Proceso Unificado de Recuperación de Información (PURI) en Redes Informáticas

Ana Haydée Di Iorio[1], Hugo Curti2, Fernando Greco3, Juan Ignacio Iturriaga4, Gonzalo Ruiz De Angeli5, Ariel Podestá6, Martín Castellote7, Bruno Constanzo8
1 Ingeniera en Informática, Docente e Investigadora en Universidad FASTA, diana@ufasta.edu.ar
2 Ingeniero en Informática, Docente e Investigador en Universidad FASTA y Universidad Nacional del Centro, hcurti@gmail.com
3 Ingeniero en Informática, Docente e Investigador en Universidad FASTA, fmartingreco@gmail.com
4 Ingeniero en Informática, Docente e Investigador en Universidad FASTA, Juan@ufasta.edu.ar
5 Estudiante en Ingeniería Informática, Investigador en Universidad FASTA, gonzalo.ruizdeangeli@gmail.com
6 Ingeniero en Informática, Docente e Investigador en Universidad FASTA, arielpodesta@gmail.com
7 Ingeniero en Informática, Docente e Investigador en Universidad FASTA, castellotemartin@yahoo.com.ar
8 Ingeniero en Informática, Investigador en Universidad FASTA, bconstanzo@ufasta.edu.ar

Resumen: Este trabajo presenta el estudio de la práctica de la informática forense en el ámbito de las redes de computadoras y otros dispositivos. El contexto es significativamente complejo, por lo que idealmente debería seguir un procedimiento ordenado y preciso que garantice el éxito de la labor del investigador. Aquí se introduce una metodología en desarrollo que viene a cubrir esta necesidad.

1. Introducción

La Informática Forense es la rama de la Forensia que trabaja con datos procesados y guardados electrónicamente en un medio computacional, enfocada en la obtención de evidencia digital que ayude a esclarecer diversos sucesos como ser delitos informáticos. Esta evidencia es concebida como aquella que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.

En el ámbito de la informática existen dos contextos temporales claramente visibles para el proceso de obtención de evidencia. Uno de ellos se ubica en el momento en el que el dispositivo se encuentra en funcionamiento y el otro en el que se encuentra apagado. Ambas situaciones presentan diferentes oportunidades de extracción de in-

formación significativa. Por consiguiente, la operación de extracción debe contemplar ambas etapas aunando sus resultados que naturalmente se complementan.

El motivo de esta distinción surge a partir del concepto de datos volátiles y datos persistentes.

Datos volátiles son todos aquellos cuya permanencia máxima en el sistema se limita al tiempo en el que el dispositivo se encuentra encendido. Ejemplos de este tipo de datos pueden ser el contenido de la memoria RAM de una PC, el tráfico de red circulando entre routers, las tablas CAM ("Content Addressable Memory" o "Memoria de Contenido Direccionable") de un switch, etc. Por el contrario, el concepto de datos persistentes aplica a todo aquella información almacenada en un dispositivo que por la naturaleza de su tecnología no requiere el suministro permanente de energía para conservar sus datos.

Desde un punto de vista simplificado podría considerarse que los datos volátiles corresponden a las acciones en curso y los persistentes al histórico de las mismas. De esta manera es clara la necesidad de complementar ambos resultados.

Según el ámbito en el cual se desarrolle la actividad será la factibilidad de hallar datos volátiles o persistentes. Por ejemplo, cuando el universo de estudio se reduce a un equipo de PC, datos persistentes existen en abundancia, y volátiles son extraíbles operando antes del apagado del equipo. Pero en cambio cuando el ambiente de estudio se ubica sobre una red informática, la riqueza de los datos volátiles es significativamente alta e inversamente proporcional a la oportunidad de recuperarlos.

En un análisis informático forense sobre una red, el valor más elevado lo tiene el tráfico en curso que es altamente volátil debido a la naturaleza de los dispositivos que se ocupan de transmitirlo. Estos dispositivos (por ejemplo: routers y switches) normalmente operan con buffers de memoria relativamente pequeños cuya finalidad es simplemente la de encolar los paquetes que se envían y reciben. Así la información permanecerá en el dispositivo hasta que finalmente los paquetes puedan retransmitirse. Siendo que habitualmente estas operaciones toman fracciones de segundo, la oportunidad de recuperar el tráfico de red es considerablemente pequeña si no se previó la necesidad de hacerlo.

