



SECURITY

Investigating the Cyber Breach

The Digital Forensics Guide for the Network Engineer

Investigating the Cyber Breach

The Digital Forensics Guide for the Network Engineer

Joseph Muniz, Aamir Lakhani

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

The first step for starting the chain of custody process is establishing a log of how the system is before you interact with it. This is the precustody state. Just as with the first responder, you need to document everything about the device using video, photography, and a journal. There is not a standard for documentation, so you really can't do it wrong regarding the style you use to document the artifact. It is import that you include enough details to determine what the system was like before the investigation, be able to clearly identify it from similar artifacts, and be able to recognize various features and settings, such as what it was plugged into. NIST offers a sample chain of custody document you could use, as shown as Figure 5-12.

Property Record Number:

Anywhere Police Department
EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____ Location of Seizure: _____

Item #	Quantity	Description of Item (Make, Model #, Location, Mark, Scratches)

Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

APR-Item-AP003 v.1 (12/2012) Page 1 of 2 pages (See back)

Technical Working Group on Biological Evidence Preservation, The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers, U.S. Department of Commerce, National Institute of Standards and Technology, 2013.

EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM
(Continued)

Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Final Disposal Authority
Release to: _____ on this document (pertaining to subject):
Request origin needed as evidence and store submitted for disposal (check appropriate disposal method):
☐ Return to Owner ☐ Auction/Debris/Donor
Name & ID of Authorizing Officer: _____ Signature: _____ Date: _____

Witness to Destruction of Evidence
Release to: _____ on this document were destroyed by Evidence Custodian
Name (print name as listed): _____ Signature: _____ Date: _____
Name & ID of witness to destruction: _____ Signature: _____ Date: _____

Release to Lawful Owner
Release to: _____ all the document(s) were released by Evidence Custodian
Name: _____ ID#: _____ to _____
Address: _____ City: _____ State: _____ Zip Code: _____
Telephone Number: _____
Phone number of law. entity that can be easily traced to the above name(s):
Signature: _____ Date: _____
Copy of Government-issued photo identification is attached: ☐ Yes ☐ No
☐ No Evidence Chain of Custody form to be submitted as a pre-condition for the Anywhere Police Department.

APR-Item-AP003 v.1 (12/2012) Page 2 of 2 pages (See front)

Technical Working Group on Biological Evidence Preservation, The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers, U.S. Department of Commerce, National Institute of Standards and Technology, 2013.

Figure 5-12 NIST Chain of Custody Document

You will find yourself in different situations as you are involved with investigations. Sometimes, artifacts are easy to transport, such as a laptop or mobile phone. For those situations, you need to use a hazmat bag and make sure it is labeled properly. Why not a regular bag? You ideally want a hazmat bag that can prevent charges from static build-up to prevent damaging the artifacts. You also want to validate what temperatures are expected if the artifact is bagged; if it's powered on, could it generate heat if contained in a tight bag or storage container? You may need to use a cooler in those situations to avoid heat damage. If you're looking for official standards around the proper hazmat bag, you could consider bags that are MIL-STD-3010 4046, EIA 541, EIA 625, or ANSI/ESD S20.20 certified. Figure 5-13 shows a common hazmat bag for a computer hard drive.



Figure 5-13 *Hazmat Bag*

The process for bagging and tagging should be pretty straightforward. You should consider collecting anything that could store data as well as documents or manuals for those devices. This means anything such as a GPS, backup system, software, and IoT devices. We recommend assigning one person for collecting and logging assets to simplify the chain of custody documentation process. That person should make sure to include the current date, time, any serial numbers, unique features of the asset, and his name on each bag containing an artifact. If the artifact is believed to have wireless or cellular services enabled, you likely need to use some form of Faraday cage designed to block these types of communications. Some hazmat bags can provide Faraday cage functionality. If they don't, you may need to move the bagged artifact into a storage container that prevents these communications. The hazmat bag shown in Figure 5-13 is priced around \$70 US because it has Faraday capabilities.

Tracking who has access to the bagged artifact is critical. You need to maintain a digital log similar to what we have shown with Autopsy. Any time an artifact is accessed or moved, there should be a log of the event. You may have a dedicated log for chain of custody or include it with your forensics management software. When the asset is not being used, it must be contained in a secured storage facility typically called an evidence room. We discussed the evidence room in Chapter 3. Your chain of custody journey should be directly linked and enforced as a requirement before accessing an evidence room storing any artifacts being investigated.

