Importance of the Forensia in Networks for the Collection of Digital Evidence

Tiffany Viviana Estupiñán Londoño, Est. Ingeniería de Sistemas[1], Karen Tatiana Mora Merchán, Est. Ingeniería de Sistemas[2], y Claudia Patricia Santiago Cely, Msc. Gestión de Información,[1]
[1]Escuela Colombiana de Ingeniería Julio Garavito, Colombia, tiffany.estupinan@mail.escuelaing.edu.co, claudia.santiago@escuelaing.edu.co,
[2]Escuela Colombiana de Ingeniería Julio Garavito, Colombia, karen.mora@mail.escuelaing.edu.co

Abstract -- Network Forensics is a sub-branch of digital forensics responsible for the collection of data that passes through the network, through techniques that perform IP tracking, network monitoring technique, packet capture and compilation of documents. All these techniques are carried out with different programs, for this article MyLanViewer and WireShark are used because they provide tools for network monitoring, packet capture, IP tracking, IP recognition and are free, throughout the article will be deepened in the architecture of the network, the typologies and topologies that exist according to the needs of the network.

Keywords – forensic network, protocols, digital evidence.

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2019.1.1.479
ISBN: 978-0-9993443-6-1 ISSN: 2414-6390

Importancia de la Forensia en Redes para la Recopilación de Evidencia Digital

Tiffany Viviana Estupiñán Londoño, Est. Ingeniería de Sistemas[1], Karen Tatiana Mora Merchán, Est. Ingeniería de Sistemas[2], y Claudia Patricia Santiago Cely, Msc. Gestión de Información,[1]
[1]Escuela Colombiana de Ingeniería Julio Garavito, *Colombia*, tiffany.estupinan@mail.escuelaing.edu.co, claudia.santiago@escuelaing.edu.co, [2]Escuela Colombiana de Ingeniería Julio Garavito, *Colombia*, karen.mora@mail.escuelaing.edu.co

***Abstract*– Network Forensics is a sub-branch of digital forensics responsible for the collection of data that passes through the network, through techniques that perform IP tracking, network monitoring technique, packet capture and compilation of documents. All these techniques are carried out with different programs, for this article MyLanViewer and WireShark are used because they provide tools for network monitoring, packet capture, IP tracking, IP recognition and are free, throughout the article will be deepened in the architecture of the network, the typologies and topologies that exist according to the needs of the network.**

***Keywords*-- forensic network, protocols, digital evidence.**

***Resumen*– Red forense es una subrama de forense digital responsable de la recopilación de datos que pasa a través de la red, a través de técnicas que realizan el seguimiento de IP, la técnica de monitoreo de red, la captura de paquetes y la recopilación de documentos. Todas estas técnicas se llevan a cabo con diferentes programas, para este artículo se utilizó MyLanViewer y WireShark porque proporcionan herramientas para realizar monitoreo de red, captura de paquetes, seguimiento de IP, reconocimiento de IP y son gratuitos, a lo largo del artículo se profundizará en la arquitectura de la red, las tipologías y topologías que existen según las necesidades de la red.**

***Palabras clave*-- red forense, protocolos, evidencia digital.**

I. Introducción

En la actualidad los datos son la posesión más importante en la industria lo cual generó un aumento a la irrupción de datos de terceros para acceder a la información ya sea para manipularla o adquirirla, a raíz de eso se creó la informática forense que según el FBI la informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en algún medio computacional, [1] cuya función principal es la aplicación de herramientas que permiten adquirir, validar y analizar los datos para una posterior presentación de los mismos.

La informática forense tiene como función principal recolectar evidencia suficiente para ser utilizada en un proceso y servir de argumento en contra de los criminales y conocer el verdadero causante del incidente, todo mediante el uso de técnicas y herramientas para identificar, recuperar reconstruir y analizar la información recolectada durante toda la investigación.

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2019.1.1.479
ISBN: 978-0-9993443-6-1 ISSN: 2414-6390

Algunos de los escenarios en donde se aplica la informática forense son en el ámbito criminal es usada como ayuda en los procesos judiciales para crímenes como homicidios, pornografía, fraude financiero, robo de información, drogas, acceso a datos privados, etc. En el ámbito de la litigación civil con casos como fraude, divorcios, discriminación, acoso, en cuanto a temas corporativos la evidencia digital proporciona evidencia en procesos como los de acoso sexual, robo, uno inadecuado de la información, espionaje industrial, entre otras.

La informática forense abarca escenarios de manera general, es por eso que se creó una sub rama llamada forensia en redes (Network forensics), según la compañía cryptomex.org la forensia en redes es la encargada de capturar, registrar y analizar los eventos de la red para descubrir los atacantes, fallos en seguridad o incidentes[2], esto se realiza con el fin de presentarla como evidencia legal o para detección de intrusos o vulnerabilidades.