En este trabajo se aborda la informática forense haciendo foco en este último escenario.

2. Seguridad Informática y Forensia en Redes

La aplicación de la Seguridad Informática podría concebirse como "Incident Response" (Respuesta ante Incidente).

Un Incident Response comprende las siguientes etapas:

- **a)** Preparación
- **b)** Detección y análisis
- **c)** Contención, erradicación y recuperación

d) Actividades post incidente (preparar infraestructura para que no vuelva a pasar)

Relación/complementación entre ambas:

a) Preparación: condicionar infraestructura para la detección de incidentes (ejemplo: sniffers, mecanismos de log)

b) Actividades post incidente: investigación sobre la información recolectada.

Por qué es necesaria la Informática Forense en redes:

a) Cuando el rastro de la evidencia termina en una IP y esa dirección corresponde a una empresa con una estructura de red montada se requiere un análisis de red puertas adentro que nos permita completar la ruta de la comunicación.

b) La tendencia de los dispositivos modernos es brindar la mayor conectividad posible, lo que hace que mucha información quede almacenada en los nodos de la red.

c) Permite detectar el nodo en el que un dato fue alterado.

3. Proyecto PURI en Redes Informáticas

El Proyecto PURI, llevado a cabo por el "Grupo de Investigación en Sistemas Operativos e Informática Forense" de la Facultad de Ingeniería de la Universidad FASTA, trabaja en la generación y formalización de un proceso único de recuperación de información digital que sirva como guía y forma de validar la labor del informático forense. Durante la evolución de este proyecto se identificaron las siguientes sub-ramas de esta ciencia:

- Forensia en Equipos (Computer Forensics)
- Forensia en Dispositivos Móviles (Mobile Devices Forensics)
- Forensia en Redes (Networking Forensics)
- Forensia en Análisis de Datos (Forensic Data Analysis)
- Forensia en Bases de Datos (Database Forensics)

Al momento de la publicación de este paper, el proyecto se halla abordando la investigación sobre la sub-rama "Forensia en Redes (Network Forensics)".

La forensia en redes, es un campo de la informática forense cuyo objeto es capturar, registrar, almacenar y analizar los eventos de la red, con el fin de determinar la fuente de uno o varios ataques a la red. O las posibles vulnerabilidades existentes en ella.

Los propósitos principales de la Forensia en Redes son la investigación de una actividad delictiva y la extracción de evidencia a partir de la reconstrucción de una sesión de datos, de los eventos pasados de redes y el análisis tráfico cifrado u oculto.

3.1. Actividades de la Forensia en Redes

De acuerdo a Simon Garfinkel, se cuenta con dos tipos de análisis forense de red: "Catch-it-as-you-can System" y "Stop, look and listen".

En el análisis forense de red del tipo **Catch-it-as-you-can System:** Todos los paquetes que pasan a través de un punto de tráfico son capturados y escritos en un medio de almacenamiento. El análisis se lleva a cabo posteriormente por lotes. Este tipo de enfoque requiere de grandes cantidades de espacio de almacenamiento, usualmente involucra un sistema RAID.

En el análisis forense de red del tipo **Stop, look and listen:** Cada paquete es analizado de forma rudimentaria en memoria y solo cierta información se almacena para un análisis futuro. Este enfoque requiere menos capacidad de almacenamiento pero puede requerir un procesador más rápido para no perder paquetes y la escucha permanente lo que ocurre en la red.

Si bien un ataque a una red involucra una complejidad adicional comparado a un ataque a un único dispositivo, en términos de cantidad de información que puede recolectar y equipos que puede vulnerar, un atacante preferiría siempre la primera opción. Esto no solo se basa en la cantidad de computadoras que pueden ser objetivo del ataque sino también en los nodos intermedios que conforman la red.

Una estrategia común para un ataque es intentar esconder toda evidencia de la presencia de un determinado malware. Una desventaja en un entorno de red para el atacante y una oportunidad para el encargado del análisis forense es justamente la cantidad de dispositivos involucrados.

