2017

A Wi-Fi Router as a Witness Device

Image Credit: (hack-wi-fi-selecting-good-wi-fi-hacking-strategy, n.d.)

Daniel Arrugueta

3/15/2017

Abstract

Witnesses often are crucial elements in solving and prosecuting criminal or civil violations. We now regularly use data that various technologies record. Digital witness devices provide a source of largely unbiased and dependable information to the investigator and prosecutor. However, many often ignore or do not even recognize commonly available electronics as potential witness devices. One such device is the wireless router found in most homes and businesses. This paper will explore the identification, potential data, and exploitation of wireless routers to obtain relevant data. Additionally, this paper will discuss the basics of the technology, related technologies, and cautions for the investigator. A field investigator without access to professional assistance will be able to follow the paper's methodologies, as will a digital forensics professional.

Keywords: wi-fi, wireless, 802.11, MAC, media access control, IMEI, MEID, tower dump

Table of Contents

1. Introduction

The successful investigation of any crime and prosecution of any violation depends on evidence, some of it in the form of witness testimony. Witnesses take many forms, offer different perspectives, embody different abilities, and present different challenges to the investigator or prosecutor. A good investigator will identify potential witnesses; determine what they offer; and then review their accounts objectively in the light of individual witness characteristics. In the case of a "who-done-it" incident, a single reliable witness can break the case.

The investigator must consider and account for numerous witness characteristics, and we can look at a few of those. Is the witness reliable (McClure, Myers, & Keefauver, 2013)? Is the witness biased in any intentional or unintentional way? Was the witness where he could perceive what he claims? Does the witness correctly remember what she claims? Did the witness take notes about the incident? Do witness accounts agree and corroborate each other? You should consider digital devices, including Wi-Fi routers, as witnesses with the same considerations (Gleeson, 2016).

For the rest of this article, I will use the terms "digital device" and "device" generically to refer to any digital consumer product (cell phone, tablet, laptop, etc.). If a point requires distinction, I will specify it.

2. Digital Witness Devices and Wi-Fi Routers

Technology continues to change every aspect of our lives. We feed on a steady diet of embarrassing and revelatory videos and recordings. There seem to be cameras everywhere, and hot microphones continue to surprise celebrities and politicians. Businesses install cameras and

sometimes microphones for security and to protect themselves from liability. Cell phones record our call histories, contacts, texts, etc.

Investigators regularly exploit these sources for evidence (Nieto, Roman, & Lopez, 2016). Cameras, microphones, and digital devices thus become witness devices. We can evaluate witness devices in many of the same ways and through many of the same considerations as human witnesses using the criteria I previously listed. From here on, I will focus the discussion and concepts on Wi-Fi routers. I will avoid as much technical discussion as I can, but some background is necessary for you to conceptualize the processes, the data, and its purpose. This article contains hyperlinks to further information and resources. If you received a printed version and need the additional material, obtain a digital copy.

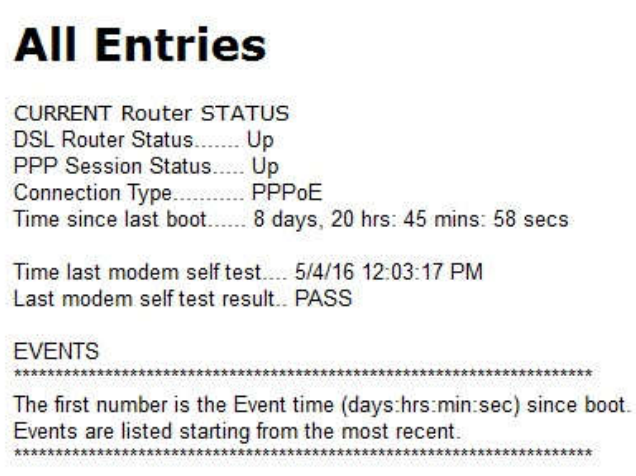
A Wi-Fi router typically is reliable in the sense that it does what it was intended to do. It will not lie or alter its data (i.e. the facts). The question of reliability then falls to two main areas: the integrity of your data, or did anyone influence or alter the original data; and how a human interprets and presents that data (Parate, & Nirkhi, 2012) and (Gleason, 2016).

Conversely, for reliability, manufacturers do not build Wi-Fi routers to do what an investigator wants. Most small-office-home-office (SOHO) routers are low-end products that simply provide wireless connections. They usually are not configured to keep detailed logs of their activity, and some cannot log activities at all. The less expensive the Wi-Fi router, the smaller its memory and the more limited its settings, storage, and capabilities. This small memory also will dictate what your Wi-Fi router "remembers" and for how long.

One last point on reliability relates to date/time stamps. If you successfully locate useful data, you must **CHECK THE TIME SETTINGS ON ALL THE DEVICES INVOLVED IN YOUR ACQUISITION**. Note and record the actual local time, the time shown on the computer

you are using, and any times, especially the most recent, reflected in your Wi-Fi router and its logs. If you see NTP or SNTP connections or access entries in a log, it means that the router reached out to an Internet based server to verify and synchronize its time setting (A list of the Simple Network Time Protocol (SNTP) time servers, 2016). These servers use GMT or UTC time settings that likely will not coincide with your local time (GMT: Greenwich Mean Time - World Time / Time Apps, n.d.) and (Current UTC — Coordinated Universal Time, n.d.). You must use this difference to offset the times in your logs and determine relevant data with regard to the time of your incident.