Es importante tener en cuenta que la información que se maneja en la red es volátil y dinámica, por lo que se pierde después de que se transmite, o el dispositivo deja de recibir impulsos eléctricos. Por esta razón la forensia en redes puede ser utilizada de dos formas, la primera a través de un monitoreo en la red, el monitoreo de red es la utilización constante del sistema en busca de cambios o defectos en la red[3] para enviar alertas mediante correo electrónico, notificaciones, etc. El monitoreo de red se encarga de detectar anomalías, cambios o irregularidades que alteren o modifiquen el tráfico de la red o detectar posibles intrusos, ya que podrían ingresar y borrar archivos de registro de un host, es por esto que la evidencia que sea recopilada en la red es la forma de comprobar lo sucedido, y la segunda forma es como apoyo a la ley mediante el análisis del tráfico para detectar información como los paquetes que están en la red[4], para después estudiar la información obtenida y realizar el análisis de tráfico para revisar los archivos transferidos, palabras clave e información útil para analizar la comunicación humana mediante la búsqueda de correos electrónicos o sesiones de chat.

A lo largo del artículo se profundizará en los protocolos más utilizados, y en la rama de red forense, con el fin de

identificar su importancia en un escenario para que permita mostrar la utilidad de las herramientas en la recolección de evidencia digital, también se realiza una descripción de las herramientas utilizadas con el fin de dar a conocer cuál fue el aporte de cada una de ellas en la investigación realizada con el escenario planteado y en los aportes finales que están más adelante en el artículo.

II. Marco Teórico

Para profundizar en red forense primero se debe tener clara la definición de red, para informática la red es un conjunto de dispositivos conectados entre sí para realizar un intercambio de información o datos[6]. La red maneja una topología que describe la forma en la que está conectada la red en donde las más utilizadas son bus, anillo, estrella, jerárquica y en malla, la red también posee una tipología encargada de realizar los intercambios la red, estos contienen distintos rangos dependiendo el rango de comunicación que se necesite según la capacidad de usuarios que van a interactuar en la red, desde la personal, metropolitana o en un área de manera virtual. Las más comunes en empresas son las redes LAN, MAN y WAN, y maneja una arquitectura de red que es el diseño de las comunicaciones en donde se realizan especificaciones, procedimientos y principios de los componentes lógicos de la organización, la arquitectura consta de una estructura por capas y un protocolo que usa cada capa [7].

La forensia en redes es la subrama de la informática forense encargada de capturar, registrar, almacenar y analizar los eventos de la red para determinar la fuente de ataques o las vulnerabilidades que tenga la red.

La forensia en redes busca entregar pruebas que sean admisibles ante la corte con la ayuda de estrategias, procedimientos y herramientas, aplicadas a la red para entregar respuestas como ¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿por qué? causo los eventos, incidentes o fraudes apoyándose en la red[22].

De acuerdo a Simón Garfinkel se tienen dos técnicas para el análisis forense de red, la primer técnica es “Catch-it-as-you-can” que consiste en capturar todos los paquetes que pasan por un determinado punto, son almacenados en un medio externo para ser analizados posteriormente, una de las desventajas es que para esta técnica se necesita una gran cantidad de almacenamientos, la segunda técnica es “Stop, look and listen” en donde cada paquete se analiza de forma habitual y solo se almacena la información que se considera relevante para la parte que está aplicando la técnica para un análisis futuro, la desventaja es que necesita un procesador mucho más rápido para no perder los paquetes. Gracias a la rama de la forensia en redes se puede realizar recuperación de evidencia, también se puede conocer si el atacante borró sus huellas, recuperar documentos y lograr las pruebas suficientes para denunciar a alguien o para comprobar quien realizó el atacante.

Para ambas técnicas se requiere almacenamiento y realizar una eliminación constante de datos antiguos para tener más espacio para los datos nuevos, algunas herramientas utilizadas para la captura y análisis de tráfico gratuitas son tcpdump, windump, wireshark, entre otros[5].

Los protocolos de red son un conjunto de reglas implementadas para establecer que un emisor y un receptor se comuniquen de manera correcta, definiendo las reglas de cómo se realizará la interacción entre los dispositivos en la red, para la investigación se realizó captura de paquetes TCP, ICMP, NTP y LLMNR.

A. TCP

El protocolo TCP es el encargado de posibilitar la administración y transferencia de datos y proporcionar una comunicación segura entre emisor y receptor mediante circuitos lógicos o servicios de conexión. debe asegurar la correcta transmisión de los datos por todas las capas de la red, realiza comprobación de si existe una duplicidad en los datos y los elimina [13][24].

B. ICMP

El protocolo ICMP, es el encargado de controlar si un paquete no alcanza su destino, si el encabezado lleva algo incorrecto o no permitido, dando una comunicación entre el ip de una máquina y otra. si tiene algún problema se generarán mensajes de error o mensajes informativos, solo informa incidentes en el momento de la entrega del paquete o errores de la red pero de forma general, los mensajes informativos son importantes porque pueden ayudar a identificar si existen fallos en el nivel de red y los mensajes de error son generados en el momento en el que es tiempo del datagrama llegue a cero y que esté en camino aun, también envía el mensaje en el momento en el que encuentra inconsistencias en la información del datagrama o también cuando se envía el datagrama al routxer equivocado [14].

C. NTP

El protocolo NTP o Network Time Protocol, diseñado para sincronizar el tiempo en una red de equipos que por encima ejecuta el protocolo UDP, generalmente usa un radio reloj o un reloj atómico como su fuente de tiempo, el NTP tiene acceso a distintas fuentes de tiempo para monitorear y detectar posibles fallos en alguno de estos [15][30].

