this can be very useful to the criminal as well as the investigator. Changing the IP addresses of the proxy servers used makes the user far more difficult to find. Finding these “free” proxies is as simple as searching Google for the term “free proxy.” Many sites maintain these lists for a variety of uses and not just for use by criminals. Persons in countries that don’t allow free and unabated access to the Internet, or those trying to prevent a repressive government from finding postings on a blog, use these proxies.

So how is this different than a web-based anonymous service? Well, a web anonymizer is a website that offers the proxy services for your web browsing. This communication uses an application protocol, specifically, Hypertext Transfer Protocol (HTTP). Internet Explorer, or any other browser or tool will use HTTP. The free proxy servers on the Internet are servers that can be connected to by various tools to reroute your Internet traffic. This can be your browser, but it can also be, an Internet Relay Chat (IRC) client or any other Internet tool that allows the user to set up a proxy connection through another server. This routes the tool’s traffic through the IP address of the proxy server thus hiding the tool’s Internet traffic. In Figure 9.5, you can see that the Local Area Network (LAN) settings are rerouted through the IP address listed as the proxy.

To Tor or not to Tor

The Onion Router (Tor) is a significant tool in the “I need to hide on the Internet” world (Figure 9.6). Tor was developed from a concept originally written about by the US Navy. According to the Tor website, “Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location” (Tor Project Anonymity Online).

Your browser normally makes a call out through your Internet Service Provider to servers on the Internet. These servers easily identify who you are by your IP address so they can communicate back with you. This exposure of your IP address is what can tell the target who you are and possibly where you are in the world. The Tor network in its simplest description strips that information out and only provides the end user with an IP address belonging to the Tor network and not you. Thus you have effectively hidden from the end website you are visiting or target user that you may be communicating with through the Internet (Please note this is an over simplification of the process and exact details of how the Tor network works can be found on the project website). The current Tor Browser bundle installs its own browser version that does not allow the user to change the proxy settings in the browser. You can still use the installed “Vadalia” (like the onion) package to proxy your own browser through the Tor network, although the Tor project no longer recommends this practice.
Using Tor during online investigations is much easier now than in the past. This is due to the increase in most users’ Internet bandwidth, the constant upgrading and improving of the Tor software and its easy integration into the popular browsers. So how does the investigator implement Tor during their investigations? Well, the simplest method is to use the Tor network to hide browsing activity. If you are investigating a webpage or website, we know that there is certain information that our browser tells that server or website about who we are and potentially where we are. Our browsers can reveal our IP addresses, what kind of browser we are using, and its version. We can use Tor to prevent a suspect webpage from identifying us.

Using Tor in your investigations is as easy as downloading it and installing the Tor browser. Go to the Tor project website (www.torproject.org) and download the current Tor Browser Bundle Windows installer. Click on the

![LAN setting tab showing proxy settings in Internet Explorer.](image)

FIGURE 9.5
executable file and the Tor project installs. Previous versions of Tor required setting the proxy settings in your browser to use the Tor network, but this is all done automatically during the installation of the latest Tor browser bundle.

The Tor project has a page you can go to that will verify that you are using the Tor network properly or you can go to one of the websites on the Internet that grabs your IP address like http://whatismyipaddress.com/ to identify what IP address you are exposing to the world.

We are now ready to go online and start our investigation without being identified. Things to note here. The online application being used by the Tor network in this configuration is the Tor browser. If you send an email to the target from your normal email client on your desktop, use another browser, instant messaging, or use P2P software you will potentially expose who you really are by your IP address. To use any other applications through the Tor network you need to set them up to use the Tor proxy settings.

Other things to consider if you are not using the Tor Browser Bundle is that your browser set up needs to turn off the running of scripts, ActiveX, and cookies. Also block pop-ups. But you say “I can’t access all the good content on the Internet”. Correct, you can’t but then the end user can’t identify you either through holes in these protocols. Each of these features enhance our web surfing experience, but they also require a code be downloaded through your browser and run on your machine. This can allow for the code to default to a port in use that is not being redirected to the Tor network, thereby exposing who you are. This may not be important in all the cases you work, but be aware of it. If you lock down your browser and don’t get the content you want, you can always relax the

FIGURE 9.6
Tor network.
controls and go back and look at the site. You know at least the risks and can make a decision based on the needs of your investigation (Figure 9.7).