Figuring the correct time offset may be challenging when working on some routers. The following graphic shows that some Netopia routers use a base reference of "Time since last boot" of the router. You may need to create a known log event to correlate the local time to the router's "last boot" and the correct time correction.



Likewise, we can dispel most typical biases in a witness device. However, we must consider technical biases. For instance, the apparent colors seen in a video may be misleading due to the light conditions present at the time of recording. A Wi-Fi router's bias will be to prioritize connection attempts and successful connections. As discussed below, the router may see other signals in the area, but it will not create data from these signals.

If a Wi-Fi router was not where it could "see" or receive information, it may not be able to offer data. However, the absence of a recording or expected data may disprove a witness claim.

Wi-Fi routers' signal strengths will vary, as will the signal interference from their surroundings. These and other factors define the network's range, and I only can offer upper limit parameters of 150 feet indoors and 300 feet outdoors. Remember, these are maximum, best of all worlds' range estimates (Mitchell, 2017).

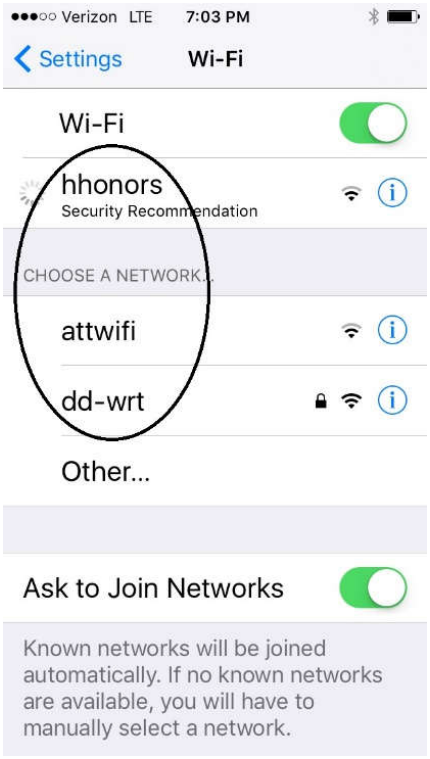
An ideal witness takes contemporaneous notes, and this also applies to a Wi-Fi router. A router's notes are logs, and whether your router keeps logs is dependent on your router model and setting. Specifically, we want connection logs. Whether the manufacturer built that model with the memory to keep logs and the default values to create logs are your initial thresholds.

Finally, let us consider corroboration. In what scenario do you have too much evidence or too many witnesses? Certainly, there is a point of diminishing returns when the volume of evidence becomes overwhelming, or the number of witnesses will tend to confuse or slow the case. However, for purposes of corroboration, I would rather have a large number of corroborating witnesses from whom to choose. Use the same analysis for witness devices, including Wi-Fi routers. If there is going to be a question about the validity or interpretation of a given data set, multiple data sets from disparate devices corroborate and strengthen all of your digital evidence.

If you think that a seized phone will render all of the data you will want or need, you may well be mistaken. Even if inconvenient, you need to collect (or designate someone to collect) all of the available digital data available to strengthen your case. A Wi-Fi router may provide evidence not available anywhere else. If a cell phone is set only to use Wi-Fi for calling or app use, getting phone subscriber data, call details, cell site records, and tower dumps will give you nothing.

3. Identifying Witness Devices

For purposes of identifying Wi-Fi routers as witness devices, you have numerous scanning options, beginning with your cell phone or any wireless capable device. The first option your device offers is the basic Setting/Wi-Fi selection. When you review the Wi-Fi section, your device tells you the available networks in the area as seen in the graphic. We will connect to and use the dd-wrt network shown last in the graphic (Unleash Your Router, n.d.).



As you can also see, I have my phone set to ask me whether to join networks. What we want is suspects who have their devices set to join automatically, which would create the connection and a logging event (Explanation of the Three-Way Handshake, n.d.).

Other options you have are specialized network identification tools and software, including directional (or Yagi) or high-performance antennas (The Yagi-Uda Antenna, n.d.) and (Khoomwong, & Phongcharoenpanich, 2016). While these tools may reveal more networks with weaker signals, they probably offer no benefit to you. You are looking for suspects whose devices connected using default abilities and variables to the strongest signal available. Their phones are looking for strong signals and easy access.

Note and document the networks in the areas, especially the unsecured networks. Some of these networks will be easily identifiable (e.g. McDonald's, Starbucks, etc.), while others will require further research to identify their source. You will need to know the physical locations of these Wi-Fi routers for most situations if you want to access their data.

4. The Passive Nature of the Connection

The key to a witness device's value is its passive nature. This is especially true when dealing with a Wi-Fi router. When you have a Wi-Fi capable digital device (e.g. a cell phone), it reads signals (beacons) from Wi-Fi routers in the area (Beacon frame, n.d.). The phone is looking for a visible network name or the Service Set Identifier "SSID" (SSID Definition, n.d.). At the same time, the phone sends out signals looking for the presence of Wi-Fi routers (actually networks) to which it previously connected. When you get home or to work and connect a cell phone to a password protected Wi-Fi network, your phone likely recorded the network name and the password you entered the first time. The next time you are in the area, your cell phone automatically finds the network and connects without the need to reenter the password.

Image Credit: (M., G., 2013)

If you, like many people, have a device set automatically to connect to any available network, whenever that device is near an open (unsecured) network, it will try to connect and record that network name for future attempts. We want this data from a router in hopes that it will include device identifiers ("MAC addresses" explained below) and a time/date stamp.