D. LLMNR

El protocolo LLMNR, Link-Local Multicast Name Resolution encargado de resolver los nombres de los sistemas informáticos cercanos funciona sobre IPv4 e IPv6 con registros similares a los del DNS, algunos de los campos que tiene el protocolo son para identificar la petición, conocer la cantidad de entradas y registros de respuesta y la cantidad de servidores que tiene [16].

Por todo lo anterior es posible evidenciar que la interacción con los usuarios es directa, lo que permite la manipulación del proceso de comunicación entre el emisor y el receptor, por esto y por el aumento del uso de la tecnología en las organizaciones, es de gran importancia el rastreo de posibles ataques a los que se encuentran vulnerables las empresas constantemente.

Razón por la cual, la seguridad se ha convertido en un tema de gran relevancia para las organizaciones, dando primordial importancia a la monitorización y análisis del tráfico en red con el fin de detectar eventos maliciosos que puedan afectar la información de la compañía o peor aún de sus clientes y proveedores. con el fin de manejar el incidente o un evento malicioso tan rápido como sea posible.

En este contexto el término "evento malicioso", hace referencia a paquetes sospechoso que se consideran que violan los principios de comunicación de esta con el fin de explotar las vulnerabilidades dando acceso al host. También hace referencia a patrones irregulares de tráfico en la red donde se pueden identificar paquetes con valores falsificados de indicadores TCP/IP o números de puerto.

Por esto, a partir de la informática forense se creó una subrama encaminada a estudiar incidentes en la red llamada Network forensic cuyo objetivo es detectar paquetes, programas o tráfico malicioso para evitar los ataques o conocer los pasos del atacante. Para lograr esto, se deben seguir técnicas para realizar una monitorización activa de la red en las que se incluye la detección de anomalías, el control de acceso y la detección de intrusos.

Esta rama de la forensia resuelve dudas como: en qué momento el atacante accede al sistema, qué protocolo de red uso el atacante, entre otras. Mediante el monitoreo de la red se pueden detectar anomalías para determinar si se realizó algún ataque, para ello se debe seguir un proceso de captura, registro, análisis y objetivos, la captura es el proceso de recopilación de los paquetes que están viajando en el medio, para seguir con el registro que es el proceso de escribir paquetes capturados en dispositivos de almacenamiento para luego analizar cada paquete y descubrir de qué tipo fue la intrusión.

La forensia en redes analiza el historial de tráfico de datos con el fin de investigar los ataques a la seguridad, reconstruyendo en secuencia las evidencias recopiladas, permitiendo de esta forma recuperar mensajes, tráfico de la red, correos y otros por medio de la recolección de paquetes.

Para realizar el análisis se cuenta con distintas técnicas como los mensajes de alerta de los IDS, examinar el evento de una alarma, examinar el encabezado del protocolo de un paquete, determinar si el evento es un virus, escaneo, etc.

La forensia en redes tiene como propósito descubrir actividades maliciosas en la red para que en el momento en el que ocurran incidentes se pueda realizar una reconstrucción de los eventos y poder realizar una extracción de la evidencia y posteriormente realizar un análisis de tráfico que esté cifrado u oculto. para realizar la adquisición de la información se debe realizar una copia forense y una copia completa, la copia forense contiene la cadena de evidencia, las firmas digitales y los controles de acceso, en cuanto a la copia completa es más compleja su adquisición ya que la velocidad en la red puede causar dificultad en la captura de paquetes o se puede capturar información que está fuera del alcance de la investigación y se puede vulnerar el aspecto de privacidad.

para esto se debe tener en cuenta la cantidad de datos, ya que puede faltar información o si por el contrario es mucha información puede ser complicado analizarla, se debe tener en cuenta siempre es aspecto legal y privacidad de la información, esta información puede ser capturada desde el Hub o desde el switch(habilitando algún puerto), para realizar el análisis de los paquetes se debe realizar una disección de paquetes que es dividir cada paquete en los distintos protocolos y ser leídos de izquierda a derecha y primero los protocolos de bajo nivel, como por ejemplo primero el encabezado TCP luego IP, después Ethernet, etc.

III. HERRAMIENTAS

Existen diferentes tipos de herramientas teniendo en cuenta la investigación realizada y el tipo de investigación recolectada, entre los más conocidos están Xplico, Network

Miner, MyLanViewer, Bro-IDS, Tcpxtract, wireshark, clamAV, etc, de las cuales se usaron MyLanViewer y wireshark.

A. Xplico

Es una herramienta forense creada para examinar y revisar, armar y acomodar los paquetes de páginas web, imágenes, sonidos, video, según el protocolo, es Open Source[25].

B. Network Miner

Es una herramienta que permite analizar y capturar paquetes, la herramienta cuenta con dos versiones, una gratuita y una paga que cuenta con más funciones que la gratuita, soporta Linux, Windows, Solaris, Mac OS [23][26].

C. Bro-IDS

Es una herramienta para detectar intrusos para UNIX/Linux que analiza el tráfico de la red para buscar eventos sospechosos en la capa de aplicación [27].

D. Tcpxtract

El protocolo LLMNR, Link-Local Multicast Name Resolution encargado de resolver los nombres de los sistemas informáticos cercanos funciona sobre IPv4 y IPv6 con registro [28].