**Tor’s hidden web services**

Gormley (2011) wrote a short article which described how drugs were blatantly being sold on the Internet and members of Congress were very concerned and demanding an investigation. Selling drugs on the Internet is nothing new. The place on the Internet “openly” selling drugs was on the Tor network through the

---

**FIGURE 9.7**

Comparison of Internet hiding tools.
use of Tor’s “Hidden Services” function. The “Silk Road” is an online market open for the sale of goods and named after the ancient road used to bring goods from the Orient to the West. (The person behind the Silk Road hidden service was arrested by the FBI as this book was going to print. Goldstein 2013). For the power users, the Tor network’s hidden services are probably nothing new. For the average online investigator though, you may have heard of Tor and may have even tried to use it. But were you aware that webpages can be concealed within the Tor network? Have you ever seen a “.onion” domain name? Hidden services were introduced to the Tor network in 2004. They are run on a Tor client using special server software. This “hidden service” uses a pseudo top-level domain of “.onion”. Using this domain, the TOR routes traffic through its network without the use of IP addresses. To get to these hidden services, you must be using the Tor network.

How do you find sites using these hidden services? Well there is not a real “Google” for finding these sites, but there are lists of the addresses that can be found on the Tor network such as the Core Onion at http://eqt5g4fuenphqinx.onion/.

Core.onion, according to its hidden services site, has been in the network since 2007. Once on the Tor network and after accessing the Core.onion, you will find a simple directory to start exploring hidden services on the Tor network (Figure 9.8).

TorDir is another directory of hidden services. It gives you access to a variety of sites that offer instant messaging services, email, items for sale, social media—type sites, and marketplaces, all concealed through the Tor network. In the markets, a variety of things are for sale, and many appear on their face to be illegal. You can find sites for the purchase of illegal drugs, pornography, including sites with descriptive names indicative of child pornography and downloads for
hacked versions of various software. File sharing also looks to be popular and can be found in several .onion sites (Figure 9.9).

Users of IRC can find similar hidden services on Tor. The Freenode website at http://freenode.net/irc_servers.shtml gives clear instructions on how to access Freenode IRC servers on Tor’s Hidden Services.

Tor is not the only anonymization service on the Internet. Ip2 is another anonymizing network that is becoming increasingly popular, which has its own “eep-sites” similar to the hidden services offered in Tor that a user can post content to like a website. Hidden services on both the Tor network and Ip2 are going to increasingly become a location that will be misused by criminals. It will also become a place on the Internet that investigators will need to become familiar with if they are to further their online investigations.

Tor and tails

Investigators that have a significant need to hide their computing system and ensure that they won’t be recovered can use a tool like the Amnesic Incognito Live System (Tails). Tails is a bootable DVD or USB drive that implements the Tor project. Tails uses the Debian Linux operating system. Using a bootable DVD or USB bypasses a computer’s operating system, with all programs being run from the DVD or USB, and loaded into the machine’s Random Access Memory (RAM). In this way data is not saved to the computer’s hard drive, even unintentionally.

Tails’ advantage is that the system uses the binaries on the DVD or USB that have been solely designed to prevent any possible exposure of the user to others on the Internet. The bootable DVD or USB drive implementation runs on its own operating system and has a solid implementation of the Tor project’s network.
This helps to ensure that the system used cannot be identified from someone wishing to identify the computer used. The downside of using Tails is none of the Windows-based collection tools previously noted will work (Figure 9.10).

**INVESTIGATIVE TIP**

**Evidence Collection in Tails**

There are some programs built into Tails as part of the Debian-based Linux distribution that can be used to collect evidence. The important thing to remember in using these programs is to save all files to your desktop and transfer them to your USB device before you shut down the program. Otherwise, the files created will be lost when the system is shut down. Two basic tools are GIMP and Open Office. Locate GIMP and start the program. After it has loaded, select File and Create, which will provide an option to capture a screenshot. After capturing a screenshot, save it to the desktop. Open Office can be used to capture text. Locate the program and open it. Capture text or make notes as you would in any word-processing program. Again, save the created file to your desktop. You also can still use the “Save As” feature in the built-in browser, which is Firefox. Again, whatever you capture or create should be saved to the desktop and moved to a USB device.

