# Unit 4: Network Investigations

4

**UNIT STRUCTURE**



## 1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Overview of enterprise networks and protocols
- Collecting and interpreting network device configuration
- Forensic examination of network traffic

## 1.2 INTRODUCTION

Tracking down computer criminals generally requires digital investigators to follow the cybertrail between the crime scene and the offender's computer. The cybertrail can cross

multiple networks and geographical boundaries, and can be comprised of many different kinds of digital evidence, including proxy and firewall logs, intrusion detection systems, and captured network traffic. Dialup server logs at the suspect's Internet Service Provider (ISP) may show that a specific IP address was assigned to the suspect's user account at the time. The ISP may also have Automatic Number Identification (ANI) logs—effectively Caller-ID—connecting the suspect's home telephone number to the dialup activity. Routers on the ISP network that connect the suspect's computer to the Internet may have associated NetFlow logs containing additional information about the network activities under investigation. Each of these logs would represent steps on the trail.[72]

Ideally, each step in the cybertrail can be reconstructed from one or more records from this evidence, enabling digital investigators to connect the dots between the crime scene and the offender's computer and establish the continuity of offense. If there is more than one type of evidence for a particular step, so much the better for correlation and corroboration purposes. Your reconstruction of events is like a scientific hypothesis. The more evidence you collect that is consistent with the hypothesis, the stronger the case for that hypothesis becomes.

Networks present investigators with a number of challenges. When the networks are involved in a crime, evidence is often distributed on many computers making a collection of all hardware or even the entire contents of a network unfeasible.

## 1.3 OVERVIEW OF ENTERPRISE NETWORKS

Digital investigators must be sufficiently familiar with network components found in a typical organization to identify, preserve, and interpret the key sources of digital evidence in an Enterprise. This chapter concentrates on digital evidence associated with routers, firewalls, authentication servers, network sniffers, Virtual Private Networks (VPNs), and Intrusion Detection Systems (IDS).

Logs generated by network security devices like firewalls and IDSs can be a valuable source of data in a network investigation. Access attempts blocked by a firewall or malicious activities

[72] Spiekermann, Daniel & Eggendorfer, Tobias (2017) Challenges of Network Forensic Investigation in Virtual Networks. Journal of Cyber Security and Mobility

detected by an IDS may be the first indication of a problem, alarming system administrators enough to report the activity to digital investigators. Routers form the core of any large network, directing packets to their destinations. Routers can be configured to log summary information about every network connection that passes through them, providing a bird's eye view of activities on a network. For example, suppose you find a keylogger on a Windows server, and you can determine when the program was installed. Examining the NetFlow logs relating to the compromised server for the time of interest can reveal the remote IP address used to download the keylogger. Furthermore, NetFlow logs could be searched for that remote IP address to determine which other systems in the Enterprise were accessed and may also contain the keylogger. As more organizations and ISPs collect NetFlow records from internal routers as well as those at their Internet borders, digital investigators will find it easier to reconstruct what occurred in a particular case.

Digital investigators may be able to obtain full network traffic captures, which are sometimes referred to as logging or packet capture, but are less like a log of activities than like a complete videotape of them—recorded network traffic is live, complete, and compelling. Replaying an individual's online activities as recorded in a full packet capture can give an otherwise intangible sequence of events a very tangible feel.[73]

## 1.4 OVERVIEW OF PROTOCOLS

To communicate on a network, computers must use the same protocol. For example, TCP/IP is the standard for computers to communicate across the Internet. The principle is fairly straightforward. Information is transmitted from a networked system in chunks called packets or datagrams. The chunks contain the data to be transferred along with the information needed to deliver them to their destination and to reconstruct the chunks into the original data. The extra information is added in layers when transmitted and stripped off in layers at the destination.[74] This layering effectively wraps or encapsulates control details around the data before they are sent to the next layer, providing modular functionality at each layer. One layer, for instance, is

[73] Spiekermann, Daniel & Keller, Jörg & Eggendorfer, Tobias (2017) Network forensic investigation in OpenFlow networks with ForCon. Digital Investigation
[74] Stevens, S W (1994) In TCP/IP Illustrated, Volume 1: The Protocols. Addison Wesley

used to specify the IP address of the destination system, and another layer is used to specify the destination application on that system by specifying the port being used by that application (there may be several ports on a server willing to receive data, and you don't want your request for a web page to end up in an SSH server). Both of these layers will contain instructions for reconstructing the separated chunks, how to deal with delayed or out-of-order deliveries, and so forth.