E. ClamAV

Es un software open source, para Linux, Windows, Solaris, Mac OS, para identificar y bloquear malware de correos electrónicos [29].

F. MyLanViewer

Es un escáner de red muy fuerte, tiene una sección para realizar Wake-On-Lan que realiza un monitoreo de IP en toda la red, logrando ver los dispositivos que están conectados y proporcionando datos como el nombre, la dirección MAC, los recursos compartidos y unos detalles más técnicos de cada dispositivo, otra de las acciones del programa es controlar direcciones IP para notificar si estas tuvieron cambios, se puede acceder a carpetas compartidas, cerrar sesiones de usuarios y poder supervisar que recursos son compartidos entre los dispositivos, puede detectar servidores DHCP que no estén autorizados, es open source y fácil de usar[17].

G. Wireshark

Es un sniffer para analizar de protocolos permitiendo realizar una captura y monitoreo de paquetes, entregando una interfaz amigable con el usuario permitiendo el filtrado de información según los protocolos que se necesitan y entregando información detallada del tráfico, es capaz de reconstruir una sesión de TCP y un UDP, permite ver lo que pasa en la red de una forma muy detallada, es open source y multiplataforma[21], generalmente es utilizado para resolver problemas en la red, examinar problemas de inseguridad, depurar la implementación de los protocolos de la red o como uso académico para entender cómo funciona una red, las ventajas de usar wireshark es que gracias a su versatilidad maneja más de 450 protocolos, soporta un estándar tcpdump para reconstruir las sesiones y tiene una interfaz gráfica completa y fácil de usar [18][19][20].

IV. Trabajo Realizado

El escenario que se plantea es una empresa de nivel medio que tiene una red LAN, que cuenta con 500 dispositivos, entre ellos switches routers computadores y teléfonos corporativos. Los dispositivos de red son Cisco, los sistemas operativos que se usan en sus equipos de cómputo son Android, Linux, MAC y Windows. No se han definido restricciones de acceso a internet.

Como primera instancia se debe tomar la mayor cantidad de paquetes para realizar un análisis más adelante, esto es realizado con WireShark y para la investigación se realizó la captura de los paquetes ICMP, TCP, UDP y LLMNR.

De acuerdo con los protocolos explicados anteriormente, en la Fig. 1 se observa la captura de paquetes del protocolo ICMP, se realizó un filtrado para que sólo capturará paquetes de este protocolo y se realizó ping a Google, se seleccionó un paquete o datagrama y se almacenó en un archivo. pcapng, parte de lo que contiene el archivo se muestra en la Fig. 2

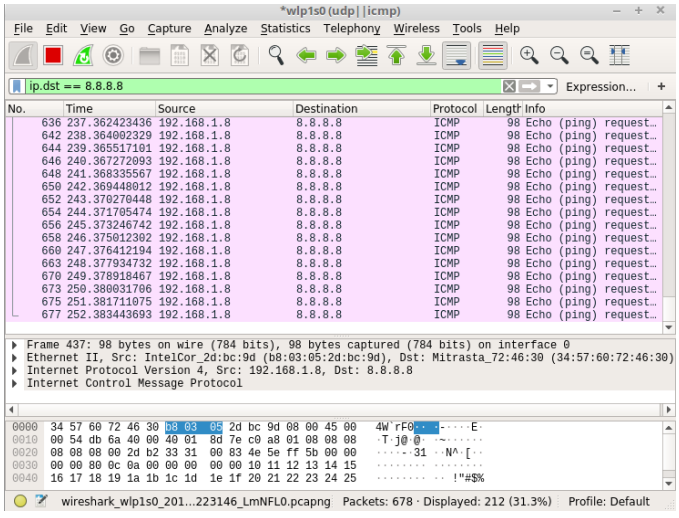

Fig. 1 Monitoreo de paquetes ICMP de Google.

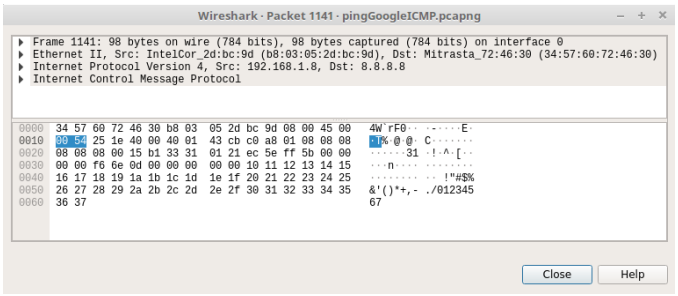

Fig. 2 Evidencia de la información que tiene un paquete ICMP.

En cuanto a la Fig. 3 se observa el tráfico del protocolo TCP con un filtro que solo muestra ese protocolo y en la Fig. 4 se observa cuáles son los datos contenidos en dicho paquete.