Note that the process of receiving signals from Wi-Fi routers in the area does not produce logs or recorded data on an individual device. The device must at least attempt if not complete a successful connection to a Wi-Fi router for any chance of recovering evidentiary data from the router.

5. Cautions and Warnings

If you will be exploiting Wi-Fi routers, you must be aware of inherent dangers. These procedures are for emergent situations when there are no digital forensics personnel available to respond to the incident scene. The more you research and know about this process, the safer you are and the better you can defend your actions.

a. Blame

If you are in a business setting, you likely will encounter multiple routers at the business, one or more of which are broadcasting Wi-Fi signals. The actions you will take to exploit the Wi-Fi router will not affect the wired network, the Point of Sale system, or the networked alarm devices. However, if anything coincidentally goes wrong while you are there or shortly after, you become a convenient target or excuse on whom to blame the problem. Bear this in mind and have a witness present. Also, take detailed notes, photograph the scene, photograph or screenshot the computer you use (theirs or yours), and document anything else that you do or see while accessing the router.

b. Changing Settings

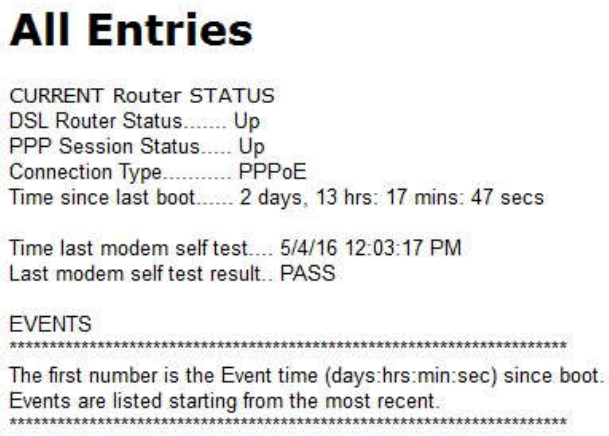
Exploiting a Wi-Fi router will requires a computer (or tablet) and the Wi-Fi router. The computer may be yours, or it may belong to the business or residence that owns the router. I will explain the basics of how the router works later, but understand that if you change its settings, it may no longer work as it did and may not broadcast the correct network name (Service Set Identifier or SSID explained below). Likewise, devices that used to connect automatically now will fail to connect.

Another issue lies with the computer you use. On a recent call, the agent trying to exploit a Wi-Fi router kept getting problematic network connections results. (The problems stemmed from IPv6 versus IPv4 addressing (IPv4 & IPv6: A Short Guide, n.d.). I will only discuss IPv4 in this article and forego a full discussion of the differences (Comparison of IPv4 and IPv6, n.d.).) To get around the issue, I had him change the network adaptor settings on his computer. If you are not sure or comfortable with these terms or issues, it is unwise to reconfigure your computer or, more so, someone else's.

c. Evidence Loss

If your Wi-Fi router did manage to record valuable data, it may be volatile and easily lost. Many routers lose their logs when they lose power. Further, any setting or selection that triggers a log reset will clear the data. I do not know of any simple process to acquire the Wi-Fi router's memory and forensically recover deleted data. Do not unplug the router or make any setting selection without carefully considering and/or researching what your action will cause.

In the next graphic, note that the router's date/time reference point is the "Time since last boot." This Netopia router's screenshot was taken two days after a power outage that cleared the logs and initialized the date/time setting.



6. Device Identifiers/Media Access Control Address

Every network capable device must have a unique Media Access Control (MAC) address, a device specific identifier (MAC Address, n.d.). That means that every device has its own

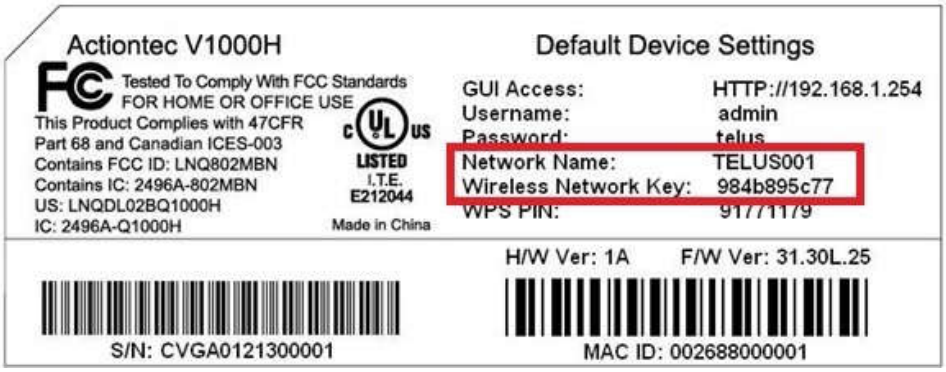
identifier that reflects the manufacturer and the individual device (analogous to a serial number for its network card). While not directly identifying an account or an individual, recovered router data later will confirm that a seized device (e.g. a cellphone) bears the same MAC address as one that connected to the router. In practice, finding a MAC address that corresponds to an Android device implies the likelihood that there is an associated Gmail account, and that Google may have a record of the MAC address and its owner and activity. Likewise for an Apple device and its corresponding data trail within Apple's servers.

Criminals can spoof MAC addresses, so eliminating that possibility may be necessary later in the investigation. However, as an initial lead, a MAC address is good evidence.

7. Accessing the Router

The first step to accessing the target router is to connect to it via network cable (Ethernet) or its wireless signal. This connection is necessary in order to access the router's control panel. While in typical situations, this would be a violation of forensic protocols, it is necessary to access the desired data. It also is more reason once again to stress the necessity for you carefully and thoroughly to document your actions. Note, too, that if the router is logging connections, your connection will show up on the log. You later can use this entry to help figure the time offset between the log times and your local time.