De todas formas, la posible falta de capacidad de almacenamiento de algunos nodos de la red le da un carácter volátil a los datos haciendo que no sea siempre una ventaja la presencia de una mayor cantidad de equipos conectados. Un ejemplo de este caso son algunos routers domiciliarios (SOHO) en los cuales, si la adquisición no se lleva a cabo en un corto tiempo se corre el riesgo de pérdida de información valiosa.

3.2. Esquema propuesto

La extracción de evidencias en esta rama podría diagramarse como una composición de etapas, no necesariamente todas imprescindibles, representado por el siguiente esquema:

Tareas de la Fase de Adquisición

I. Obtención de la información en crudo

a. Sniffing (escucha) de tráfico de red
- En medios guiados (ejemplo: 802.3 (cable UTP para Ethernet))
- En medios no guiados (ejemplo: 802.11 (WiFi), 802.16 (WiMax))

b. Obtención de datos en caliente en nodos de red (routers, switches, access-points, etc).
- Envíos y recepciones en curso
- Logs volátiles
- Caches
- Tablas de configuración temporal. (Por ejemplo la tabla "Content addressable memory", en el caso de un switch).
- Cualquier otra información volátil (por ejemplo estadísticas de cantidad de tráfico)

c. Obtención de datos en caliente de equipos origen/destino (ejemplo PC, tablet, celular)
- Envíos y recepciones en curso
- Logs volátiles
- Caches (ejemplo cache DNS)
- Configuraciones temporales (ejemplo IP actual)
- Otra información volátil (cualquier otro dato de red que el dispositivo brinde)

d. Obtención de datos en persistentes de nodos de red
- Firmware
- Configuraciones establecidas
- Logs almacenados (tanto de tráfico de red como de utilización del dispositivo)
- Estadísticas de tráfico de red

e. Obtención de datos persistentes de equipos origen/destino
- Configuraciones utilizadas
- Logs de red
- Archivos vinculados al tráfico de red
- Caches persistentes
- Configuraciones y datos registrados por aplicaciones de red de alto nivel (ejemplo Voip)

Tarea de la Fase de Análisis – Etapa Extracción Lógica

II. Filtrado

Aplicación de filtros y separadores según diversos criterios (por ejemplo según protocolo) sobre todo el volumen de información recuperada. Esta etapa aplica principalmente al lote de captura de paquetes de red debido a su inherente tamaño.

Tarea de la Fase de Análisis – Etapa Análisis de Relaciones

III. Análisis Semántico de los paquetes almacenados

Consiste en el análisis específico de la actividad del usuario. El objetivo es determinar exactamente cuáles fueron sus acciones y en orden fueron efectuadas.

IV. Análisis en servicios sobre infraestructura de red
Análisis sobre aplicaciones y servicios montados sobre la infraestructura de red (ejemplo Voip)

A continuación se presenta el desarrollo de estos puntos contenidos en el esquema previo:

I. Obtención de la información en crudo

La obtención de la información en crudo comprende la captura de todo dato vinculado al tráfico de red que tuvo lugar en el entorno de los dispositivos asociados al caso en cuestión. Este tráfico, no necesariamente debe limitarse estrictamente a aquellos envíos cuyo origen o destino sea uno de los dispositivos directamente relacionados al incidente, sino que también es de importancia para el estudio, el que ha tenido lugar entre nodos intermediarios en las comunicaciones.

De todas maneras, esta obtención no se limita solamente a los paquetes de red sino que contempla también toda configuración e información que hayan utilizado los dispositivos para llevar a cabo las transmisiones efectuadas.

a. Sniffing (escucha) de tráfico de red

La escucha del tráfico de red consiste en la captura directa del mismo a través de herramientas de software y/o dispositivos informáticos. Se realiza la lectura de todos los paquetes que circulan en el ámbito de red dado, almacenándose completamente para su posterior análisis.

Respecto del formato de almacenamiento del tráfico de red, se recomienda utilizar Pcap.

Pcap es un formato de registro de tráfico de red pero también es el nombre de una interfaz de aplicación implementada a través de una librería que brinda funcionalidades de captura de paquetes de red a las aplicaciones que la utilicen. Pcap fue inicialmente creada para ejecutarse en linux pero existe su paralela para hacerlo en Windows (WinPcap).