To communicate with machines on different networks, computers must run higher-level protocols such as Internet Protocol (IP) at the network layer and Transport Control Protocol (TCP) at the transport layer. The Transmission Control Protocol (TCP) is a connection-mode service, often called a virtual-circuit service that enables transmission in a reliable, sequenced manner that is analogous to a telephone call. TCP differs from the User Datagram Protocol (UDP), which is connectionless, meaning that each datagram is treated as a self-contained unit rather than part of continuous transmission, and delivery of each unit is not guaranteed—analogous to a postal letter. Both TCP and UDP use ports to keep track of the communication session.[75]

## 1.5 EVIDENCE PRESERVATION ON NETWORKS

There are some unique forensic challenges associated with preserving digital evidence on networks. Although some network-related data are stored on hard drives, more information is stored in the volatile memory of network devices for a short time or in-network cables for an instant. Even when collecting relatively static information such as firewall log files, it may not be feasible to shut down the system that contains these logs and then make a bitstream copy of the hard drive. The system may be a part of an organization's critical infrastructure and removing it from the network may cause more disruption or loss than the crime. Alternately, the storage capacity of the system may be prohibitively large to copy. So, how can evidence on a network be collected and documented in a way that demonstrates its authenticity, preserves its integrity and maintains the chain of custody?

[75] Davie, B and Gross, J (2016) A Stateless Transport Tunneling Protocol for Network Virtualization. Internet Draft, Informational: New York, NY

In the case of log files, it is relatively straightforward to make copies of the files, calculate their message digest values (or digitally sign them), and document their characteristics (e.g., name, location, size, MAC times). All this information can be useful for establishing the integrity of the data at a later date and digitally signing files is a good method of establishing chain of custody, provided only a few people have access to the signing key. A failure to take these basic precautions can compromise an investigation. In 2000, for example, an individual known as Maxus stole credit card numbers from the Internet retailer CD Universe and demanded a $100,000 ransom. When denied the money, he posted 25,000 numbers on a web site. Employees from one or more of the computer security companies that handled the break-in inadvertently altered log files from the day of the attack—this failure to preserve the digital evidence eliminated the possibility of a prosecution.[76]

Networked systems can also contain crucial evidence in volatile memory, evidence that can be lost if the network cable is disconnected or the computer is turned off. For instance, active network connections can be used to determine the IP address of an attacker. Methods and tools for preserving volatile data on Windows and UNIX systems are covered in Malware Forensics.

In addition to preserving the integrity of digital evidence, it is advisable to seek and collect corroborating information from multiple, independent sources. Last but not least, when collecting evidence from a network, it is important to keep an inventory of all the evidence with as much information describing the evidence as possible (e.g., filenames, origin, creation times/dates, modification times/dates, a summary of contents). Although time-consuming, this process facilitates the pin-pointing of important items in the large volume of data common to investigations involving networks.

## 1.6 COLLECTING AND INTERPRETING NETWORK DEVICE CONFIGURATION

Network devices are generally configured with minimal internal logging to conserve storage space and for optimal performance. Some network device functions are so thoroughly engineered to optimize performance that they are not normally logged at all. Although these devices can be

[76] Mosharaf Kabir Chowdhury, N M, and Boutaba, R (2009) Network virtualization: state of the art and research challenges. IEEE Commun. Mag. 47, 20–26

configured to generate records of various kinds, the logs must be sent to a remote server for safekeeping because these devices do not contain permanent storage. Central syslog servers are commonly used to collect the log data.