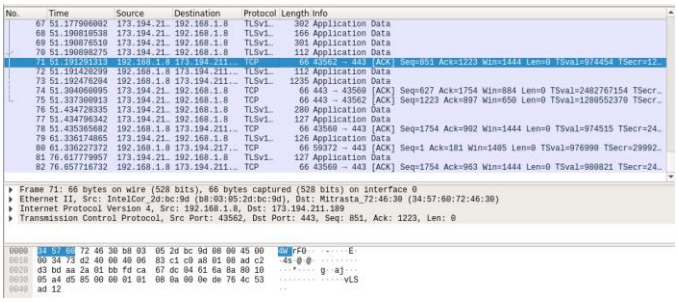

Fig. 3 Monitoreo de paquetes TCP.

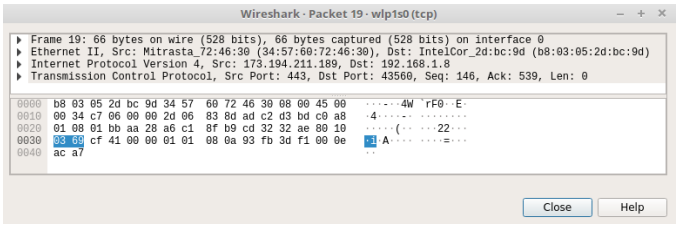

Fig. 4 Visualización del contenido del paquete TCP.

Se procede a la captura y recolección de los paquetes NTP para revisar si el atacante realizó un ataque de reflejo y así obtener una lista de host de los administradores con el comando “Monlist” y después realizar una denegación de servicio para inactivar las direcciones de la lista, en la Fig. 5 y Fig. 6 se observa la recolección de datos y la manera en que muestra los datos el archivo, para esta captura no se realizó el filtro, de manera que adicionalmente se observa cómo pasan paquetes de los protocolos DNS y MDNS.

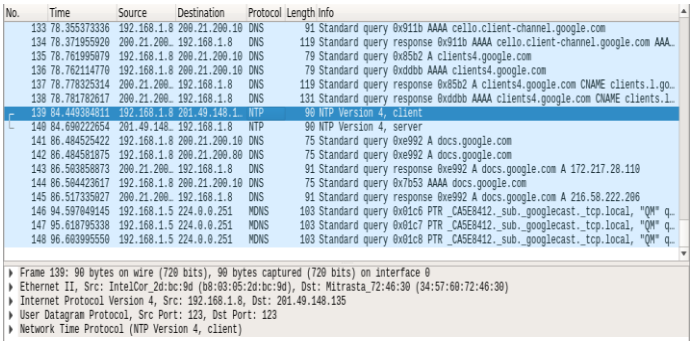

Fig. 5 Captura de paquetes NTP.

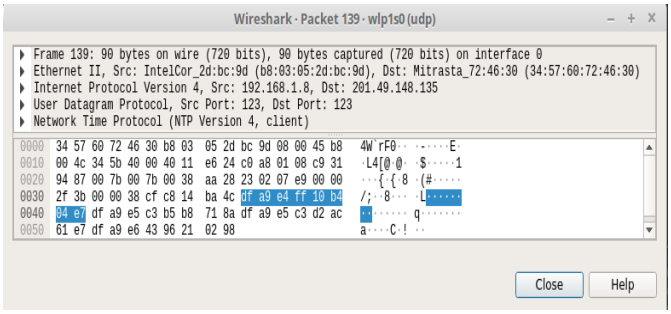

Fig. 6 Datos del paquete capturado del protocolo NTP.

La última captura realizada fue la del protocolo LLMNR en la que no se realizó el filtrado para lograr observar distintos paquetes de los protocolos NBNS, MDNS y SSDP, como aparece en la Fig. 7.

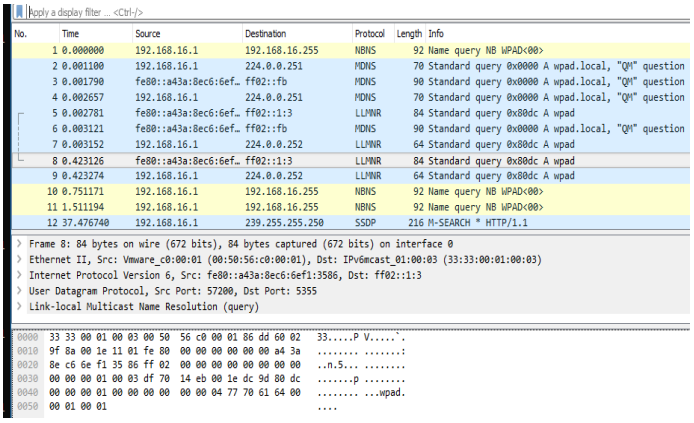

Fig. 7 Monitoreo de paquetes y captura de paquete LLMNR.

Después de realizar la captura de paquetes necesarios, con la ayuda de la herramienta de MyLanViewer se puede conocer todos los dispositivos que están conectados a la red, con sus respectivos datos, como se aprecia en la Fig. 8.