Esta librería genera volcados de captura tráfico de red en un formato (Pcap al igual que la misma librería) considerablemente difundido, aceptado y compatible con las herramientas de sniffing más conocidas a nivel global que se encuentran en permanente desarrollo.

- **En medios guiados**

El sniffing (escucha) en medios guiados consiste en la captura de todo el tráfico de red que circula por medios de transmisión de este tipo (por ejemplo cables UTP). Para llevar a cabo esta actividad es necesario contar o bien con una derivación física hacia el dispositivo que se encuentre capturando el tráfico, o bien con uno que ya se halle funcionando de intermediario de las comunicaciones a capturar.

La derivación física mencionada puede materializarse de tres maneras diferentes.

- A través de un Hub (repetidor) que por su naturaleza expone todo el tráfico que lo circula hacia todas sus bocas de salida permitiendo conectar a una de ellas el "sniffer" (o dispositivo de escucha).
- A través de un Switch (conmutador) configurable que permita replicar todo el tráfico hacia una de sus bocas donde se ubicaría el "sniffer".
- A través de un empalme físico que interconecte las vías de tránsito de la red a las de escucha del dispositivo en escucha.

En el caso en que se cuenta previamente con un dispositivo que ya actúa como intermediario de transmisión (por ejemplo un equipo servidor funcionando como proxy o un router), lo que se requiere es simplemente agregarle la capacidad de poder almacenar el tráfico que lo transita en un dispositivo de almacenamiento masivo (por ejemplo un disco rígido).

Cuando el dispositivo de escucha (sniffer) se encuentra conformado como un equipo del tipo PC, existe numeroso software disponible para llevar a cabo esta tarea. Una opción recomendada es "Wireshark". Esta herramienta es de código abierto, de interfaz gráfica de usuario y compatible con Windows y Linux.

- **En medios no guiados**

El sniffing en medios no guiados es esencialmente diferente del llevado a cabo en medios guiados, debido a la naturaleza de los mismos. Las transmisiones en estos últimos se realizan en forma inalámbrica. De esta manera los componentes físicos a utilizar para implementar un mecanismo de sniffing serán significativamente distintos.

A gran escala, las formas de implementar la infraestructura necesaria para llevar a cabo el sniffing sobre medios no guiados pueden ser básicamente las siguientes:

- Contar con un “Access Point” (punto de acceso) al cual los dispositivos a escuchar deban conectarse a fin de integrar la red. Dicho punto de acceso, debería o bien tener la capacidad de registrar todo el tráfico que manipula o bien poder ser configurado para dirigir el tráfico a un dispositivo dedicado a efectuar el sniffing.
- Configurar un dispositivo de transmisión inalámbrica para realizar efectivamente el sniffing de los dispositivos a su alcance. Típicamente esto puede llevarse a cabo disponiendo de un teléfono móvil o un notebook que utilizando un software especializado para tal fin cumpla esta función.

Al igual que en el caso de medios guiados, existen numerosos productos de softwares que proveen funcionalidades útiles para efectuar sniffing sobre medios no guiados. Por ejemplo kismet o airodump.

b. Obtención de datos en caliente en nodos de red (routers, switches, access-points, etc).

El método más directo de obtener este tipo de datos es a través de la configuración provista por el mismo dispositivo. De acuerdo a la complejidad y capacidad del dispositivo en cuestión será la funcionalidad disponible. Por ejemplo, la información en caliente extraíble de un router hogareño suele comprender estadísticas de cantidad de tráfico enviado y recibido, tablas de asignación DHCP, registros de acceso al mismo, IP pública de conexión a Internet, entre otros datos.

c. Obtención de datos en caliente de equipos origen/destino (ejemplo PC, tablet, celular)

El objetivo de esta etapa es extraer toda la información administrativa, de configuración y de registro de sucesos contenida en los equipos origen y destino del incidente (ejemplo computadoras personales). Cabe destacar que este tipo de operación puede no limitarse estrictamente a dispositivos que conformen únicamente el destino u origen. Otros vinculados indirectamente (por ejemplo, equipos en la misma red local) podrían brindar información de utilidad para el caso.

