking y piratería.

En 1984, el FBI forma el Magnetic Media Program que más tarde, en 1991, constituye el Computer Analysis and Response Team (CART).

En 1988, se crea la International Association of Computer Investigative Specialists (IACIS), que certificará a profesionales de agencias gubernamentales en el Certified Forensic Computer Examiner (CFCE) [G12] y la CFEC- Computer Forensic External Certification [G12], una de las certificaciones más prestigiosas en el ámbito forense.

El libro "A forensic methodology for countering computer crime", de P. A. Collier y B. J. Spaul define, en 1992, el término "computer forensics". Otros libros posteriores continuarán desarrollando el término y la metodología como el libro "High-Technology Crime: Investigating Cases Involving Computers" de Kenneth S. Rosenblatt.En 1995, se funda la International Organization on Computer Evidence (IOCE) con el objetivo de ser un punto de

encuentro entre especialistas en evidencia electrónica e intercambio de información. A partir de 1996, la Interpol organiza los International "Forensic Science Symposium" como foros para debatir los avances forenses, uniendo fuerzas y conocimientos.

En agosto de 2001 nace la "Digital Forensic Research Workshop" (DFRWS) un nuevo grupo de debate y discusión internacional para compartir información relacionada con forensia digital [G08].

Se puede afirmar que a partir del año 2000 la informática forense llega a la madurez, especialmente, a través del RFC 3227 [G10] y las Guías del Reino Unido, Hong Kong, Australia, las guías del Departamento de Defensa DoD (Department of Defense) de Estados Unidos y el Departamento de Justicia DoJ (Department of Justice) de Estados Unidos.

Actualmente, varios países como Estados Unidos, Gran Bretaña, Francia, Australia, Hong Kong disponen de organizaciones muy especializadas en temas de informática forense, sobresaliendo las siguientes guías:

- DoJ EEUU Investigación en la Escena del Crimen Electrónico [G13] (Guía DoJ 1) Departamento de Justicia de los EEUU
- DoJ EEUU Examen Forense de Evidencia Digital (Guía DoJ 2) Departamento de Justicia de los EEUU
- ACPO Guía De Buenas Prácticas Para Evidencia Basada En Computadores (Guía Reino Unido)
- Guía para El Manejo De Evidencia En IT (Guía Australia)
- ISFS Computación Forense [G06] Parte 2: Mejores Prácticas (Guía Hong Kong)

En el Ecuador, la situación de la informática forense y forensia en redes es bastante incipiente y se menciona a continuación.

1.5.2 ANTECEDENTES DE LA INFORMÁTICA FORENSE EN EL ECUADOR

El 19 de mayo de 1998 nace el Instituto Ecuatoriano de Propiedad Intelectual (IEPI) que, si bien no se relaciona con informática forense, constituye el ente rector de patentes, delitos e infracciones a la propiedad intelectual del software, estableciendo al estado ecuatoriano como su defensor. Entonces, el IEPI queda instaurado como la autoridad administrativa ecuatoriana a cargo de los delitos a la propiedad intelectual mientras que, la Fiscalía General del Estado es la autoridad judicial a cargo de delitos civiles y penales incluyendo destrucción y mal uso de equipos y programas informáticos, según lo establece el código de procedimiento civil.

En octubre 2007, el Dr. Santiago Acurio del Pino, ecuatoriano, Director de la Unidad de Delitos Informáticos de la Fiscalía General del Estado, publicó el documento "ECUADOR: Introducción a la Informática Forense. [G02]", donde describe los principios básicos y los principales términos.

En agosto 2008, la empresa BANRED presentó, en Quito, la primera Conferencia sobre Informática Forense para el Sector Financiero. La exposición estuvo a cargo del ecuatoriano Ricardo Ortega Ortega y otros expertos de Brasil y Argentina.

En el año 2009, se crea en el Ecuador la empresa DIGIWARE, subsidiaria de una empresa colombiana del mismo nombre, dedicada a investigar temas de seguridad, con el Ing. Ramón Valdez a la cabeza. Este mismo año en el Ecuador, la Escuela Politécnica Nacional inicia cursos de informática forense en varias entidades públicas con el Máster Ricardo Ortega.

Posteriormente, la Ing. Lilia Quituisaca Samaniego (Universidad Central del Ecuador) publicó el documento digital denominado "Informática Forense" con el objetivo de socializar el tema entre los especialistas informáticos. Aparece, además, en el Ecuador la empresa Blue Hat Consulting dedicada a dictar cursos de Hacking Ético y el uso de herramientas de vulnerabilidad y protección.

Finalmente, en el año 2011, la Escuela Politécnica Nacional empieza a dictar cursos de Hacking Ético con los Ingenieros Pablo Pazmiño y Pedro Ponce.

1.5.3 ¿POR QUÉ ES ATRACTIVO EL DELITO INFORMÁTICO?

El delito informático es atractivo principalmente por estas diez razones:

1. **DEPENDENCIA DE LA TECNOLOGÍA:** la relación estrecha con la tecnología hace que los usuarios se conviertan en dependientes de ella.

2. **ANONIMATO Y SUPLANTACIÓN DE IDENTIDAD:** la relativa facilidad para — "desaparecer" en el mundo virtual dificulta el rastreo de los responsables de acciones maliciosas u ilegales. Además, es sencillo para el atacante hacerse encubrir su identidad o hacerse pasar por otros usuarios.

3. **FACILIDAD DE ADAPTACIÓN:** las herramientas pueden ser modificadas fácilmente para adaptarse al medio y a las dificultades encontradas durante su empleo.

4. **ESCALABILIDAD:** un solo programa dañino (de ataque [G17] o transacción) puede generar grandes ingresos.

5. **UNIVERSALIDAD DE ACCESO:** cualquiera puede convertirse en un delincuente porque las herramientas están al alcance de todos, al igual que las víctimas.

6. **PROLIFERACIÓN DE HERRAMIENTAS Y CÓDIGOS:** este ítem se encuentra relacionado directamente con el punto anterior, ya que internet provee las herramientas necesarias para que cualquier persona con escasos conocimientos pueda cometer un delito informático.

7. **DIFICULTAD PARA PERSEGUIR A LOS CULPABLES**: Las jurisdicciones internacionales son un obstáculo que dificulta establecer caminos legales para llegar a un atacante.

8. **INTANGIBILIDAD DE LAS PRUEBAS:** si tenemos en cuenta que este tipo de delitos se llevan a cabo en el mundo virtual, obtener pruebas válidas para lograr que la corte las comprenda y considere, representa cierta dificultad y prolijidad en el diseño y exposición de las evidencias.

9. **GRUPOS DE DELINCUENTES PROFESIONALES:** miles de grupos integrados por distintos personajes con diversos niveles de conocimiento, muchos de ellos relacionado solo virtualmente.

10. **ESCASA CONCIENCIA POR PARTE DEL USUARIO:** Los usuarios pueden acceder a todo tipo de tecnología sin recibir capacitación al respecto.

El Dr. Santiago Acurio define el siguiente triángulo del delito informático:

Gráfico 06 : Triángulo del delito, se combina el motivo, la oportunidad y los medios. Ref. [R]

1.6 HIPÓTESIS O IDEA A DEFENDER

La hipótesis central de este trabajo, que responde a la pregunta rectora (definida en 1.3.7) y es se plantea a continuación:

Existen programas de software libre adecuados para realizar las actividades de análisis forense y la prevención de incidentes de seguridad, pero hacen falta estudios de casos y guías para que los oficiales de seguridad y los administradores de sistemas y redes puedan conocer y aplicar estas soluciones adecuadamente.

1.7 OPERACIONALIZACIÓN DE LA INVESTIGACIÓN

1.7.1 VARIABLES

VARIABLE INDEPENDIENTE

Colecciones de programas para forensia en redes y protección contra incidentes de seguridad.

VARIABLES DEPENDIENTES

- Detección de vulnerabilidades
- Monitoreo y seguimiento
- Bloqueo de intrusiones
- Facilidad de implementación y uso
- Costos en la implementación

1.7.2 DIMENSIONES

DIMENSIÓN TECNOLÓGICA:

- Detección de vulnerabilidades
- Monitoreo y seguimiento de incidentes
- Bloqueo de intrusiones
- Facilidad de implementación y uso

DIMENSIÓN ECONÓMICA

- Costos de implementación

1.7.3 INDICADORES

NÚMERO DE USUARIOS

- Utilización del software libre
- Facilidad de implementación y uso

NÚMERO DE VULNERABILIDADES

- Seguridad perimetral
- Nivel de seguridad moderado

CAPITAL INVERTIDO

- Costos en la implementación

1.8 PROCEDIMIENTO Y MARCO METODOLÓGICO

1.8.1 METODOLOGÍA

El método de análisis que se utilizará es el deductivo ya que se partirá de conocimientos generales aceptados como válidos para llegar a una conclusión de tipo particular.

1.8.2 TÉCNICAS

Para la realización de este trabajo se usaron las siguientes técnicas:

- Encuestas y entrevistas a técnicos
- Investigación Bibliográfica
- Investigación en Internet
- Observación

- Análisis
- Validación de lo investigado al utilizar máquinas virtuales y reales

1.8.3 UNIVERSO Y/O MUESTRA

La unidad de observación y análisis, el objeto de este trabajo, son las colecciones de CDs y DVDs que incluyen forensia en redes.

La planificación contempla realizar encuestas al menos a veinte entidades públicas y entrevistas al menos a cinco funcionarios responsables de seguridades.

CAPÍTULO II: LAS REDES Y EL ANÁLISIS FORENSE

"Conoce a tu enemigo y conócete a ti mismo y podrás librar cien batallas sin desastre".
--Sun Tzu, El Arte de la Guerra

2.1 INTRODUCCIÓN

Las redes de computadores por cable o por aire son la vía de acceso de los usuarios, pero también de intrusos y atacantes. Salvo pocos expertos, la mayoría de usuarios, así como la mayoría de informáticos, asume que el protocolo TCP/IP es sólido y por lo tanto, confiable. Esto es relativamente cierto cuando se lo usa en condiciones normales pero también es cierto que los atacantes, trabajando en equipo y compartiendo información, se dan modos para conocer los usuarios y las contraseñas estándar, averiguar nuevas vulnerabilidades y forzar errores o comportamientos anormales en el protocolo TCP/IP. Esto se puede dar mediante el envío de paquetes incompletos, envío de paquetes fuera de secuencia, alterando las cabeceras de las tramas, o simplemente vulnerando los computadores por los que pasa el tráfico, y comprometiendo, en consecuencia, la información que pasa por ese computador.

Las palabras, el vocabulario y los términos usados en seguridades e informática forense deben ser adecuados y cautelosos, sorteando exageraciones, juicios de valor y evitando vulnerar los derechos humanos o civiles de los involucrados. Es así que no se habla de ataques sino de "incidentes", y no se habla de atacante sino "intruso". Solamente luego de concluido el análisis forense y jurídico se podrá determinar si en verdad el intruso fue un atacante o fue simplemente un curioso, y si el incidente fue un ataque que amerita castigo.

¿QUÉ ES LA FORENSIA EN REDES?

El análisis forense aplicado a redes de computadoras se conoce como "forensia en redes" o "network forensics" y busca conocer quién vulnera un sistema, cómo, cuándo, y las consecuencias de este acto dentro de una red en un período determinado de tiempo, así como el vector de ataque [G25]. En ciertos casos, se denomina "forensia en redes" al rastreo de correos electrónicos para conocer su origen, aunque la tendencia es separar esta actividad del concepto general; ya que el rastreo de correo electrónicos puede hacerse con un conocimiento básico de redes, mientras que la forensia en redes exige un alto conocimiento de las redes, protocolos, servidores y dispositivos de comunicación.

La forensia en redes es entonces una rama especializada de la informática forense. Esta rama del conocimiento tiene ciertas particularidades. La forensia en redes, por ejemplo, tiene un mayor alcance, ya que cubre todos los dispositivos de red y a veces debe incluir a internet, con sus enlaces, servidores y equipos de comunicación y las distintas huellas y logs [G29] que va dejando el paso de un intruso a través de las redes. Otra diferencia es que los distintos computadores o dispositivos de comunicación pertenecen a distintas organizaciones que no siempre están dispuestas a cooperar o que tienen distintas políticas para respaldo y entrega de registros de uso o de acceso.

PARTICULARIDADES DE TCP/IP

A continuación se presentan algunas particularidades del protocolo TCP/IP que, desde el punto de vista de la forensia en redes, son importantes e inherentes al protocolo y no se pueden cambiar. Éstas representan a la vez una ventaja y una desventaja puesto que son conocidas tanto por los responsables de seguridad como por los intrusos y atacantes. La

persona que realiza forensia en redes debe conocer estas y otras particularidades para poder cumplir eficientemente su análisis.

NO EXISTE EL ANONIMATO 100% AL NAVEGAR POR INTERNET

La dirección MAC [G51] y las características de un computador son prácticamente únicas, y si eso no es suficiente, cada proveedor de internet lleva un registro de ingreso y tiempos para control de facturación de cada uno de sus usuarios. Por lo tanto, es posible determinar con precisión toda la cadena desde el computador de origen hasta el computador de destino; es posible, pero no siempre es viable como veremos más adelante.

La mayoría de personas creen que existe el anonimato en la navegación por internet, en el uso de la telefonía o en el uso de las redes. Dicho en otras palabras, se sienten libres de hacer lo que sea porque piensan que el computador no está controlado ni sujeto a restricciones. Esta suposición es falsa, ya que todo usuario contrata algún servicio que lleva control de facturación; todo usuario se conecta a internet o a una red a través de una infraestructura que puede llegar a ser identificada perfectamente. Esto se aplica igualmente a las redes inalámbricas.

TODO USUARIO RECIBE UNA IP PÚBLICA EXCLUSIVA O COMPARTIDA

Todo usuario ingresa a la red local a través de una IP privada o pública, pero para navegar es necesario usar una IP pública, perfectamente conocida e identificada. Esta IP pública es asignada por el proveedor de internet y puede ser compartida por decenas o cientos de usuarios, esto hace posible que, a la larga, se pueda identificar a cada usuario. La IP pública se puede averiguar fácilmente con servicios www.verip.es o www.ipchicken.com y cientos de sitios similares.

Su IP real es: [redacted]

Ver Mapa

Dirección IP Properties	Values
Navegador:	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) ; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; AskTbATU3/5.14.0.19709; .NET4.0C)
Hora local:	Domingo, 01 de Julio de 2012 9:47:20 Sun, 1 Jul 2012 14:47:20 UTC
Pais:	uy-Uruguay
Ciudad:	
Idioma(s):	es-ec
Nombre de Host:	

Navegador (Usuario-Agente) Exposed Headers	Values
Accept:	image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, */*
Accept-Encoding:	gzip, deflate
Connection	close

Computer/Device Properties	Values
Javascript:	Javascript 1.3 JScript 5.8.18702
Cookies Enabled:	yes
Java Enabled:	yes
Flash Enabled:	yes - version 10
CPU class/type:	CPU Class x86
Screen Width:	1920
Screen Height:	1080
Screen Color Depth:	32
Window Width:	970 (50.5% of 1920)
Window Height:	842 (78.0% of 1080)

Gráfico 07: Información de ip real del host. Ref. [2-01]

Aquí se demuestra que el servidor de destino es capaz de detectar (y por consiguiente, de almacenar, catalogar) e informar a posibles interesados acerca de las características del

computador de origen, como el tipo de CPU, resolución de pantalla, idioma, ubicación regional, etc.

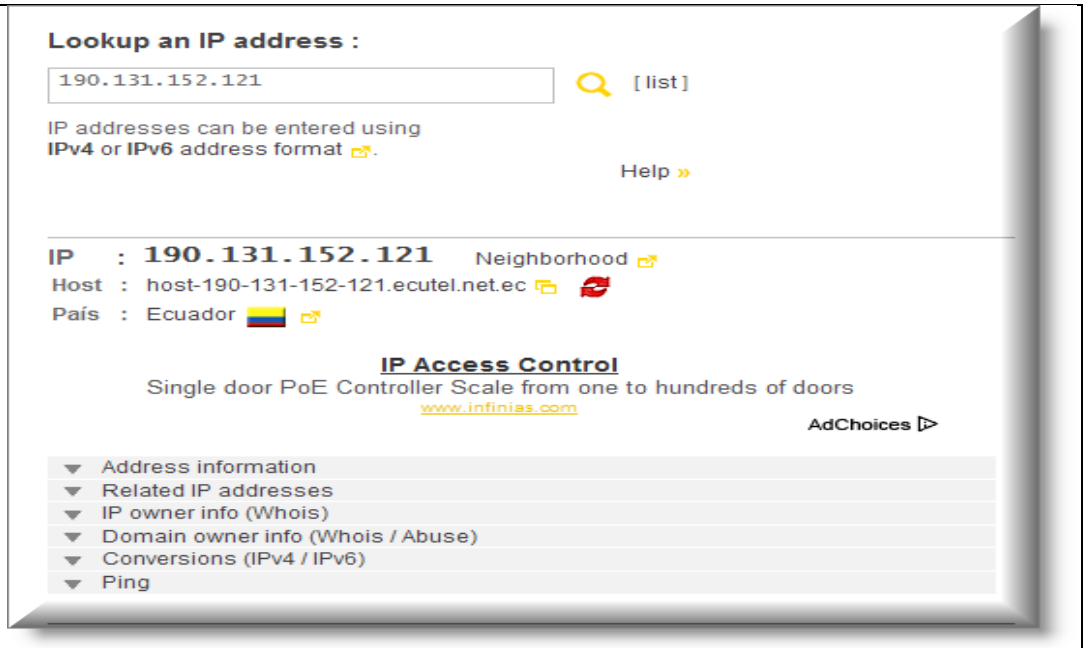


Gráfico 08: Información ubicación de host (MAC/IP) en el sitio iplookup . Ref. [2-02]

Es perfectamente posible conocer la pareja MAC/IP [G52] y así establecer el equipo desde el cual se realizó la conexión. El protocolo TCP/IP exige conocer la dirección MAC de origen de una conexión y, en casi el cien por ciento de ocasiones, se graban los registros de acceso de cuándo y desde qué pareja MAC / IP o ubicación se produjo el acceso. Es muy difícil si no imposible, falsificar una dirección IP.

En otros sitios como www.geoiptool.com se puede observar la ubicación en un mapa de google y que permite conocer dentro de un rango aproximado de 40 kilómetros la geolocalización de una dirección IP.

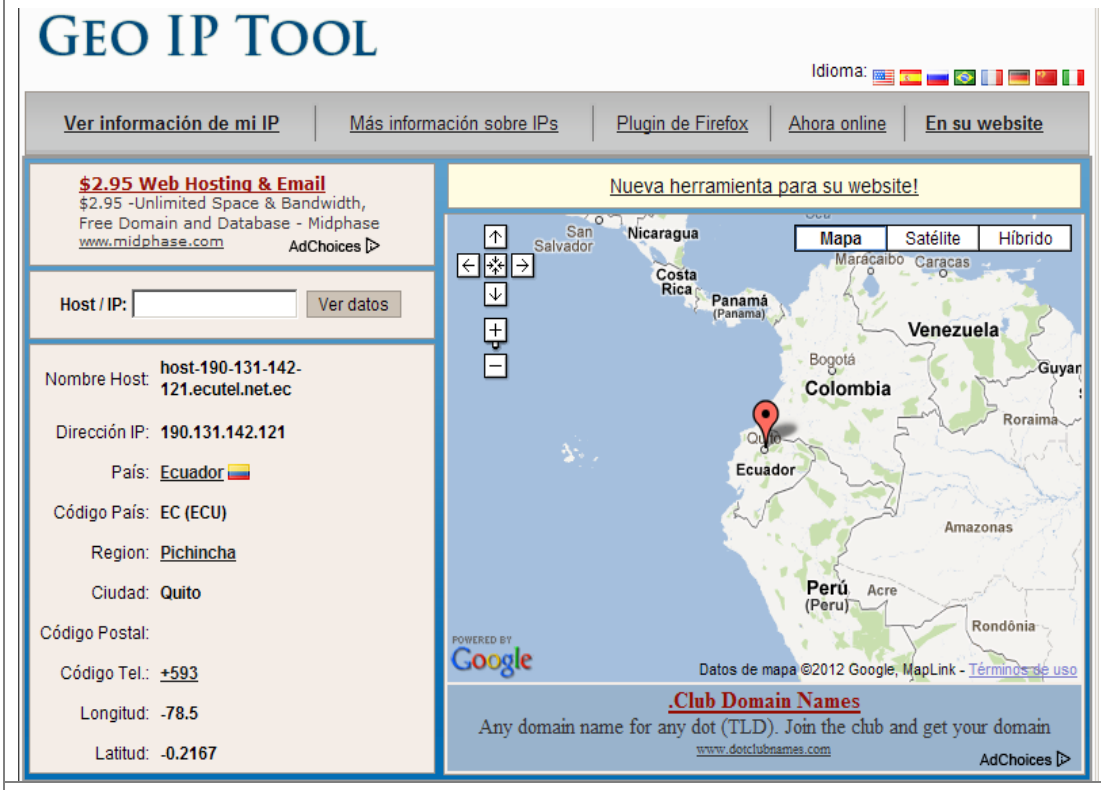


Gráfico 09: Geoip Tool en funcionamiento Ref. [2-03]

Incluso existen servicios que ofrecen rastreo y rescate de equipos o dispositivos móviles basados en la dirección IP pública que se utiliza para navegar[1].

[1] Servicios de Geo localización, www.preyproject.org

En definitiva, estamos demostrando que no existe la navegación anónima ya que siempre se puede conocer el origen de una conexión.

Frente a esta falta de privacidad, han surgido servicios como proxy servers o el proyecto TOR [2] que ofrecen lo que se conoce como "navegación anónima". Estos servidores reciben la conexión perfectamente identificable y la canalizan por servidores geográficamente distantes (por ejemplo en Bélgica, Holanda, Canadá), pero la realidad es que solamente introducen un equipo intermediario. En el año 2012, se conoció que sí es posible averiguar la dirección IP original de un navegante usando el cache almacenado en los servidores de TOR, con lo cual la "navegación anónima" no es posible a menos que se adopten precauciones extremas. El mismo sitio TOR alerta acerca del uso de otros protocolos y del envío de información que pueden revelar el origen de la conexión.

Sin embargo, la batalla continúa entre aquellos que buscan un anonimato al usar el internet y aquellos que buscan encontrar las huellas y el origen de los hechos ilícitos. En los casos de redes locales, es bien sabido que los sistemas operativos más utilizados para puertas de enlace (Linux y Windows) almacenan registros de todo el tráfico de red, a menos que alguien lo haya eliminado deliberadamente. De hecho, una de las primeras tareas de un atacante, cuando logra ingresar a una red, es borrar sus huellas, destruyendo los logs de acceso y los registros de intentos fallidos. Esta tarea no siempre se logra, ya que las organizaciones grandes ponen a salvo tales registros en otros computadores o en otros medios a los que un atacante podría no tener acceso.

[2] Proyecto TOR, (www.torproject.org)

En consecuencia, el investigador forense tiene a su alcance los registros de actividad de los diferentes equipos por los cuales ingresó el atacante (vector de ataque); aunque existen ciertas condiciones, puesto que estos registros se borran cada cierto tiempo y muchos administradores de equipos pueden negarse a proporcionar esta información a menos que exista un requerimiento judicial.

LOGS Y REGISTROS DE ACCESOS [G29].

La mayoría de servidores de internet con una IP pública se encuentran bajo ataque constante. Es responsabilidad de los administradores bloquear e impedir tales intentos mediante técnicas de detección IDS y prevención IPS.

Aquí se presenta un log real, de una actividad ilícita usando el comando lastb:

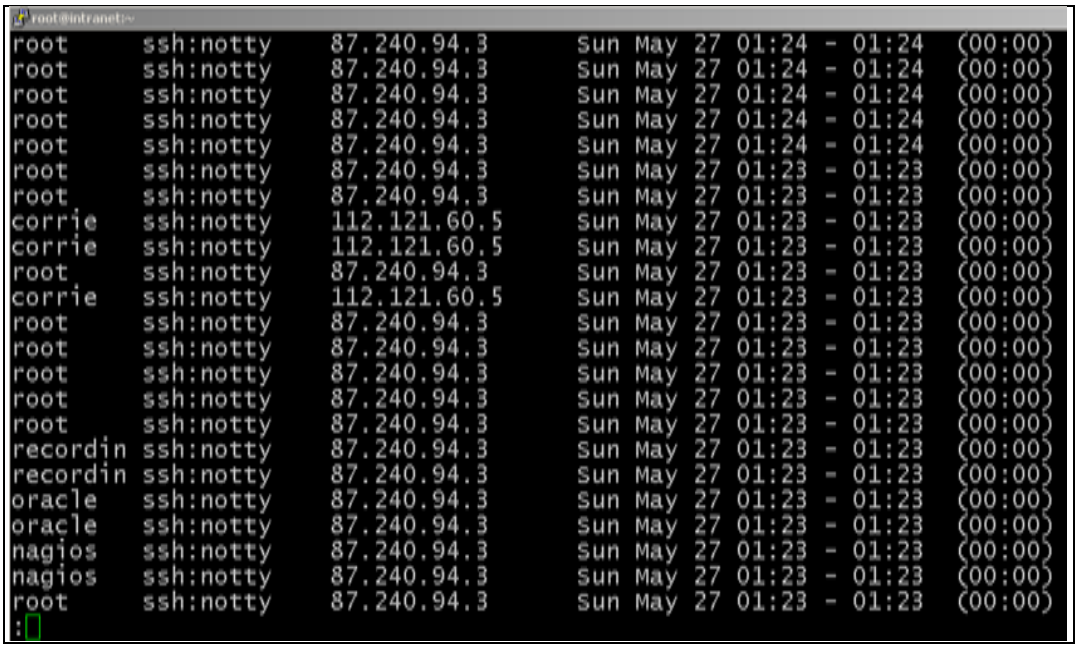


Gráfico A1: Comando linux –lastb.

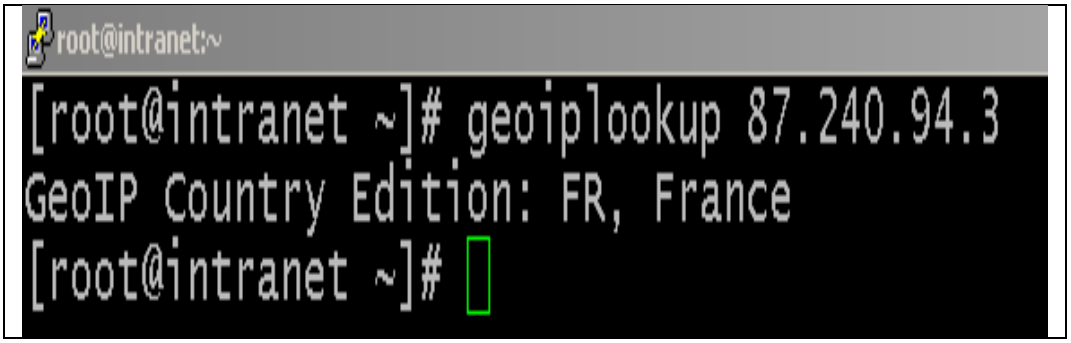


Gráfico A2: Comando linux – geoiplookup.

Los programas **nmap** y **netstat** permiten conocer los puertos abiertos de un computador. Los sniffers como **iptraf, ethereal, winpcap y wireshark** permiten "olfatear", mirar y capturar todo el tráfico de una red.

En resumen, se demuestra aquí que el protocolo TCP/IP no es tan seguro como parece, ya que tiene características que lo vuelven vulnerable y que revelan tanto el origen como el destino de la conexión. Otro hecho que estamos demostrando es que existen suficientes herramientas para monitorear y conocer el tráfico de una red pero se debe recordar que en ambientes de intenso tráfico, los logs se borran en un corto tiempo y es por eso importante una intervención rápida.