In some cases, you likely can't bag and tag an artifact. For example, removing the device would impact the company in a negative way, the device is unable to be moved, there is data on the device not related to the case that can't leave the location, and so on. Examples include network devices such as routers that may have evidence of the crime

but also are currently routing live traffic on the customer's network. In these situations, your approach to investigate these devices will likely be different. Let's look more closely at this type of situation next.

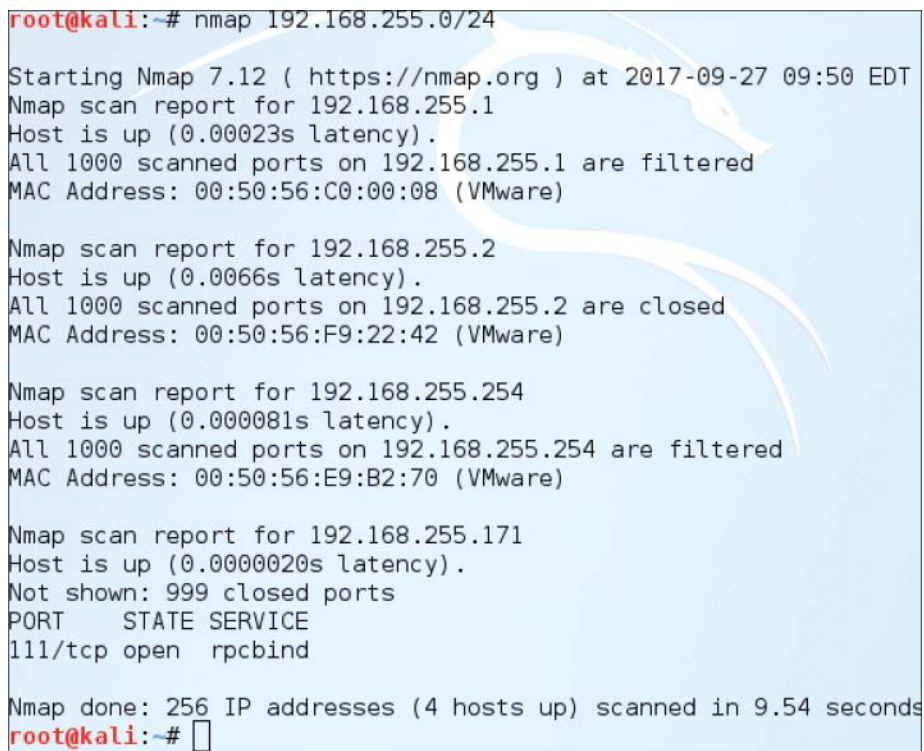
Network Investigations

This section describes how to investigate live network devices you are not permitted to power off or remove from a customer's location. Devices that could meet these criteria are routers, switches, firewalls, intrusion prevention technology, or even some huge power generators that physically weigh multiple tons and contain radioactive material. Powering down any of these devices could take a company offline and potentially cripple the business. A power generator like one found at a SCADA organization could be harmful if shut down. This means you need to obtain evidence without impacting the device's operational state. You could do this by pulling records directly from the device or looking at the device's digital footprint on the network.

In Chapter 8, we dive deeper into investigating networks, including tools used to detect threats within live traffic as well as historical captures of security events. An example of a historical capture is replaying a packet capture that recorded an event triggered by a security tool. For this section, we focus on the investigation process you should consider as you plan your approach to abstract evidence from these types of network-based devices. Think of this as obtaining records and data about what is happening between devices versus evidence pulled from end-user systems.

Before diving into a network, you should first understand the scope of what is considered in play. This means obtaining a network diagram, understanding how data flows from system to system, recognizing the types of data being processed, and highlighting which networks are to be considered for investigation, along with any devices found on those network segments that should be listed on your asset sheet. Devices that are not on the asset sheet but are going to be considered for the investigation should be evaluated using the preinvestment procedures covered earlier in this chapter. You may not be authorized to evaluate devices on the network for privacy or other reasons; however, you may have the green light to evaluate their network footprint. You still need to log any device on your asset list, regardless if you plan to access it and comment about its role for the investigation. This way, if you later discover one or more of these devices needs to be investigated due to recently discovered evidence, you can quickly identify what you currently know about the device.