Connect to the router, whether by Ethernet (network) cable or via an actual wireless

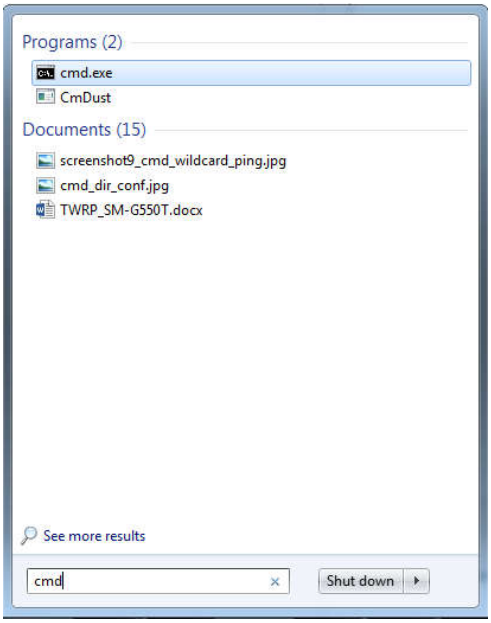


connection. If you connect via cable, your computer should automatically see the router, assign

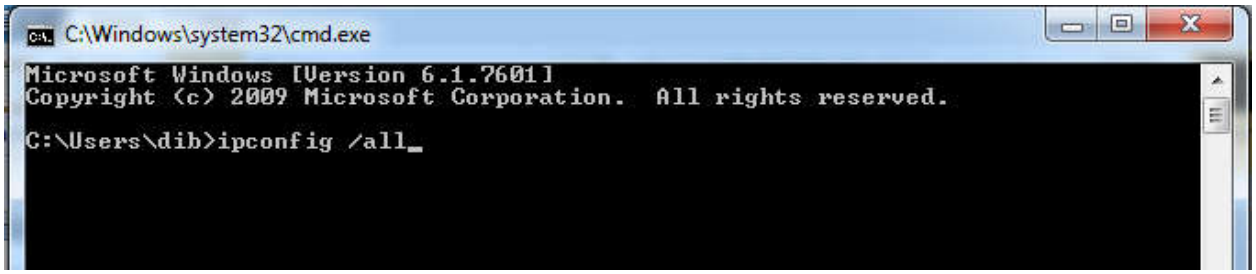
an IP address, and establish the connection. If your connection is via wireless signal, you will have to connect to the wireless network via either open network or using the network password if on a secured network (Telus, 2016).

Look on the router itself to see if it has a label reflecting a URL or instructions for accessing the router configuration. Some routers will allow access by entering a URL into your browser (URL, n.d.). See the accompanying graphic showing the IP address to type into your browser, as well as the Username and Password to access the router just above the red square showing the Network Name (SSID Definition, n.d.).

If you do not see such a label or information, the process is more entailed. In Windows, put your cursor in the lower left hand corner of your desktop and click on the Start button, the Pearl, or whatever Microsoft is calling it when you read this, and type, "cmd." The first option that appears should be a terminal icon. Click on, "cmd.exe," and open the terminal window. (The instructions from here on will be Windows-centric, although procedures for other operating systems will be similar.)

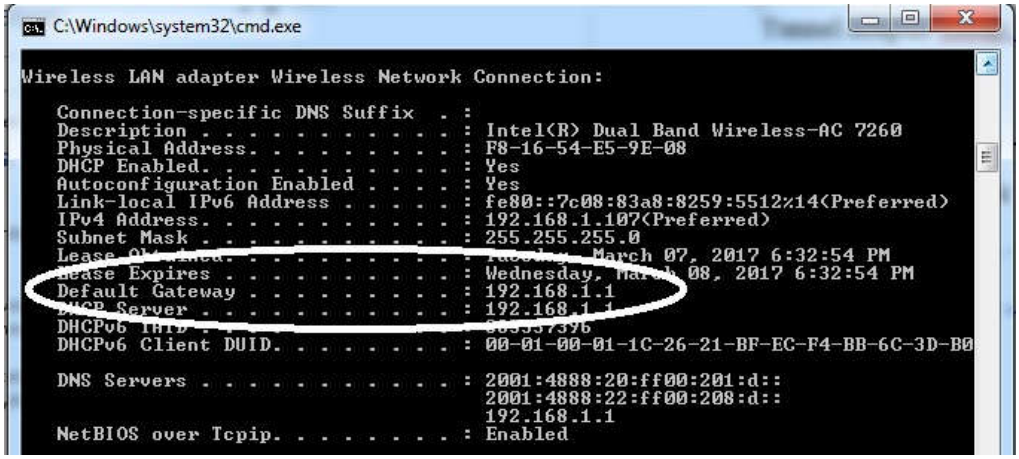


Once the window opens, type, "ipconfig /all." (For Linux and Apple devices, use "ifconfig.")