Una buena noticia, es que ya hay esfuerzos iniciales de numerosas instituciones y empresas preocupadas por la ciberseguridad en el país, tales como el Comando Conjunto de FFAA, la Policía Judicial, Superintendencia de Telecomunicaciones, Universidades, Empresas particulares y personas como las mencionadas en el capítulo 1, que realizan esfuerzos para difundir la ciberseguridad. Lamentablemente, estos esfuerzos aislados todavía están lejos de constituirse en centros de respuesta a nivel de país. Una iniciativa de este tipo requeriría equipamiento, personal y una legislación conforme al alcance del proyecto de seguridad.

2.2 DISPONIBILIDAD DE INFORMACIÓN ACERCA DEL ANÁLISIS FORENSE.

Se ha diseñado un Glosario en el Capítulo 6, con conceptos relacionados a seguridad informática, informática forense, grupos de respuesta inmediata, grupos de cooperación.

Gráfico 10: Captura de pantalla de web con noticias de seguridad informática Ref. [2-04]

2.2.1 SITIOS WEB ESPECIALIZADOS EN SEGURIDAD

- Norton SafeWeb, https://safeweb.norton.com/
- All Nettools, http://www.all-nettools.com/toolbox/privacy.htm
- Anonymous Surfing, http://www.anonymizer.com
- CYBERPASS, http://www.cyberpass.net

- KIOSKEA, http://es.kioskea.net
- TOR Project, http://www.torproject.org
- CERT - INSTITUTE CARNEGIE MELLON, www.cert.org

Gráfico 11: Captura de pantalla: CERT- Carnegie Mellon University Ref. [2-05]

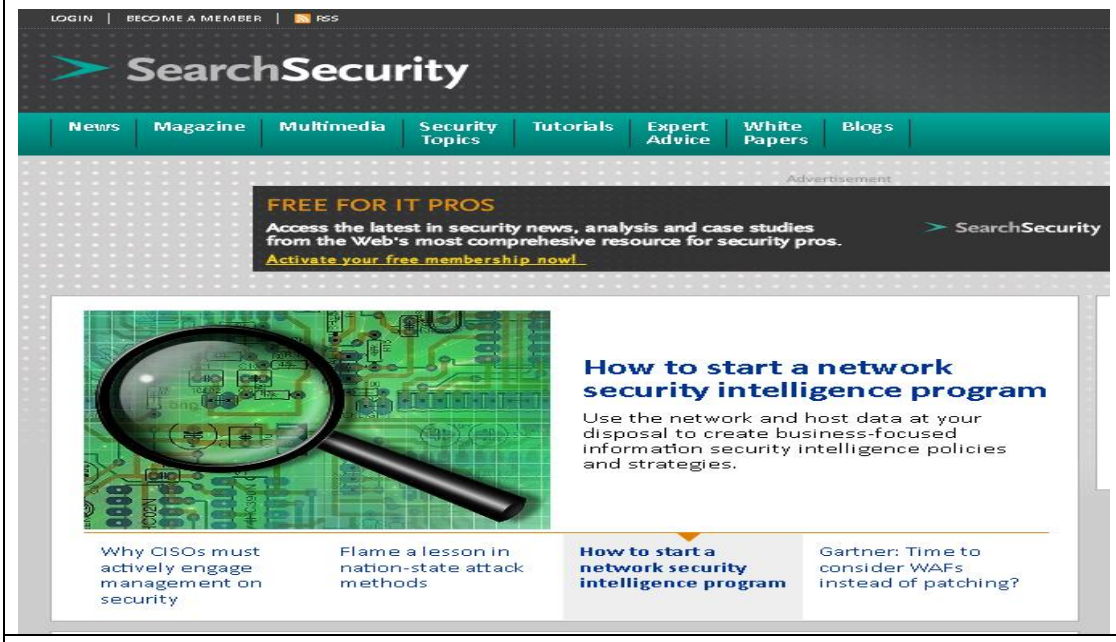


Gráfico 12: Captura de pantalla: web de seguridad Ref. [2-06]

Gráfico 13: Eventos de base de datos de vulnerabilidades open source (OSVDB). Ref [2-07]

2.2.2 CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

- **DELITO INFORMÁTICO**

El Dr. Santiago Acurio, Director de Tecnología de la Fiscalía General del Estado, define al delito informático como:

> *"Todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera"* [3].

- **INCIDENTE INFORMÁTICO**

Un incidente es cualquier suceso o acontecimiento no planeado que pueda causar o cause lesiones daño al equipo o al ambiente. Un incidente de seguridad es*: "cualquier evento adverso, real o potencial, vinculado a la seguridad de los sistemas informáticos o a las redes informáticas. Es el acto de violar una política de seguridad explícita o implícita".*[4]

2.2.3 TIPOS DE INCIDENTES Y/O DELITOS INFORMÁTICOS

Según el Dr. Acurio en la fuente de ref. 1 expone que los incidentes sujetos a análisis forense se pueden representar como indica el gráfico 14. En el que se puede apreciar que entre el

---

[3] *Dr. Acurio, Santiago, Derecho Penal Informático, PUCE 2010.*

[4] www.cert.org

emisor (fuente de información) y el receptor (destinatario de la información), el ***flujo normal sigue el camino más corto***.

1) En los ***incidentes de interrupción*** de información, el receptor no recibe la información, produciéndose una falta de servicio. Lo que se conoce como ***DoS o Denegación de Servicio***.
2) En los ***incidentes de intercepción*** de información, el receptor recibe información, pero también lo recibe un tercero, este ataque es denominado Man in Middle (MiM) [G20]. (sniffer, robo de identidad**,** (cyberbulling) [G30], robo de contraseñas, desvío de tráfico).
3) En los ***incidentes de modificación*** de la información, el receptor recibe ***información modificada***, distinta de la que se emite, el ataque se denomina Replay [G21].
4) En los incidentes de fabricación de información, el receptor recibe información que nunca fue generada por el emisor (suplantación de identidad o phishing [G20]).

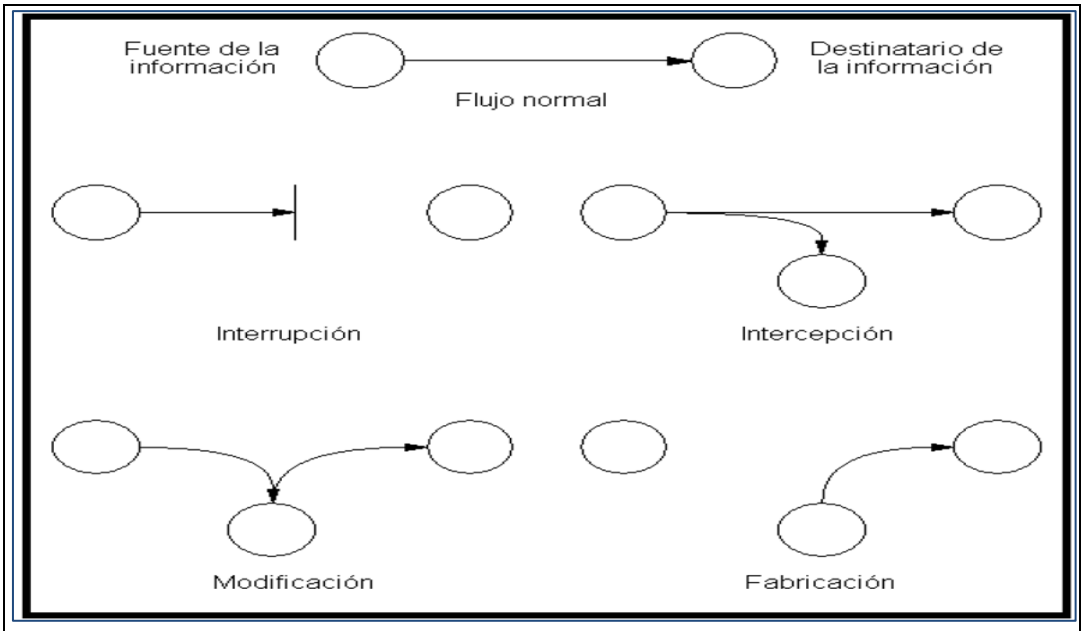


Gráfico 14: Tipos de incidentes y/o delitos informáticos. Ref. [X]

2.2.4 TIPOS DE DELITOS INFORMÁTICOS SEGÚN NACIONES UNIDAS	
1)	**DELITO DE FALSIFICACIÓN INFORMÁTICA**
Manipulación de los datos de entrada	Este tipo de fraude informático, conocido también como sustracción de datos, es muy común ya que es fácil de cometer y difícil de descubrir. No requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
Manipulación de programas.	Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método comúnmente utilizado es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal
Manipulación de los datos de salida.	Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude del que son objeto los cajeros automáticos, donde se falsifican las instrucciones de la computadora en la fase de adquisición de datos. En la actualidad se usan equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
Fraude efectuado por manipulación informática.	Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas", apenas perceptibles, de transacciones financieras se van sacando repetidamente de una cuenta y se transfieren a otra.
2)	**DELITO DE FALSIFICACIÓN INFORMÁTICA**
Como objeto	Cuando se alteran los datos almacenados en el computador.
Como instrumento	Las computadoras pueden utilizarse para falsificar documentos, hacer copias, modificar o crear documentos.

3)	**DELITO DE SABOTAJE**
Sabotaje informático	Es el acto de borrar, suprimir o modificar, sin autorización, funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.
Virus	Serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así el Caballo de Troya.
Gusanos	Se fabrican de forma análoga a los virus, con miras a infiltrarlo en programas legítimos de procesamiento de datos para modificar o destruir los datos. Es diferente del virus porque no puede regenerarse. Las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus por ejemplo: dar instrucciones a un sistema de un banco para que transfiera continuamente dinero a una cuenta ilícita.
Bomba lógica o cronológica	Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, a diferencia de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten, por lo que de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño.
Piratas informáticos o hackers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. Los piratas informáticos se hacen pasar por usuarios legítimos del sistema. Esto suele suceder en los sistemas con

	contraseñas débiles.
Reproducción no autorizada de programas informáticos.	Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

Tabla 01 : Clasificación de los delitos informáticos según Naciones Unidas [Ref. W]

2.2.5 NAVEGACIÓN ANÓNIMA

Se llama navegación anónima al uso de programas o mecanismos que buscan impedir que el sistema de cómputo destinatario, al queremos llegar, pueda obtener la información de nuestro sistema de cómputo (dirección IP, MAC, resolución de pantalla, cookies y los miles de datos que se pueden obtener a través de una conexión TCP/IP).

Aquí un interesante texto sobre el anonimato:

> *"Existen muchas situaciones en las que convendría navegar anónimamente sin dejar trazas de nuestra identidad, ya que con estos datos y mediante programas de búsqueda de personas por su dirección de correo, se puede obtener la identidad del cibernauta, incluyendo su número de teléfono, dirección, y más. Por ejemplo, la red de DoubleClick fue capaz de identificar las preferencias sobre vacaciones en cruceros*

de más de 10 millones de personas en la red. Gracias a esa información, les enviaba anuncios a la medida de sus gustos"[5].

¿CÓMO SE NAVEGA ANÓNIMAMENTE?

1) ANONIMIZADORES

El servicio de anonimato actúa como un filtro de seguridad entre tu navegador y el sitio Web que deseas visitar. Te conectas al anonimizador, introduces el URL al que deseas ir, entonces éste se adentra en la Red en busca de la página que deseas ver y te la muestra. Si posteriormente vas siguiendo enlaces de una página a otra, se presentarán asimismo a través del anonimizador, el servicio de navegación anónima más conocido es Anonymous Surfing.

Sus inconvenientes:

- ✓ No funcionan con todos los sitios ni con los servidores seguros.
- ✓ Tampoco se reciben cookies (que puede representar un alivio al tema de privacidad).
- ✓ Desactivan todos los programas en Java, JavaScript, etc. (ventaja o inconveniente según quien las use).
- ✓ Ralentizan la navegación.
- ✓ Para un servicio óptimo hay que pagar.
- ✓ Añaden a las páginas que visitamos banners con publicidad de sus patrocinadores.

2) SERVIDORES PROXY [G54]

También se puede navegar anónimamente a través de un servidor proxy. La idea básica de un servidor proxy es actuar de pasarela (Gateway) entre tu máquina o tu red y la Internet.

[5] *Voight, J, "Beyond the banner",http://www.iec.csic.es/criptonomicon/anonimato.html*

Normalmente se usan para llevar las peticiones del cliente a través de unos cortafuegos (firewall). El proxy espera a una petición desde el interior del cortafuego y la despacha al servidor remoto en el exterior, lee la respuesta y la envía de vuelta al cliente.

En la práctica, todos los clientes en una subred salen a través del mismo proxy, por lo que también pueden prestar servicios como caché de documentos que son necesidades de seguridad de muchas organizaciones. De esta forma se reduce el coste de tráfico de red, ya que a menudo gran cantidad de documentos son recuperados desde el caché local una vez que la petición inicial ha sido hecha.

Así pues, el servidor proxy actúa de manera semejante a un anonimizador, ya que es el que recupera las páginas Web, en lugar de la persona que está navegando. Sin embargo, presentan una serie de limitaciones frente a los anonimizadores:

- ✓ No impiden que las cookies se sigan almacenando en el disco duro del usuario.
- ✓ Normalmente todas las visitas quedan registradas en el proxy.
- ✓ La dirección IP del servidor proxy, por defecto, refleja tu nombre de dominio o se acerca mucho.

Se puede navegar anónimamente a través de proxies en:

- proxy1.emirates.net.ae, HTTP port 8080
- wwwcache.marques.co.za, HTTP port 3128
- proxy.chs.edu.sg, HTTP port 3128
- proxy.pty.com, HTTP port 8080
- proxy.silcom.com, HTTP port 3128
- proxy.tmc.edu.tw, HTTP port 3128

- webcache.ms.mff.cuni.cz, HTTP port 8080
- littlehat.zetnet.co.uk, HTTP port 8080
- proxy.networld.it, HTTP port 80 g
- proxy.hro.nl, HTTP port 80
- Digilab.tau.it, HTTP port 80
- proxy.ecity.net, HTTP port 80
- proxy.ipm.lviv.ua, HTTP port 80

3) EL ANONIMATO ES UN ESTILO.

Por muy eficaces que parezcan, ninguno de los métodos de navegación anónima asegura una navegación totalmente incógnita, especialmente si tu estilo de navegación es despreocupado. He aquí algunos consejos prácticos para maximizar la utilidad de proxy y túnel anónimo:

- ✓ Si viertes opiniones, no llames demasiado la atención y no dejes datos personales.
- ✓ Los plugins pueden hacer imposible el anonimato: usa FlashBlock y NoScript
- ✓ Carga el navegador en modo privado: de esta forma, no se crearán cookies peligrosas
- ✓ Si transmites información importante, cifra los datos con PGP u otros programas
- ✓ En última instancia, el anonimato sólo es una herramienta, y como tal puede usarse para los más diversos propósitos. Hay quien ataca las redes por la posibilidad que tienen los criminales de ocultar su actividad, mientras que otros ven en ellas una autopista para la libertad de expresión.
- ✓ El uso que hagas de ellas depende exclusivamente de ti.

4) LOS TÚNELES CIFRADOS DE TOR

TOR, es el sistema de navegación anónima más popular. Se trata de una red de "túneles" por los cuales los datos de navegación, debidamente cifrados, atraviesan múltiples nodos hasta

llegar a su destino. En la práctica, equivale a navegar anónimamente, puesto que nadie puede reconducir esos datos a tu IP real. A continuación se muestra es el panel de control de Tor, que aparece una vez que instalado el paquete completo. Si usas Firefox, no necesitas tocar nada. Una vez que Tor esté conectado a su red de túneles, te bastará hacer clic en *TorButton*, la extensión que modifica la configuración de Firefox para que use Tor a la hora de navegar. En esta captura de ejemplo, la conocida página *GeoBytes* afirma que estamos en Texas, a más de ocho mil kilómetros de sitio real.

Gráfico 15: Captura de pantalla de consola TOR. Ref. [2-08]

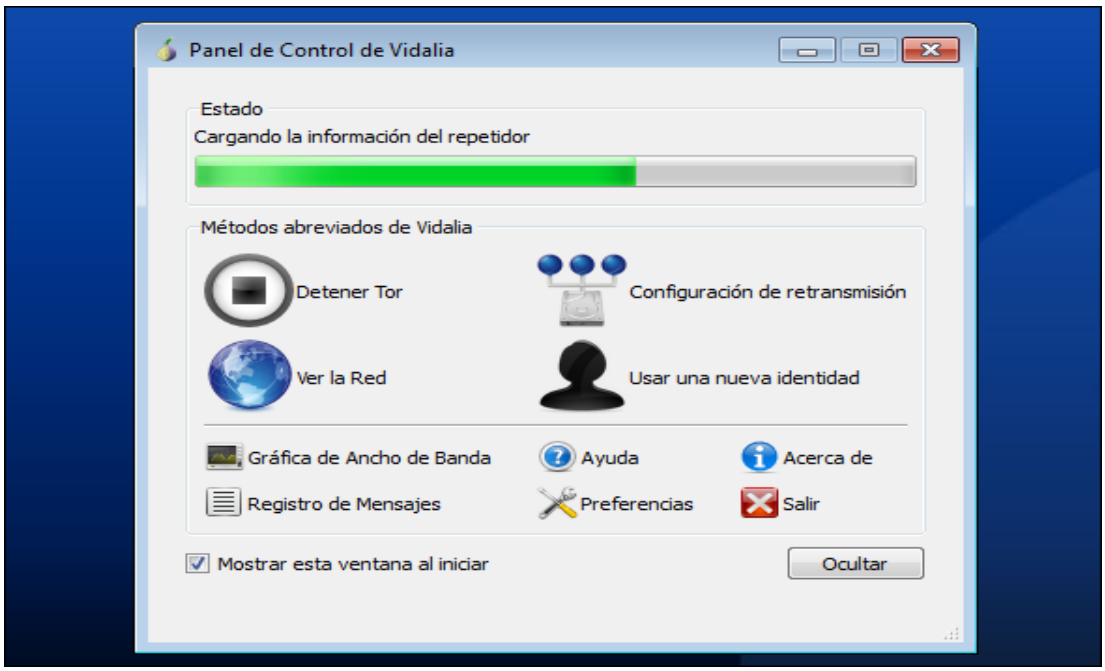


Gráfico 16: Captura de pantalla de la configuración de TOR. Ref. **[2-09]**

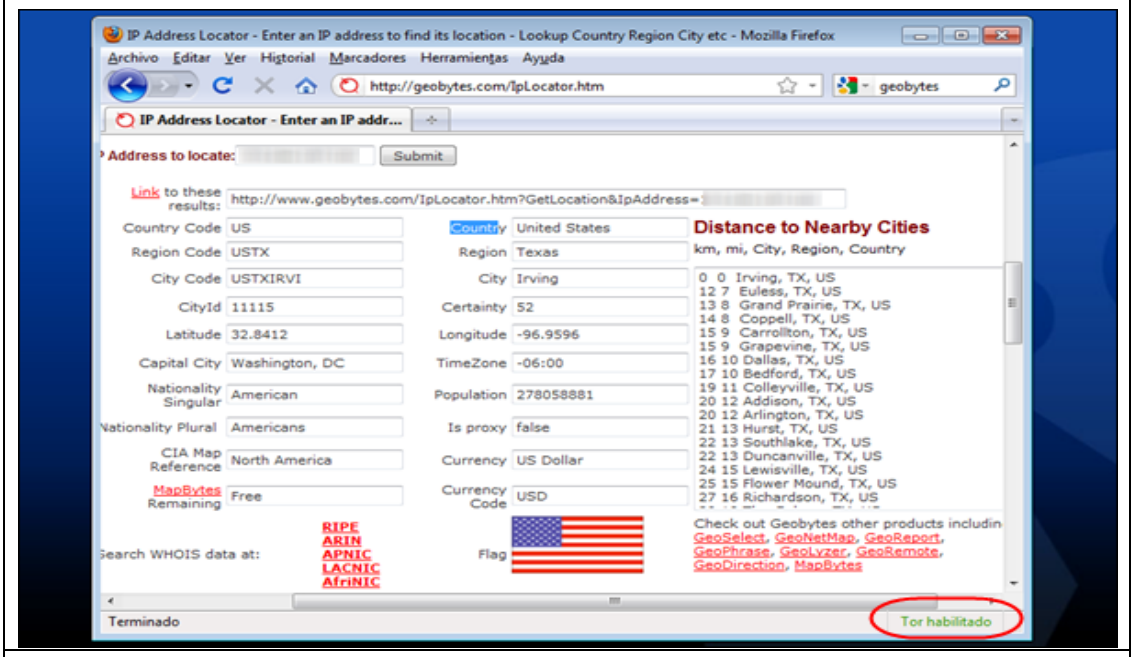


Gráfico 17: Captura de pantalla del funcionamiento web con TOR habilitado. Ref. [2-10]

2.3 ENCUESTA DE INCIDENTES DE SEGURIDAD

Ver Anexo 1: Modelo de Encuesta a Responsables de Centros de Datos

Se recibieron un total de 72 respuestas, de las cuales 42 (58%) corresponden a técnicos varones, y 30 (42%) corresponden a técnicos y oficiales mujeres.

2.3.1 GRÁFICAS DE RESULTADOS

1. GÉNERO	
	Frecuencia
FEMENINO	30
MASCULINO	42
TOTAL	72

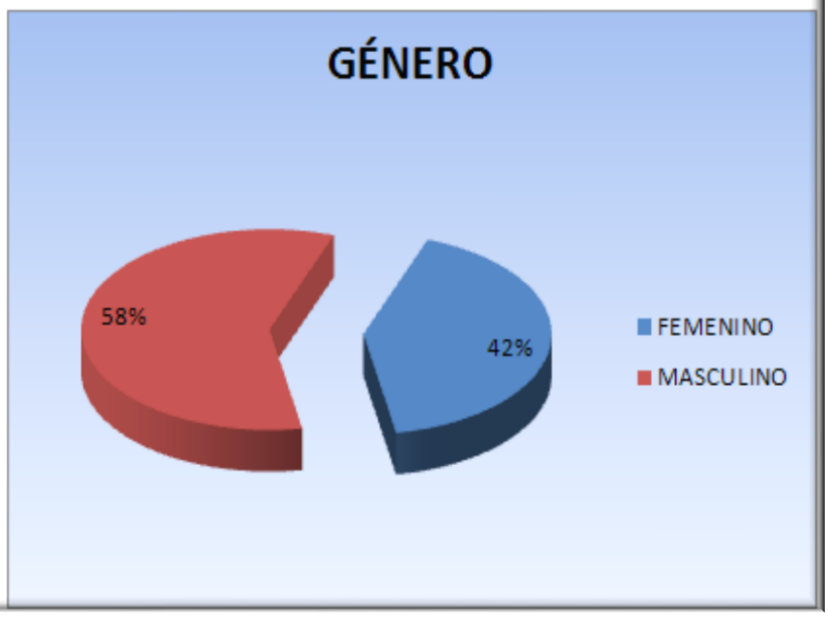


Gráfico A3: Resultado de encuestas, según el género.

El 58% de encuestados son varones.

3. TAMANO DE LA ORGANIZACION

	Frecuencia	Porcentaje
EMP. PÚBLICA GRANDE	60	83%
EMP. PÚBLICA MEDIAN	12	17%
Total	72	100%

Gráfico A4: Resultado de encuestas, según tamaño de la organización.

El 60% de encuestados pertenecen a empresas grandes.

4. ORGANIZACIÓN DEDICADA A LA SEGURIDAD CIUDADANA

	Frecuencia	% Acumulado	PARETO (80 - 20)
SI	48	67%	80%
PARCIALMENTE	18	92%	80%
NO	6	100%	80%
Total	72		

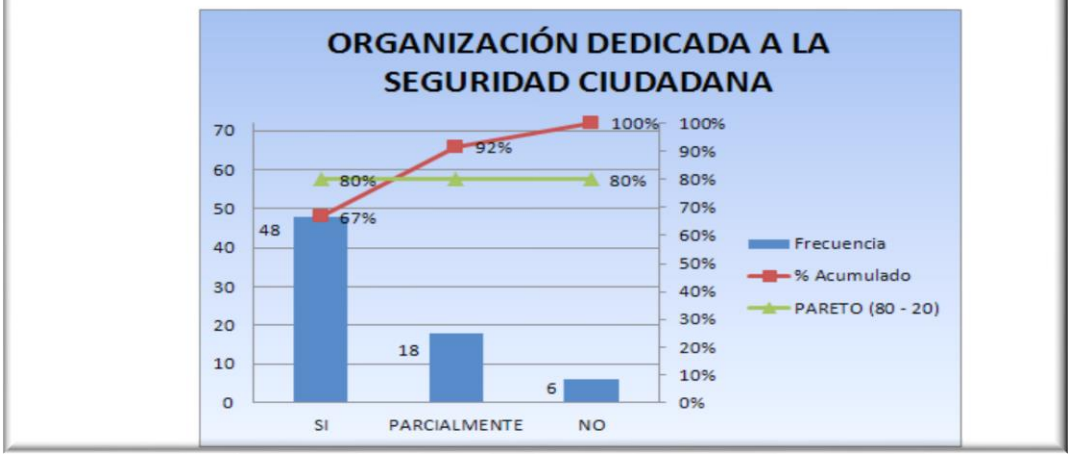


Gráfico A5: Resultado de encuestas, según el nivel de dedicación a la seguridad ciudadana.

Se encuentra que el 92 % tiene por misión, preservar la seguridad ciudadana.

6. LA INFORMÁTICA FORENSE SE PARECE AL HACKING ÉTICO

	Frecuencia	Porcentaje	% Acumulado
NO	48	67%	67%
NO, SE PARECEN EN ALGO	24	100%	100%
Total	72		

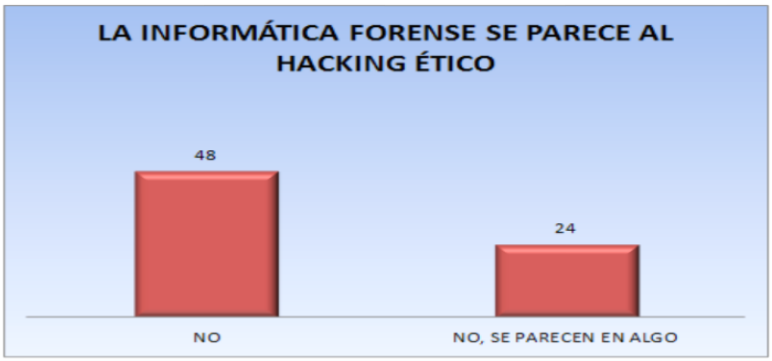


Gráfico A6: Resultado de la pregunta: La informática forense se parece al hacking ético?.

El 62 % responde que las dos disciplinas, no tienen relación.

7. CONOCE USTED LOS PRINCIPIOS DE LA INFORMÁTICA FORENSE

	Frecuencia	% Acumulado	PARETO (80 - 20)
POCO	30	42%	80%
NADA	26	78%	80%
LO NECESARIO	16	100%	80%
Total	72		

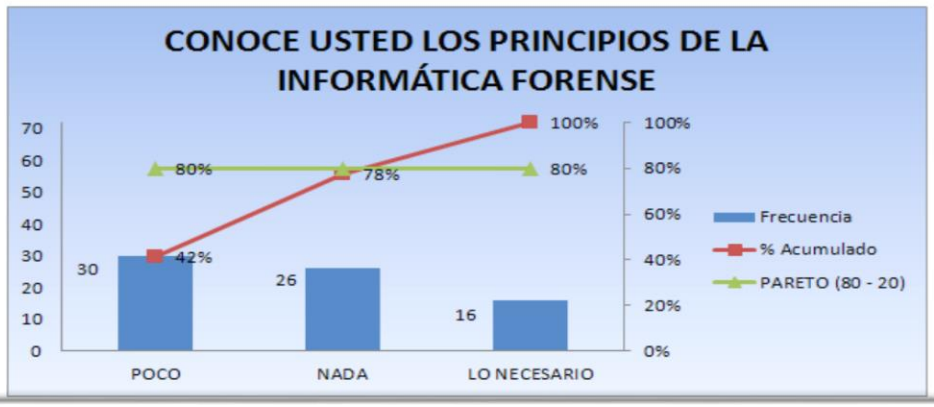


Gráfico A7: Resultado de la pregunta: Conoce usted los principios de la informática forense?.