You can use various tools to discover and validate devices on a network. The most common tool available on Kali Linux is Nmap, which is short for Network Mapper. The simplest use of Nmap is typing `nmap <scan type> <options> <target(s)>`. For example, you might type `nmap 192.168.1.0/24` to scan the entire 192.168.1.0 class C network. Another use could be typing `nmap -A thesecurityblogger.com` to enable OS and version detection for scanning thesecurityblogger.com website. Figure 5-14 shows a scan of a simple class C subnet with Nmap.



```

root@kali:~# nmap 192.168.255.0/24

Starting Nmap 7.12 ( https://nmap.org ) at 2017-09-27 09:50 EDT
Nmap scan report for 192.168.255.1
Host is up (0.00023s latency).
All 1000 scanned ports on 192.168.255.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.255.2
Host is up (0.0066s latency).
All 1000 scanned ports on 192.168.255.2 are closed
MAC Address: 00:50:56:F9:22:42 (VMware)

Nmap scan report for 192.168.255.254
Host is up (0.000081s latency).
All 1000 scanned ports on 192.168.255.254 are filtered
MAC Address: 00:50:56:E9:B2:70 (VMware)

Nmap scan report for 192.168.255.171
Host is up (0.0000020s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp   open  rpcbind

Nmap done: 256 IP addresses (4 hosts up) scanned in 9.54 seconds
root@kali:~#

```

Figure 5-14 *Nmap Example*

There are many ways to use Nmap, which you can find at <https://nmap.org>. In Chapter 8, we look deeper at using Nmap with Wireshark and SNORT to detect various forms of network attacks. From an investigation viewpoint, it is important to know that performing Nmap scans could trigger existing security solutions as well as add your digital footprint to the security logs you want to investigate. Mapping a network is a common step that attackers use after they breach a network; therefore, you need to make sure you are authorized to perform scans so that you don't upset the security group monitoring the network you are investigating. You also should document your device's network settings to ensure you do not impact the investigation in a negative way. You could use filters to weed out your device while searching logs and make notes about the IP address you used in the case file so that other investigators know what impact you had on the network during your investigation.

You can also run Nmap by downloading the Windows version of the software. There are also many other scanner tools available, such as Angry IP Scanner located at angryip.org. Whichever tool you decide to use, make sure to log your results in your case management tool. For our example, we use Angry IP Mapper and upload the results, as shown in Figure 5-15, to our forensic case file. We make comments on the case file about any

device found and label that device with relevant information regarding our investigation. For example, we may find that the device at 192.168.40.5 is a server that is currently being investigated, and the device at 192.168.40.10 is a laptop owned by an employee who is not part of the investigation. We want to make a note of the device so that later if we find evidence of this device during our network investigation, we could correlate any time the device was seen to see whether it needs to be evaluated based on probable cause found during the investigation.