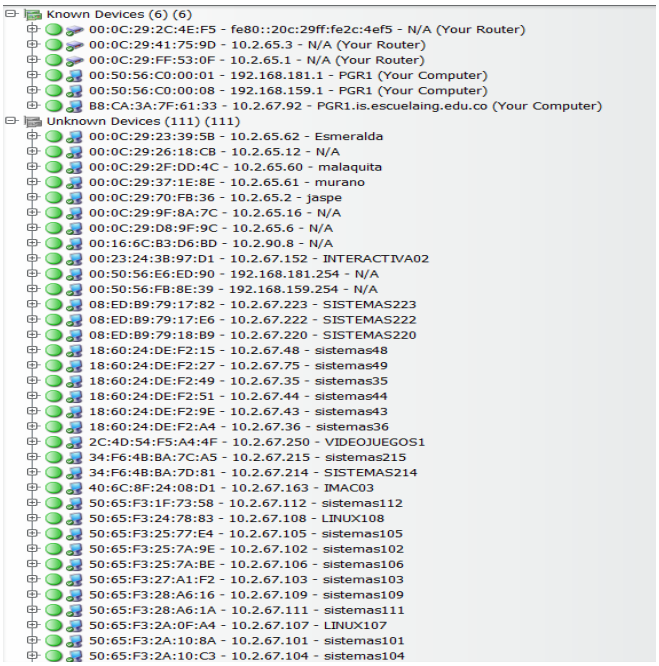

Fig. 8 Dispositivos que están en la misma red.

También se tiene acceso a la subnet ingresando la IP y el rango como se observa en la Fig. 9, también se accede a los eventos realizados por el computador, los cuales entregan una breve descripción e información como la dirección IP, la dirección MAC, entre otras cosas como se aprecia en la Fig.10.

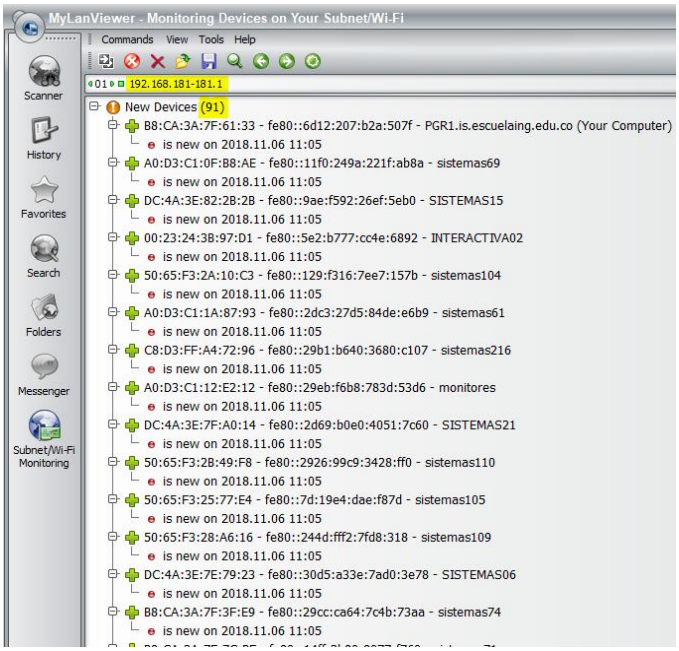

Fig. 9 Monitoreo de los equipos de una red específica.

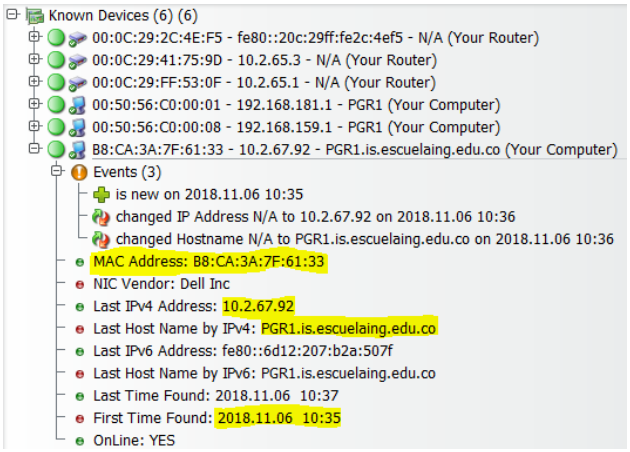

Fig. 10 Acceder a eventos de un dispositivo específico.

Una de las funciones importantes que brinda la herramienta es la opción de conocer la IP externa del dispositivo como se observa en la Fig. 11 y Fig. 12.

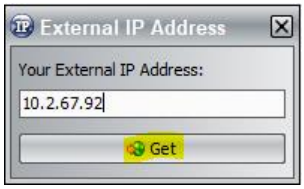

Fig. 11 IP interna del dispositivo para conocer la IP externa.

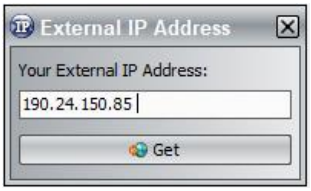

Fig. 12 Adquisición de la IP externa del dispositivo.

La herramienta permite la realización de un ping para comprobar si se puede llegar o no hasta otro dispositivo, brindando la opción de entregar un informe con todos los resultados obtenidos en la búsqueda, también se obtiene el historial de usuario y con ello se conoce qué usuarios han realizado login en la máquina, antes de realizar la gestión forense como se observa en la Fig. 13.