El 63% responde no tener conocimientos de los principios de la informática forense.

8. CUANDO APLICARIA SU ORGANIZACION EL ANALISIS FORENSE ?

	Frecuencia	% Acumulado	PARETO (80 - 20)
POSIBLES DELITOS	40	56%	80%
SOLO EN DELITOS	30	97%	80%
MUERTES	2	100%	80%
Total	72		

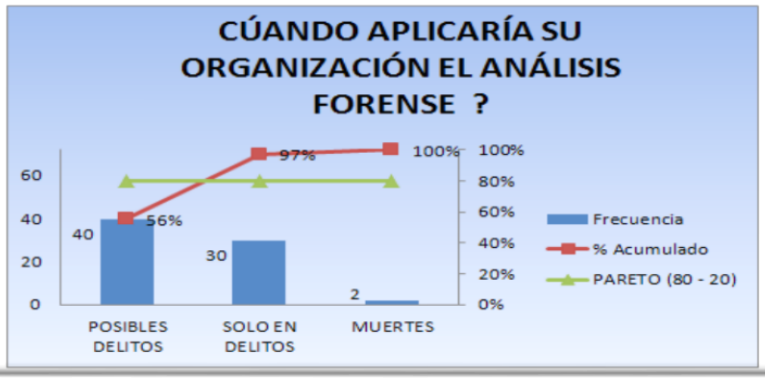


Gráfico A8: Resultado de la pregunta: Cuándo aplicaría su organización el análisis forense?.

El 97% de los encuestados relacionan el análisis forense con delitos.

9. MEDIDAS QUE SU ORGANIZACION TOMARIA EN UNA ESCENA DE UN INCIDENTE INFORMÁTICO

	Frecuencia	% Acumulado	PARETO (80 - 20)
IMPEDIR ACCESO	42	40%	80%
TOMAR EVIDENCIAS	22	62%	80%
LLAMAR A LA PJ	22	83%	80%
LLAMAR A ESPECIALISTAS	12	94%	80%
TOMAR FOTOS Y VIDEOS	6	100%	80%
Total	104		

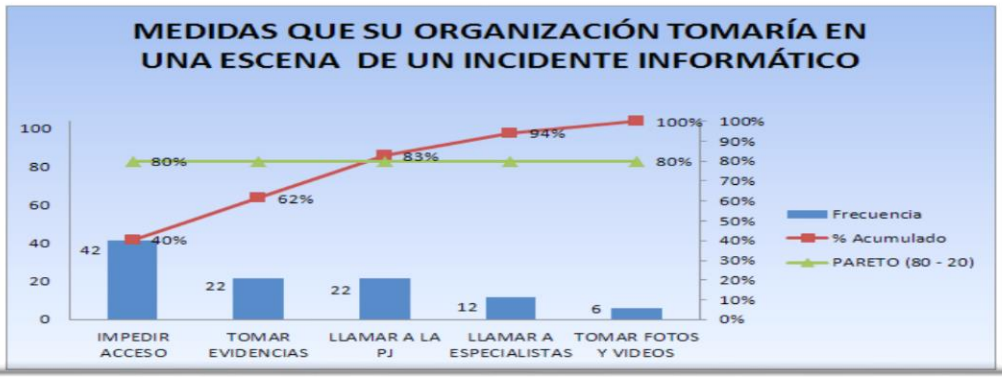


Gráfico A9: Medidas que su organización tomaría en una escena de un incidente informático.

El 83% responde que tomaría la siguiente medida: impedir acceso.

10. EL PRINCIPIO DE LOCARD ES ?

	Frecuencia	% Acumulado	PARETO (80 - 20)
UNA RELACIÓN ENTRE LA ESCENA, LA VÍCTIMA Y EL AUTOR	30	42%	80%
UN ESTÁNDAR MUNDIAL	24	75%	80%
UNA FORMA DE SACAR	18	100%	80%
Total	72		

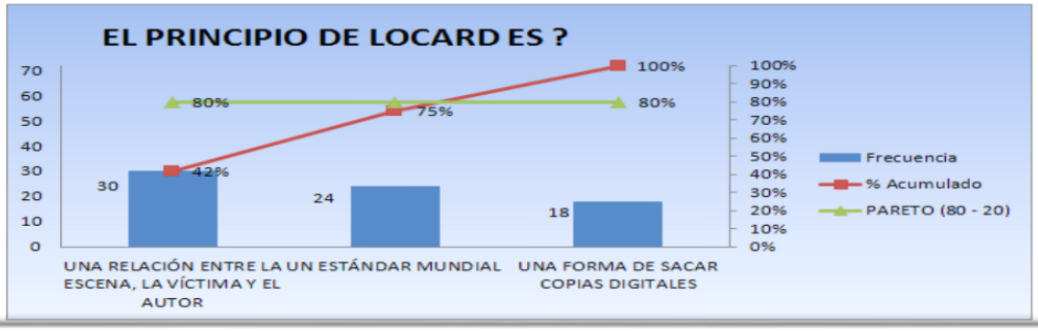


Gráfico A10: Resultado de la pregunta: ¿El principio de Locard es?.

El 42% responde que es: "Una relación entre la escena, la víctima y el autor".

13. EN NUESTRA ORGANIZACION SABEMOS LO QUE ES EL DEBIDO PROCESO

	Frecuencia	% Acumulado	PARETO (80 - 20)
POCO	48	67%	80%
NADA	12	83%	80%
LO NECESARIO	12	100%	80%
Total	72		

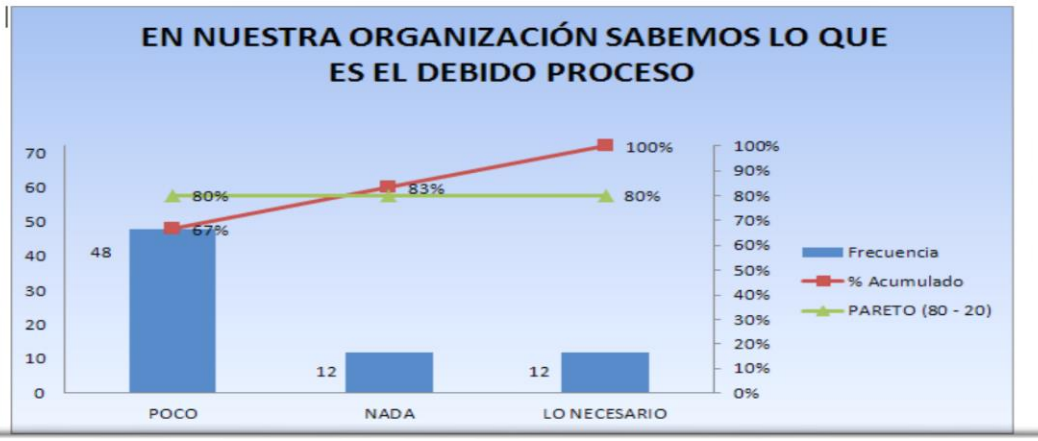


Gráfico A11: Resultado de la pregunta: En la organización sabemos lo que es el debido proceso.

El 67% responde "Poco" y el 16% responde "Nada".

14. POR FAVOR INCLUIR NOMBRES DE ORGANIZACIONES QUE REALICEN INFORMÁTICA FORENSE

RESPUESTAS : NINGUNA

15. POR FAVOR INCLUIR NOMBRES DE CERTIFICACIONES REGIONALES O MUNDIALES PARA INFORMÁTICA FORENSE

RESPUESTAS : NINGUNA

16. CUÁNTOS INCIDENTES DE SEGURIDAD O DELITOS CONOCE DE PRIMERA MANO QUE SE SOLUCIONARON CON ANÁLISIS FORENSE

RESPUESTAS : NO HAY PRECISION EN RESPUESTAS, MUY GENERAL

17. CUÁNTOS INCIDENTES DE SEGURIDAD O DELITOS CONOCE DE PRIMERA MANO QUE PUDIERAN SOLUCIONARSE CON ANÁLISIS FORENSE

RESPUESTAS : RESPUESTAS VAGAS Y ESCASAS

18. MENCIONE ALGUNOS PROGRAMAS PROPIETARIOS PARA INFORMÁTICA FORENSE

RESPUESTAS : NINGUNA

19. MENSIONE ALGUNOS PROGRAMAS PROPIETARIOS DE SOFTWARE LIBRE PARA INFORMÁTICA FORENSE

RESPUESTAS : NINGUNA

20. LE PARECE CONFIABLE EL SOFTWARE LIBRE PARA INFORMÁTICA FORENSE

RESPUESTAS : NINGUNA

Gráfico A12: Resultado de las preguntas 14-20.

No hay aportes significativos.

2.3.2 INTERPRETACIÓN DE LAS ENCUESTAS

Como se puede evidenciar en las respuestas de la 14 a la 20 donde se pide puntualizar nombres de empresas, organizaciones o programas. No se obtuvo prácticamente ningún resultado, demostrando un total desconocimiento de la informática forense y de los programas de software libre utilizados para el desarrollo del análisis forense.

Las respuestas 1 a 13 están explicadas junto a su respectivo gráfico.

2.4 VULNERABILIDADES IMPORTANTES DEL TCP/IP

El diseño y el funcionamiento de TCP/IP contienen varias vulnerabilidades [G05] que deben ser tomadas en cuenta. Entre las más destacadas se pueden citar:

2.4.1. LA MAYORÍA DE PROTOCOLOS DE TCP/IP NO SON CIFRADOS

Esto significa que la mayoría de paquetes, texto e información viaja sin cifrar por los distintos computadores que componen la red de internet desde el origen hasta el destino y, por lo tanto, dicha información está disponible para cualquiera que tenga los medios, los conocimientos y la oportunidad para obtener dicha información.

Esto se agrava por el hecho de que muchos computadores realizan grabación de logs o caché de la información. Nuestra comunicación, nuestros mensajes, las páginas que hemos visitado, lo que hemos escrito en los formularios web, en la barra de direcciones, en los mensajes de correo, o en los mensajes instantáneos, en twitter, Facebook, etc., se encuentran por lo tanto, almacenada en decenas, quizá cientos de computadores diseminados por internet.

Existen protocolos cifrados como https, ftps, pop3s, imaps, pero la inmensa mayoría de usuarios no los conoce y no los usa.

2.4.2 UN GRUPO DE MÁQUINAS COMPARTEN LA MISMA ID DE RED

Esta característica intrínseca, propia del diseño de TCP/IP permite que un computador de la red pueda husmear en el tráfico que circula por la red. Esto se conoce como sniffing y puede ser un simple olfateo de la red o una búsqueda de palabras clave, passwords y otros datos de interés. El sniffing se agrava por el hecho de que muchas tarjetas de red pueden activar el

modo conocido como "promiscuo" es decir que pueden aceptar todo el tráfico que viaja por la red local.

En el Gráfico A13, se puede apreciar el programa wireshark que está recopilando todos los paquetes de una pequeña red local que sirvió como ejemplo.

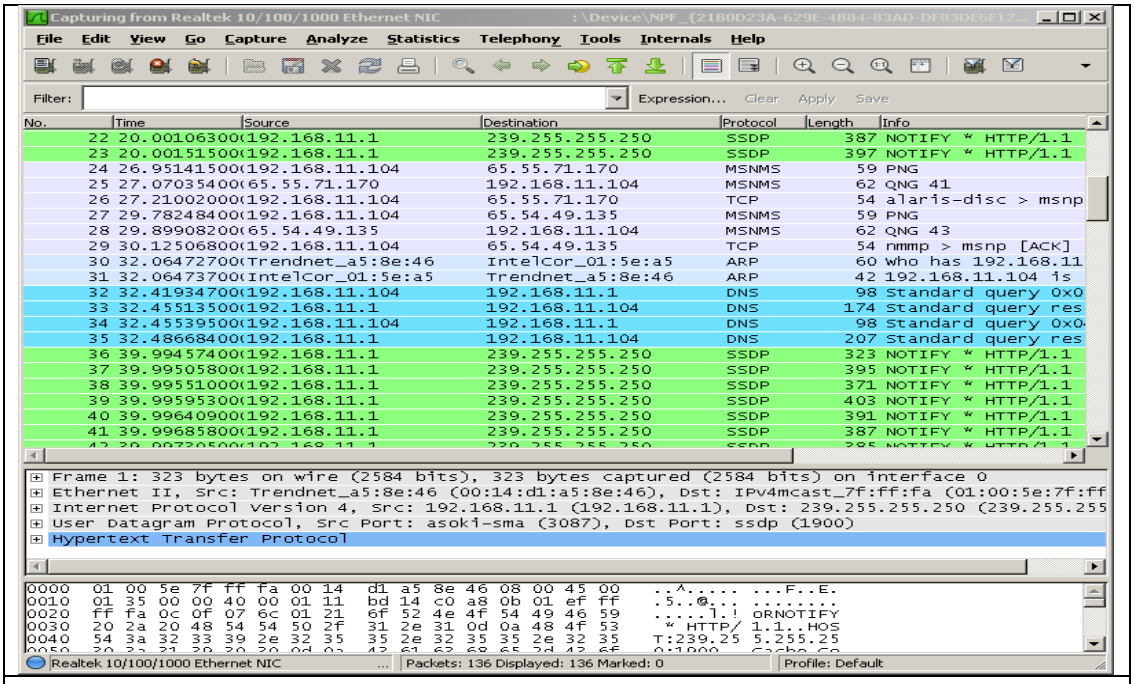


Gráfico A13: Captura de pantalla de wireshark

En esta pequeña muestra se puede mirar el tráfico de messenger, el tráfico ARP y DNS, lo que permite conocer la dirección MAC de las tarjetas de red de los otros computadores, así como la marca de la tarjeta de red. Se puede apreciar el tráfico ARP desde un equipo a otro. También se puede apreciar el tráfico DNS desde el computador con la IP 192.168.11.104 hacía el router 192.168.11.1. Se puede ver una tarjeta de red de marca Intel (de la maq. 192.168.11.104) y otra de marca Trendnet.

En el panel central podemos mirar el paquete completo desarticulado en sus distintos componentes, mientras en el panel inferior podemos mirar el paquete en modo de texto y donde podríamos abarcar todo el escrito, el mensaje, las claves o números escritos.

En conclusión, la mayoría de protocolos de TCP/IP son vulnerables al uso de sniffings. El sniffing es una técnica poderosa que permite olfatear, husmear, espiar una red en busca de algo interesante.

2.4.3 TODO TRÁFICO DE TCP/IP DEBE PASAR POR UNA PUERTA DE ENLACE O SERVIDOR PROXY

La configuración de red de todo computador que desee navegar por internet debe incluir una puerta de enlace o un equipo servidor proxy. Esta configuración puede ser alterada en el equipo de origen o cuando el equipo de puerta de enlace haya sido infectado o sustituido.

Esta característica permite ataques del tipo Man In The Middle. El MitM puede incluir algunos de los siguientes subataques:

- ✓ Intercepción de la comunicación (eavesdropping [G53]), incluyendo análisis del tráfico y posiblemente un ataque a partir de textos planos (plaintext) conocidos.
- ✓ Ataques a partir de textos cifrados escogidos, en función de lo que el receptor haga con el mensaje descifrado.
- ✓ Ataques de sustitución.
- ✓ Ataques de repetición.
- ✓ Ataque por denegación de servicio (denial of service [G19]). El atacante podría, por ejemplo, bloquear las comunicaciones antes de atacar una de las partes. La defensa en ese caso pasa por el envío periódico de mensajes de status autenticados.

El término **MitM** se emplea para referirse a manipulaciones activas de los mensajes más que para denotar intercepción pasiva de la comunicación, donde se usa el término ***sniffing.***

2.4.4 TODO EQUIPO NECESITA TENER ASIGNADO UN SERVIDOR DNS

Esta característica permite alterar el mecanismo de recuperación de nombres a través de su IP. Por ejemplo se puede lograr que www.pichincha.com vaya a un sitio malicioso para obtener información de usuarios, contraseñas, claves.

Este mecanismo ya fue aprovechado por el troyano **DNS Changer** que infectó y sigue infectando a cientos de miles de computadores. Los computadores infectados tienen en su DNS alguna de las siguientes direcciones que corresponden a servidores que fueron intervenidos por el FBI y fueron desconectados, como consecuencia de lo cual miles de equipos se vieron imposibilitados de navegar por internet.

Starting IP	Ending IP	CIDR
85.255.112.0	85.255.127.255	85.255.112.0/20
67.210.0.0	67.210.15.255	67.210.0.0/20
93.188.160.0	93.188.167.255	93.188.160.0/21
77.67.83.0	77.67.83.255	77.67.83.0/24
213.109.64.0	213.109.79.255	213.109.64.0/20
64.28.176.0	64.28.191.255	64.28.176.0/20

Gráfico 18: Direcciones IP servidores DNS fraudulentos (DNS Changer). Ref. [2-11]

2.4.5 TODO EQUIPO NECESITA UNA DIRECCIÓN MAC

Esta característica tiene sus ventajas y sus desventajas. Entre las desventajas consta que puede resultar sencillo clonar la dirección MAC y generar tráfico malicioso haciendo creer al equipo de destino que está comunicándose con el equipo clonado, cuando en realidad está

comunicándose con el equipo fantasma. Esto da origen a varios tipos de ataques como MitM, phishing, sniffing, suplantación de identidad, alteración de DNS y otros.

2.5 VULNERABILIDADES DE PAQUETES Y PROGRAMAS POPULARES

Todo software, al ser un producto diseñado y desarrollado por grupos de programadores, están potencialmente expuestos a que no se realicen todas las pruebas de integridad y funcionalidad del mismo, por lo que tienen vulnerabilidades [G05]; muchas de las cuales ya ha sido identificadas y se publican en las páginas orientadas a seguridad, y otras se van descubriendo conforme se los va explotando. Estas fallas de programación y/o seguridad se las clasifica de acuerdo a su origen y se destacan:

- Vulnerabilidades de desbordamiento de buffer
- Vulnerabilidades de error de formato de cadena
- Vulnerabilidades de Cross Site Scripting XSS
- Vulnerabilidades de Inyección SQL
- Vulnerabilidades de Inyección de Caracteres CRLF
- Vulnerabilidades de denegación del servicio
- Vulnerabilidades Inyección múltiple HTML Multiple HTML Injection
- Vulnerabilidades de ventanas engañosas Window Spoofing
- Vulnerabilidades de día cero [G22], son aquellas que son descubiertas y publicadas, antes de que el proveedor desarrolle un parche.

2.6 LA FORENSIA EN REDES

¿QUÉ ES?

Es la disciplina técnico–científica que permite conocer quién, qué, cuándo y cómo se produjo un incidente de seguridad en una red de equipos.

¿CÓMO FUNCIONA?

La forensia en redes se basa en la certeza de que no existe el anonimato ni en la navegación ni en el uso de internet. Aunque se utilicen programas que ofrecen navegación anónima como TOR, Proxy y otros; estos servicios también pueden resultar comprometidos o pueden contener fallas.

La forensia en redes se basa en utilizar los conocimientos acerca del funcionamiento del protocolo TCP/IP y de las herramientas que utilizan los crackers para atacar un sistema de cómputo. Esta especialidad informática se vale de técnicas y programas que buscan los logs y los archivos de actividad de los distintos protocolos TCP/IP. Muchas veces se vale de técnicas de "hacking ético" para obtener acceso a información o equipos que normalmente no están disponibles para el usuario promedio.

La diferencia entre el hacking ético y el hacking malicioso es el uso que se le da a la información y acceso obtenido. Ambas modalidades de hacking comparten prácticamente las mismas metodologías y herramientas, motivo por el cual muchos programas antivirus van a impedir que los programas de hacking entre en ejecución. Entonces, se vuelve imprescindible usar una máquina virtual, un CD Vivo (Live CD) o un dispositivo de arranque que no contenga antivirus ni cortafuegos. Para el hacking ético (y aquí otra

semejanza con el hacking malicioso) no es recomendable utilizar una máquina común y corriente que pueda ser fácilmente identificada o que pueda contener información personal del investigador o de la institución.

Así como no existe una sola forma o vector de ataque, no es posible establecer o recomendar un único programa que sirva para investigar o frenar todos los ataques. Lo que se ha hecho en este trabajo es presentar una serie de pautas que siguen los atacantes bajo distintos ambientes y evaluar una serie de programas que pueden ayudar a identificar y obtener evidencias de la actividad del atacante.

EL TIEMPO ES UN FACTOR IMPORTANTE

Es posible rastrear por completo el tráfico y la actividad del atacante desde el equipo de origen hasta el equipo de destino, siempre y cuando se lo haga antes de que alguno de los equipos, a lo largo de la ruta, borre los registros y, por supuesto, siempre que exista la colaboración de los equipos intermedios. En todo caso, se debe actuar de inmediato y en este sentido ayuda la injerencia de los grupos de intervención de emergencias CSIRT [G15].

2.7 EL DEBIDO PROCESO

El debido proceso se denomina a la serie de pasos y medidas que se deben seguir para realizar, adecuadamente y dentro de la legalidad, el análisis forense. Este proceso debe ser cuidadosamente planeado y llevado a la práctica porque debe quedar documentado y ajustado a lo que establecen los estándares. Cualquier actividad ilegal o conflictos con la ley darán como resultado la total invalidación del trabajo de investigación y el desprestigio del investigador.

La Fiscalía y la Policía Nacional del Ecuador han elaborado el Manual de Procedimientos Investigativos[6]. Además, la Fiscalía General del Estado ha elaborado el Manual de Manejo de Evidencias Digitales y Entornos informáticos V 2.0 [7]

El debido proceso se refiere al respeto de los procedimientos que se deben seguir durante un proceso de investigación y posible sanción a los culpables de un ilícito.

El **Art. 76** de la *Constitución del Ecuador 2008* define las siete garantías básicas que deben respetarse en el proceso que se investiga, así como las 12 garantías que comprende el derecho a la defensa. Son de particular importancia las siguientes:

Garantía 2: se presumirá la inocencia de toda persona, y será tratada como tal, mientras no se declare su responsabilidad mediante resolución firme o sentencia ejecutoriada.

Garantía 3*:* Nadie podrá ser juzgado por un acto u omisión que al momento de cometerse no esté tipificado en la ley.

---

[6] Policía Nacional del Ecuador y la Fiscalía General del Estado, Manual de procedimientos investigativos.http://www.dnpj.gob.ec/portal/files/MANUAL%20%20FISCALIA-POLICIA%20JUDICIAL%202011.pdf.

[7] Fiscalía General del Estado, "Manual de Manejo de Evidencias Digitales y Entornos informáticos V 2.0". http://www.oas.org/juridico/english/cyb_pan_manual.pdf.

Garantía 4: Las pruebas obtenidas o actuadas con violación de la Constitución o la ley no tendrán validez alguna y carecerán de eficacia probatoria.

j) Quienes actúen como testigos o peritos estarán obligados a comparecer y responder

m) Recurrir (impugnar) el fallo o resolución.

El debido proceso puede ser violentado por acción u omisión (**Art. 437** de la Constitución 2008). Esto significa que en el análisis forense es tan importante el resultado como la forma en que se llegó al resultado. Dicho de otra manera, no se pueden violar las leyes para obtener evidencias (tales como videos o grabaciones clandestinas, pinchar las líneas telefónicas, invadir propiedad privada, romper la confidencialidad, y cualquier forma de atentar contra los derechos humanos y las garantías constitucionales). Cualquier prueba obtenida violando una norma, ley o derecho internacional es inmediatamente invalidada.

Es importante destacar que el **Art. 169** de la misma constitución, al hablar del debido proceso, establece que no se sacrificará la justicia por la sola omisión de formalidades. Por lo tanto, el debido proceso se refiere a derechos fundamentales de carácter jurídico y no al simple papeleo o el cumplimiento de trámites. Hay que señalar, sin embargo, que la línea divisoria es confusa y se presta a interpretaciones por lo que es preferible no incurrir en causales que puedan invalidar el proceso.

El Dr. Santiago Acurio en su publicación *Derecho Penal Informático,* expone:

> *"De acuerdo a la Constitución Política de la República, en su Título IV, Capítulo 4to, en la sección décima al hablar de la Fiscalía General del Estado, en su Art. 195 señala que: "La Fiscalía dirigirá, de oficio o a petición de parte la investigación pre*

procesal y procesal penal". Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala que "el ejercicio de la acción pública corresponde exclusivamente al fiscal". De lo dicho podemos concluir que el dueño de la acción penal y de la investigación tanto pre procesal como procesal de hechos que sean considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio es el Fiscal. Es por tanto el Fiscal quien deberá liderar dentro de la investigación de esta clase de infracciones de tipo informático para lo cual contara como señala el Art. 208 del Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial quien realizará la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control de la Fiscalía, en tal virtud cualquier resultado de dichas investigaciones se incorporaran en su tiempo ya sea a la Instrucción Fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudaran posteriormente al representante de la Fiscalía a emitir su dictamen correspondiente"[8].

2.8 LA CADENA DE CUSTODIA

El Dr. Julián Halanoca define así la cadena de custodia:

"Es un conjunto de procedimientos ineludibles, en los que prima el tema de seguridad, estos procedimientos se encuentran destinados principalmente a garantizar que el elemento material probatorio o la evidencia física hallada, una vez

[8] Santiago Acurio, *Derecho Penal Informático*, PUCE, 2008.

que ha cumplido con sus requisitos (identificación, recolección, embalaje y rotulación), sea la misma que se encontró en la escena del crimen"[9].

2.9 LA EVIDENCIA DIGITAL.

La palabra EVIDENCIA proviene de latín "*indictum*" que significa signo aparente y probable, señal, muestra o indicación. Evidencia es todo aquello dejado por el autor del delito, como huellas, muestras, rasgos particulares, material sensible significativo que se percibe con los sentidos y tiene relación directa con el hecho investigado.

La evidencia digital [G32] es entonces una evidencia relacionada con información computarizada.

"Cualquier dato que puede establecer que un crimen se ha ejecutado (commit) o puede proporcionar un enlace (link) entre un crimen y su víctima o un crimen y su autor".[10] *[Casey, 2004]*

"Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático". Según el Dr. Julián Hanaloca.

En palabras del Dr. Santiago Acurio (año 2007) la evidencia digital *"es un tipo de prueba física. Está constituida por campos magnéticos y pulsos electrónicos que pueden ser*

---

[9] Halanoca Huamán, Julián, Artículo : "La escena del delito y la cadena de custodia en el nuevo proceso penal", *http://agendamagna.wordpress.com/2009/02/10/julian-cesar-halanoca-huaman/*

[10] Casey, Eoghan, "Handbook of Computer Investigation", 2004

recolectados y analizados con herramientas y técnicas especiales. Ejemplos: archivos, imágenes, sonidos, correos electrónicos, etc."

¿En qué se diferencia la evidencia del indicio?

"El término "evidencia" y el término "indicio", procesalmente hablando, significan exactamente lo mismo. En latín se decía "indictum" y definía a todo aquello que era signo aparente y probable de que existe alguna cosa y también era sinónimo de señal o muestra. Puede decirse que es todo elemento que se percibe con los sentidos y que tiene relación con un hecho que se investiga. La prueba de indicios es indirecta; a partir de un hecho conocido presume la existencia de otro que no se conoce. Por ejemplo: si en un lugar se encuentran manchas de sangre, se presume que alguien sufre una herida o está lastimado. Las manchas de sangre por sí mismas no prueban nada; solo nos llevan a presumir la existencia de otros hechos por una conexión lógica"[11].