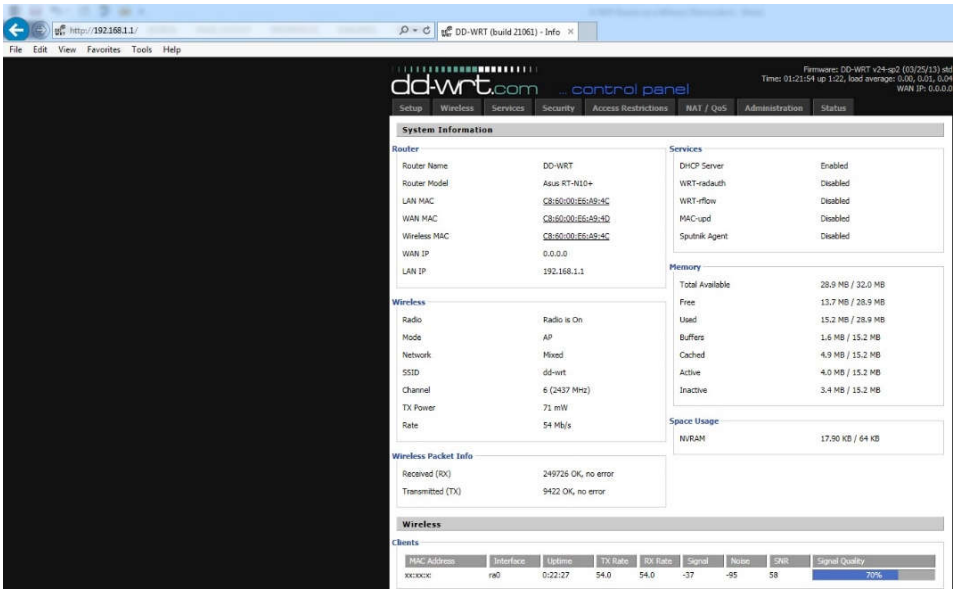
Now, you are looking for a “Default Gateway” to find the connection address you will need. If your connection is wireless, look for something that says Wireless LAN Adapter with a Default Gateway that has values entered. Depending on your computer and configuration, you may see several Wireless LAN Adaptors, but only one will have the Default Gateway value. See an example in the screenshot.

As you can see, the Default Gateway IPv4 address in this example is 192.168.1.1. It is likely that the address you will see will begin with a 192, but it may not.



If you connect directly to the router via Ethernet cable, you will look for Ethernet adapter Local Area Network Connection with a Default Gateway value. In either case, note the IPv4 address that you see.

Now, open an Internet browser and enter that Default Gateway IP address in the browser window. For our example, Internet Explorer is the browser, and we type the default gateway IP, preceded by http://, into the URL window as in the next screenshot (e.g. type out “http://192.168.1.1”).

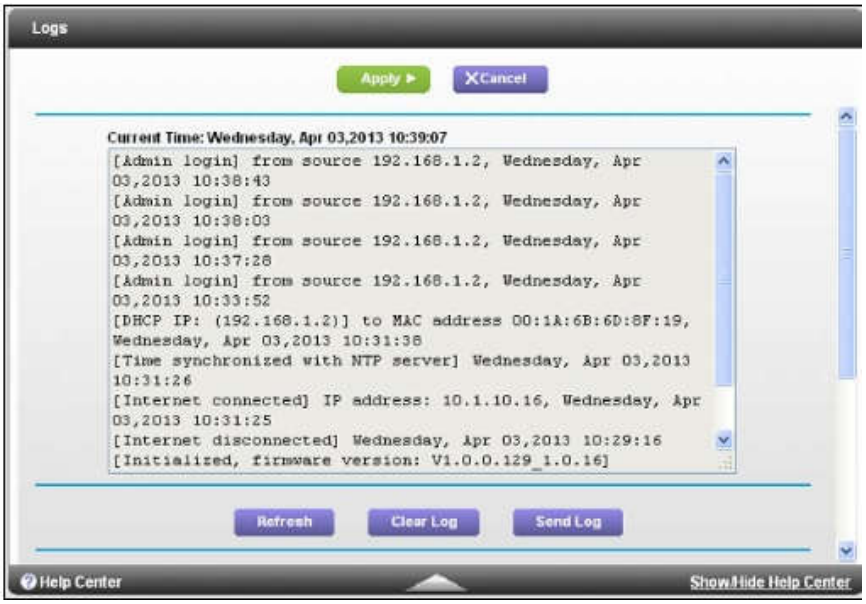


When you hit enter, the browser will open the initial router interface as if it was a web page. At this point, you will see some basic information about the router, but getting anything further will require logging into the router itself.

Selecting any of the subsequent tabs on the control panel results in a login prompt.

Most people never reset the default login name and password for their router (Craig, & Patryk, 2009). Look on the router itself for a label with the information as shown above. (See the Telus graphic under Section 7, Accessing the Router.) If you do not find one, search the Internet for "(router make/model) router default password." If the owner did change the default password, you will need someone to tell you what it is. There is no maximum number of attempts that will result in a locked or wiped router. If you have an idea what the login and password might be, you can attempt your guesses.

Once connected, you will have to determine whether and where the router has logs. Often, "Advanced," "Administration," or "Diagnostics" tabs are good places to start looking. Internet searches related to logging on your particular model are a good resource. For instance, a Netgear Nighthawk router can keep valuable logs and has online information available (How do I view the activity logs of my Nighthawk router?, 2016).



However, look at the screenshot. While it shows that a device connected, the date and time, and the device's MAC address, there is no "save log" selection available. "Send Log" will attempt to initiate an email client to transmit the log, but this may be a problem if you are using a business' computer. "Clear Log" will do just that and delete the log data. So the issue of how to save this data becomes important. If you are not sure, get help. Before you get help, write down the relevant entries and record the MAC addresses that may be important.