- **Envíos y recepciones en curso**

  Los envíos y recepciones en curso pueden capturarse a través de los mecanismos de sniffing previamente mencionados.

- **Logs, caches y configuraciones de red volátiles**

Durante el funcionamiento de un equipo (ejemplo: computadora personal), un volumen considerable de este tipo de información es mantenido en memoria para dar soporte a la conectividad al mismo con el entorno.

Estos datos pueden ser de diversas índoles. Desde los que determinan el enrutamiento de los paquetes (por ejemplo la información entregada por el comando "netstat -r" en ambiente Linux) hasta aquellos propios específicamente de un software en particular como puede ser una URL establecida para un cliente de escritorio remoto (ejemplo Remmina).

Este proceso entonces consiste en recorrer el sistema operativo y las aplicaciones que utilicen servicios de red en busca de valores de configuración establecidos.

- **Otra información volátil (cualquier otro dato de red que el dispositivo brinde)**

Un ejemplo de otra información volátil potencialmente útil es la lista de puertos en escucha. Esta lista puede accederse a través del comando "netstat -l" en un ambiente de Windows.

d. Obtención de datos en persistentes de nodos de red

La información persistente de los nodos de red es extraíble en principio desde el mismo software provisto por cada dispositivo.

A nivel general la información obtenible de la mayoría de los nodos de red hogareños, como podría ser un router, comprende el firmware del dispositivo, configuraciones establecidas, logs almacenados (tanto de tráfico de red como de utilización del dispositivo) y estadísticas de tráfico de red.

Uno de los ataques conocidos es la alteración del firmware del dispositivo. Para corroborar si un ataque de este estilo ha ocurrido puede obtenerse el firmware actual del mismo y constatarlo con el brindado por el fabricante.

e. Obtención de datos persistentes de equipos origen/destino

Los datos de red persistentes extraíbles de un dispositivo de usuario (ejemplo tablet o computadora personal) son conformados en gran medida por el histórico de actividad en la red llevada a cabo por el usuario del equipo.

Ejemplos:

- Archivo "C:\WINDOWS\system32\drivers\etc\hosts". Archivo de enrutamiento estático para destinos específicos.

- Directorio "C:\Users\username\AppData\Local\Microsoft\Windows\Temporary Internet Files". Directorio de almacenamiento de archivos temporales de navegación.

II. Filtrado

El resultado de la captura del tráfico de red, realizada en los pasos anteriores, suele ser significativamente voluminoso. Esto sumado a que no se encuentra naturalmente ordenado por ningún criterio más que el orden secuencial en el cual los paquetes fueron transitando por la red, lleva a la ineludible necesidad de contar con un mecanismo de filtrado de este tráfico.

En este paso no solamente tiene lugar el descarte de aquella información irrelevante del tráfico capturado sino también el ordenamiento y la clasificación del mismo según el criterio que se requiera. Por ejemplo, si lo que investiga es estrictamente vinculado a la navegación web entonces deberá filtrarse el tráfico y extraerse únicamente aquellas comunicaciones llevadas a cabo a través del protocolo HTTP.

La librería "Pcap", previamente mencionada, provee mecanismos para llevar a cabo estas operaciones. Dispone de una sintaxis similar a la de ciertos lenguajes de programación contemporáneos, permitiendo operar en profundidad con todo el tráfico de red capturado. El uso concreto de estas librerías es posible a través de diversas aplicaciones de software que exponen su funcionalidad. Wireshark y Tcpdump son ejemplos de este tipo de software.

A continuación se presentan algunos filtros implementados bajo la sintaxis de Pcap:

Sintaxis	Filtro
ftp	Solo tráfico vía FTP.
ip.addr == 192.168.1.126	Solo paquetes cuya IP destino u origen sea 192.168.1.126.
tcp.port == 80	Navegación convencional por web browser.
!arp	Todo el tráfico excluyendo aquellos paquetes sobre el protocolo ARP.

III. Análisis Semántico de los paquetes almacenados

Para tener una comprensión de alto nivel respecto a la actividad de un usuario en una red se precisa conocer cuáles fueron las aplicaciones o protocolos que utilizó, obtener el tráfico generado y ordenar la información para reconstruir su trazabilidad.