El indicio es la presunción de que algo puede haber acontecido, es un principio de prueba. Encontrar algo, por ejemplo un reloj, es un indicio de que a una persona puede haberle sucedido un hecho grave, pero no está confirmado, se necesitan pruebas para completar lo que se busca constatar. La evidencia es la prueba del que el hecho aconteció, sucedió inexorablemente. Ejemplo: Es evidente de que si llueve mucho las calles estén mojadas.

Para el Dr. Julián Halanoca, son términos distintos:

[11] http://estudiemosderecho.blogspot.com/2009/05/indicios-presunciones-y-evidencias.html

> *"Indicio es todo aquello que nos informa de "algo"; por ejemplo una mancha roja en el piso nos permite conocer que hay una sustancia que no debía de estar en el lugar; pero habría que preguntarnos: ¿De qué se trata?, es natural que aún no lo sabemos, podría ser tinta roja, pintura, salsa de tomate, sangre, etc. Evidencia es aquello que nos permite una información particular sobre "algo"; para completar el ejemplo anterior, si a esa misma mancha roja le aplicamos peróxido de hidrógeno (agua oxigenada), pudiera ser que no tenga ninguna reacción, por lo que nos orientamos a pensar que no se trata de ninguna secreción orgánica; pero si comienza a aparecer una espuma blanquecina, significa entonces que se trata de una secreción orgánica; entonces, ello es evidente*".

Podemos decir que, para el público en general, el indicio y la evidencia son conceptos distintos, pero para el proceso de investigación, significan lo mismo y que adicionalmente se pueden convertir en pruebas cuando el juez así lo considere. Esto se dará cuando se haya comprobado la validez del indicio/evidencia.

Entonces, procesalmente hablando, es lo mismo evidencia que indicio pero no es lo mismo evidencia que prueba. Se habla de "prueba" cuando el juez se ha convencido de la validez de la "evidencia". Obtener pruebas es uno de los objetivos de la informática forense es decir, proporcionar suficiente evidencia para que el juez se convenza de la validez. Esto se conoce como "criterios de admisibilidad de la evidencia".

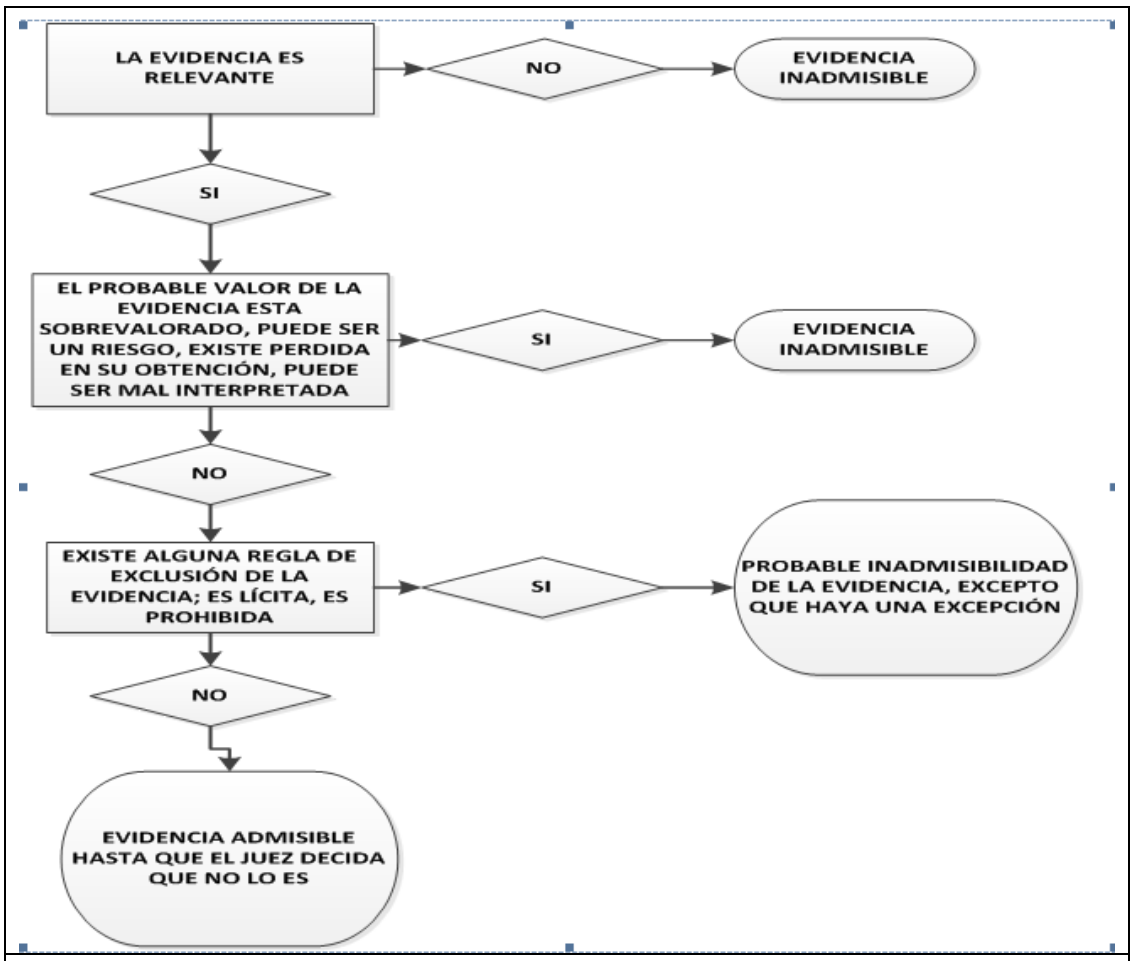


Gráfico 19: Admisibilidad de la evidencia según Santiago Acurio (15/ 04/ 2010.) Ref. [R]

2.10 LAS ETAPAS DEL ANÁLISIS FORENSE.

El análisis forense [G01], se divide en tres etapas perfectamente identificadas:

a) Etapa de Planificación

b) Etapa de ejecución

c) Etapa de presentación de resultados

2.10.1 PLANIFICACIÓN

La planificación consiste en preparar al personal, los materiales, los lugares de almacenamiento y los cronogramas de ejecución. Es importante que toda la fase de ejecución se realice de manera planificada para evitar errores y para evitar invalidar el debido proceso o arruinar las evidencias por falta de una etiqueta, por falta de una adecuada cadena de custodia, o de algo que se debió planificar.

2.10.2 EJECUCIÓN

METODOLOGÍA DE ANÁLISIS FORENSE

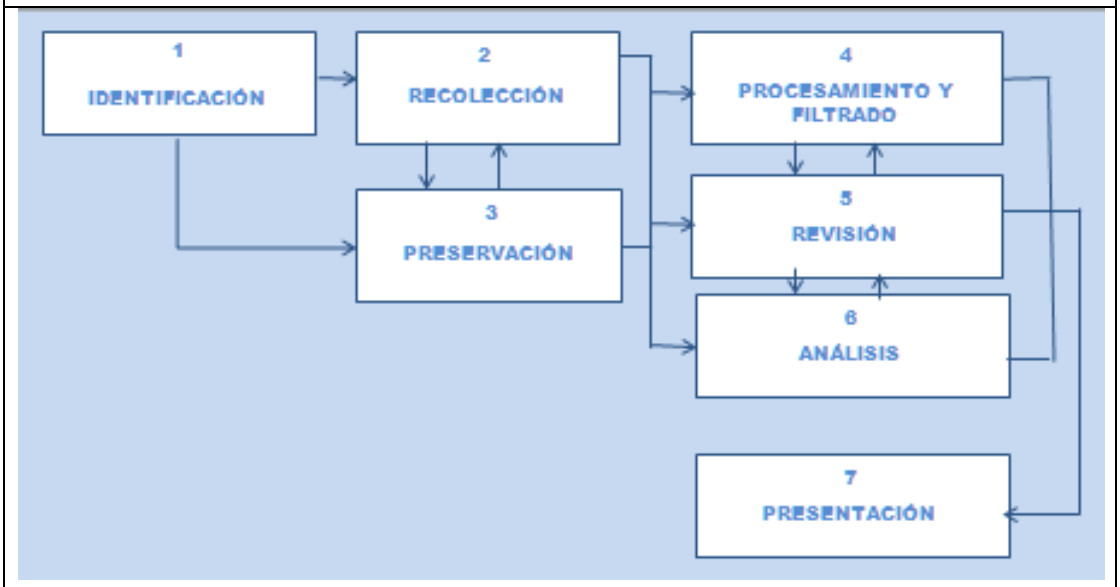


Gráfico 20: Metodología de Análisis Forense. Ref. [S]

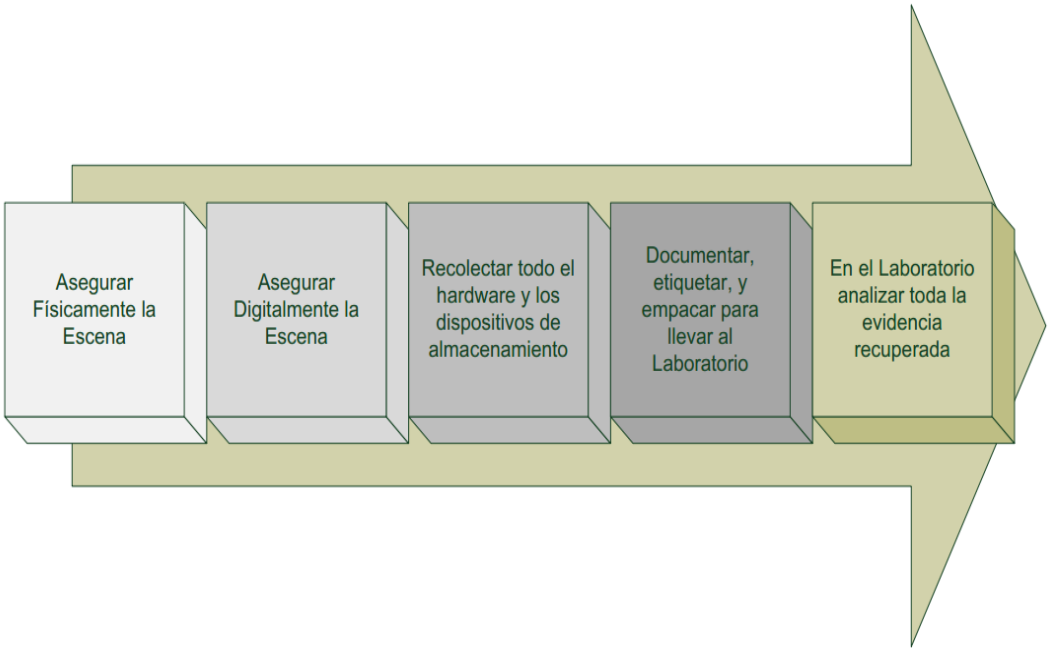


Gráfico 21: Metodología tradicional para recolectar evidencias. Ref. [S]

En el siguiente capítulo se describen estos pasos que se deben usar con software libre, aclarando que no existe un único programa que contemple todos los pasos. Deberán usarse diversos programas y que además tendrán que estar de acuerdo con el ambiente de trabajo, con la plataforma tecnológica y con el tiempo transcurrido.

2.10.3 PRESENTACIÓN E INFORME

En esta fase se presentan las evidencias recopiladas durante el análisis forense.

Se deben tomar en cuenta, entre otras, las siguientes pautas:

1) El informe debe limitarse al alcance del trabajo.

2) El informe no debe aventurar suposiciones del investigador.

3) Es válido plantear una o más "hipótesis de trabajo" y presentar evidencias que descarten o sustenten tales hipótesis de trabajo.

4) El informe debe limitarse a los aspectos técnicos, dejando las demás áreas para los respectivos especialistas.

5) El informe debe presentarse a tiempo, dentro de los plazos procesales. Lamentablemente la no presentación oportuna de un informe lo descalifica. Se pueden pedir prórrogas antes de que se venza el plazo.

6) El contenido del informe, generalmente, debe tener un resumen general, una relación de antecedentes, actividades realizadas, relación de evidencias encontradas, conclusiones y en caso aplicable, recomendaciones. Se deberán adjuntar los anexos del caso.

7) Se debe recordar que las evidencias deben ser admisibles, es decir que cualquier persona con suficientes conocimientos que las mire debe llegar a las mismas conclusiones. No es válido poner "esto es así porque yo lo digo o porque yo lo comprobé", sino que debe demostrarse el método de comprobación que, por supuesto, debe ser reproducible. Afortunadamente, la evidencia digital se puede reproducir tantas veces como sean necesarias sin que se pierda ni la calidad ni la validez de la evidencia.

CAPÍTULO III: PROGRAMAS LIBRES PARA FORENSIA EN REDES

"Las oportunidades se multiplican a medida que se las toma".
-Sun Tzu-, El Arte de la Guerra

3.1 INTRODUCCIÓN

El alto costo de los programas forenses conocidos (ENCASE cuesta casi 4.000 dólares por licencia, FKT cuesta casi 7.000 por licencia) hace difícil que la mayoría de expertos puedan disponer de una licencia. Además, estos programas se concentran en la computación forense, es decir no disponen, o disponen de muy pocas herramientas de ayuda para la forensia en redes. Por lo tanto, la mayoría de herramientas para forensia en redes han sido tomadas de las herramientas de hacking ético, esto es, análisis de vulnerabilidades, tests de penetración, sniffing, análisis de logs.

3.2 ANÁLISIS DE ALTERNATIVAS

En el siguiente cuadro se pueden mirar los conjuntos (suites) de programas que consisten en varios mecanismos para realizar distintas actividades de análisis forense.

3.2.1 SUITS MULTIPROPÓSITO PARA INFORMÁTICA FORENSE

PROGRAMAS MULTIPROPÓSITO PARA INFORMÁTICA FORENSE				
PRG.FORENSE	**S.O**	**LICEN.**	**VER**	**DESCRIPCION**
Internet Evidence Finder IEF	Windows	Comercial	5.4	Computer Forensics Solution
SANS Investigative Forensics Toolkit - SIFT	Ubuntu	Libre	2.1	Sistema operativo forense multipropósito
EnCase	Windows	Comercial	7.03	Herramienta forense
FTK	Windows	Comercial	4.0.1	Herramienta cumunmente usada para análisis de información de medios computacionales.
Digital Forensics Framework	Windows / Linux / MacOS	GPL	1.1	DFF es tanto unas herramientas de investivación, como una plataforma de desarrollo.
PTK Forensics	LAMP	Libre/com.	2.0	GUI para el Sleuth Kit
The Coroner's Toolkit	Unix-like	IBM Public License	1.19	Una suit de programas para análisis en UNIX
COFEE	Windows	Propietaria	n/a	Suit de herramientas de Micro-soft, solamente disponible para departamentos legales.
The Sleuth Kit	Unix-like/Win	IPL, CPL, GPL	3.1.1	Una librería de herramientas para Unix y Windows
Categoriser 4 Pictures	Windows	Libre	4.0.2	Herramienta para desarrollar categorización de imagenes, para departamentos legales.
Paraben P2 Commander	Windows	Comercial	n/a	Herramienta forense de propósito general

PROGRAMAS MULTIPROPÓSITO PARA INFORMÁTICA FORENSE				
Open Computer ForensicsArchitec	Linux	LGPL/GPL	2.3.0	Arquitectura para laboratórios de Computer forense.
SafeBack	N/a	Comercial	3.0	Media digital para recuperación de evidencias y respaldos.
Windows To Go	N/a	Comercial	n/a	Sistema Operativo booteble.
Forensic Assistant	Windows	Comercial	1.2	Analizador de las actividades del usuario (E-mail, IM, Docs, Browsers), más un set de herramientas forenses.
PeerLab	Windows	Comercial	1.30	Analizador de archivos compartidos y mensajería instantánea.
OSForensics	Windows	Libre/ comercial	0.99f	Herramienta forense de propósito general para e-mail, archivos, imágenes & búsquedas.
X-Way Forensics	Windows	Comercial	16.1	Herramienta forense de propósito general, con editor hexadecimal WinHex.
bulk_extractor	Windows, Linux	Dominio público	1.1	Herramienta forense basada en strems de caracteres, característica usada para recuperación de direcciones e-email, número de teléfonos, urls y otros objetos de identificación.

Tabla A01 : Suits y programas multipropósito para Informática Forense

PRINCIPALES EMPRESAS DESARROLLADORAS DE SUITS DE PROGRAMAS PARA ANÁLISIS FORENSE	
Digital Intelligence	**DIGITAL INTELLIGENCE SOFTWARE** Digital Intelligence ha creado muchas herramientas de software in-house especialmente para uso forense. Estas herramientas incluyen DriveSpy, Image, Part, PDBlock and PDWipe.
AccessData	**ACCESSDATA** Desde 1987, AccessData ha sido líder en la recuperación de la contraseña y la criptografía aplicada. Las herramientas disponibles son: forenses último kit de herramientas, kit de Password Recovery Toolkit y Registry Viewer de herramientas de forense.
paraben forensic tools	**PARABEN FORENSIC TOOLS** Paraben tiene un software forense para PDAs, recuperación de la contraseña, la búsqueda de texto, adquisición de datos, análisis de e-mail y mucho más.
Passware	**PASSWARE** Una solución completa para el descubrimiento de evidencia cifrada, cifrado de análisis, recuperación de la contraseña y el descifrado. Los mejores productos de venta de Passware son ampliamente utilizados por las fuerzas de seguridad y se incluyen en Certificado de Informática Forense de formación.
Belkasoft forensics made easier	**BELKASOFT** Belkasoft ofrece una gama de productos que permiten a los investigadores forenses acceso rápido y amplio análisis de evidencia digital almacenada en los discos duros de los sospechosos o abandonados para imágenes de disco.

2) FIRMAS RECONOCIDAS DE SOFTWARE FORENSE	
susteen	**SUSTEEN** Susteen ha desarrollado varios productos de software y hardware en colaboración con numerosas empresas de renombre internacional. Susteen ha ampliado su ámbito de aplicación en el contexto mundial y en la actualidad tiene en marcha varios proyectos.
Hot Pepper Technology	**HOT PEPPER TECHNOLOGY** Susteen ha desarrollado varios productos de software y hardware en Colaboración con Empresas de gran renombre internacional. Susteen ha ampliado su ámbito de aplicación.
DATALIFTER	**STEPANET DATALIFTER** DataLifter Stepanet es una suite de productos basados en años de experiencia de investigación. Estas herramientas se han diseñado específicamente para ayudar en Informática Forense, Auditoría Informática, Seguridad de la Información y Recuperación de Datos.

Tabla A02 : Principales empresas desarrolladoras de software para Informática Forense

3.2.2 PROGRAMAS PROPIETARIOS O CON MARCAS REGISTRADAS (™)

Definición: Programas propietarios son aquellos que requieren un pago por licencia. En la Tabla A01, constan con el texto "Comercial" en la columna titulada "LICENCIA" y a continuación se presenta los sitios web de dos de los más conocidos:

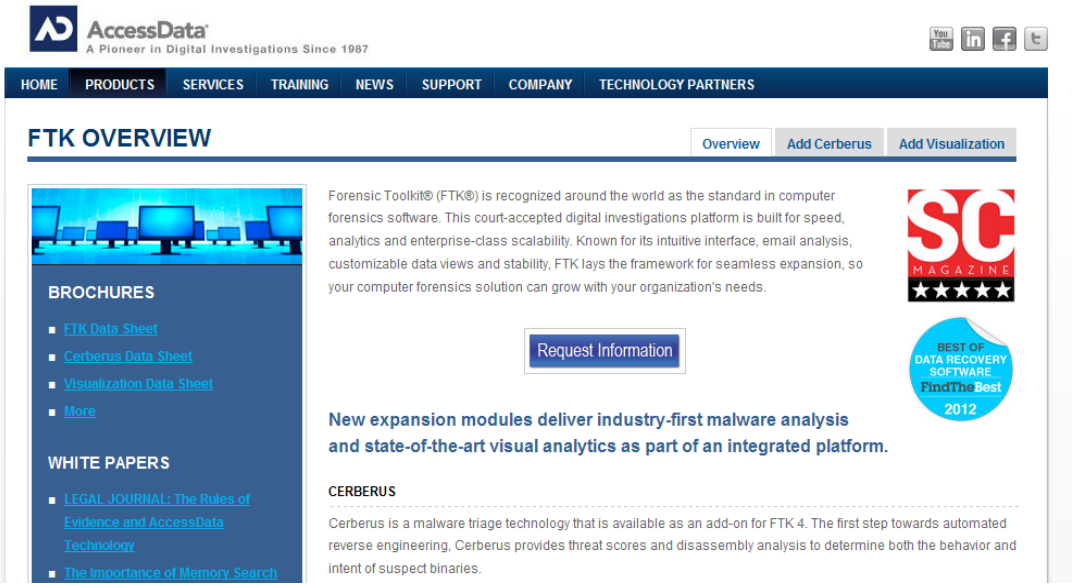


Gráfico 22: Sitio del software propietario Access Data – FTK. Ref. [3-01]

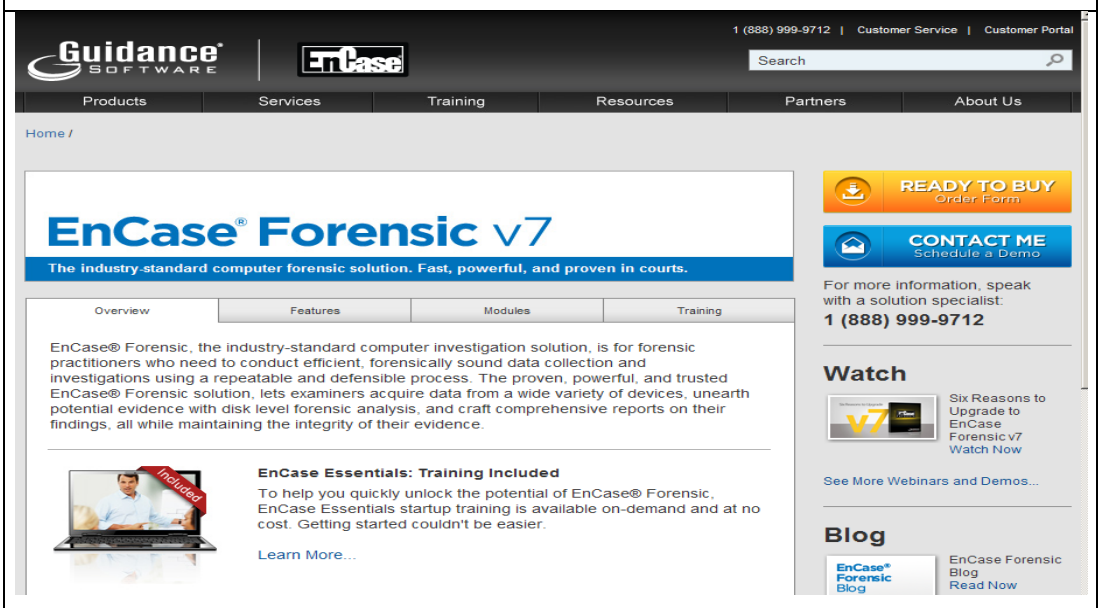


Gráfico 23: Sitio del software propietrio EnCase Forensic Ref. [3-02]

3.2.3 PROGRAMAS LIBRES

Definición: Programas libres, son aquellos que conceden estas libertades. De acuerdo con tal definición, un software es "libre" o Licencia GPL, cuando garantiza las siguientes *libertades:*

LIBERTADES DEL SOFTWARE LIBRE	
LIBERTAD	**DESCRIPCIÓN**
0	La libertad de usar el programa, con cualquier propósito.
1	La libertad de estudiar cómo funciona el programa y modificarlo, adaptándolo a tus necesidades.
2	La libertad de distribuir copias del programa, con el prójimo.
3	La libertad de mejorar el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie.
Las libertades 1 y 3 requieren acceso al código fuente, porque estudiar y modificar software requiere tener acceso al código fuente. El usuario común no distingue entre software libre y software gratis. Ambos no cobran por el uso del programa (licencia). La diferencia con el software gratis es que no se proporciona código fuente.	

Tabla 02 : Libertades que garantiza el software libre. Ref. [3-100]

PROGRAMAS LIBRES PARA ANÁLISIS FORENSE			
PROGRAMAS LIBRES SUITES (CONJUNTOS) INTEGRADOS			
PRG.FORENSE	**VERS.**	**ORIGEN**	**DESCRIPCIÓN**
AUTOPSY	3.0	Brian Carrier	Interface gráfica para líneas de comando en las herramientas de investigación y análisis digital The Sleuth Kit.
BACKTRACK	5.0 R2	Backtrack	Analizador para pruebas de penetración y auditoria de seguridad con capacidad de ejecutar levantamiento forenses.
CAINE	2.5.1	Nanni Bassetti	Live CD en Linux, agrupa un número de herramientas de análisis.
DIGITAL FORENSICS FRAMEWORK	1.2.0	ArxSys	Analiza volumenes, archivos del sistema, datos de usuarios del sistema, aplicación de datos, extracción de metadatos, ítems borrados/ocultos.
OSFORENSICS	1.0.1005	Passmark Software	Aplicación Windows para llevar a cabo un gran rango de tareas forenses.
P2 SHUTTLE FREE	No conocido	Paraben	Limitada solución libre, hasta la version P2 Shuttle Pro, para montaje de disco remote, captura de red RAM, búsquedas

PRG.FORENSE	VERS	ORIGEN	DESCRIPCIÓN
PALADIN	2.06	Sumuri	Live boot CD basada en Ubuntu.
SIFT	2.12	SANS	Aplicación preconfigurada VMware Múltiples herramientas digital forense.
THE SLEUTH KIT	3.2.3	Brian Carrier	Comandos de línea UNIX, herramientas para análisis forense del volumen
UBUNTU GUIDE	No conocido	How-To Geek	Guía de Unbuntu live disk para recuperar particiones, archivos, etc.
VOLATILITY FRAMEWORK	2.0	Volatile Systems	Conjunto de herramientas para la extracción de artefactos de RAM

Tabla A03 : Programas libres suites (conjuntos) integrados

SOFTWARE LIBRE PARA FORENSIADE REDES Y ANÁLISIS DE INTERNET			
PRG.FORENSE	**VERS.**	**ORIGEN**	**DESCRIPCIÓN**
CHROMEANALYSIS	1.0.1	Foxton Software	Google Chrome, análisis del histórico de datos del explorador Chrome.

PRG.FORENSE	VERS	ORIGEN	DESCRIPCIÓN
CHROMECACHEVIEW	1.4	Nirsoft	Lee la carpeta de Google Chrome y despliega la lista de todos los archivos almacenados.
FOXANALYSIS	1.4.2	Foxton Software	Análisis básico de los datos del internet, del explorador Firefox versiones 1, 2 y 3.
IECACHEVIEW	1.46	Nirsoft	Despliega varios detalles de archivos en la cache del Internet Explorer; número de intentos, los últimos accesos, etc.
IECOOKIESVIEW	1.74	Nirsoft	Extrae varios detalles de los cookies del Internet Explorer.
IEHISTORYVIEW	1.7	Nirsoft	Extrae las últimas URLS visitadas.
IEPASSVIEW	1.26	Nirsoft	Extrae password de IE vs. 4 a 8
MOZILLACACHEVIEW	1.51	Nirsoft	Lee el folder de cache de los browsers Firefox/Mozilla/Netscape
MOZILLACOOKIEVIEW	1.36	Nirsoft	Obtained cookies de los web browsers Firefox/Mozilla/Netscape
MOZILLAHISTORYVIEW	1.45	Nirsoft	Lee el archivo history.dat de Firefox/Mozilla/Netscape Web browsers, y despliega las páginas visitadas.
MYLASTSEARCH	1.55	Nirsoft	Extrae las consultas en Google, Yahoo and MSN, Twitter, Facebook, MySpace.