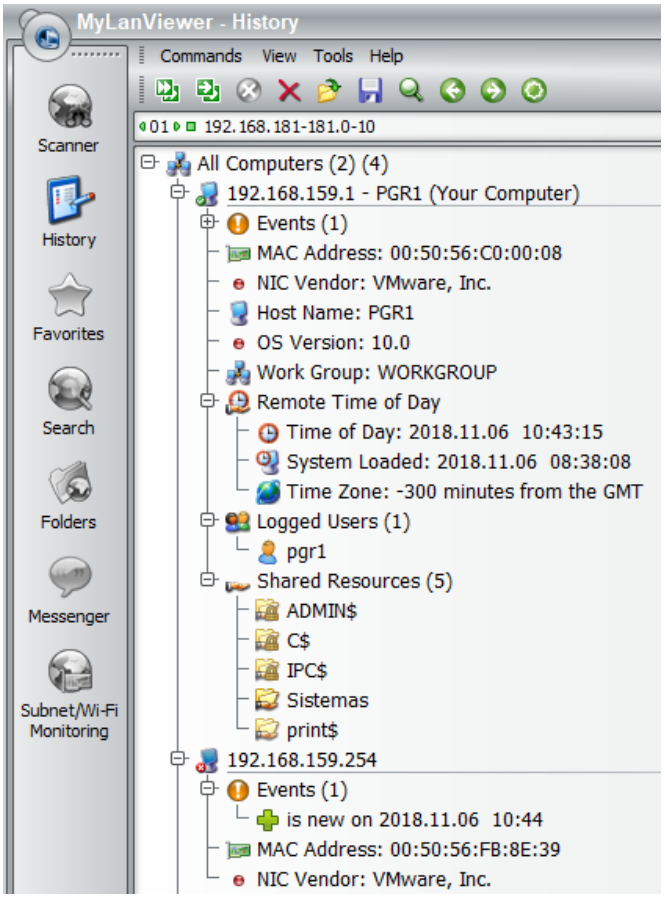

Fig. 13 Historial de un dispositivo, con toda la información.

Cuando se conoce la IP del atacante se utiliza la función para conocer el IP junto con alguna información adicional, como se aprecia en la Fig. 14.

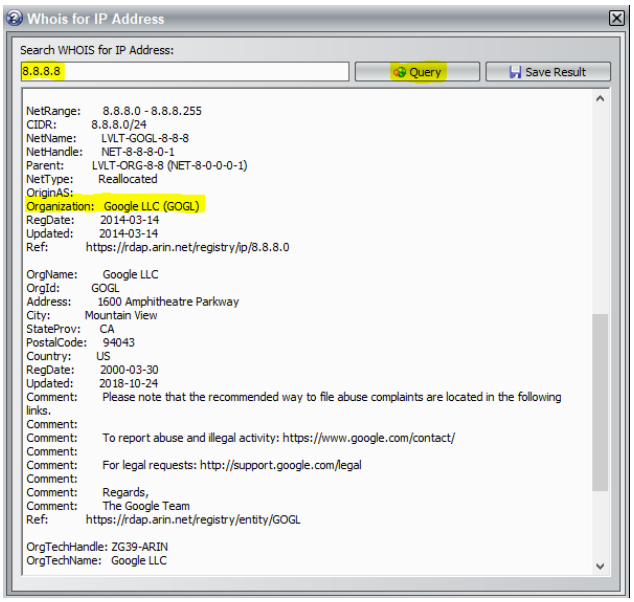

Fig. 14 Informe de datos sobre una IP.

Al analizar los datos de la red, podemos buscar todos los paquetes de una dirección de origen específica o todos los paquetes que van a un puerto específico. También podemos querer encontrar paquetes que tengan una determinada palabra clave en ellos

V. Conclusiones

El monitoreo de red es muy útil para encontrar fallas en la seguridad de la red, detectar intrusos, capturar paquetes para posteriormente analizarlos y descubrir la posible ruta de acceso y huida de quien realizó las modificaciones en el sistema.

Wireshark es una herramienta útil para la captura de paquetes y tiene una ventaja, es multiplataforma lo que hace mucho más fácil el uso de la misma herramienta en los distintos sistemas operativos.

La información que pasa en la red es volátil por eso es pertinente encontrar maneras para controlar o reaccionar frente a un incidente y una de las maneras más eficientes es realizando un monitoreo y un análisis de la red, para esto se debe contar con las herramientas necesarias y las políticas pertinentes para generar una buena infraestructura y así, en el caso de requerirse, lograr generar una evidencia digital que sea admisible ante la corte.

References

[1] Alvarado, K. P. (n.d.). *monografias.* Retrieved from Arquitecturas de red: https://www.monografias.com/docs114/arquitecturas-red/arquitecturas-red.shtml#arquitecta

[2] Cano, O. S., Beceiro, D. I., Alberto, M. T., & Lombart, A. C. (n.d.). *scholar.google.com.* Retrieved from Análisis preliminar de los resultados de una: https://scholar.google.com/scholar?q=Cano%2C%20D.%2C%20et%20al.%3A%20An%C3%A1lisis%20preliminar%20de%20los%20resultados%20de%20una%20clasificaci%C3%B3n%20de%20unidades%20de%20llanto%20seg%C3%BAn%20tres%20arquitecturas%20de%20redes%20neuronales.%20Memorias

[3] Cárdenas, R. G. (n.d.). *http://cryptomex.org.* Retrieved from Computo forense redes: http://cryptomex.org/SlidesForensia/ForensiaRedes.pdf