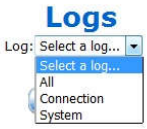
Generally, on a window like you see here, click on Cntl+A (the Control key and the letter A key at the same time) to see if that selects all of the data in the log (Keyboard Shortcuts for Windows, n.d.). If it does, either right click and "Copy," or Cntl+C. Now paste what you copied into Note, Notepad, or some other text editor and save the file to your own flash drive or other media.

If Cntl+A did not select all of the text, you may double click on a word within the log to highlight it. Now do a Cntl+A, copy the text, and follow the same steps as above to save the log. You also may be able to place your cursor within the log, hold down your left mouse or touchpad button, and scroll through the relevant area to select it.

If all else fails, determine if you need to figure in a time offset as mentioned above. Find the relevant time of your incident and any potentially relevant portions of the log. With the data showing on the screen, take a screenshot of what is on the monitor by using Cntl+PrntScrn (Control and Print Screen) or whatever steps correspond to the computer you are using. Alternatively, use a camera, even a cell phone camera, to photograph the relevant portions of the logs. Save the screenshots or photos to your media, or paste a series of these screenshots into a graphics-capable text document that you then save.

On a Linksys router, the logs may be under Router Settings/Troubleshooting/Logs as you can see in the next graphic. Each manufacturer will determine where the router keeps its logs, if the router created them at all (Linksys Official Support - Enabling the Logs feature using your Linksys Smart Wi-Fi Account, n.d.).

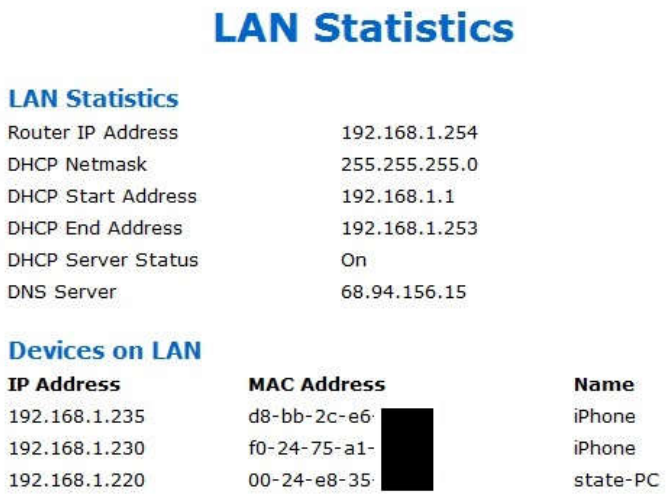
Occasionally, the tabs and labels you find will be misleading. Though a Netopia router may show you a choice for Logs/Connection, you actually have to select "All" to see the connections, IP assignments, and MAC addresses as seen in the next screenshot.




```
08:19:17:30 LHD: IP  192.168.1.220, MAC 00-24-e8-35-
08:19:16:01 TR-069: ACS URL not resolved
08:19:16:01 TR-069: Resolving ACS URL - Retry 6338
08:19:14:01 TR-069: ACS URL not resolved
08:19:14:01 TR-069: Resolving ACS URL - Retry 6337
08:19:13:28 LHD: Interface  N/A, State
08:19:13:28 LHD: IP  192.168.1.133, MAC a0-ed-cd-6e-
08:19:12:01 TR-069: ACS URL not resolved
08:19:12:01 TR-069: Resolving ACS URL - Retry 6336
08:19:10:01 TR-069: ACS URL not resolved
08:19:10:01 TR-069: Resolving ACS URL - Retry 6335
08:19:08:27 LHD: Interface  N/A, State
08:19:08:27 LHD: IP  192.168.1.230, MAC f0-24-75-a1-9d-65
08:19:08:27 LHD: Interface  N/A, State
08:19:08:27 LHD: IP  192.168.1.46, MAC 28-ef-01-38-
08:19:08:25 LHD: Interface  N/A, State suspect
08:19:08:25 LHD: IP  192.168.1.230, MAC f0-24-75-a1-
08:19:08:25 LHD: Interface  N/A, State suspect
08:19:08:25 LHD: IP  192.168.1.46, MAC 28-ef-01-38-
```

The connection history clearly shows numerous MAC addresses and their related connection details. (I partially obscured the MAC's.)

Another misleading tab on the Netopia dealt with locating currently connected devices. Instead of being a separate data point under the Wireless statistics, the logs listed all connected devices under LAN Statistics. (Again, the MAC's are partially obscured.)



LAN Statistics

LAN Statistics

Router IP Address	192.168.1.254
DHCP Netmask	255.255.255.0
DHCP Start Address	192.168.1.1
DHCP End Address	192.168.1.253
DHCP Server Status	On
DNS Server	68.94.156.15

Devices on LAN

IP Address	MAC Address	Name
192.168.1.235	d8-bb-2c-e6-	iPhone
192.168.1.230	f0-24-75-a1-	iPhone
192.168.1.220	00-24-e8-35-	state-PC

8. Next Steps

If you successfully collected relevant log information, use appropriate legal process to try to obtain further information about your suspect device(s). This may prove difficult and convoluted depending on the service provider you approach. You can also use tower-dump device registration data to cross-reference and corroborate your findings.

There are important considerations related to tower dumps. First, the data I am referencing here is "registration" data, not call data (Rothman, 2009). Mobile devices send out requests to identify cell towers in the area. As each tower responds, the device keeps a record of the tower, and the tower records the identification of the device in case of a call or data request. In a heavily trafficked area, this tower data may overwrite in less than twenty-four hours. In most situations, seventy-two hours is a generous threshold. If you want this data, you need to proceed with exigency. Secondly, the cellular response from a tower dump will be voluminous. You need to limit your time window as much as possible in your legal request.