PRG.FORENSE	VERS.	ORIGEN	DESCRIPCIÓN
PASSWORDFOX	1.30	Nirsoft	Extrae los nombres de los usuarios y passwords almacenados mediante el browser Mozilla Firefox.
OPERACACHEVIEW	1.37	Nirsoft	Lee el folder de cache de Opera Web browser y lo despliega.
OPERAPASSVIEW	1.05	Nirsoft	Desencripta el contenido del archivo de passwords de Opera Web browser (wand.dat)
WEB HISTORIAN	No conocido	Mandiant	Revisa la lista de URLs almacenadas en el archivo histórico de los browser más comúnmente usados.

Tabla A04 : Software libre para forensia de redes y análisis de actividad en Internet

PROGRAMAS LIBRES ANÁLISIS FORENSE EN COMPUTADORES INDIVIDUALES		
PRG.FORENSE	**ORIGEN**	**DESCRIPCIÓN**
OSForensics	Passmark Software	Suite de Aplicación para un amplio rango de tareas forenses
FTK Imager	AccessData	Herramienta para copias - imagen, visor de disco y monta imagenes

PRG.FORENSE	ORIGEN	DESCRIPCIÓN
Forensic Image Viewer	Sanderson Forensics	Para vistas de fotos, imagenes, datos (extract Exif & GPS data)
FoxAnalysis	forensic-software	Basic analysis of internet history data from Firefox
Mail Viewer	MiTec	Visores de archivos (Outlook Express, Windows Mail/ Live Mail, Mozilla Thunderbird, EML)
USBWrite Blocker	DSi	Habilitador de soft.(write-blocking of USB ports
Encrypted Disk Detector	JAD Software	Detecta encriptaciones de drives físicos para TrueCrypt, PGP, or Bitlocker
DumpIt	MoonSols	Genera : physical memory dump of Windows 32 & 64 bit machines
PST Viewer	Lepide Software	Abre y mira (no exporta) Outlook PST files sin necesidad de Outlook
P2 eXplorer	Paraben	Virtually mount drives & forensic images

Tabla A05 : Programas libres para análisis forense en computadores individuales

SOFTWARE LIBRE PARA ANÁLISIS DE DISCOS E IMÁGENES DE DISCOS			
PRG.FORENSE	**VERS.**	**ORIGEN**	**DESCRIPCIÓN**
DumpIt	No conocida	MoonSols	Genera dump de memoria física de máquinas de Windows, 32 bits 64 bit.
Encrypted Disk Detector	No conocida	JADsoftware	Revisa drives físicos locales en (sistemas TrueCrypt, PGP, or Bitlocker encrypted volumes).
FAT32 Format	1.05	Ridgecrop	Habilita gran capacidad de disco para ser formateado como FAT32
FTK Imager	3.1.0	AccessData	Herramienta de copias forence (Imaging tool, disk viewer and image mounter)
Guymager	0.6.5	vogu00	Copiador forense multitarea sobre Linux
HotSwap	6.0.0	Kazuyuki Nakayama	"Safely remove SATA disks", similar to the "Safely Remove Hardware" icon in the el área de notificaciones.
P2 eXplorer	3.1	Paraben	Monta drives virtualmente & copia imagen forense.
Tableau Imager	1.11	Tableau	Herramienta para copias imagenes y se usa con productos de la misma casa Tableau.
VHD Tool	2.0	Microsoft	Convierte imagenes de disco a format VHD, el cual es montable en el administrador de discos de windows.

Tabla A06 : Software libre para análisis de discos e imágenes de discos

PROGRAMAS LIBRES PARA ANÁLISIS DE CORREOS ELECTRÓNICOS			
PRG.FORENSE	**VERS.**	**ORIGEN**	**DESCRIPCIÓN**
EDB Viewer	No conocida	Lepide Software	EDB-Abre y visualiza archivos DBD. No necesita conexión al Exchange.
Gmail Parser	1.0.0	Woanware	Analiza varios artefactos Gmail, desde los archivos HTML tomados.
Mail Viewer	1.8.3	MiTeC	Visualizador de Outlook Express, Windows Mail/Windows Live Mail, Mozilla Thunderbird , Base de Datos de mensajes o simples archivos EML
OST Viewer	No conocida	Lepide Software	Abre y presenta (no exporta) los archivos de Outlook OST sin conectar a un servidor Exchange.
PST Viewer	No conocida	Lepide Software	Abre y visualiza (no exporta) los archivos de Outlook PST sin necesidad de Outlook

Tabla A07 : Programas libres para análisis de correos electrónicos

SOFTWARE LIBRE PARA OBTENCIÓN DE INFORMACIÓN			
PRG.FORENSE	**VERS.**	**ORIGEN**	**DESCRIPCIÓN**
Agent Ransack	2010 (762)	Mythicsoft	Busca múltiples archivos con op. booleanos y análisis con Perl Regex.

PRG.FORENSE	VERS.	ORIGEN	DESCRIPCIÓN
EvidenceMover	No conocida	Nuix	Copia datos entre localizaciones, con comparación de archivos, verificación y login (usuario, password)
FastCopy	2.08	Shirouzu Hiroaki	Permite etiquetación rápida, copia / borra, software Windows. Puede verificar con SHA-1, etc
File Signatures	9Mar2012	G.Kessler	Tabla del archivo firmas digitales.
Forensic Test Images	Varios	Varios	Análisis y validación de archivos que se presume y/o tiene imágenes
HashMyFiles	1.88	Nirsoft	Calcula MD5 y hashes SHA1 [G34]
MobaLiveCD	2.10	Mobatek	Ejecuta desde Linux live CDs en su imagen ISO sin que tener que arrancarlo
Mouse Jiggler	1.2	Arkane Systems	Automáticamente mueve el puntero del mouse parando el protector de pantalla, hibernación, etc.
Notepad ++	6.0.0.	Notepad +	Reemplazo Avanzado de Notepad.
NSRL	2.35	NIST	Conjunto de Hash de archivos conocidos
Quick Hash	1.5.2	Technlogy	Un Linux & Win GUI para hashing SHA1 de archivos ind. o recursivos.
USB Write Blocker	1.0	DSi	Habilita puertos de escritura, en bloqueamiento de USBs.

PRG.FORENSE	VERS.	ORIGEN	DESCRIPCIÓN
Win. Forensic Environment	Varios	Troy Larson	Guía para crear y trabajar con CD boot de Windows.

Tabla A08 : Software libre para obtención de información

SOFTWARE LIBRE PARA ANÁLISIS DE ARCHIVOS Y DATOS			
PRG.FORENSE	**VERS.**	**ORIGEN**	**DESCRIPCIÓN**
Advanced Prefetch Analyser	2.4	Allan Hay	Lee archivos prefetch Windows XP, Vista and Windows 7
A**analyzeMFT**	2.0	David Kovar	Analiza el MFT de un archivo de sistema NTFS, entregando resultados para ser analizado con otros software
Audit Viewer	No con.	Mandiant	Visualizador para auditoria
DCode	4.02.0.930	Digital Detective	Convierte varios tipos de datos a formato de tiempo y fecha.
Defraser	1.3.0	Varios	Detector total y parcial de archivos de multimedia en muchos medios.
eCryptfs Parser	2011-09-22	Ted Technology	Analizador recursivo de los encabezados de directorios y archivos encriptados. Entrega el tipo de algoritmo usado, tamaño del archivo original, firmas usadas, etc.

PRG.FORENSE	VERS.	ORIGEN	DESCRIPCIÓN
Encryption Analyzer	3.5	Passware	Busca en un computador por passwords protegidos y archivos encriptados, reporta la complejidad de la encripciones y opciones de descripción por cada archivo.
Forensic Image Viewer	1.03	Sanderson Forensics	Busca datos en varios formatos de: imagen, dibujos, gráficos embebidos, extracción de imágenes embebidas, datos GPS, etc.
Highlighter	No conocido	Mandiant	Examina archivos logs usando texto, gráficos o vistas histogramas.
Live Detector	No conocido	H-11 Digital Forensics	Recoge datos volátiles, cuentas y passwords de identificación, artefactos de browser, comportamiento de usuarios e información del Sist. WIN.
LiveContactsView	1.10	Nirsoft	Mira y exporta detalle de los contactos de Windows Live Messenger.
RSA Netwitness Investigator	9.7.5.4	EMC	Captura y analiza paquetes de la red.
Memoryze	No conocido	Mandiant	Adquiere y/o analiza imágenes RAM, incluyendo el archivo page en el sist.
MFTview	1.1.0	Sanderson Forensics	Displays and decodes contents of an extracted MFT file
NetSleuth	No conocido	NetGrab	Network monitoring tool, with covert “silent portscanning”

PRG.FORENSE	VERS.	ORIGEN	DESCRIPCIÓN
PsTools	2.44	Microsoft	Suite de comandos en línea útiles Win.
Shadow Explorer	No conocido	Shadow Explorer	Buscar y extraer archivos de copias ocultas
Simple File Parser	1.3	Chris Mayhew	Herramienta GUI para analizar archivos lnk, prefetch y listar artefactos de salto.
SQLite Manager	0.7.7	Mrinal Kant, Tarakant Tripathy	Software adicional (Add on) de Firefox, habilita la visualización de cualquier base de datos SQLite
Strings	2.42	Microsoft	Herramienta de línea de comando para búsqueda de textos.
Structured Storage Viewer	3.3.1	MiTec	Visualiza y administra archivos basados almacenamiento estructurado MS OLE.
TimeLord	No conocido	Paul Tew	Utilidad para el tiempo, zonas horarias, hora de BIOS, formatos de tiempo., etc
Windows File Analyzer	2.5	MiTeC	Analiza thumbs.db, Prefetch, archivos INFO2 y .lnk

Tabla A09 : Software libre para análisis de archivos y datos

PROGRAMAS PARA MAC OS			
PRG.FORENSE	**VERS.**	**ORIGEN**	**DESCRIPCIÓN**
Disk Arbitrator	0.4.1	Aaron Burghardt	Bloquea el sistema de archivos de arranque (the mounting of file systems), asemejando un bloqueador de escritura con desabilitación de una escritura arbitraria.
Epoch Converter	No conocido	Blackbag Technologies	Convierte tiempo epoch a hora local y hora UTC
FTK Imager CLI for Mac OS	2.9.0	AccessData	Comandos de línea (Mac OS), versión de Copiador FTK de AccessData.
IORegInfo	No conocido	Blackbag Technologies	Listas de ítems conectados al computador (ejemplo: SATA, USB y FireWire Drives, software RAIDs asignado). Ubica información de particiones, tamaño, tipos y el bus al cual el dispositivo está conectado.
Mac Memory Reader	3.0.0	Cyber Marshal	Utilitario de línea de comando para la captura física de la línea de la RAM MAC.
PMAP Info	No conocido	Blackbag Technologies	Despliega el particionamiento físico del dispositivo especificado. Puede ser usado para una sacar el mapa total de la información del drive, contabilizando todos los sectores usados.

Tabla A10 : Programas para Mac OS

PROGRAMAS LIBRES PARA DISPOSITIVOS MÓVILES			
PRG.FORENSE	**VERS.**	**ORIGEN**	**DESCRIPCIÓN**
iPhone Backup Browser	R38	René Devichi	Vista desencriptada de backup de iPad, iPod y iPhones
iPhone Analyzer	2.00	Leo Crawford	Explora la estructura del archivo interno del iPad, iPod and iphone
Rubus	No conocido	CCL Forensics	Desensambla y presenta la estructura funcional del archivo de backup BlackBerry .ipd

Tabla A11: Programas libres para Dispositivos Móviles

PROGRAMAS LIBRES PARA VISUALIZAR ARCHIVOS			
PRG.FORENSE	**VERS.**	**ORIGEN**	**DESCRIPCIÓN**
Excel 2007 Viewer	1.00	Microsoft	Visualiza hojas Excel
PowerPoint 2007 Viewer	1.00	Microsoft	Visualiza presentaciones PowerPoint
Microsoft Visio 2010 Viewer	1.00	Microsoft	Visualiza diagramas Visio
Microsoft Word Viewer	1.00	Microsoft	Visualiza documentos Word

PRG.FORENSE	VERS.	ORIGEN	DESCRIPCIÓN
VLC	2.0.1	VideoLAN	Visualiza archivos multimedia, DVD, Audio CD, VCD, etc

Tabla A12: Programas libres para visualizar archivos

PROGRAMAS LIBRES PARA ANÁLISIS DE REGISTRO DE WINDOWS			
PRG.FORENSE	**VER**	**ORIGEN**	**DESCRIPCIÓN**
ForensicUserInfo	1.04	Woanware	Extrae información de usuario desde la SAM, SOFTWARE y archivos ocultos del SYSTEM, desencriptar el LM/NT hashes desde el archivo SAM
Process Monitor	3.0	Microsoft	Examina procesos de Windows y registros nocivos en tiempo real.
Registry Decoder	1.2	Inst.Nac. Justicia US	Para la adquisición, análisis, y reporte del contenido del registro.
RegRipper	No con	Harlan Carvey	Herramienta para extracción y correlación de datos del registro.
Regshot	1.8.3	Regshot	Toma instancias de lo que ocurre en el registro, permitiendo comparaciones, eje. Presenta los cambios en el registro después de que el software fue instalado.

PRG.FORENSE	VER	ORIGEN	DESCRIPCIÓN
USB Device Forensics	1.06	Woanware	Detalla los dispositivos USB previamente anexados, sobre registros exportados ocultos.
USBDeview	2.06	Nirsoft	Detalla los dispositivos USB previamente anexado (attached).
UserAssist	2.4.3	Didier Stevens	Desplega la lista de programas que se ejecutan, con un contador de corrida y la última hora y fecha que fue ejecutado.

Tabla A13 : Programas libres para análisis de registro de windows

PROGRAMAS LIBRES PARA ANÁLISIS DE APLICACIONES			
PRG.FORENSE	**VERS.**	**ORIGEN**	**DESCRIPCIÓN**
LiveContactsView	1.10	Nirsoft	Despliega y exporta detalles de los contactos Windows Live Messenger.
SkypeLogView	1.21	Nirsoft	Despliega el chat y llamadas con Skype.

Tabla A14 : Programas libres para registro de windows

3.2.4 PROGRAMAS EN AMBIENTE LIVE CDS

Los siguientes son CDs o DVDs que se descargan de internet y que se graban en una unidad de CD. Su diseño permite arrancar el computador desde la unidad de CD evitando o ahorrando la instalación en el disco duro.

FORENSICS LIVE CDS		
NOMBRE	**REF.**	**DETALLE**
BACKTRACK	[3-84]	Un Live CD construido en base de Ubuntu, (primera versión fue construida sobre Slackware). La última versión tiene "modo forense".
MATRIX	[3-85]	Live CD basado en la distribución Debain, con herramientas de computación forense y respuesta a incidentes.
CAINELive CD	[3-86]	Un forensic Live CD desarrollado en base a Ubuntu.
DEFT Linux	[3-87]	Un Live CD basado en Xubuntu con herramientas para computación forense y respuesta a incidentes. Este Live CD, se lo reconoce como muy liviano y rápido, creado por especialistas. El primer live CD con AFF, dhash and Xplico.
THE FARMER'S BOOT CD		Un Live CD Linux diseñado y optimizado para la pre visualización de datos en forma de forensia de sonido. Contiene una serie de programas especializados en forensia que sirven para tener una vista previa en ambos sistemas operativos Windows y Linux.
FCCU Gnu /Linux Boot CD	[3-89]	Un Live CD construido sobre Live Debian con muchas herramientas con fines forenses.
GRML	[3-90]	Un Live CD forense construido sobre Debian.
HELIX3 (HELIX3 PRO)	[3-91]	Un live CD construido sobre Ubuntu, con herramientas especiales para respuestas a incidentes y descubrimientos electrónicos.

NOMBRE	REF.	DETALLE
MACQUISITION BOOT CD	[3-92]	Un live CD construido para obtener imagenes de sistemas Macintosh.
SLACKWARE LIVE	[3-93]	A Live CD Linux construido sobre características de Slackware, con una amplia variedad de herramientas open source, enfocados tanto en pruebas y exámenes como respuesta a incidentes, como a exámenes de computación forense.
PLAINSIGHT	[3-94]	Un Linux Live CD con un número de aplicaciones como TestDisk, PhotoRec, etc.
RECOVERY IS POSSIBLE	[3-95]	El primer y único disponible en el mercado forense de sonido, en disco de arranque de Windows. Incluye soporte integrado (built-in driver) de acceso al sistema de archivos NTFS y el software incorporado de bloqueo de escritura (built-in software write bloc King).
SAFE Boot Disk	[3-96]	Dos Live CDs construidos sobre Slackware and Ubuntu. Incluye SMART y otras herramientas forenses.
SMART Linux	[3-97]	A Live CD built on top of Debian Live with many tools with forensic purpose.
SPADA	[3-98]	A forensic Live CD built on top of Knoppix.
WinFE	[3-99]	Windows Forensic Environment (aka WinFE, Windows FE)

Tabla A15: Programas libres en Lives CD

3.2.5 PROGRAMAS PARA AMBIENTE WINDOWS

Si el investigador se siente cómodo manejando un ambiente Windows, puede optar por los siguientes programas:

PROGRAMAS PARA AMBIENTE WINDOWS	
NOMBRE	**DETALLE**
BLACKTHORN GPS FORENSICS	Blackthorn sigue apoyando a los examinadores y los operadores, herramienta única y poderosa optimizada para el análisis forense de dispositivos GPS.
BRINGBACK	by Tech Assist, Inc.
BELKASOFT EVIDENCE CENTER	This product makes it easy for an investigator to search, analyze and store digital evidence found in Instant Messenger histories, Internet Browser histories and Outlook mailboxes.
CD/DVD INSPECTOR	This is the only forensic-qualified tool for examinination of optical media. It has been around since 1999 and is in use by law enforcement, government and data recovery companies worldwide
EMAIL DETECTIVE - FORENSIC SOFTWARE TOOL	by Hot Pepper Technology, Inc
ENCASE	by Guidance Software
FBI	by Nuix Pty Ltd
FORENSIC TOOLKIT (FTK)	by AccessData
HBGARY RESPONDER	Windows Physical Memory Forensic Platform

NOMBRE	DETALLE
ILOOK INVESTIGATOR	by Elliot Spencer and U.S. Dept of Treasury, Internal Revenue Service - Criminal Investigation (IRS)
MERCURY INDEXER	by MicroForensics, Inc.
P2 POWER PACK	by Paraben
PRODISCOVER	by Techpathways
SAFEBACK	by NTI and Armor Forensics
X-WAYS FORENSICS	by X-Ways AG
DATEDECODER	Una herramienta en línea de commando que decodifica y codifica formatos de fecha y hora encontrados en el sistema windows y los despliega de forma entendible a los humanos.
RECYCLEREADER	Una herramienta en línea de comandos que despliega el contenido de la carpeta recycle en win XP, Vista and 7.
DSTRINGS	Una herramienta en línea de comando que busca por cadenas en un archivo dado. Tiene la capacidad de comparar la salida de cadenas de caracteres (strings) con un diccionario, buscando emparejar los resultados con filtro solicitado. Busca también por direcciones IP.

NOMBRE	DETALLE
UNIQUE	A command line tool similar to the Unix uniq. Allows for unique string counts, as well as various sorting options.
HASHUTIL	by Live-Forensics HashUtil.exe will calculate MD5, SHA1, SHA256 and SHA512 hashes. It has an option that will attempt to match the hash against the NIST/ISC MD5 hash databases.
WINDOWSSCOPE PRO, ULTIMATE, LIVE	Comprehensive Windows Memory Forensics and Cyber Analysis, Incident Response, and Education support. Software and hardware based acquisition with CaptureGUARD PCIe and ExpressCard WindowsSCOPE Live provides memory analysis of Windows computers on a network from Android phones and tablets.

Tabla A16: Programas para ambiente windows

3.3 PROGRAMAS Y HERRAMIENTAS DISPONIBLES PARA FORENSIA EN REDES

3.3.1 PLATAFORMA WINDOWS		
NOMBRE	**REF**	**DETALLE**
BURST	[3-05]	Costoso servicio de geolocalización
CHKROOTKIT	[3-06]	Programa verifica se existe RootKits instalados en un sitio.
CRYPTCAT	[3-07]	Cryptcat es una utilidad simple para Unix que lee y escribe datos a través de conexiones de red, utilizando el protocolo TCP o UDP, mientras que la encriptación de los datos que se transmiten. Está diseñado para ser un fiable" back-end "de la herramienta que se puede utilizar directamente o accionado fácilmente por otros programas y scripts.
ENTERASYS DRAGON	[3-08]	Sistema de detección de Intrusiones, incluye reconstrucción de sesiones
IPFIX/NETFLOW V5/9	[3-09]	Collector MNIS es un colector IPFIX que, también, soporta el flujo de red permitido. Fue diseñado para ser usado con el exportador MNIS, el cual es un paquete de inspección y pruebas profundas usado para decodificar más de 300 protocolos sobre los 20 Gbps y reporta la información en IPFIX

NOMBRE	REF	DETALLE
MANTARO NETWORK INTELLIGENCE SOLUTIONS (MNIS)	[3-10]	MNIS es una comprensiva y escalable plataforma de red inteligente para forensia de redes y varias otras aplicaciones. Está desarrollado con alertas de metadatos de alta velocidad de inspección. Puede ser usado para entender incidentes de red antes y después de que un evento ocurra. Trabaja en la escala de ambientes y de redes LAN hasta 20 Gbps en proveedores de servicio.
MAXMIND	[3-11]	Servicios de Geolocalización IP de datos de geo ubicación IP, geolocalización de fuera de línea. Libre GeoLite country database. APIs programables.
NETCAT	[3-12]	Herramienta de red que permite a través de intérprete de comandos y con una sintaxis sencilla abrir puertos TCP/UDP en un HOST
NETFLOW/FLOWTOOLS	[3-13]	El propósito de NetFlow es recoger información de tráfico IP y enviar paquetes UDP y SCTP (los registros) a un servidor NetFlow Collector o NetFlow Analyzer.
NETDETECTOR	[3-14]	NetDetector es un sistema cuyas características permiten garantizar seguridad en la red, basado en detección de firmas anómalas, analíticas y forenses. Además, es una completa solución de firewall, IDS, IPS, para servicios de red de misión crítica.
NETINTERCEPT	[3-15]	NetIntercept captura todo paquete y re ensambla hasta 999,999 conexiones TCP a la vez, reconstruyendo archivos que fueron enviados sobre su red y creando una base de datos de hallazgos.

NOMBRE	REF	DETALLE
NETVCR	[3-16]	NetVCR entrega una salida comprensiva en una red de tiempo real; administra servicios y aplicaciones en tiempo real. Está integrado a una solución de un solo punto que decisivamente reemplaza los múltiples puntos de monitoreo de performance. NetVCR's, tiene arquitectura escalable, fácil de adaptar a centros de datos, redes centrales, oficinas remotas, oficinas centrales de LAN y requerimientos WAN.
NIKSUN FULL FUNCTION APPLIANCE	[3-17]	Puma NIKSUN, un portátil de la red de monitoreo de dispositivo, permite a los clientes aprovechar el estado-del-arte de tecnología del desempeño en monitoreo red, la seguridad y el cumplimiento. Instalado en unos pocos pasos, Puma ofrece, con una funcionalidad excepcional, rendimiento de renombre NIKSUN y la tecnología de monitoreo de seguridad en cuestión de minutos para el personal de campo. Puma, ahora es capaz de monitorear redes a velocidades de 10G. La monitorización en tiempo real de 10G, para el conjunto Puma, es un valor agregado para el producto. Esta herramienta es especial (go-to) para la monitorización portátil y es una instrumento forense para profesionales de la red.
NETOMNI	[3-18]	NetOmni provee una visibilidad global a través de la red. De esta manera los profesionales de IT pueden administrar múltiples productos y proveedores desde una localización central. NetOmni implementa las mejores prácticas, a fin de administrar el proceso de seguridad en la red con una modelo que garantice los Acuerdos de Nivel de Servicio (SLA), Calidad de Servicios (QoS).

NOMBRE	REF	DETALLE
IPFIX/NETFLOW V5/9	[3-19]	Colector MNIS es un collector IPFIX que soporta el flujo de red permitido. Puede ser creado para aplicarse con MNIS Exporter, el cual es un Paquete de Inspección profunda, que puede ser usado para decodificar más de 300 protocolos en redes de hasta 20 Gbps y reportan la información en IPFIX.
NETSLEUTH	[3-20]	NetSleuth es una herramienta de análisis de red libre, con licencia GPL. Sirve para reconocimiento de host, usando la interfaz pcap. Realiza rastreos de host y análisis de red. También cuenta con un sniffer, silente, que no requiere enviar paquetes por la red, para identificar dispositivos.
NETWORKMINER	[3-21]	NetworkMiner es una herramienta de análisis forense de red (NFAT) para Windows. Puede ser usada como un sniffer passive / herramienta de captura de paquetes en orden para detector del sistema operativo, sesiones, hostnames, puertos abiertos, etc., sin poner ningún tráfico en la red. También puede trabajar con interfaz de archivos PCAP, para el análisis de archivos fuera de línea. El propósito es colectar datos (como evidencia forense), así como recoger información sobre el tráfico de red. NetworkMiner es, desde el primer release del año 2007, la más popular herramienta entre los equipos de respuesta a incidentes, y los encargados de hacer cumplir la ley. NetworkMiner hoy es utilizado por empresas y organizaciones de todo el mundo. NetworkMiner está disponible tanto en open source, así como en herramienta comercial para network forensics.

NOMBRE	REF	DETALLE
PCAP2WAV	[3-22]	Decodificador de VoIP/RTP es parte de un subproyecto pcap2wav de Xplico que soporta y decodifica los siguientes códigos de audio: G711ulaw, G711alaw, G722, G729, G723, G726 and MSRTA (x-msrta: Real Time Audio).
RKHUNTER	[3-23]	Rkhunter (o Rootkit Hunter) es una herramienta de Unix que detecta los rootkits, los backdoors y los exploit locales mediante la comparación de los hashes MD5 de ficheros importantes con su firma correcta en una base de datos en línea, buscando los directorios por defecto (de rootkits), los permisos incorrectos, los archivos ocultos, las cadenas sospechosas en los módulos del kernel, y las pruebas especiales para Linux y FreeBSD.
NGREP	[3-24]	Sniffer Open source
NSLOOKUP	[3-25]	Herramienta de línea de comando usada para encontrar direcciones IP, desde un nombre de dominio.
SGUIL	[3-26]	Para Red de Monitoreo de Seguridad (NSM) y análisis por eventos de alertas de IDS.
SNORT	[3-27]	Snort es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza un dominio de colisión).
SSLDUMP	[3-28]	SSLDUMP es un SSL/TLS analizador de protocolos de red. Este identifica conexiones TCP en la interfaz de red seleccionada. Cuando identifica tráfico SSL/TLS. Cuando esta identifica tráfico SSL/TLS, este decodifica el registro y despliega en una forma textual a la interfaz de salida.