Un primer paso para detectar aplicaciones en los paquetes capturados, es a través del puerto contenido en sus encabezados. Internet Assigned Numbers Authority (IANA) define una convención entre cliente y servidor que designa determinados puertos conocidos o "well known ports" a cada protocolo. No obstante, no existen mecanismos que aseguren que el tráfico se intercambia respetando esta convención y, en caso que sea respetado, en varios escenarios esto nos daría una idea del protocolo pero no de la aplicación que lo utiliza. Una ventaja es que algunas aplicaciones tienen puertos fijos asignados para sus comunicaciones aunque no en todos los casos éstos son oficializados.

Para aquellas situaciones en las que la detección de aplicaciones por puertos conocidos no es adecuada o cuando la aplicación en cuestión utiliza puertos no oficiales, el análisis semántico de la carga de los paquetes nos brinda un importante suplemento de información. Esto implica un profundo conocimiento tanto de los protocolos de red como los de las aplicaciones.

Actualmente no hay herramientas que den una solución integral a esta problemática. Sin embargo existen frameworks para análisis de tráfico de redes. Bro es un ejemplo con más de 15 años de investigación que, entre otras capacidades, cuenta con un generador de parsers para protocolos de red llamado BinPAC, que permite definir protocolos con un lenguaje semántico de alto nivel. Varias implementaciones basadas en Bro realizan un análisis de los paquetes capturados en distintas capas de red con el fin de clasificar el flujo. A través del análisis exhaustivo de la carga útil de los paquetes estas implementaciones apuntan a descubrir cúal es el protocolo de capa de aplicación que origina cada flujo.

Estas soluciones, sin embargo, se vuelven inefectivas en determinadas circunstancias, por ejemplo bajo altas tasas de tráfico que requieren un alto poder computacional o cuando se utilizan mecanismos de cifrado de extremo a extremo. Crotti et.al presentan una alternativa basada en el análisis estadístico del tráfico de red de nivel de capa de aplicación, enfocándose en valores como el tamaño de los paquetes IP, su tiempo de inter-arribo y su cardinalidad en el flujo.

Las principales ventajas de esta aproximación son el bajo requerimiento de recursos computacionales en comparación a las técnicas anteriores y su compor-

tamiento robusto en frente a la presencia de tráfico generado por nuevos protocolos de capa de aplicación.

IV. Análisis en servicios sobre infraestructura de red

Los servicios sobre infraestructura de red son normalmente soluciones comerciales que se montan sobre una red existente. Los ejemplos más comunes se relacionan con el intercambio de información y contenidos multimediales por red. Dentro del ámbito de las comunicaciones podemos encontrar ejemplos de voz (VOiP), video (videoconferencia) y datos (transferencia y compartición de recursos) aunque también los ejemplos abarcan otros ámbitos como seguridad (vigilancia remota), entretenimiento (streaming en vivo o bajo demanda) o educación y capacitación (plataformas de e-learning) entre otros.

Un punto positivo es que en algunos casos estos servicios proveen logs o sistemas de monitoreo bastante completos que pueden contener la información que se requiere. Ofreciendo la posibilidad de acceder rápidamente al conjunto de registros necesarios muy fácilmente organizables cronológicamente. Sin embargo, en las situaciones en las que no se cuenta con logs, los mismos no contienen la información buscada o simplemente no se los considera posible evidencia digital, debemos recurrir al análisis del resto de los hosts de la red y del tráfico que fluye en la misma. Bajo este escenario podemos encontrarnos con situaciones que agregan complejidad:

Soluciones cerradas: es el caso en el que el servicio es solicitado a una empresa con una solución que va desde el hardware hasta el software y la documentación relativa a la implementación del servicio a bajo nivel no se encuentra disponible. Dentro de este punto, un servicio puede incluir dispositivos no genéricos diseñados para una solución comercial como pueden ser los teléfonos SIP basados en hardware. El inconveniente que conlleva es que las herramientas forenses orientadas al ámbito en cuestión (medios de comunicación para este ejemplo) puedan no brindar soporte y se tenga que buscar alternativas puntuales para llevar a cabo la adquisición y/o análisis.