Wireless providers maintain device MAC addresses, as well as the expected mobile identifiers (IMSI, IMEI, MEID, etc.). If you captured a device MAC, you can serve wireless providers with legal process for subscriber information corresponding to the MAC address that you seized. By calling the providers individually, they may tell you whether that MAC is registered on their network, however, they often refuse to divulge any information until they receive a legal demand. Pursuing this route is analogous to seeking tower dump data where you have to serve every provider in the incident area. If any telecoms reply that they do not maintain MAC information, you have other options.

In addition to approaching Google or Apple for information, there is another avenue for identifying the device from its MAC address. (The MAC address identifies the wireless network card within the device.) A cell phone's International Mobile Equipment Identity (IMEI), or the CDMA equivalent, the Mobile Equipment Identifier (MEID), is associated with the device's MAC address during manufacture (International Mobile Equipment Identity, n.d.) and (Mobile Equipment Identifier, n.d.). The first half (the first three sets of double characters) of the MAC address comprises an Organizationally Unique Identifier (OUD) (Organizationally Unique

Identifier, n.d.). You can check these OUI's online to determine the type of device for which you are searching (MAC Address and OUI Search, n.d.).

Once you know the manufacturer of your suspect phone, you can send that manufacturer legal process requesting the IMEI corresponding to the MAC address you acquired. The IMEI also will identify a particular phone, but it does this using a data point that cell providers will recognize and for which they can provide subscriber information and history. You will need to contact providers to determine if the device is on their respective networks. There is no guaranteed correlation between an IMEI and a carrier, other than technological requirements dealing with GSM (AT&T and T-Mobile) and CDMA networks (Sprint, U.S. Cellular, and Verizon) (Segan, 2015).

9. Using Logs from Password Protected Networks

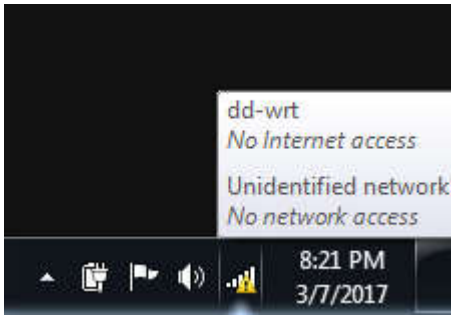
In most situations, you will look for open or "unsecured" networks to which a potential suspect's phone connected automatically. However, let us consider the situation if you have a secured network router as a witness device.

To join a secured network, you need the password to authenticate and allow the connection. Most people have their phones set to save the password and automatically rejoin networks as already mentioned. From then on, whenever you are in range of that secured network, your phone will join automatically.

In the case of an incident where you had a secured network and there is a log, you should check for any connections around your incident time. Any successful connections establish two facts: 1) the MAC address of the device that connected; and 2) the device that connected had the password stored. This indicates that the device had connected to this network on previous

occasions, and the device owner knew the password at some point. If you find this, you could have an inside violator involved in the offense.

10. Proactive Use



In our example, we connected wirelessly to a Wi-Fi network that could have been set to log connections and even to transmit those logs to a remote server. However, note the next screenshot that shows that the sample router for this article did not have Internet access. Wireless devices just look for available Wi-Fi networks, whether or not there is an Internet connection. You could use such a configuration as a "honeypot" at a desired location capturing MAC addresses for later use or for generating leads (Parate, & Nirkhi, 2012). By setting up a Wi-Fi router that you configured to log connections, you can start recording MAC addresses that join your router and know that they were within the range parameters we discussed.

11. Consider the Evidence from Both Sides

Whether or not you manage to capture connection data from a Wi-Fi router, the network's existence still may prove useful. As mentioned above, when a device (cellphone, tablet, computer, etc.) connects to a network, it keeps a record of that connection. When you extract the data from a device, the data may include a list of networks to which the device connected at some point. (Unfortunately, these records often do not include a date/time stamp.) However, even if the unsecured Wi-Fi router you investigated did not keep logs, showing that a cell phone connected to the router at some point still may be valuable to your case by placing the device at the location.

12. Summary

Witness devices offer the same value to an investigation as a human witness and arguably more objectively. While exploiting these methods entails a learning curve, using proper care as provided here, you might now safely attempt the procedure. Otherwise, you may be able to ask for help from digital forensics personnel. After reading this, you now know that these devices may be present and of use when conducting your next incident investigation.

See below for the summarized collection steps, but please ensure that you understand Section 5 – Cautions and Warnings. I hope you found this informative and useful. Please contact me if I can answer any questions about what you read.

Caveat: The content of this communication is entirely my own and does not reflect the opinions of or endorsement by any federal agency or the government as a whole.