NOMBRE	REF	DETALLE
TCPDUMP	[3-29]	Tcpdump es un herramienta en línea de comandos, cuya utilidad principal es analizar el tráfico que circula por la red. Funciona con la mayoría de sistemas operativos, en windows toma el nombre de windump.
TCPXTRACT	[3-30]	Herramienta para extraer los archivos del tráfico de red basadas en las firmas de archivos
TCPFLOW	[3-31]	Programa que captura los datos transmitidos como parte de conexiones TCP (flujos), almacena datos en una forma que es conveniente para el análisis de protocolo y depuración.
TRUEWITNESS	[3-32]	Sniffer para forensia open source

Tabla A17: Programas y herramientas disponibles para forensia en redes

3.3.2 LINUX/OPEN-SOURCE		
NOMBRE	**REF.**	**DETALLE**
OMNIPEEK	[3-33]	OmniPeek es una herramienta forense para capturar, almacenar y analizar tráfico de información histórica.
WHOIS	[3-34]	Servicio Web y herramienta de línea de comando para mirar un registro de información por internet.
WIRESHARK / ETHEREAL	[3-36]	Analizador de protocol open source. Antes se lo conocía como Ethereal.
KISMET	[3-37]	Kismet es un 802.11 layer2 wireless detector de red, sniffer e IDS

NOMBRE	REF.	DETALLE
XPLICO	[3-38]	Analizador de tráfico de red gráfico, Open Source. Programa que permite analizar las capturas hechas con programas como Tsahark, en ambiente open Source. Grafica capturas de texto, correo, voz, etc
OPEN SOURCE NETWORK FORENSIC ANALYSIS TOOL (NFAT).		Soporta protocolos: HTTP, SIP, FTP, IMAP, POP, SMTP, TCP, UDP, IPv4, IPv6,..Decodificador y Sniffer de VoIP. Codec de audio codec soportado G711ulaw, G711alaw, G722, G729, G723, G726 and MSRTA

Tabla A18: Programas linux/open-source

COMMAND-LINE TOOLS	
NOMBRE	**DETALLE**
ARP	Visor de contenido de su cache ARP.
IFCONFIG	Despliega su dirección MAC e IP.
PING	Envía paquetes para probar máquinas remotas.
SPLITCAP	SplitCap es un archivo .pcap, open source libre.
TCPDUMP	Captura paquetes.
SNOOP	Captura paquetes y despega su contenido (solaris).
NEMESIS	Crea paquetes arbitrariamente
TCPREPLAY	Repite paquetes capturados
TRACEROUTE	Mira una ruta de red.
GNETCAST	Reescritura de netcat en licencia GNU

NOMBRE	DETALLE
PACKIT	Generador de paquetes.
NMAP	Utilitario para exploración de red y auditoria de seguridad.
XPLICO	Herramienta Open Source Network Forensic Analysis

Tabla A19: Herramientas de Lìnea de comando

ARP AND ETHERNET MAC TOOLS	
NOMBRE	**DETALLE**
ARPING	Transmite tráfico ARP
ARPDIG	Prueba en la LAN, por direcciones MAC.
ARPWATCH	Busca cambios ARP.
ARP-SK	Ejecuta ataques de denegación de servicio.
MACOF	Tabla CAM de ataques
ETTERCAP	Ejecuta varios ataques de red de bajo nivel.

Tabla A20: Herramientas arp, ethernet y mac

CISCO	
CDPD	Transmite y recibe mensajes CDP: proporciona capacidades de falsificación

Tabla A21: Herramienta CISCO

ICMP LAYER TESTS AND ATTACKS	
NOMBRE	**DETALLE**
ICMP-RESET	Resetea arbitrariamente conexiones TCP.
ICMP-QUENCH	Cola del protocolo de control de mensajes de internet
ICMP-MTU	Tamaño máximo de los paquetes
ISH	ICMP shell (semejante a SSH, pero usa ICMP)
ISNPROBER	Isnprober es una herramienta que las muestras de los números de secuencia TCP o IP iniciales de identificación y puede utilizar esa información para determinar si un conjunto de direcciones IP pertenecen a la misma pila TCP / IP (máquina) o no.

Tabla A22: Herramientas ICMP probadores de capas e incidentes.

IP LAYER TESTS	
NOMBRE	**DETALLE**
IPERF	Prueba multicast IP
FRAGTEST	Prueba reensamblar fragmentos IP

Tabla A23: Herramientas de prueba para el protocolo IP

UDP LAYER TESTS	
NOMBRE	**DETALLE**

UDPCAST	Incluye UDP-receiver y UDP-sender

Tabla A24: Herramientas de prueba para el protocolo UDP

TCP LAYER		
NOMBRE	**REF.**	**DETALLE**
LFT	[3-40]	LFT es la herramienta todo-en-uno traceroute, ya que puede servir de punto de diferentes sondas que utilizan ICMP, UDP, TCP y protocolos, o el método de rastreo RFC1393. Por ejemplo, en lugar de sólo lanzar sondas UDP en un intento de obtener ICMP "TTL excedido" de los ejércitos en el camino, LFT puede enviar TCP SYN o sondas FIN orientar los servicios arbitrarias.
ETRACE	[3-41]	Basados en rastreo de Internet Rastreo de armas de fuego y análisis
FIREWALK	[3-42]	Firewalking es una técnica desarrollada por Mike Schiffman y David Goldsmith que emplea como traceroute-técnicas para analizar las respuestas de paquetes IP para determinar filtros ACL de puerta de enlace y las redes del mapa.Firewalk la herramienta emplea la técnica para determinar las reglas de filtrado en su lugar en un dispositivo de reenvío de paquetes. La nueva versión de la herramienta, Firewalk / GTK introduce la opción de utilizar una interfaz gráfica y un correcciones de errores.

Tabla A25: Herramientas de prueba para el protocolo TCP

3.3.3 ANTIFORENSIC

Estos programas los podrá usar el investigador luego de un trabajo de investigación, o puede también ser usado por un hacker para borrar sus huellas.

NOMBRE	REF.	DETALLE
DARIK'S BOOT AND NUKE	[3-43]	El programa está diseñado de forma segura borrar un disco duro hasta que los datos se eliminan definitivamente
ERASER	[3-44]	Funciona con cualquier dispositivo que funcione con Windows. Borra archivos, carpetas y sus homólogos que hayan sido eliminados
EVIDENCE ELIMINATOR	[3-45]	Programa de software que se ejecutaba en el Microsoft Windows sistema operativo. El programa elimina información oculta para el usuario del disco duro que los procedimientos normales pueden dejar de eliminar.
HASH (TOOL)	[3-46]	Herramienta para que las personas puedan evadir la detección, mientras que penetrar en un sistema.
PARETOLOGIC PRIVACY CONTROLS	[3-47]	Sigilo operación, borra los rastros de una sesión. Compatible con windows
SLACKER	[3-48]	Metasploit slacker, se oculta datos en el espacio de holgura del sistema de archivos FAT o NTFS. FragFS hi
STEGANOS PRIVACY SUITE	[3-49]	Completo kit dedicado por completo a la seguridad de tu sistema, tanto en local como en Internet.
ETRACE	[3-41]	Rastreo de armas de fuego es el seguimiento sistemático de la circulación de un arma de fuego desde su creación por el fabricante o su introducción en el comercio de Estados Unidos por el importador, a través de la cadena de distribución para la primera compra.

NOMBRE	REF.	DETALLE
FIREWALK	[3-42]	Firewalking emplea métodos semejantes a las técnicas de traceroute para analizar las respuestas de paquetes IP, sirve para determinar filtros ACL de puerta de enlace y el mapa de red. La herramienta Firewalk emplea la técnica para determinar las reglas de filtrado, en un dispositivo de reenvío de paquetes. La nueva versión de la herramienta, Firewalk / GTK introduce la opción de utilizar una interfaz gráfica y correcciones de errores.
THE ONION ROUTER	[3-50]	Tor (The Onion Router). Proteje la privacidad. Protege de la vigilancia y el análisis de tráfico de red. Forma subredes anónimas en el internet.
TIMESTOMP	[3-51]	Programa que permite la supresión o modificación de información relacionada con el sello de tiempo en los archivos.
WINCLEAR	[3-52]	Winclear es una goma de borrar el historial de Internet que protege su privacidad en Internet, mediante la limpieza de todas las pistas de su Internet y actividad de la computadora.
WINDOW WASHER	[3-53]	Es una herramienta de seguridad y privacidad de Windows. Se limpia automáticamente todas las configuraciones que se generan durante el uso diario de la computadora.

Tabla A27: Programas y herramientas antiforensic

3.3.4 REGIONAL REGISTRIES		
ARIN AfriNIC	[3-35]	American Registry for Internet Numbers (ARIN) African Network Information Center (AfriNIC)

APNIC LACNIC RIPE NCC		Asia Pacific Network Information Centre (APNIC) Latin American and Caribbean IP Address Regional Registry (LACNIC) RIPE Network Coordination Centre (RIPE NCC)

Tabla A28: Programas y herramientas disponibles para forensia en redes

CAPÍTULO IV: GUÍA RÁPIDA PARA FORENSIA EN REDES USANDO SOFTWARE LIBRE

"Un general sabio se ocupa de abastecerse del enemigo"
-Sun Tzu,- El Arte de la Guerra

4.1 FINALIDAD DE LA GUÍA

Esta guía presenta los pasos para realizar un análisis forense de una red con miras a determinar qué, quién, cuándo y cómo se produjo algún incidente de seguridad. No se busca que sea una guía mecánica paso-por-paso sino más bien una serie de pautas a seguir para realizar el análisis forense.

4.2 CONSIDERACIONES

Considerando la gran cantidad de posibilidades que existen para una intrusión, no es viable considerar todos los casos posibles, por lo que se ha preferido mantener la guía general.

Adicionalmente, considerando la naturaleza delicada de las funciones de análisis forense y de hacking ético, se han omitido intencionalmente detalles para evitar que lectores ocasionales puedan vulnerar sistemas, argumentando que los pasos y acciones están documentados en un trabajo de tesis.

Finalmente, para asegurar la confidencialidad, en este documento se han omitido capturas de pantallas que revelan la identidad de las entidades y las redes analizadas.

4.3 GUÍA

Las fases para un análisis forense son:

Fase 1: Planificación

Fase 2: Ejecución del análisis

Fase 3: Presentación de resultados

4.3.1 FASE 1: PLANIFICACIÓN

PASO 1.1: ESTABLECER REQUERIMIENTOS

En esta fase se realiza un detalle de las personas, materiales, herramientas y tiempos que se van a emplear durante la ejecución del trabajo. Se puede desarrollar un cronograma en una herramienta para gestión de proyectos.

1) Lo que no se debe hacer durante el análisis

   - Anonimato: no revelar el nombre ni datos de la persona que hace el análisis.
   - No abuso: No realizar acciones que pueden disparar alarmas y alertas como bloqueos de direcciones IP.
   - No cambios: No modificar el escenario ni la información.
   - No ofrecer información involuntaria: No usar máquinas con información personal del analista o de terceros.

2) Lo que se debe hacer.

- Recordar que no existe el anonimato al 100% sino tan solo ayudas para proteger la identidad

- Navegación anónima: usar sistemas de protección de identidad, proxy servers o navegación anónima, que ofrecen un alto grado de seguridad aunque no es garantía de absoluto anonimato. Al menos, el destinatario final no podrá conocer nuestra identidad ni ubicación.

- Planificación cuidadosa. Es mejor pensar antes de actuar

- Registro minucioso de actividades realizadas

- Revisión minuciosa de actividades y retroalimentación

- Cambio frecuente de estrategia para evitar ser identificado

- Usar una máquina limpia, esto es, que no tenga nada de información personal o empresarial. Esto se consigue fácilmente con un disco exclusivo para análisis forense o con una máquina virtual con información forense.

- Almacenar fuera de línea todos los resultados parciales y finales

- Sanitizar la máquina utilizada cada vez que se concluye el trabajo

3) Herramientas necesarias

- Computador con suficiente capacidad de disco, memoria, pantalla, red

- Dispositivo para arranque exclusivo, como por ejemplo una USB con Linux, un CD Live o algo similar

- Si el trabajo se va a desarrollar durante varios días, es preferible usar software de virtualización o software que conserva el estado del disco duro como Deep Freeze, Sand Box, etc.

- Un adecuado ancho de banda

4) Información que se debe obtener

Solicitar la mayor cantidad posible de información acerca del alcance y objetivos del trabajo.

4.3.2 FASE 2: EJECUCIÓN

PASO 2.1: PROTEGER LA IDENTIDAD DE LOS INVESTIGADORES

1) Usar equipos o dispositivos que no se puedan asociar con el investigador o la entidad que realiza la investigación. Se puede usar una máquina virtual. Tratándose de una guía basada en software libre, se recomienda el uso de XEN en sistemas Linux o de VirtualBOX en Windows.

2) Usar programas como Tor (una variedad de Mozilla Firefox) que se conecta a servidores en Europa para evitar que el sistema de destino conozca el origen de la comunicación.

3) Aplicar en todo momento las normas para ajustarse al debido proceso y la cadena de custodia [G09].

4) Aplicar en todo momento las pautas para recopilación y almacenamiento de evidencias publicadas por la Fiscalía y la Policía Nacional.

PASO 2.2: CONOCER EL OBJETIVO

1) Reconocimiento de la red.

2) Descubrimiento de redes al alcance (acceso inalámbrico).

3) Se puede conocer las distintas redes al alcance a través de programas como wirelesskeyview.zip o bluetoothview.zip de www.nirsoft.net.

4) Mediante programas como AirHack, de www.backtrack.org, se pueden conocer claves débiles.

5) Mediante listas de passwords por default se pueden conocer claves estándares para dispositivos que no fueron debidamente asegurados.

PASO 2.3: DESCUBRIMIENTO DE EQUIPOS Y DISPOSITIVOS DENTRO DE LA RED

1) Conocer el estado de la red mediante el uso de programas como nmap, ipscan, kaboodle.

2) En el gráfico A15, se puede ver en acción el programa Angry IP Scanner, descubriendo los equipos de la red.

3) En el gráfico A16, se muestra el programa SharesEnum, el mismo que crea una lista de todos los recursos compartidos de una red Windows Samba en Linux/Solaris.

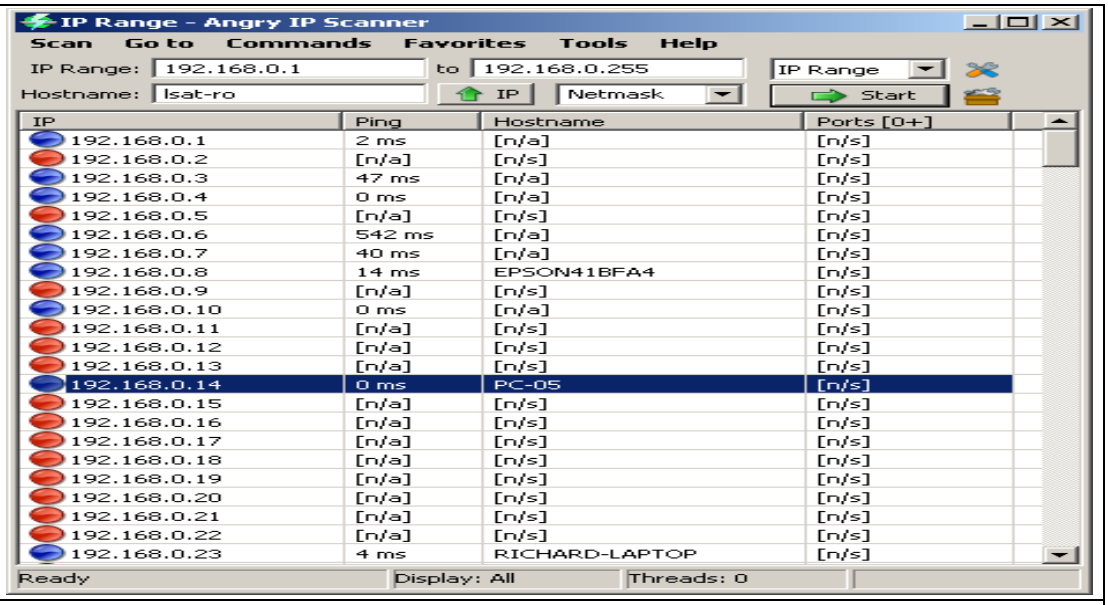


Gráfico A15: Reporte programa Angry IP Scanner.

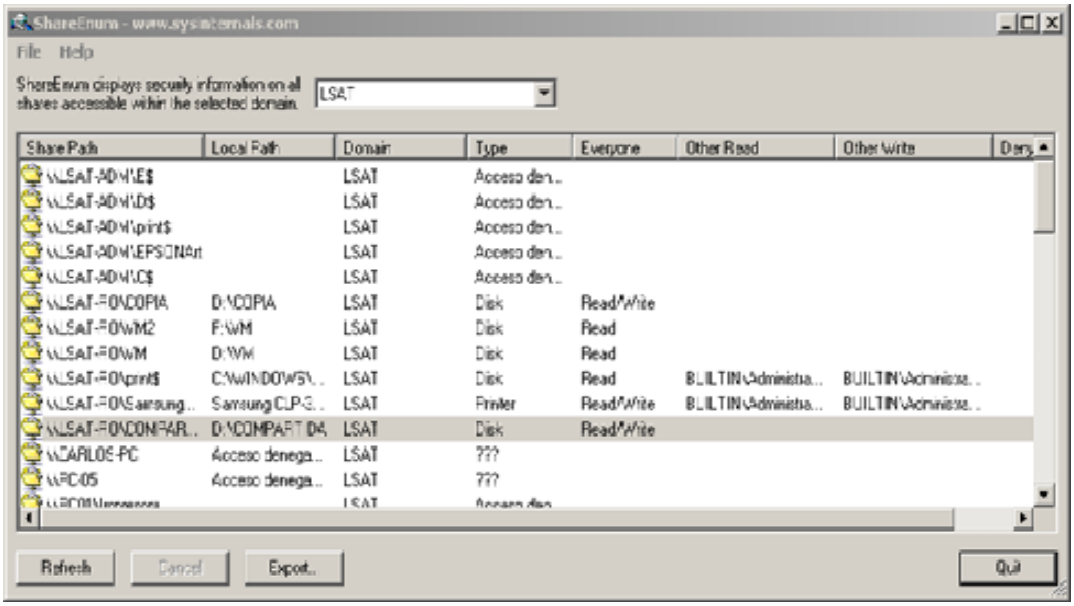


Gráfico A16: Reporte programa SharesEnum

PASO 2.4: OBTENER EL CATÁLOGO DE EQUIPOS, SERVICIOS, EQUIPOS.

1) Obtener detalles de comunidades SMNP

   Existen programas gratuitos como SNMPWALK que permiten navegar por las bases de datos MIB de las comunidades SMNP y muestran detalles acerca del hardware, software y recursos de la red.

2) Obtener detalles de inventarios de equipos

   Programas libres como OCS Inventory, NG, se usan para recopilar y mostrar reportes sobre los equipos, programas y servicios de una red.

3) Obtener detalles de LDAP y Active Directory

   Programas como ldapbrowser permiten conocer detalles de una red bajo Active Directory.

4) Obtener el detalle general de vulnerabilidades

   Esto se puede obtener con programas libres como Nessus.

5) Obtener detalle específico de vulnerabilidades

6) Obtener usuarios y contraseñas del objetivo

   Una vez que se conoce la marca y modelo del equipo, es muy probable que no se le haya asignado una contraseña distinta a la de fábrica. En la mayoría de casos, los usuarios de hogar o de empresas pequeñas dejan los dispositivos sin configurar y sin asegurar.

7) Usuarios y contraseñas de fábrica, de sitios especializados como los de la ***Ref. [4-01].***

8) Obtener Usuarios y contraseñas débiles. ***Ref. [4-02].***

Existen programas libres que permiten obtener usuarios y contraseñas de relativa debilidad, con programas como Ophcrack, OpenWall, Cain & Abel, Kon Boot.

9) Usuarios y contraseñas a la venta

En el mercado negro se consigue por $ 250 dólares o menos, un usuario y contraseña de los servicios populares como Hotmail, Gmail, Facebook, etc. Incluso se pueden conseguir bases de datos con gran cantidad de usuarios y contraseñas. Estas bases de datos se logran de diversas maneras: ingeniería social, phishing, keyloggers, etc.

10) Obtención de usuarios y contraseñas

Si lo anterior falla, el investigador puede por su propia cuenta realizar manualmente, o de forma automatizada con programas como John the Ripper [G36] o rootkits [G24] , una serie de pruebas de ensayo y error para averiguar los usuarios y contraseñas de un sistema.

Por diccionario

Por fuerza bruta [G38]

Por ingeniería social [G16]

John The Ripper [G36]

En la siguiente tabla, se presenta un comparativo de la funcionalidad de programas orientados a obtener usuario y password y el sistema operativo aplicable:

PROGRAMAS QUE PERMITEN OBTENER USUARIO Y CONTRASEÑA

SOPORTE DE SO	OPHCRACK	ONTP&RE	PCLN	KON-BOOT	C&A	LCP
Windows 7 [32-bit]	•	•	•	•[1]		
Windows 7 [64-bit]		•				
Windows Vista [32-bit]	•	•	•	•		
Windows Vista [64-bit]		•				
Windows XP	•	•	•	•	•	•
CARACTERÍSTICAS	**OPHCRACK**	**ONTP&RE**	**PCLN**	**KON-BOOT**	**C&A**	**LCP**
Recuperación password actual	•				•	•
Resetear /Blanquear/Borrar Password		•	•	•		
Causes Encrypted File Loss		•	•	•		
Proceso Relativamente rápido		•	•	•		
Open Source	•		•			
Booteable (No Instalable)	•	•	•	•		
Instala como una aplicación windows					•	•
Necesidad de acceso a otras cuentas					•	•
Interfaz gráfica	•		•	•	•	•
Interfaz de línea de comando	•	•				
Rompe cualquier Password		•	•	•		
Rompe pequeños y débiles Passwords	•				•	•
La mayor cantidad de proceso es automático	•		•	•		
Rompe Passwords Remotamente						

Tabla A29: Cuadro comparativo de programas que permiten obtener usuario y contraseña.

11) Si es en Linux, usar los comandos: last y lastb, para confirmar que los servidores han sido o no atacados.

12) Resetear (suprimir o reiniciar) contraseña de administrador.

Si la clave no se pudo conseguir por otros medios, o si la clave es demasiado fuerte, es posible suprimirla siguiendo procedimientos que no vamos a explicar aquí, pero que se pueden mirar en diferentes links especializados según la plataforma Windows, Iphone, Mac, Linux, detallados en la ***Ref. [4-03]*** y un cuadro comparativo de funcionalidades de programas en ambientes windows.

PASO 2.5: LOGIN AL COMPUTADOR OBJETIVO

Los protocolos TCP/IP disponen de una muy amplia variedad de trabajo remoto, sea mediante:

- El login al computador objetivo.
- El uso de directorios, carpetas y archivos remotos.
- A través de la ejecución remota de comandos.
- La administración remota.
- Y muchas técnicas que salen del alcance de esta investigación.

1) Existen muchas maneras de realizar un login (una conexión que utiliza CPU, memoria y dispositivos del computador objetivo), dependiendo del sistema operativo de origen y de destinatario

- En el caso de Linux, Unix, Solaris, HP/UP y similares, existen varios protocolos estándares que permiten acceder remotamente a un servidor. Es suficiente que el servidor esté corriendo cualquiera de los protocolos de conexión ssh, login, vnc, rdp, ftp, con sus respectivos puertos. La mayoría de estos protocolos tienen asociados, por omisión, su usuario y contraseña. También, es posible que esté instalada alguna versión de VNC.

- En el caso de Windows, existen varias maneras de acceder remotamente a un computador utilizando las facilidades de Windows. Éstas no se limitan al explorador de Windows ni al CMD. Se puede mencionar el Cliente de Acceso Remoto, que utiliza el protocolo RDP; el mecanismo de Terminal Server disponible en las versiones Server de Windows. También es posible que esté instalada alguna versión de VNC o de acceso remoto.

2) Otra forma es acceder, indirectamente, al equipo a través de un tercer equipo desprotegido pero que permita el acceso a recursos compartidos (carpetas o recursos). El uso de recursos compartidos, acceso a directorios o carpetas

   Si el login no se puede realizar al computador objetivo, todavía queda la posibilidad de acceder a recursos compartidos (conocidos como shares), mediante mecanismos de NETBIOS, SAMBA, IPC, RPC, NFS y otros protocolos que ponen a disposición de la red los directorios, archivos e impresoras.

3) También es posible acceder a la administración remota mediante técnicas de registro remoto, administración remota de comunidades snmp, administración remota mediante directorio activo, directorios públicos como LDAP, X.509, NIS, páginas amarillas o los

conocidos rootkits, que permiten a los atacantes tomar control remoto del teclado, el ratón y el monitor.

4) Uso de backdoors o rootkits.

Consiste en utilizar vulnerabilidades de algunos paquetes tales como servidor web, ftp, correo, mensajería, base de datos, para obtener, ya sea, información del computador objetivo o para tener acceso (login) a shares (recursos compartidos).

Los virus y programas promocionales en internet son frecuentemente usados como vehículos para insertar backdoors, rootkits [G24], keyloggers y programas para obtener información.

5) Inyección de código

Consiste en aprovecharse de formularios web mail diseñados para incluir un código, generalmente, SQL malicioso de tal manera que el computador objetivo revele información reservada como usuarios, contraseñas, permisos, contenidos de directorios y otra información que puede servir al atacante para introducirse en el equipo objetivo (login) o para obtener información que de otra manera, es inaccesible.

6) Determinar claves de archivos protegidos con clave

Para la gran mayoría de programas protegidos con clave existen programas que pueden quebrar esa clave. Por ejemplo, existen crackers (programas que rompen claves) para:

- Microsoft Office
- Archivos comprimidos zip, rar
- Carpetas comprimidas con ASF Windows

- Archivos de correo .PST

7) Determinar mecanismo de cifrado de información

Los mecanismos de cifrado de información varían de simples hasta muy complejos. Si el computador objetivo es de alguna entidad dedicada a la seguridad, debe valerse de mecanismos de cifrado fuerte, posiblemente claves simétricas con certificados digitales de 1024 bits o más. Un error frecuente de los encargados de seguridad es almacenar las claves simétricas en el mismo lugar, por lo que un atacante o un investigador puede, con relativa facilidad, dar con las parejas de certificados para descifrar (desencriptar la información [G31]).

8) Diccionarios previamente hasheados [G34] o encriptados

En internet existen varios diccionarios, en diferentes idiomas, que contienen palabras frecuentemente usadas como contraseñas pero convertidas a su respectivo código cifrado. Esto facilita la ruptura y obtención de claves por simple comparación. Se compara la clave cifrada con cada palabra del diccionario, pero no se la compara con la palabra original sino con la palabra cifrada, dando como resultado una igualdad cuando se ha encontrado la palabra adecuada. Se obtiene mirando la palabra sin cifrar y se obtiene la clave.

9) Buscadores de información

Existe gran cantidad de software libre para búsqueda de texto específico o patrones.

10) Visualizadores de archivos

Existe gran cantidad de software libre para leer archivos.

11) Honeypots o honeynets

Son mecanismos que engañan a un intruso confiado, haciéndole creer que logró ingresar a un sistema o logró vulnerar seguridades cuando en realidad está dentro de un programa que sólo aprueba comandos y acciones permitidas por el Honey Pot o Honey Net. Estas técnicas se consideran técnicas de contra espionaje o de desinformación. El investigador deberá estar atento para detectar si ha caído en una trampa, si el intruso a su vez ha caído en una trampa o ha instalado una. En una honeypot (un equipo) o honeynets (red de equipos), generalmente, se colocan documentos o archivos inofensivos o claramente desinformativos con el objetivo de simular piezas valiosas y distraer al atacante. Esto permite, además, conocer el origen del atacante, ya que sólo este tendrá acceso a la información falsa. Digamos que "hay una reunión reservada de seguridad el lunes 20 a las 20 horas en x lugar", todos quienes asistan a dicha reunión serán obviamente víctimas de la información falsa y podrán ser capturados "in fraganti" o en términos legales "en delito flagrante".

PASO 2.6: ANÁLISIS FORENSE, CRUCE DE INFORMACIÓN Y LÍNEA DE TIEMPO

1) El análisis forense no se limita a extraer la primera evidencia de una honeypot o honeynet sino que se debe verificar la autenticidad, el origen y el momento en que dicha información fue generada.

2) Para evitar ser víctimas de honey pots [G39], canarios, honey nets y técnicas de desinformación, el investigador deberá cotejar distintas fuentes de información y construir una línea de tiempo que pueda usarse para corroborar los datos. Si dos o más

fuentes de información distinta y confiable muestran la misma información, es más probable que sea verdadera.

3) Determinar la actividad realizada

Afortunadamente casi el 100% de servidores tienen activo el log del sistema o el registro de sucesos (Windows). Entonces se puede mirar el log del sistema, conformado por una serie de archivos, que no se explicará aquí, pero que se almacenan en /var/log bajo Linux o en /Windows/system32/config bajo Windows.