In addition to generating useful logs, network devices can contain crucial evidence in volatile memory, evidence that can be lost if the network cable is disconnected or the device is shut down or rebooted. Routers are a prime example of this. Most routers are specialized devices with a CPU; ROM containing power-on self-test and bootstrap code; flash memory containing the operating system; nonvolatile RAM containing configuration information; and volatile RAM containing the routing tables, ARP cache, limited log information, and buffered packets when traffic is heavy.[77]

Routers are responsible for directing packets through a network to their destination and can be configured using Access Control Lists (ACLs) to make basic security-related decisions, blocking or allowing packets based on simple criteria. For instance, some organizations implement simple egress and ingress filtering in their border routers (blocking outgoing packets that have source addresses other than their own, and blocking incoming packets that contain source addresses belonging to them). This simple concept—only data addressed from the organization should be allowed out—greatly limits a malicious individual's ability to conceal his location. In some cases, digital investigators must document how a router is configured and other data stored in memory.

## 1.7 VIRTUAL PRIVATE NETWORKS

Many organizations use Virtual Private Networks (VPN) to allow authorized individuals to connect securely to restricted network resources from a remote location using the public Internet infrastructure. For instance, an organization might use a VPN to enable travelling sales representatives to connect to financial systems that are not generally available from the Internet. Using a VPN, sales representatives could dial into the Internet as usual (using low cost, commodity Internet service providers) and then establish a secure, encrypted connection the

[77] Corey, V, Peterman, C, Shearin, S., Greenberg, M S, and Van Bokkelen, J (2002) Network forensics analysis. IEEE Int. Comput. 6, 60–66

organization's network. A VPN essentially provides an encrypted tunnel through the public Internet, protecting all data that travels between the organization's network and the sales representative's computer.

Newer operating systems, including Windows 2000/XP/Vista, have integrated VPN capabilities, implementing protocols like Point to Point Tunneling Protocol (PPTP) and IPsec to establish VPN. Newer network security devices like the Cisco ASA and Juniper SA Series also support VPN services via SSL, enabling users to establish a virtual connection simply using a web browser. Digital investigators most commonly encounter VPN logs as a source of evidence associated with remote users accessing secured resources within the network from the Internet.

## 1.8 FORENSIC EXAMINATION OF NETWORK TRAFFIC

The contents of network traffic can be invaluable in a network investigation, because some evidence exists only inside packet captures. Many host-based applications do not keep detailed records of network transmissions, and so capturing network traffic may provide you with information that is not recorded on a host. Furthermore, captured network traffic can contain full packet contents, whereas devices like firewalls and routers will not. Even an IDS, which may record some packet contents, typically only does so for packets that specifically trigger a rule, whereas a sniffer can be used to capture all traffic based upon the requirements of the investigator.[78]

### Extracting Statistical Information From Network Traffic

Whether you are approaching network traffic without any leads or you have some items like IP addresses that you can use to filter or search, you should examine the set of packets in a methodical manner to extract data of interest for your investigation.[79] Examples of data you might want to extract include:

- Statistics
- Alert data

[78] Hunt, R, and Zeadally, S (2012) Network forensics: an analysis of techniques, tools, and trends. IEEE Comput. 45, 36–43

[79] Jain, R, and Paul, S (2013). Network virtualization and software defined networking for cloud computing: a survey. IEEE Commun. Mag. 51, 24–31

- Web pages
- E-mails
- Chat records
- Files being transferred
- Voice conversations

**Extracting Statistics**

You can easily generate a set of statistics regarding a set of network traffic that may help to guide your investigation. Common statistics that you will find useful include:

- Protocol usage
- Network endpoints
- Conversations
- Traffic volumes

## 1.9 INTRUSION DETECTION SYSTEMS

In addition to programs that simply capture and display network traffic based on general rules, there are programs that monitor network traffic and bring attention only to suspicious activity. These programs are called Intrusion Detection Systems (IDS). Some of these systems such as Bro (www.bro-ids.org) can be configured to store all traffic and then examine it for known attacks and to archive significant features of network traffic for later analysis. Other systems such as Snort (www.snort.org) inspect the traffic and store only data that appear to be suspicious, ignoring anything that appears to be acceptable. These systems are not primarily concerned with preserving the authenticity and integrity of the data they collect, so additional measures must be taken when using these tools.[80]

Although they are not designed specifically for gathering evidence, logs from an IDS can be useful in the instance of an offender breaking into a computer. Criminals who break into computers often destroy evidence contained in log files on the compromised machine to make an investigator's job more difficult. However, an IDS keeps a log of attacks at the network level that investigators can use to determine the offender's IP address. For example, if fraud is committed

[80] Delgadillo, K (2015) Netflow services and applications. Cisco Whitepaper, 1996 (accessed November 5, 2015)

using a networked computer and investigators find that the computer was compromised and then scrubbed of all evidence, they may be able to determine which IP address was used by examining the log file from an IDS on the network.