References:

1. A list of the Simple Network Time Protocol (SNTP) time servers. (2016, January 19). Retrieved March 15, 2017, from https://support.microsoft.com/en-us/help/262680/a-list-of-the-simple-network-time-protocol-sntp-time-servers-that-are-available-on-the-internet
2. Beacon frame. (n.d.). Retrieved March 15, 2017, from https://en.wikipedia.org/wiki/Beacon_frame
3. Comparison of IPv4 and IPv6. (n.d.). Retrieved from http://www.ibm.com/support/knowledgecenter/ssw_ibm_i_71/rzai2/rzai2compipv4ipv6.htm
4. Craig, V., & Patryk, S. (2009). Insecurity by Obscurity: A Review of SoHo Router Literature from a Network Security Perspective. Journal of Digital Forensics, Security and Law, Vol 4, Iss 3, pp 5-16 (2009), (3), 5.
5. Current UTC — Coordinated Universal Time. (n.d.). Retrieved March 15, 2017, from https://www.timeanddate.com/worldclock/timezone/utc
6. Explanation of the Three-Way Handshake. (n.d.). Retrieved March 15, 2017, from https://support.microsoft.com/en-us/help/172983/explanation-of-the-three-way-handshake-via-tcp-ip
7. Gleeson, J. (2016). The judge, the advocate and the expert witness – revisiting the seminal views of Sir Owen Dixon in the modern context. Australian Journal of Forensic Sciences, 48(4), 366-380. doi:10.1080/00450618.2016.1152573
8. GMT: Greenwich Mean Time - World Time / Time Apps. (n.d.). Retrieved March 15, 2017, from https://greenwichmeantime.com/
9. *hack-wi-fi-selecting-good-wi-fi-hacking-strategy* [graphic]. (n.d.). Retrieved from https://img.wonderhowto.com/img/24/65/63570569473000/0/hack-wi-fi-selecting-good-wi-fi-hacking-strategy.1280x600.jpg
10. How do I view the activity logs of my Nighthawk router? (November 28, 2016). Retrieved March 24, 2017, from https://kb.netgear.com/24224/How-do-I-view-the-activity-logs-of-my-Nighthawk-router
11. International Mobile Equipment Identity. (n.d.). Retrieved March 22, 2017, from https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity
12. IPv4 & IPv6: A Short Guide. (n.d.). Retrieved from http://mashable.com/2011/02/03/ipv4-ipv6-guide/
13. Keyboard Shortcuts for Windows. (n.d.). Retrieved from https://support.microsoft.com/en-us/help/126449/keyboard-shortcuts-for-windows
14. Khoomwong, E., & Phongcharoenpanich, C. (2016). Design of a Dual-Band Bidirectional Antenna Using Superellipse-Monopole-Fed Rectangular Ring for IEEE 802.11 a/b/g/n Applications. International Journal of Antennas & Propagation, 1-11. doi:10.1155/2016/9368904
15. Linksys Official Support - Enabling the Logs feature using your Linksys Smart Wi-Fi Account. (n.d.). Retrieved from http://www.linksys.com/us/support-article?articleNum=143693

16. MAC Address and OUI Search. (n.d.). Retrieved from http://www.whatsmyip.org/mac-address-lookup/
17. M., G. (2013, May 29). 10 Modi per Amplificare il Segnale Wifi di Casa. Retrieved March 22, 2017, from http://www.tecnomani.com/10-modi-per-amplificare-il-segnale-wifi-di-casa/
18. MAC address. (n.d.). Retrieved March 15, 2017, from https://en.wikipedia.org/wiki/MAC_address
19. McClure, K. A., Myers, J. J., & Keefauver, K. M. (2013). Witness Vetting: What Determines Detectives' Perceptions of Witness Credibility?. Journal of Investigative Psychology & Offender Profiling, 10(3), 250-267.
20. Mitchell, B. (2017, February 28). What is the Range of a Typical WiFi Network? Retrieved March 15, 2017, from https://www.lifewire.com/range-of-typical-wifi-network-816564
21. Mobile Equipment Identifier. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Mobile_equipment_identifier
22. Nieto, A., Roman, R., & Lopez, J. (2016). Digital Witness: Safeguarding Digital Evidence by Using Secure Architectures in Personal Devices. IEEE Network, 30(6), 34-41. doi:10.1109/MNET.2016.1600087NM
23. Organizationally Unique Identifier (OUI) https://en.wikipedia.org/wiki/Organizationally_unique_identifier
24. Segan, S. (2015, February 6). CDMA vs. GSM: What's the Difference? Retrieved from http://www.pcmag.com/article2/0,2817,2407896,00.asp
25. Parate, S., & Nirkhi, S. M. (2012). A Review of Network Forensics Techniques for the Analysis of Web Based Attack. International Journal of Advanced Computer Research, 2(6), 114-119.
26. Rothman, W. (2009, March 20). Giz Explains: How Cell Towers Work. Retrieved from http://gizmodo.com/5177322/giz-explains-how-cell-towers-work
27. SSID Definition. (n.d.). Retrieved from http://www.pcmag.com/encyclopedia/term/51942/ssid
28. Telus. (2016, July 5). Retrieve Your Wireless Network Password. Retrieved March 24, 2017, from https://www.telus.com/en/bc/support/article/forgot-wireless-network-password
29. The Yagi-Uda Antenna. (n.d.). Retrieved March 21, 2017, from http://www.antenna-theory.com/antennas/travelling/yagi.php
30. URL. (n.d.). Retrieved March 15, 2017, from https://en.wikipedia.org/wiki/Uniform_Resource_Locator
31. What's My IP Address?. (n.d.). Retrieved March 22, 2017, from http://obsolete.whatsmyip.org/

Appendix A

Summarized Steps:

Here are the summarized steps to check for and extract router logs. If you need further information, please refer to Section 7 above.

a. Identify potential witness devices

b. Make detailed notes of what you are about to do

c. Connect to the router(s), either by Ethernet cable or by joining the network

d. Open Command Prompt/Terminal window

e. Determine the Gateway IP address

f. Open a browser and access the IP address to bring up the router control panel

g. Log into the router's interface

h. Locate and review logs (if present)

i. Save log data by exporting logs, copying log data into another document, or photographing the relevant log data.