Muchos programas almacenan los links de los últimos archivos utilizados. Cada programa requiere una revisión. Afortunadamente existen programas que muestran las últimas actividades.

4) Determinar una línea de tiempo

Un paso crucial en el análisis forense es determinar la línea de tiempo desde el inicio del ataque hasta la culminación. Esta línea de tiempo ayuda a determinar la motivación y la oportunidad.

5) Determinar el vector de ataque

Aquí el análisis forense se vuelve complicado ya que podrían estar involucrados distintos dispositivos, por cable, por aire, dispositivos móviles, cortafuegos, IPS, routers, servidores, tabletas, teléfonos inteligentes, etc.

Lo mejor en este punto es que el investigador se capacite e investigue los dispositivos con los que se sienta más afín.

6) Simular el ataque.

Es necesario simular varias veces un ataque, para demostrar el nivel de vulnerabilidad de la red o el nivel de seguridad de la misma.

4.3.3 FASE 3: PRESENTACIÓN DE RESULTADOS

En esta fase se presentan las evidencias en formato digital debidamente hasheadas (aplicando algoritmos como md5, sha1, etc.).

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

"La mejor victoria es vencer sin combatir y ésa es la distinción entre el hombre prudente y el ignorante".
-Sun Tzu-, El Arte de la Guerra

5.1 CONCLUSIONES

5.1.1 RELACIONADAS CON LA SITUACIÓN ACTUAL DE LA INFORMÁTICA FORENSE

1. A nivel mundial, la situación actual de la informática forense, la forensia en redes y el hacking ético es de una relativa madurez, solidez y colaboración entre países y grupos de trabajo.

2. En el Ecuador, lamentablemente la situación es muy diferente. Existen pocas iniciativas privadas y la colaboración entre la Fiscalía General y la Policía Nacional. No existe un grupo de respuesta inmediata frente a incidentes, ni existe un grupo organizado al cual se pueda acudir para solicitar capacitación, apoyo o intervención unificada.

3. En el Ecuador existen pocas empresas que realizan capacitación pero que buscan imponer sus propias soluciones propietarias y sus técnicos especialistas para dichas soluciones. Nadie duda de la efectividad de sus soluciones y de sus técnicos, pero a la larga, crean dependencia tanto de la solución propietaria como de los técnicos.

4. En el Ecuador no existe una política gubernamental conocida ni estandarizada para proteger las redes y los activos informáticos en las entidades públicas. Cada entidad toma sus propias medidas, lo cual encarece los costos y multiplica los esfuerzos.

5.1.2 RELACIONADAS CON PROGRAMAS DE SOFTWARE LIBRE PARA INFORMÁTICA FORENSE

1. En internet existen gran variedad de programas de la categorías software libre (fundamentados en las cuatro libertades incluyendo el código fuente) y software gratuito (que no tiene costo pero que no dan código fuente).

2. No existe una única solución que pueda ser aplicable a todos los casos, debido a que las circunstancias, las preferencias y los ambientes que se analizan son tan variados que no es posible nombrar programas que se destaquen.

3. Existen colecciones de CDS y DVDs de software libre que pueden ayudar en la realización de un análisis forense y hacking ético, tales como CAINE, Backtrack, Insert, Helix y otros, pero se requiere de especialistas que comprendan las implicaciones y las distintas formas de usar de cada uno de estos programas. No es posible sacar provecho de ninguno de estos programas si no se dispone de profundos conocimientos de estas disciplinas y de los protocolos TCP/IP, lo cual lo convierte en herramientas altamente especializadas para uso exclusivo técnicos experimentados.

4. Existen programas independientes que ayudan a realizar tareas específicas de hacking ético y análisis forense como extraer claves de archivos, extraer las claves de Windows, de Messenger, obtener el historial de búsquedas en internet, etc. Esto hace parecer a la informática forense y al hacking ético como algo trivial y al alcance de cualquiera, aunque en realidad no sea así. Si bien estos programas son utilizados por los investigadores, se debe recordar que la investigación va más allá de obtener una clave y acceder a un sistema.

5. Los servidores modernos (basados principalmente en Linux, Solaris, Windows Server) disponen de suficientes herramientas de registro, monitoreo y detección de intrusos para que no pase desapercibida alguna actividad anormal por parte de algún usuario travieso o malicioso. Lamentablemente esta información se pierde a menos que se actúe a tiempo. Es posible que en los logs de muchos servidores todavía esté disponible la actividad maliciosa de muchos atacantes, a la espera de que alguien solicite el reporte de actividad.

5.2 RECOMENDACIONES

5.2.1 PARA LOS OFICIALES DE SEGURIDAD

1. Es recomendable que los oficiales de seguridad, estén informados y convencidos que para protegerse de la criminalidad informática, en primer lugar, deben conocer las necesidades de protección de su entorno, las fuentes de peligro e intrusión, las técnicas de manipulación y encubrimiento de los ciber-delicuentes; luego, deben adoptar sin demora herramientas e infraestructura para análisis, monitoreo y protección que no se limite a cortafuegos y antivirus, sino que empiecen con un buen diseño de la red, una asignación adecuada de permisos y recursos, una estrategia probada de monitoreo y control constante de incidentes reales y potenciales en su red.

2. Es recomendable que los oficiales de seguridad entiendan que, no necesariamente, lo más costoso es lo mejor; ya que las soluciones de seguridad están mejorando e innovando constantemente. Tampoco existe la garantía de que un programa comercial sea mejor que un programa de software libre, por lo que una mente abierta

y una capacitación constante son las mejores herramientas para obtener un balance adecuado entre costos y beneficios.

5.2.2 PARA LAS ENTIDADES E INSTITUCIONES

1. Sería adecuado que las entidades e instituciones afines compartan sus problemáticas, necesidades y soluciones, tanto para disminuir costos como para mejorar sus niveles de seguridad.
2. Es recomendable que las entidades dedicadas a la seguridad ciudadana promuevan, impulsen y apoyen la creación de grupos de respuesta inmediata frente a incidentes de seguridad. Un pequeño porcentaje de los presupuestos destinados a seguridad podrían servir para apoyar la creación de grupos especializados de respuesta inmediata que una vez conformados actuarían independientemente.
3. Debería crearse una guía unificada de análisis forense aplicable a entidades de seguridad ciudadana.

5.2.3 PARA EL PÚBLICO EN GENERAL

1. Crear foros en la que el público sea informado de los incidentes de seguridad informática y adoctrinado en las formas de evitar o mitigar el impacto de los mismos.
2. Es necesario educar a la comunidad sobre los delitos informáticos e incentivar las denuncias de las víctimas o las personas que conocen potenciales amenazas. Promover la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos, es una labor importante. Se debe, además, difundir los canales

adecuados, así como las herramientas útiles para asegurar que sus computadores están libres de programas maliciosos: antivirus, control de accesos remotos, claves débiles, recursos innecesariamente compartidos, información confidencial no protegida, entre otros que sean factibles de ser administrados a nivel de usuario.

CAPÍTULO VI: GLOSARIO

"La gran sabiduría no es algo obvio, el mérito grande no se anuncia."
-Sun Tzu-, El Arte de la Guerra

[G01] ANÁLISIS FORENSE

El análisis forense es el proceso mediante el cual se recopila y analiza la evidencia digital [G32] encontrada en una escena.

Para realizar debidamente el análisis forense, no es suficiente conocer de informática, tampoco es suficiente conocer de leyes o de criminalística. El análisis forense nada tiene que ver con auditoría informática, tiene su propio procedimiento.

[G02] INFORMÁTICA FORENSE

El FBI define la informática (o computación) forense como: la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

Otro concepto que se encuentra en varias publicaciones, y es acogido por varios especialistas, dice que "la informática forense es el estudio completo de un sistema computacional que sufrió un ataque o que se usó para cometer un ilícito". [Cano, 2005]. ***Ref. [B].***

Otro concepto: "Es la ciencia y técnicas para realizar un examen profesional de sistemas informáticos o electrónicos emitiendo un informe de apoyo en casos legales, judiciales, tributarios, industriales, comerciales, policiales, militares, etc". [Casey, 2004]. ***Ref. [C].***

Los objetivos de la informática forense (Ricardo Ortega 2008) son:

1) **Técnico:** Identificar los hechos, víctimas y daños causados al sistema o a terceros.
2) **Remedial:** corregir los daños causados al sistema informático.
3) **Cumplimiento de la ley:** Perseguir y procesar debidamente a los autores.
4) **Preventivo:** Crear y aplicar medidas para prevenir casos similares; crear conciencia acerca de las técnicas utilizadas para cometer estos ilícitos y las formas de detectarlos y prevenirlos; crear conciencia acerca de los procedimientos, el correcto manejo de evidencias y cadena de custodia.

[G03] SOFTWARE LIBRE

Es el tipo de programa que se tiene como base la libertad de los usuarios para usar, ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Las cuatro libertades de los usuarios son: La libertad de usar el programa, con cualquier propósito. La libertad de estudiar cómo funciona el programa y adaptarlo a sus necesidades. La libertad de distribuir copias. La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie.

[G04] TCP/IP (PROTOCOLO DE CONTROL DE TRANSMISIÓN/PROTOCOLO DE INTERNET).

TCP/IP son las siglas de Protocolo de Control de Transmisión/Protocolo de Internet (en inglés *Transmission Control Protocol/Internet Protocol*). Estos son un sistema de protocolos que hacen posibles servicios Telnet, FTP, E-mail, y otros entre ordenadores que no pertenecen a la misma red.

El modelo TCP/IP, tiene 4 capas y cada una tiene tareas y protocolos que le permiten su funcionamiento:

Capa de acceso a la red: específica la forma en la que los datos deben enrutarse, sea cual sea el tipo de red utilizada.

Capa de Internet: es responsable de proporcionar el paquete de datos (datagrama).

Capa de transporte: brinda los datos de enrutamiento, junto con los mecanismos que permiten conocer el estado de la transmisión.

Capa de aplicación: incorpora aplicaciones de red estándar (Telnet, SMTP, FTP, etc.).

[G05] VULNERABILIDADES

Son los riesgos reales o hipotéticos que pueden tener los sistemas y programas. Se diferencian de los incidentes en que estos son el uso real de una vulnerabilidad.

[G06] COMPUTACIÓN FORENSE (COMPUTER FORENSICS)

Es la disciplina técnico científica que consiste en descubrir, interpretar y presentar la información de un sistema informático.

[G07] FORENSIA EN REDES (NETWORK FORENSICS)

Es la disciplina técnico científica cuyo objetivo es descubrir los rastros y movimientos de un intruso dentro de una red informática.

[G08] FORENSIA DIGITAL (DIGITAL FORENSICS)

Es la disciplina técnico científica que consiste en esclarecer hechos (quién, cómo, cuándo, por qué). Esto es, aplicar la criminalística tradicional a la tecnología digital.

[G09] CADENA DE CUSTODIA

Es el proceso ininterrumpido y documentado que permite demostrar la autenticidad (originalidad) e integridad de la evidencia física.

[G10] RFC 3227

Es una guía para recolectar y archivar evidencia (Guidelines for Evidence Collection and Archiving), escrita en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group. Es un documento que provee una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones. Describe las mejores prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos. También explica algunos conceptos y pasos.

[G11] CEH - CERTIFIED ETHICAL HACKER

Es la certificación oficial de hacking ético desde una perspectiva independiente de fabricantes. El Hacker Ético es la persona que lleva a cabo intentos de intrusión en redes y/o sistemas utilizando los mismos métodos que un delincuente informático. La diferencia más importante es que el Hacker Ético tiene autorización para realizar las pruebas sobre los sistemas que ataca. El objetivo de esta certificación es adquirir conocimientos prácticos sobre los sistemas actuales de seguridad.

[G12] CFEC - COMPUTER FORENSIC EXTERNAL CERTIFICATION

Es una credencial que otorga la International Asociación for Computer Information Systems (IACIS - www.iacis.org), que se encuentra diseñada para personas que no pertenezcan a instituciones judiciales o de policía. El programa cuenta con algunas diferencias, dada su función y su grupo de usuarios, pero con el mismo contenido para los aplicantes externos. Para acceder a esta certificación, es necesario girar US$1250 a IACIS y tramitar una forma de aplicación con múltiples datos del aspirante. La aplicación es evaluada por el comité de IACIS. Si la forma es aceptada, se inicia el proceso de evaluación, que consiste en el análisis de seis diskettes especialmente preparados y un disco duro con una disposición especial. Cada uno de los diskettes establece un problema técnico y forense para que aplicante los resuelva, documentando sus hallazgos en un reporte donde detalle sus análisis. Al final del proceso, cuya duración máxima es cinco meses, se efectúa un examen sobre el desempeño y las conclusiones del investigador en cada uno de los ejercicios. El examen requiere que el aplicante demuestre su competencia y claridad para el desarrollo de las actividades forenses.

[G13] CCCI - CERTIFIED COMPUTER CRIME INVESTIGATOR.

Nivel básico y avanzado. Es una credencial otorgada por la HTCN (High Tech Crime Network). Cada una de las certificaciones requiere que el aplicante cuente con un curso de entrenamiento, un número de horas y exámenes escritos debidamente aprobados en centros de entrenamiento autorizados. El propósito de la certificación es desarrollar un alto nivel de profesionalismo y entrenamiento contínuo, que soporte investigaciones de crímenes de alta tecnología en la industria y las organizaciones. El costo de la certificación es de US$250, valor requerido para evaluar la forma de aplicación y analizar la experiencia del aspirante; así como, para cubrir los gastos relacionados con el registro ante notaría de la experiencia certificada y los títulos adjuntos.

[G14] CERT

Computer Emergency Response Team o equipo de respuesta para emergencias de computadores, cuyo centro de control está en la Universidad Carnegie Mellon.

[G15] CSIRT

Grupos de respuesta rápida a incidentes de seguridad de alcance mundial.

[G16] INGENIERÍA SOCIAL

La ingeniería social consiste en manipular personas, es decir, aprovecharse de la inocencia y bondad de los usuarios de redes para obtener información acerca de la red o de la persona. Este proceso consiste en contactar un usuario, normalmente haciéndose pasar por otra persona, para obtener información acerca del sistema informático y probablemente para obtener directamente una contraseña. En forma similar, se puede crear una falla de seguridad en el sistema remoto al enviar un troyano a alguno de los usuarios de la red. Lo único que se necesita es que uno de los usuarios abra el adjunto para que el atacante externo obtenga el acceso a la red interna.

Éste es el motivo por el que las políticas de seguridad deberían ser más exhaustivas e incorporar los factores humanos (por ejemplo, informar a los usuarios acerca de los problemas de seguridad), ya que el nivel de seguridad de un sistema se determina por la fuerza de su eslabón más débil.

[G17] ATAQUE (ATAQUE INFORMÁTICO)

Un ataque informático es un método por el que un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (computador, red privada, etcétera).

[G18] TIPOS DE ATAQUES INFORMÁTICOS

Hay diversos tipos de ataques informáticos, algunos son:

- Ataque de denegación de servicio (Denegation of Service –DoS-).
- Hombre en el medio (Man in the middle –MiM-).
- Ataque de replay.
- Ataque de día cero.

[G19] ATAQUE DE DENEGACIÓN DE SERVICIO

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente, se provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

[G20] MAN IN THE MIDDLE.

A veces abreviado MitM o Mim, es una situación donde un atacante supervisa una comunicación entre dos partes y falsifica los intercambios para hacerse pasar por una de ellas.

[G21] ATAQUE DE REPLAY

Una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida o retardada. Es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado.

[G22] ATAQUE DE DÍA CERO.

Ataque realizado contra un ordenador, a partir del cual se explotan ciertas vulnerabilidades, o agujeros de seguridad de algún programa o programas, antes de que se conozcan las mismas, o que, una vez publicada la existencia de la vulnerabilidad, se realice el ataque antes de la publicación del parche que la solvente.

[G23] EXPLOIT

Exploit (del inglés to exploit, explotar, aprovechar) es el nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa. El fin puede ser la destrucción o inhabilitación del sistema atacado, aunque normalmente es un intento por violar las medidas de seguridad para poder acceder al sistema de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.

Los exploits se pueden caracterizar según las categorías de vulnerabilidades utilizadas:

- Vulnerabilidades de desbordamiento de buffer
- Vulnerabilidades de condición de carrera
- Vulnerabilidades de error de formato de cadena

- Vulnerabilidades de Cross Site Scripting XSS
- Vulnerabilidades de Inyección SQL
- Vulnerabilidades de Inyección de Caracteres CRLF
- Vulnerabilidades de denegación del servicio
- Vulnerabilidades Inyección múltiple HTML Múltiple HTML Injection
- Vulnerabilidades de ventanas engañosas o mistificación de ventanas Window Spoofing

Cada una de estas vulnerabilidades tiene uno o más exploits que se aprovechan para atacar al programa y por consiguiente al computador objetivo.

[G24] ROOTKIT

Es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers con el objetivo de acceder ilícitamente a un sistema informático. Hay rootkits para una amplia variedad de sistemas operativos como Linux, Solaris o Microsoft Windows. Por ejemplo, el rootkit puede esconder una aplicación que lance una consola cada vez que el atacante se conecte al sistema a través de un determinado puerto. Los rootkits del kernel o núcleo pueden contener funcionalidades similares.

Un backdoor (puerta trasera o código secreto) puede permitir también que los procesos lanzados por un usuario sin privilegios de administrador ejecuten algunas funcionalidades reservadas únicamente al superusuario. Todo tipo de herramientas útiles para obtener información de forma ilícita se pueden ocultar mediante rootkits

Los rootkits tratan de encubrir a otros procesos que están ejecutando acciones maliciosas en el sistema. Por ejemplo, si en el sistema hay una puerta trasera para llevar a cabo tareas de espionaje, el rootkit ocultará los puertos abiertos que delaten la comunicación; o si hay un sistema para enviar spam, ocultará la actividad del sistema de correo.

Los rootkits, al estar diseñados para pasar desapercibidos, no pueden ser detectados fácilmente. Si un usuario intenta analizar el sistema para ver qué procesos están ejecutándose, el rootkit mostrará información falsa, mostrando todos los procesos excepto el suyo propio y los que está ocultando. Si se intenta ver un listado de los ficheros de un sistema, el rootkit hará que se muestre esa información pero ocultando la existencia del propio fichero del rootkit y sus procesos.

Cuando el antivirus haga una llamada al sistema operativo para comprobar los ficheros existentes o cuando intente averiguar qué procesos están en ejecución, el rootkit falseará los datos y el antivirus no podrá recibir la información correcta para llevar a cabo la desinfección del sistema.

[G25] VECTOR DE ATAQUE

Es la ruta o camino que sigue un atacante para llegar al computador atacado.

[G26] HACKER

Persona que tiene un conocimiento profundo acerca del funcionamiento de redes, por lo que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos. Sin embargo, el cracker lo hace con fines de protagonismo. Según esta definición, el hacker es el bueno y el cracker es el malo.

Hasta hace pocos años el término hacker era un término despectivo asignado a todo aquel que husmeaba o se colaba furtivamente en sistemas de cómputo sin importar sus motivaciones.

Por asociación, el término "hackear" significa esquivar o evitar las seguridades, mientras que "crackear" significa romper las seguridades. Ambos verbos llevan al mismo resultado: introducirse en un sistema de cómputo o red.

[G27] CRACKER

Persona que trata de introducirse a un sistema sin autorización y con la intención de realizar algún tipo de daño u obtener un beneficio. En este caso, el cracker es un "rompedor" de seguridades y actúa para perjudicar a los responsables del sistema de cómputo.

[G28] HACKING ÉTICO

El hacking ético es una forma apegada a la ética de hacer hacking, en contraposición al hacking no ético o sea hacking malicioso.

Una definición de hacking ético la encontramos en el sitio web www.ricardoortega.com: "el Hacking ético es la aplicación de pruebas de vulnerabilidad y test de penetración sobre un sistema de cómputo, realizada por personal especializado, con el consentimiento de los responsables del sistema de cómputo, para determinar el nivel de seguridad del referido sistema de cómputo y con el compromiso de revelar a los responsables la totalidad de las vulnerabilidades encontradas; esto en contraposición al hacking no ético en donde el atacante aplica pruebas de vulnerabilidad, aplica exploits y aplica test de penetración para introducirse al sistema, alterar el sistema, reservarse conocimientos, divulgar a terceros o

explotar las vulnerabilidades encontradas. Es decir que el acto es exactamente el mismo en ambos casos, incluso las herramientas pueden ser las mismas, pero la finalidad es distinta: finalidad ética vs. finalidad no ética".

Hacking ético, se define como: Una forma de referirse al acto de una persona que usa sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, con el objetivo de reportarlas y que se tomen medidas, sin hacer daño.

La idea es tener el conocimiento de cuales elementos dentro de una red son vulnerables y corregirlo antes que ocurra hurto de información, por ejemplo.

Estas pruebas se llaman "pen tests" o "penetration tests" en inglés. En español se conocen como "pruebas de penetración", donde se intenta, de múltiples formas, burlar la seguridad de la red para robar información sensitiva de una organización, para luego reportarlo a dicha organización y así mejorar su seguridad.

Se sugiere a empresas que vayan a contratar los servicios de una empresa que ofrezca el servicio de hacking ético, y que la misma sea certificada por entidades u organizaciones con un buen grado de reconocimiento a nivel mundial.

Las personas que hacen estas pruebas pueden llegar a ver información confidencial, es recomendable verificar el nivel de confiabilidad del asesor de seguridad.

[G29] LOGS Y SUCESOS DEL SISTEMA

Los logs o registros de eventos del sistema son archivos donde se van almacenando los distintos sucesos que se producen en un sistema de cómputo.

En Linux se almacenan en el directorio: /var/log

En Windows XP: /Windows/system32/config/*.evt (archivos con extensión .evt)

En Windows Vista/7: Windows/SYSTEM32/EVT/*.evtx (archivos con extension .evtx)

[G30] CYBERBULLING

Es el término en inglés que se refiere al acto de atormentar y molestar a otra persona usando medios electrónicos como email, mensajería instantánea, blogs, páginas web, SMS, entre otros.

[G31] CRIPTOGRAFÍA

Cifrado de información buscando ocultar el contenido.

[G32] EVIDENCIA DIGITAL

La evidencia digital tiene varias definiciones, según varios autores:

"Cualquier dato que puede establecer que un crimen se ha ejecutado (commit) o puede proporcionar un enlace (link) entre un crimen y su víctima o un crimen y su autor" [Casey, 2004].

"Es un tipo de prueba física. Está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. Ejemplos: archivos, imágenes, sonidos, correos electrónicos, etc." [Acurio, 2007]

[G33] NORMAS DE SEGURIDAD SERIE ISO 27000

Las normas ISO 27000 tienen aproximadamente 5 años de publicadas. Proporcionan un marco de referencia para gestión de la seguridad de la información. No mencionan a la informática forense pero son un buen marco de referencia para aplicar mecanismos de seguridad.

[G34] HASH

Función hash, es una función computable mediante un algoritmo. Se llaman funciones hash criptográficas a aquellas que se utilizan en el área de la criptografía. Este tipo de funciones se caracterizan por cumplir propiedades que las hacen idóneas para su uso en sistemas que desean dotar de seguridad. Estas propiedades las hacen resistentes frente ataques maliciosos que intentan romper esa seguridad.

[G35] EXPLOITS

Pieza de software, un fragmento de datos, o una secuencia de comandos, hecha para aprovechar un error, fallo o vulnerabilidad de un software o una función de un sistema informático, con el fin de comportamiento anómalo, inesperado o fallo en la funcionalidad. Este tipo de comportamiento suele incluir cosas tales como tomar el control de un sistema informático o permitir la escalada de privilegios o un ataque de denegación de servicio.

[G36] JOHN THE RIPPER

Es un programa que nos permite recuperar contraseñas a partir de los datos que existen en nuestro sistema. Actualmente está disponible para Unix/Linux, Windows, DOS, BeOS y OpenVMS. El propósito principal de esta herramienta es la detección se contraseñas débiles por parte del administrador del sistema.

John the Ripper no es un simple programa de cracking de contraseñas por fuerza bruta [G38] ya que dispone de varios modos de funcionamiento que permiten una búsqueda "inteligente" de las contraseñas más inseguras.

[G37] BACKDOOR

Una puerta trasera es un medio de acceso a un programa de ordenador que no pasa por los mecanismos de seguridad. Un programador puede, a veces, instalar una puerta trasera para que se pueda ingresar al programa con fines de resolución de problemas o de otro tipo. Sin embargo, los atacantes suelen utilizar puertas traseras que se detectan o se instalan como parte de un exploit. En algunos casos, un gusano está diseñado para tomar ventaja de una puerta trasera creado por un ataque anterior. Por ejemplo, Nimda logrado entrar por una puerta trasera dejada por Code Red.

[G38] ATAQUE POR FUERZA BRUTA

En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

[G39] HONEY POTS

Es una técnica para detección de intrusiones, usada para estudiar el movimiento de los hackers, así también para preparar el sistema para futuros ataques. Lo malo de esta técnica es que se requiere gran cantidad de recursos, para montar el módulo central de análisis.

[G40] ATAQUES POR DICCIONARIO

Un ataque de diccionario es un método de cracking que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario. Este tipo de ataque suele ser más eficiente que un ataque de fuerza bruta, ya que muchos usuarios suelen utilizar una palabra existente en su lengua como contraseña para que la clave sea fácil de recordar, lo que no es una práctica recomendable.

[G41] INCIDENTE

Cualquier intento de violar la política de seguridad, una penetración exitosa, un comprometimiento peligroso de un sistema, o de cualquier acceso no autorizado a la información.

[G42] RESPUESTA A INCIDENTES

Cómo una organización responde a un incidente.

[G43] PLAN DE RESPUESTA A INCIDENTES (IRP).

Una política que define como una organización responde a un incidente.

[G44] EQUIPO DE RESPUESTA A INCIDENTES (IRT).

También conocido como un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT). El grupo de personas encargadas de responder cuando un fallo de seguridad se ha producido.

[G45] SEGURIDAD INFORMATICA.

El término seguridad de la información abarca una amplia gama de actividades de una organización, incluye productos y procesos creados para evitar el acceso no autorizado, modificación y supresión de información. Seguridad de la información incluye tres áreas de atención primaria: física, operacional y de gestión. Un plan eficaz de seguridad informática debe evaluar los riesgos y crear estrategias y métodos para hacerles frente.

1.- La seguridad física: Consiste en la protección de sus activos y la información de acceso físico por personal no autorizado, abarcan todo lo que esté relacionado con el diseño físico o la seguridad física de la red.

2.- Seguridad operacional: Se ocupa de la forma en la que la organización hace las cosas, esto incluye computadoras, redes, y sistemas de comunicaciones. Aspectos operativos de seguridad incluyen control de acceso, autenticación y seguridad de topologías. Después de que la instalación de la red se ha completado, se debe considerar las operaciones diarias de la red, las conexiones con otras redes, planes de copia de seguridad y planes de recuperación. En resumen, ese enfoca en la topología y las conexiones.

3.- Gestión y políticas: Las acciones que se toman a este nivel afectan a toda la empresa, por lo que requieren apoyo de la Dirección. Los puntos que deben ser considerados son:

- Políticas administrativas.
- Requisitos del diseño de software.
- Planes de recuperación de desastres.
- Las políticas de información.
- Las políticas de seguridad.
- Políticas de uso.

- Políticas de gestión de usuarios.
- Políticas Administrativas

[G46] OPEN SOURCE VULNERABILITY DATABASE (OSVDB).

El proyecto promueve una mayor colaboración abierta entre empresas y particulares, eliminar trabajos redundantes y reduce los gastos inherentes al desarrollo y mantenimiento en bases de datos de vulnerabilidades en línea.

[G47] WIKILEAKS

Wikileaks(del inglés leak, «fuga», «goteo», «filtración [de información]»), es una organización mediática internacional sin ánimo de lucro que publicaba a través de su sitio web, informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes.