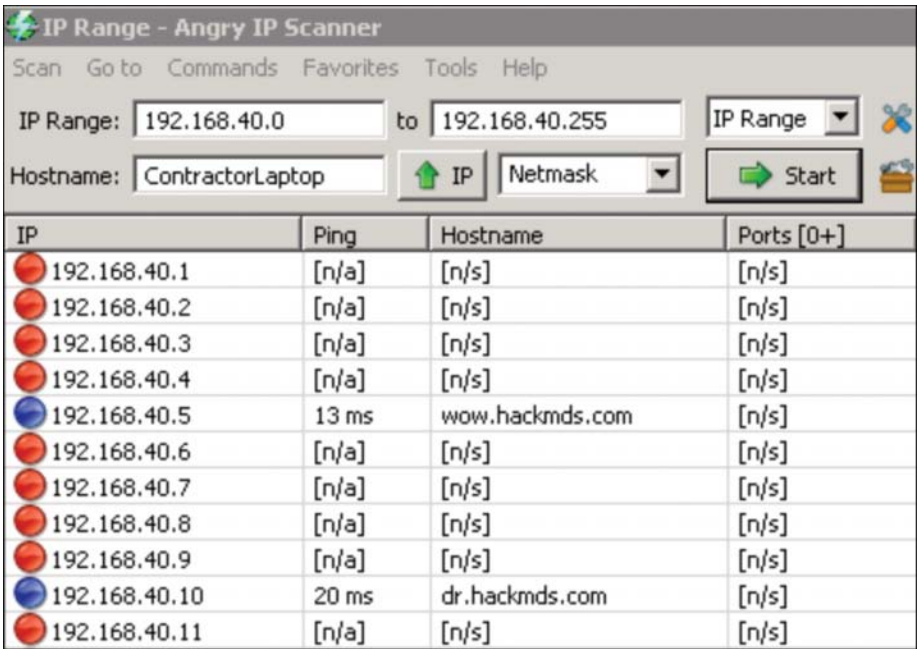


Figure 5-15 *Angry IP Scan*

You will likely want to diagram the network you are investigating based on what you find as you perform your investigation, regardless of whether a diagram is provided by the customer. Many times, people don't know what is on their network because networks constantly change after a diagram is developed. Many investigators use Microsoft tools like Visio, PowerPoint, or Adobe products to develop diagrams. One free version you could use is SolarWind's Draw.io at www.solarwindsmsp.com. This simple tool is cloud based, so you don't install software. It is effective at accomplishing your diagram needs. Other options are LucidChart and Dia Diagram. Figure 5-16 shows how to use the Draw.io software for building a basic diagram.

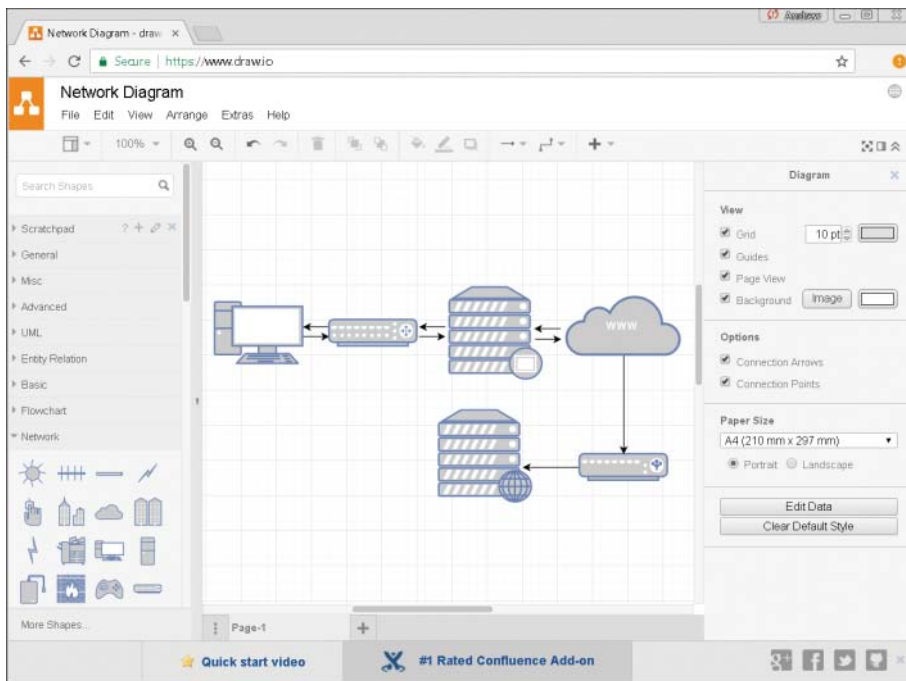


Figure 5-16 Draw.io Diagram

You will likely identify many security and network tools that contain logs. You need to collect logs, routing tables, application data, and any records from these tools that could be relevant to your case. Records need to be time stamped, labeled according to where they appear on your network diagram, and indicate who collected the data. Sometimes you are provided the data by an outside party, such as the asset owner, but best practice is to have somebody from your investigation team involved with the data collection so that it can be logged and validated properly. If you need to use another party to pull the data you are requesting, make sure to label that data with that person's contact information, time of work, and where it came from. We describe how to collect the various types of network data in Chapter 8.

Each piece of data should be organized in a separate folder pertaining to the device it was pulled from and filed in your case management program. One method we use is to create a folder representing the network and place any documentation used to validate the entire network, including scans and diagrams. Within that folder, we create folders for each device tagged and store any logs, packet captures, IP tables, and so on we have obtained for the device in that folder. This approach keeps our findings organized, simplifying linking data to where it was obtained. There is no wrong way to organize your findings outside of doing something that causes you to lose files. Looking back at our Autopsy example, we would create events within the software and label the folders storing each data artifact being captured.