Protocolos de red propios: Este punto es transversal al resto ya que en cualquiera de las situaciones puede darse que adicionalmente a la complicación puntual surja la situación en que el servicio opere bajo un protocolo propio. Este escenario no solo impacta en el análisis de los paquetes sino también en la detección y filtrado de los mismos. El primer paso es basarse en la documentación del servicio, en caso de estar disponible, o en un análisis del comportamiento del mismo en la red en caso contrario, para establecer los filtros pertinentes. Desde aquí comienza la tarea de reconstruir la comunicación deseada que, si no se cuenta con un software específico, deriva en un trabajo inevitablemente manual.

Complejización de la topología: Un servicio puede estar montado sobre una red propia con servidores dedicados o pueden existir el caso en que se comparta al-

guno de los dos elementos mencionados anteriormente con la red de base. Esto puede llevar a que el tráfico capturado desde un punto determinado de la red no contenga los paquetes inherentes al servicio de interés. Es por esto que un análisis adicional de la topología de red es necesario antes de comenzar la captura. Esta situación únicamente se aplica cuando la captura de tráfico en nodos intermedios de la red puede ser fuente de información valiosa. Por ejemplo, cuando el el tráfico de datos no se encuentra cifrado.

Tráfico cifrado: un método de protección ante técnicas de sniffing es el cifrado de la información. Si bien es un aspecto positivo desde el punto de vista de la protección de la información del usuario, esto genera una complicación adicional al momento de llevar a cabo un proceso forense. Bajo esta dificultad una solución planteada es trabajar sobre la memoria RAM de los dispositivos cliente. Esto requiere un conocimiento específico de los dispositivos involucrados tanto para la adquisición de datos como para el análisis sobre los mismos. Matthew Simon y Jill Slay (2006) en su publicación "Voice over IP: Forensic Computing Implications" hacen referencia a esta complicación adicional de trabajar con tráfico cifrado enfocándose en un servicio de VOiP. Plantean la solución de trabajar sobre la memoria RAM del dispositivo que aloja al teléfono SIP basado en software. En su review de 2012, Slay et.al confirman que la estrategia es eficiente para confirmar la existencia de una comunicación e incluso recuperar parte de los paquetes correspondientes utilizando un dump de memoria posterior a la finalización de la comunicación.

4. Conclusiones y Trabajo a Futuro

El análisis informático forense orientado al ámbito de redes es significativamente más complejo y desafiante que aquel limitado a dispositivos puntuales como ser una PC de escritorio.

La mayor riqueza de la información extraíble de un ambiente de red reside en los datos volátiles.

Es fundamental prever con anticipación la necesidad de la realización de un análisis informático forense sobre un ambiente de red, a fin de garantizar el éxito del mismo.

La rapidez con la que se actúe en este tipo de contextos será directamente proporcional a la probabilidad de éxito te que tenga el investigador.

En estos casos el estudio excede los límites de los dispositivos origen/destino del incidente ya que su comunicación se produce sobre una infraestructura distinta.

El Grupo de Investigación está en proceso de incorporación de estas actividades de Forensia en Redes, a las Fases y Etapas definidas en PURI ©, a fin de completarlo y extenderlo desde el entorno de computadora personal a dispositivos móviles y a Redes.

Referencias

1. https://www.wireshark.org/
2. http://www.tcpdump.org/pcap.htm
3. Comunicaciones y Redes de Computadoras - 6ta Edición - William Stallings
4. http://www.internetassignednumbersauthority.org/
5. https://www.bro.org/index.html
6. Simon M, Slay J. Voice over IP: forensic computing implications. 4th Australian digital forensics conference; Diciembre 2006.
7. Jill Slay, Matthew Simon, David Irwin: Voice Over IP And Forensics: A Review of Recent Australian Work. 1st International Conference on Digital Forensics and Investigation (ICDFI); Septiembre 2012.
8. Manuel Crotti, Francesco Gringoli, Paolo Pelosato, Luca Salgarelli: A statistical approach to IP-level classification of network traffic. DOI: 10.1109/ICC.2006.254723 Conference: Communications, 2006. ICC '06. IEEE International Conference on, Volume: 1