While investigating a large-scale network intrusion, network traffic showed the intruder connecting to a compromised system and placing an unknown executable on the system via SMB. A subsequent forensic examination of the compromised computer revealed that the intruder had deleted the unknown executable and it could not be recovered from the hard drive. Although available tools for examining network traffic could not extract the file automatically, we were able to recover the unknown executable manually and examine it to determine its functionality. The information obtained from this executable helped advance the investigation in a variety of ways.

For example, A financial services company offered customers personalized web service to monitor their financial information, including credit ratings. Each customer had an account that could be verified for two levels of access, Tier 1 and Tier 2. The Tier 1 authentication would allow a customer to view commercially available information collected at the site. To view or to make changes to their financial data, they needed a Tier 2 authentication, which required a different password and answers to some challenge questions.[81]

Web administrators would authenticate to both servers as well, but at Tier 2 their accounts had administrative access to the web site and its databases and thus to everyone's financial information. During routine maintenance, several fixes to minor problems were implemented simultaneously. As a result of the interactions of these fixes, every account on the system had full administrative access to all the accounts at Tier 2.

The problem went undetected for several months until reported by one of the customers. The administrative access was not obvious and could be discovered only by trying to access someone else's financial information. It would not occur to most customers to try the experiment. Since it was one of the customers who discovered the problem, though, it obviously could happen. Forensic investigators were asked to analyze available logs covering the vulnerable period to determine whether it was likely that any customers had exploited the information of others.

[81] Khan, S, Gani, A, Abdul Wahab, A W, Shiraz, M, and Ahmad, I (2015) Network forensics: review, taxonomy, and open challenges J Netw Comput Appl 66, 214–235

## 1.10 LET' S SUM UP

In order to conduct an investigation involving computer networks, practitioners need to understand network architecture, be familiar with network devices and protocols, and have the ability to interpret the various network-level logs. Practitioners must also be able to search and combine large volumes of log data using search tools like Splunk or custom scripts. Perhaps most importantly, digital forensic analysts must be able to slice and dice network traffic using a variety of tools to extract the maximum information out of this valuable source of network-related digital evidence.

## 1.11 FURTHER READING


- Bunker, M., & Sullivan, B. (2000). CD Universe Evidence Compromised. MSNBC, June 7.
- Comer, D. E. (1995). Internetworking with TCP/IP Volume I: Principles, Protocols, and Architecture (Third Edition). Upper Saddle River, NJ: Prentice Hall.
- Villano, M. (2001). Computer Forensics: IT Autopsy, CIO Magazine, March (http://www.cio.com/article/30022/Computer_Forensics_IT_Autopsy).
- Plonka, D. (2000). FlowScan: A Network Traffic Flow Reporting and Visualization Tool. Usenix.
- Casey, E. (2004a). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.


## 1.12 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

**1) What are Intrusion Detection Systems?**

In addition to programs that simply capture and display network traffic based on general rules, there are programs that monitor network traffic and bring attention only to suspicious activity. These programs are called Intrusion Detection Systems (IDS).

**2) Short note on protocols?**

To communicate on a network, computers must use the same protocol. Information is transmitted from a networked system in chunks called packets or datagrams. The chunks contain the data to be transferred along with the information needed to deliver them to their destination and to reconstruct the chunks into the original data. The extra information is added in layers when transmitted and stripped off in layers at the destination. This layering effectively wraps or encapsulates control details around the data before they are sent to the next layer, providing modular functionality at each layer.

**3) How to generate statistics from a set of network traffic?**

You can easily generate a set of statistics regarding a set of network traffic that may help to guide your investigation. Common statistics that you will find useful include:

- Protocol usage
- Network endpoints
- Conversations
- Traffic volumes

**1.13 ACTIVITY**

Explain briefly about Network investigations along with how networks are used in the forensic examination? Write a relevant case study pertaining to network traffic and examination? (800-1000 words)