[G48] SOFTWARE ANTIVIRUS

El principal método para prevenir la propagación de código malicioso implica el uso de software antivirus. El software antivirus es una aplicación que se instala en un sistema para proteger y para escanear en busca de virus, así como gusanos y caballos de troya. La mayoría de los virus tienen características que son comunes a las familias de virus. El software antivirus busca estas características o huellas digitales para identificar y neutralizar estos virus antes de que afecten al PC y/o red LAN.

[G49] FALSO POSITIVO.

Un evento marcado que no es realmente un evento y ha sido falsamente señalado como de interés.

[G50] LA OFICINA FEDERAL DE INVESTIGACIONES (FBI).

Es una agencia gubernamental que pertenece al Departamento de Justicia de Estados Unidos que funciona como un organismo federal de investigación criminal y una agencia de inteligencia interna (contrainteligencia).

[G51] DIRECCIÓN MAC

En las redes de computadoras, la dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el identificador único organizacional (organizationally unique identifier).

[G52] MAC/IP

Dirección física del dispositivo de (48 bits, 6 bloques hexadecimales) y dirección lógica del dispositivo (32 bits, 4 bloques decimales).

[G53] EAVESDROPPING.

Eavesdropping, término inglés que traducido al español significa escuchar secretamente, se ha utilizado tradicionalmente en ámbitos relacionados con la seguridad, como escuchas telefónicas.

Se ha convertido en parte de la jerga habitual en criptografía y se refiere a ataques de escuchas, tanto sobre medios con información cifrada, como no cifrada.

[G54] PROXI

Los proxies tienen muchas utilidades, generalmente funcionan junto con las firewalls, se usan de cache para acelerar la navegación en LANs o hasta en ISP. Si nos conectamos a un servidor X mediante un proxy, nosotros hacemos el pedido al proxy, el proxy lo hace al servidor X y nos envía la respuesta a nosotros. Por lo tanto en X queda registrado que se conectó el proxy y no directamente nosotros.

Aunque en los logs del proxy puede figurar nuestra IP y a donde nos conectamos. En definitiva usando proxies ocultamos nuestra IP y por lo tanto nos ANONIMIZAMOS.

El proxy también tiene sus desventajas, como posibilidad de recibir contenidos que no están actualizados, tener que gestionar muchas conexiones y resultar un cuello de botella, o el abuso por personas que deseen navegar anónimamente. También el proxy puede ser un limitador, por no dejar acceder a través suyo a ciertos protocolos o puertos.

CAPÍTULO VII: BIBLIOGRAFÍA

"El que es prudente y está a la espera de un enemigo que no lo es, será victorioso".
-Sun Tzu-, El Arte de la Guerra

7.1. LIBROS.

[A] PROAÑO FREIRE MARGOTH, "ESTUDIO DE SOFTWARE LIBRE PARA REALIZAR EL ANÁLISIS FORENSE EN REDES DE COMPUTADORES PARA ENTIDADES ECUATORIANAS DEDICADAS A LA SEGURIDAD CIUDADANA", PUCE, 2012 DICIEMBRE.

[B] CANO JEIMY, "ESTADO DEL ARTE DEL PERITAJE INFORMÁTICO EN LATINOAMÉRICA", ALFA-REDI, 2005.

[C] CASEY EOGHAN, "HANDBOOK OF COMPUTER INVESTIGATION", ELSEIVER ACADEMIA PRESS, 2004,2005.

[D] LÓPEZ DELGADO MIGUEL, "ANÁLISIS FORENSE DIGITAL", CRIPTORED, 2007.

[E] EC_COUNCIL PRESS, "COMPUTER FORENSICS INVESTIGATING NETWORK INSTRUSIONS & CYBERCRIME", ELSEVIER, 2006.

[F] STEVE BUNTING &WILLIAM WEI, "ENCASE COMPUTER FORENSICS", ELSEVIER, 2006.

[G] MICHAEL T. SIMPSON, KENT BACKMAN AND JAMES E CORLEY, "HANDS-ON ETHICAL HACKING NETWORK DEFENSE", ELSEVIER, 2003.

[H] IDO DUBRAWSKY; "HOW TO CHEAT AT SECURITY YOUR NETWORK", ELSEVIER, 2007.

[I] BILL NELSON, AMELIA PHILLIPS, CHISTOPHER STEUART; GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS, ELSEVIER, 2010.

[J] DEBRA LITTLEJOHN SHINDER, SCENE OF THE CYBERCRIME COMPUTER FORENSICS HANDBOOK, ELSEVIER, 2002.

[K] KEVIN KARDWELL (USA), THE BEST DAMN CYBERCRIME AND DIGITAL FORENSICS, BOOK PERIOD 2007.

[L] HARLAN CARVEY, WINDOWS REGISTRY FORENSICS ADVANCED DIGITAL FORENSIC ANALYSIS OF THE WINDOWS REGISTRY, ELSEVIER, 2011.

[M] CHRIS SANDERS, PRACTICAL PACKET ANALYSIS USING WIRESHARK TO SOLVE REAL – WORLD NETWORK PROBLEMS, ELSEVIER, 2011

[N] JESSE VARSALONE, CISCO ROUTERS AND SWITCH FORENSICS, ELSEVIER, 2009.

[O] SERGIO RODRIGUES NUNES, WEB ATTACK RISK AWARENESS WITH LESSONS LEARNED FROM HIGH INTERACTION HONEY POTS, THESIS CARNEGIE MELLOR INSTITUTE, 2009.

[X] ACURIO SANTIAGO, DERECHO PENAL INFORMÁTICO, PUCE, 2010.

[X1] ACURIO SANTIAGO, DERECHO PENAL INFORMÁTICO, PUCE, 2008.

7.2. DOCUMENTOS DIGITALES.

[P] ORTEGA, RICARDO (ECUADOR), DOCUMENTO DIGITAL,

http:// www.ricardoortega.com/informaticaforense.ppt.

[Q] QUITUISACA, LILIA (UCE ECUADOR), DOCUMENTO DIGITAL.

http://www.scribd.com/doc/24759421/informaticaforense

[R] ACURIO, SANTIAGO, DELITOS INFORMÁTICOS.

www.cavaju.com/.../los-delitos-informaticos-en-el-ecuador-parte-ii/

[S] ACURIO, SANTIAGO; FISCALÍA GENERAL DEL ESTADO ECUADOR, DOCUMENTO DIGITAL ECUADOR: INTRODUCCIÓN A LA INFORMÁTICA FORENSE

http://dialnet.unirioja.es/servlet/articulo?codigo=2390567

[T] ONU, DOCUMENTO DEL VI CONGRESO LATINOAMERICANO EN REFERENCIA "TIPOS DE DELITOS INFORMÁTICOS"; 1998; COLONIA-URUGUAY.

[U] RFC3227: ESTÁNDAR INTERNACIONAL PARA INFORMÁTICA FORENSE.

http://rfc.net/rfc3227.html

[V] IOCE, OTRO ESTÁNDAR DE INFORMÁTICA FORENSE *[G02]*

www.preyproject.orgdigit_tech.html

[W] ISO/IEC 27037, ESTÁNDAR DE TECNOLOGÍA DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD EN EL PROCESO DE IDENTIFICACIÓN, RECOLECCIÓN, CAPTURA Y PRESERVACIÓN DE LA EVIDENCIA DIGITAL, PARA SU ADMISIBILIDAD TRANSNACIONAL O LOCAL

http://webstore.iec.ch/webstore/webstore.nsf/artnum_pk/47060?opendocument&mlref=jp.

[Y] POLICÍA NACIONAL DEL ECUADOR Y LA FISCALÍA GENERAL DEL ESTADO, MANUAL DE PROCEDIMIENTOS INVESTIGATIVOS.

http://www.dnpj.gob.ec/portal/files/MANUAL%20%20FISCALIA-POLICIA%20JUDICIAL%202011.pdf

[Z] FISCALÍA GENERAL DEL ESTADO, "MANUAL DE MANEJO DE EVIDENCIAS DIGITALES Y ENTORNOS INFORMÁTICOS V 2.0"

http://www.oas.org/juridico/english/cyb_pan_manual.pdf

7.3 REFERENCIAS DE INTERNET.

CAPÍTULO I: INTRODUCCIÓN

[1-01] BASE DE DATOS OPENSOURSE DE VULNERBILIDADES;

http://www.osvdb.org/

[1-02] VULNERABILIDADES SERVIDOR APACHE TOMCAT;

http://osvdb.org/search/search?search%5bvuln_title%5d=apache+tomcat&search%5btext_type%5d=titles&search%5bs_date%5d=&search%5be_date%5d=&search%5brefid%5d=&search%5breferencetypes%5d=&search%5bvendors%5d=&search%5bcvss_score_from%5d=&search%5bcvss_score_to%5d=&search%5bcvss_av%5d=&search%5bcvss_ac%5d=*&search%5bcvss_a%5d=*&search%5bcvss_ci%5d=*&search%5bcvss_ii%5d=*&search%5bcvss_ai%5d=*&kthx=search*

[1-03] ALERTAS PUBLICADAS DEL CSIRT ARGENTINA;

http://www.icic.gob.ar/paginas.dhtml?pagina=123&anio=2012&mes=6

[1-04] PORTADA DEL TRATADO DE LOS VENENOS 1814;

http://www.securitybydefault.com/2011/02/historia-de-la-ciencia-forense.html.

[1-05] DFRWS (DIGITAL FORENSIC RESEARCH WORKSHOP); GRUPO DE DEBATE Y DISCUSIÓN INTERNACIONAL SOBRE TEMAS DE FORENSIA DIGITAL;

www.dfrws.org.

[1-06] WEB DE EXPERTOS EN SEGURIDADES Y ANÁLISIS FORENSE;

www.criptored.com , http://haddensecurity.wordpress.com/tag/cert/

[1-07] INFORMÁTICA FORENCE-CAPACITACIÓN;

www.cec-epn.edu.ec.

[1-08] EMPRESA DE SEGURIDAD;

www.digiware.net.

[1-09] PROYECTO CERT ECUADOR;

https://sites.google.com/site/certecuadorcc/

[1-10] SUPERINTENDENCIA DE TELECOMUNICACIONES;

http://www.supertel.gob.ec

[1-11] BLOG LEGAL (ECUADOR);

http://www.interfutura.ec/blog/delitos-informaticos-en-ecuador-lo-quvendria-en-la-nueva-legislacion/

[1-12] PUBLICACIONES DE SEGURIDAD;

http://www.cavaju.com/2012/02/29/los-delitos-informaticos-en-el-ecuador-parte-ii/

[1-15] BLOG DE LEGAL Y FORENSE;

http://forensicsource.blogspot.com/2012/02/internet-evidence-finder-vs-netanalysis.html

CAPÍTULO II: LAS REDES Y EL ANÁLISIS FORENSE

[2-01] DIRECCION DE IP REAL;

www.verip.es

[2-02] UBICACIÓN DE HOST (MAC/IP);

www.iplookup.net

[2-03] MAPAS DE GOOGLE CON UBICACION APROXIMADA DEL HOST IP;

www.geoiptool.com

[2-04] CAPTURA DE PANTALLA DE WEB CON NOTICIAS DE SEGURIDAD INFORMÁTICA;

www.seguridadpc.net

[2-05] CERT DEL INSTITUTO CARNEGIE MELLON;

www.cert.org

[2-06] SITIO WEB DE SEGURIDAD;

www.searchsecurity.com

[2-07] BASE DE DATOS DE VULNERABILIDADES OPEN SOURCE (OSVDB);

www.osvdb.org.

[2-08] CONSOLA DE TOR;

www.torproyect.org.

[2-09] INTERFAZ DE INSTALACION DEL PROGRAMA TOR.

127.0.0.1

[2-10] CAPTURA DE PANTALLA DEL FUNCIONAMIENTO WEB CON TOR HABILITADO.

http://geobytes.com/iplocator.htm

[2-11] PAGINAS CON INFORMACION DEL VIRUS DNS CHALENGER

http://www.dns-changer.eu

http://www.dcwg.org/detect

[2-12] SITIO CON FACILIDADES DE NAVEGACIÓN ANÓNIMA; J. VOIGHT, "BEYOND THE BANNER";

www.iec.csic.es/criptonomicon/anonimato.html

[2-13] SITIO DE FACILIDADES PARA SERVICIOS PROXI;

www.proxy4free.com.

[2-14] PÁGINAS WEB DE SEGURIDAD

NORTON SAFEWEB;

https://safeweb.norton.com/

ALL NETTOOLS;

http://www.all-nettools.com/toolbox/privacy.htm

ANONYMOUS SURFING;

http://www.anonymizer.com

CYBERPASS

http://www.cyberpass.net

KIOSKEA;

http://es.kioskea.net

TOR PROYECT;

http://www.torproject.org

CERT CARNEGIE MELLON UNIVERSITY

www.cert.org

[2-15] PROXIS ANÓNIMOS.

proxy1.emirates.net.ae, http port 8080

wwwcache.marques.co.za, http port 3128

proxy.chs.edu.sg, http port 3128

proxy.pty.com, http port 8080

proxy.silcom.com, http port 3128

proxy.tmc.edu.tw, http port 3128

webcache.ms.mff.cuni.cz, http port 8080

littlehat.zetnet.co.uk, http port 8080

proxy.networld.it, http port 80

proxy.hro.nl, http port 80

digilab.tau.it, http port 80

proxy.ecity.net, http port 80

proxy.ipm.lviv.ua, http port 80

[2-16] PÁGINA DE AYUDA PARA NAVEGACION ANÓNIMA.

www.iec.csic.es/criptonomicon/anonimato.html

[2-17] PUBLICACIÓN LEGAL DEL DR.HALANOCA HUAMAN, JULIAN

http://agendamagna.wordpress.com/2009/02/10/julian-cesar-halanoca-huaman/

CAPÍTULO III: PROGRAMAS LIBRES PARA FORENSIA EN REDES

[3-01] FORENSIC TOOLKIT (FTK)

http://www.accessdata.com/products/ftk/

[3-02] SOFTWARE PROPIETRIO ENCASE FORENSIC;

www.guidancesoftware.com/encase-forensic.htm.

[3-03] NETWORK FORENSICS PACKAGES AND APPLIANCES;

http://www.forensicswiki.org/wiki/tools:network_forensics

[3-04] E-DETECTIVE;

http://www.edecision4u.com/; http://www.digi-forensics.com/home.html

[3-05] BURST;

http://www.burstmedia.com/release/advertisers/geo_faq.htm

[3-06] CHKROOTKIT;

http://www.chkrootkit.org

[3-07] CRYPTCAT;

http://farm9.org/cryptcat/

[3-08] ENTERASYS DRAGON;

http://www.enterasys.com/products/advanced-security-apps/index.aspx.

[3-09] IPFIX/NETFLOW V5/9;

http://www.mantaro.com/products/mnis/collector.htm

[3-10] MANTARO NETWORK INTELLIGENCE SOLUTIONS (MNIS);

http://www.mantaro.com/products/mnis/index.htm;
http://www.mantaro.com/products/mnis/network_intelligence_applications.htm#network_forensics

[3-11] MAXMIND;
http://www.maxmind.com

[3-12] NETCAT;
http://netcat.sourceforge.net/

[3-13] NETCNETFLOW / FLOWTOOLS_AT;
http://www.cisco.com/warp/public/732/tech/nmp/netflow/index.shtml;
http://www.splintered.net/sw/flow-tools/; http://silktools.sourceforge.net/;
http://www.vmware.com/vmtn/appliances/directory/293

[3-14] NETDETECTOR;
http://www.niksun.com/product.php?id=4

[3-15] NETINTERCEPT;
http://www.sandstorm.net/products/netintercept

[3-16] NETVCR;
http://www.niksun.com/product.php?id=3

[3-17] NIKSUN FULL FUNCTION APPLIANCE;
http://www.niksun.com/product.php?id=11

[3-18] NETOMNI;
http://www.niksun.com/product.php?id=1

[3-19] IPFIX/NETFLOW V5/9;
http://www.mantaro.com/products/mnis/collector.htm

[3-20] NETSLEUTH;
http://www.netgrab.co.uk/

[3-21] NETWORKMINER;

http://sourceforge.net/projects/networkminer/;

http://www.netresec.com/?page=networkminer

[3-22] PCAP2WAV;

http://pcap2wav.xplico.org/

[3-23] RKHUNTER;

http://rkhunter.sourceforge.net/

[3-24] NGREP;

http://ngrep.sourceforge.net/

[3-25] NSLOOKUP;

http://en.wikipedia.org/wiki/nslookup; http://en.wikipedia.org/wiki/nslookup

[3-26] SGUIL;

http://sguil.sourceforge.net/

[3-27] SNORT;

http://www.snort.org/

[3-28] SSLDUMP;

http://ssldump.sourceforge.net/

[3-29] TCPDUMP;

http://www.tcpdump.org

[3-30] TCPXTRACT;

http://tcpxtract.sourceforge.net/

[3-31] TCPFLOW;

http://www.circlemud.org/~jelson/software/tcpflow/

[3-32] TRUEWITNESS;

http://www.nature-soft.com/forensic.html

[3-33] OMNIPEEK;

http://www.wildpackets.com/solutions/network_forensics; www.wildpackets.com/products/network_analysis/omnipeek_network_analyzer/ forensics _search.

[3-34] WHOIS;

http://en.wikipedia.org/wiki/whois

[3-35] REGIONAL REGISTRIES;

http://www.arin.net/registration/agreements/bulkwhois.pdf; http://www.arin.net/community/rirs.html; http://www.arin.net/index.shtml american registry for internet numbers (arin); http://www.afrinic.net/ african network information center (afrinic; http://www.apnic.net/ Asia pacific network information centre (apnic); http://www.lacnic.net/en/ Latin American and Caribbean ip address regional registry; (lacnic); http://www.ripe.net/ ripe network coordination centre (ripe NCC)

[3-36] WIRESHARK / ETHEREAL;

http://www.wireshark.org/

[3-37] KISMET;

http://www.kismetwireless.net/

[3-38] XPLICO;

http://www.xplico.org/

[3-39] SPLITCAP;

http://splitcap.sourceforge.net/

[3-40] LFT;

http://pwhois.org/lft

[3-41] ETRACE;

http://www.bindshell.net/tools/etrace

[3-42] FIREWALK;

http://www.packetfactory.net;

http://www.forensicswiki.org/wiki/category:anti-forensics_tools

[3-43] DARIK'S BOOT AND NUKE;

http://www.forensicswiki.org/wiki/category:anti-forensics_tools

[3-44] ERASER;

http://www.forensicswiki.org/wiki/category:anti-forensics_tools

[3-45] EVIDENCE ELIMINATOR;

http://www.forensicswiki.org/wiki/category:anti-forensics_tools

[3-46] HASH (TOOL);

http://www.forensicswiki.org/wiki/category:anti-forensics_tools

[3-47] PARETOLOGIC PRIVACY CONTROLS;

http://www.forensicswiki.org/wiki/category:anti-forensics_tools

[3-48] SLACKER;

http://www.forensicswiki.org/wiki/category:anti-forensics_tools

[3-49] STEGANOS PRIVACY SUITE;

http://www.forensicswiki.org/wiki/category:anti-forensics_tools

[3-50] THE ONION ROUTER;

http://www.forensicswiki.org/wiki/category:anti-forensics_tools

[3-51] TIMESTOMP;

http://www.forensicswiki.org/wiki/category:anti-forensics_tools

[3-52] WINCLEAR;

http://www.forensicswiki.org/wiki/category:anti-forensics_tools

[3-53] WINDOW WASHER;

http://www.forensicswiki.org/wiki/

[3-54] CD/DVD INSPECTOR;

http://www.infinadyne.com/cddvd_inspector.html

[3-55] EMAIL DETECTIVE;

http://www.hotpepperinc.com/emd

[3-56] ENCASE;

http://www.guidancesoftware.com/

[3-57] FBI;

http://www.nuix.com

[3-58] FORENSIC TOOLKIT (FTK);

http://www.accessdata.com/product/ftk/

[3-59] HBGARY RESPONDER PROFESSIONAL;

http://www.hbgary.com

[3-60] ILOOK INVESTIGATOR;

http://www.ilook-forensics.org

[3-61] MERCURY INDEXER;

http://www.MicroForensics.com

[3-62] ONLINEDFS;

http://www.cyberstc.com

[3-63] OSFORENSICS;

http://www.osforensics.com

[3-64] P2 POWER PACK;

https://www.parabenforensics.com/catalog/product_info.php?cpath=25&products_id=187

[3-65] PRODISCOVER;

http://www.techpathways.com/ProDiscoverWindows.htm

[3-66] SAFEBACK;

http://www.forensics-intl.com/safeback.html

[3-67] X-WAYS FORENSICS;

http://www.x-ways.net/forensics/index-m.html

[3-68] DATEDECODER;

http://www.live-forensics.com/dl/DateDecoder.zip

[3-69] RECYCLEREADER;

http://www.live-forensics.com/dl/RecycleReader.zip

[3-70] DSTRINGS;

http://www.live-forensics.com/dl/Dstrings.zip

[3-70] UNIQUE;

http://www.live-forensics.com/dl/Unique.zip

[3-71] HASHUTIL;

http://www.live-forensics.com/dl/HashUtil.zip

[3-72] WINDOWSSCOPE PRO ULTIMATE LIVE;

http://www.live-forensics.com/dl/HashUtil.zip

[3-73] LINRES;

http://www.niiconsulting.com/innovation/linres.html

[3-74] SMART;

http://www.asrdata.com

[3-75] SECONDLOOK;

htp://secondlookforensics.com/

[3-76] TRUEWITNESS;

http://www.nature-soft.com/forensic.html

[3-84] BACKTRACK;

http://remote-Exploit.org/backtrack.html

[3-85] MATRIX;

http://www.matriux.com/

[3-86] CAINELive CD;

http://caine-live.net

[3-87] DEFT LINUX;

http://www.deftlinux.net

[3-89] FCCU GNU/LINUX BOOT CD;

http://www.lnx4n6.be

[3-90] GRML;

http://grml.org

[3-91] HELIX3 (HELIX3 PRO;

http://e-fense.com

[3-92] MACQUISITIONBOOT CD;

http://masterkeylinux.com

[3-93] SLACKWARE LIVE;

http://masterkeylinux.com

[3-94] PLAINSIGHT;

http://www.plainsight.info

[3-95] RECOVERY IS POSSIBLE;

http://www.tux.org/pub/people/kent-robotti/looplinux/rip/

[3-96] SAFE BOOT DISK;

http://www.forensicsoft.com/catalog/product.php

[3-97] SMART LINUX;

http://asrdata2.com

[3-98] SPADA;

http://spada-cd.info

[3-99] WINFE;

http://winfe.wordpress.com

[3-100] LIBERTADES DEL SOFTWARE OPEN SOURCE;

http://www.fsf.com/

CAPÍTULO IV: GUÍA RÁPIDA PARA FORENSIA EN REDES USANDO SOFTWARE LIBRE

[4-01] USUARIOS Y CONTRASEÑAS DE FÁBRICA;

http://default-password.info
http://www.unknownpassword.com
http://www.defaultpassword.us
http://defaultpasswords.in
http://www.phenoelit-us.org/dpl/dpl.html
http://www.corrupteddatarecovery.com/pages/Default-Passwords-Data-Recovery.asp
http://www.defaultpassword.com

[4-02] OBTENER USUARIOS Y CONTRASEÑAS DÉBILES

Ophcrack: *www.ophcrack.org,*
http://www.youtube.com/watch?v=uxwM-cIqiB8
OWL (OpenWall): *http://www.openwall.com/Owl*
Cain & Abel: *http://www.oxid.it/cain.html*
Kon Boot: *http://www.piotrbania.com/all/kon-boot*

[4-03] ELIMINAR CLAVES DE ADMINISTRADOR

PARA WINDOWS:

http://pogostick.net/~pnh/ntpasswd/bootdisk.html

http://www.piotrbania.com/all/kon-boot

PARA IPHONE:

http://www.superunlockiphone.com

PARA MAC:

http://osxdaily.com/2010/08/10/forgot-mac-password-how-to-reset-mac-password

PARA LINUX:

http://diariolinux.com/2008/01/15/resetear-password-de-root

http://www.muylinux.com/2009/07/28/como-recuperar-la-contrasena-de-root/

ANEXO

"Existen cinco clases de espías": el espía nativo, el espía interno, el doble agente, el espía liquidable y el espía flotante. Cuando están activos todos ellos, nadie conoce sus rutas: a esto se le llama genio organizativo, y se aplica al gobernante. Los espías nativos se contratan entre los habitantes de una localidad. Los espías internos se contratan entre los funcionarios enemigos. Los agentes dobles se contratan entre los espías enemigos. Los espías liquidables transmiten falsos datos a los espías enemigos. Los espías flotantes vuelven para traer sus informes".

-Sun Tzu El Arte de la Guerra.

ANEXO 1

ENCUESTA REALIZADA A TÉCNICOS Y OFICIALES DE SEGURIDAD

Aplicable a Oficiales de seguridad, responsables de tecnología, técnicos informáticos, técnicos de soporte, webmasters, personal técnico de sistemas y/o tecnología.

Esta es una encuesta de investigación estrictamente académica. La información recopilada es totalmente anónima y no compromete ni al encuestado ni a su entidad.

PERFIL DE LA PERSONA ENCUESTADA		
1	Género	☐ Femenino ☐Masculino
2	Tipo de organización	☐ Pública ☐ Privada ☐ Mixta
3	Tamaño de la organización	☐ Grande ☐ Mediana ☐ Pequeña
4	Organización dedicada a la seguridad ciudadana	☐ Si ☐ Parcialmente ☐ No
5	Nivel de autoridad de la persona encuestada	☐ Ejecutivo ☐ Directivo ☐ Apoyo ☐ Técnico

ACERCA DE LA INFORMÁTICA FORENSE		
6	La informática forense es lo mismo que el hacking ético	☐ Si ☐ No ☐ Se parecen en algo
7	En su organización conoce Ud. o alguien los principios de la informática forense	☐ Nada ☐ Poco ☐ Lo necesario ☐ Mucho
8	Cuándo aplicaría su organización el análisis forense	☐ Solo en delitos ☐ Posibles delitos ☐ Muertes
9	Medidas que su organización tomaría en una escena de un incidente o delito informático	☐ Ninguna ☐ Impedir el acceso ☐ Tomar fotos y videos ☐ Tomar evidencias ☐ Llamar a especialistas ☐ Llamar a la PJ
10	El principio de transferencia de Locard es	☐ Una forma de sacar copias digitales ☐ Un estándar mundial ☐ Una relación entre la escena, la víctima y el autor del delito
11	En nuestra organización sabemos qué es y cómo mantener una cadena de custodia	☐ Nada ☐ Poco ☐ Lo necesario ☐ Mucho

ACERCA DE LA INFORMÁTICA FORENSE		
12	En nuestra organización sabemos cómo manejar y almacenar evidencias digitales	☐ Nada ☐ Poco ☐ Lo necesario ☐ Mucho
13	En nuestra organización sabemos lo que es el debido proceso	☐ Nada ☐ Poco ☐ Lo necesario ☐ Mucho
14	Por favor incluir nombres de organizaciones que realizan informática forense	
15	Por favor incluir nombres de certificaciones regionales o mundiales para informática forense	
16	Cuántos incidentes de seguridad o delitos conoce de primera mano que se resolvieron con análisis forense	

ACERCA DE LA INFORMÁTICA FORENSE		
17	Cuántos incidentes de seguridad o delitos conoce de primera mano, que pudieron o pueden solucionarse con análisis forense	
18	Mencione algunos programas propietarios para análisis forense	
19	Mencione algunos programas software libre para análisis forense	
20	¿Le parece confiable la calidad del software libre para trabajos de informática forense?	

Sus comentarios finales:

_____

_____

Margoth Proaño Freire agradece sus respuestas a la presente encuesta