[4] ccm. (n.d.). *Topología de red.* Retrieved from ccm: https://es.ccm.net/contents/256-topologia-de-red#simili_main

[5] cisco. (2008, 12 17). *Protocolo Network Time Protocol: Informe oficial de Mejores Prácticas.* Retrieved from cisco: https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/19643-ntpm.html#ntpoverview

[6] ediciones-eni.com. (n.d.). *El protocolo de resolución local LLMNR (Link Local Multicast Name Resolution).* Retrieved from ediciones-eni.com: https://www.ediciones-eni.com/open/mediabook.aspx?idR=16235b5c43d41e08b8842836d739ba71

[7] *El protocolo ICMP*. (n.d.). Retrieved from Herramientas Web para la Enseñanza de Protocolod de Comunicación: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html
[8] Hauben, R. (n.d.). *Protocolo de Control de Transmisión.* Retrieved from columbia: http://www.columbia.edu/~rh120/other/tcpdigest_paper.txt
[9] ionos.e. (n.d.). *ionos.es.* Retrieved from Conoce los tipos de redes más importantes: https://www.ionos.es/digitalguide/servidores/know-how/los-tipos-de-redes-mas-conocidos/
[10] Iorio, A. H., & FASTA, U. (n.d.). *La Informática Forense y el proceso de recuperación de información.* Retrieved from a Universidad FASTA: http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/1560/Inform%C3%A1tica%20Forense%20Proceso.pdf?sequence=1
[11] Javier, p. (n.d.). *pandorafms.org.* Retrieved from Monitoreo de Red: qué debemos saber: https://blog.pandorafms.org/es/monitoreo-de-red-que-debemos-saber/
[12] mylanviewer. (n.d.). *Products overview*. Retrieved from mylanviewer: http://www.mylanviewer.com/
[13] oracle. (n.d.). *Guía de administración del sistema: servicios IP*. Retrieved from oracle: https://docs.oracle.com/cd/E19957-01/820-2981/ipov-10/
[14] neo.lcc.uma.es. (n.d.). *El protocolo ICMP*. Retrieved from Herramietas web para la enseñanza de protocolos d comunicacion: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html
[15] Rebeca. (n.d.). *nextu*. Retrieved from CONOCE LOS TIPOS DE REDES INFORMÁTICAS: https://www.nextu.com/blog/tipos-de-redes/
[16] Rouse, M. (2005, 09). *network forensics.* Retrieved from Network monitoring: https://searchsecurity.techtarget.com/definition/network-forensics
[17] S.A, P. I. (n.d.). *ANÁLISIS DE TRÁFICO*. Retrieved from postech.com: http://postech.com.mx/Postech/ES/analysis.php
[18] wireshark. (n.d.). *Learn Wireshark.* Retrieved from Wireshark Training: https://www.wireshark.org/#learnWS
[19] alfon. (2008, 02 14). *Análisis de red con Wireshark. Interpretando los datos.* Retrieved from Seguridad y Redes: https://seguridadyredes.wordpress.com/2008/02/14/analisis-de-red-con-wireshark-interpretando-los-datos/
[20] Febrero, B. M. (2011, 02). *ANÁLISIS DE TRÁFICO CON WIRESHARK*. Retrieved from INTECO-CERT: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf
[21] geekytheory. (2018). *Pásate a Premium*. Retrieved from geekytheory: https://geekytheory.com/curso/wireshark/instalar-wireshark
[22] infosec institute. (n.d.). *Computer Forensics: Network Forensics Analysis and Examination Steps*. Retrieved from resources.infosecinstitute.com: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/digital-forensics/network-forensics-analysis-and-examination-steps/#gref
[23] netresec. (2018). *Network Forensics and. Retrieved* from netresec: https://www.netresec.com/
[24] sites.google.com. (2018). protocolos de red. Retrieved from todo sobre redes informatica: https://sites.google.com/site/todosobreredesinformatica/protocolos-de-red
[25] Xplico: Herramienta Forense. Ubuntobook. Febrero de 2012 https://ubuntubook.wordpress.com/2012/02/23/xplico-herramienta-forense/
[26] NetworkMiner. M. J. Montes. Abril de 2014. https://hacking-etico.com/2014/04/09/networkminer/
[27] Bro – IDS. Un sistema de detección de intrusiones basado en políticas especializadas.Alfon. Marzo 2011 https://seguridadyredes.wordpress.com/2011/03/23/bro-ids-un-sistema-de-deteccion-de-intrusiones-basado-en-politicas-especializadas/
[28] TCPXtract (Network Traffic Extracción):: Herramientas. Gustavo Sied. Febrero de 2014 https://blog.sied.com.ar/2014/02/tcpxtract-network-traffic-extraccion-herramientas.html
[29] ¿Qué es ClamAV y cómo funciona?. Team Towebs. Septiembre de 2016. https://blog.towebs.com/que-es-clamav-y-como-funciona/
[30] ¡Cuidado! Los riesgos de los protocolos BGP, FTP y NTP. Panda Security. Octubre de 2018, https://www.pandasecurity.com/spain/mediacenter/seguridad/riesgo-protocolos-bgp-ftp-ntp/