**Tracking criminals who use anonymous methods to hide**

We have discussed many tools to use to hide ourselves online. We know our investigative targets can do the same thing. So how is it that we can track those who use these kinds of services for criminal purposes? There are many different things that can be done mechanically to track criminals online. What the investigator needs to know at the start is that a knowledgeable criminal maintains their security and use of the technology to prevent identification and will be harder to locate and identify than those that are not as diligent. One of the best methods of
identifying people online is the same tactic that hackers have used for years, social engineering. In the context of Internet investigations, social engineering is the act of manipulating people to do something or reveal information.

This kind of tactic has long been the criminal’s mainstay. A simple but effective ruse could be faking a telephone call to the target stating your calling from the company’s “Help” desk. The criminal asks the target for assistance with an issue. During this conversation the criminal gets the target to reveal his login and password as he is helping work through a computer problem on the network. This seems overly simple and unlikely, but it is how many famous hackers like Kevin Mitnick got the right information to allow access to networks they were attacking. Kevin Mitnick has said that “Social engineering is using manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, and the request is usually to release information or to perform some sort of action item that benefits that attacker.” Investigators when trying to identify those using anonymization need to be thinking in the same terms. Get the criminal to reveal certain things about themselves that they would not normally do. Security-conscience targets are probably less likely to do this; however, everyone makes mistakes.

CRIMINALS USING ANONYMIZATION

If you ask Hector Xavier Monsegur, aka Sabu, about what whether or not using anonymization is a good thing, you might get a loud “Yes.” As a member of the LulzSec hacking group, an offshoot of Anonymous, he regularly protected his identity through the use of the Tor. According to articles about his arrest he logged into a channel on IRC one time without using Tor and revealed his actual IP address. The FBI was able to use this information to identify who he was and charge him with crimes related to his hacking. The lesson on both sides is that when anonymization tools are used they can effectively hide your activity, both criminal and investigative. However, one slip and your real identity can be revealed. For law enforcement, this can ruin months of work and the potential prosecution of the targets.

Tools for catching the hiding Internet target

The basics of catching a target hiding on the Internet require that there be some interaction in most cases. That interaction could be trading an email, communicating in a chat room, or getting them to visit a website or social media page. In each of these situations, there are things that could be implemented that might help to reveal usable information about the target. The investigator has to remember though that the information identified online may be an IP address that is hidden behind a proxy or other hiding technique. Identifying the real IP address used by the target could lead to identifying the real person who is the target of the investigation. You can easily identify if the target is using the Tor network by checking the IP address you have through the publicly available list of exit nodes used by the Tor network. The Tor networks’ last server on its network is called the “exit node.” This is the last computer server in the Tor chain that is identifiable by the investigator in the network. You can identify this IP address by going to the Tor Project website,
www.torproject.org, and checking around on their project portal pages. They have a public list of the exit nodes for research purposes.

We can start with the simplest of the tools for identifying a target and that is an email. We spent some time in Chapter 8 talking about IP addresses and tracing them to their source. Reading an email header, if not spoofed, can give the investigator a direction to locate the target. Other effective techniques that can be used are tools like those from ReadyNotify.com or AnonymousSpeech.com. These websites offer tools that add content to the email, or documents attached to the email, that when opened by the target can track the target’s IP address. Each of these services will identify the receiver’s IP address. There are limitations with their usage. Some email tools like Microsoft Outlook require that the attachment be accepted to allow for the tracking tool to work.

**More proactive methods**

There are some more proactive methods of identifying anonymous users on the Internet. Two companies have tools that can add in this more technical method. This is far beyond the basic level but is worth mentioning here for the basic investigator to know that with the right skills and technology most targets can be found. The Gamma Group, a British company, sells its software to governments solely for criminal investigations. Its product FinSpy, part of the FinFisher product suite, is a proactive tool used to identify, track, and monitor targets on the Internet. Details on the tool are limited publicly but some reports identify that it is being deployed around the world in various investigations.

Another tool designed specifically to assist in the identification of Internet users of anonymous technology is ACAV by Vere Software. Under a grant from the USDOJ, Vere Software and their partner, the University of Nevada, Reno’s Computer Science and Engineering Department, developed a tool called ACAV. ACAV was designed to assist state and local law enforcement investigators identify criminal users of anonymization. Both of these companies reportedly release their tools only to law enforcement investigators.

---

**THE HEWLETT-PACKARD LESSON**

In 2006, Hewlett-Packard investigators were called to task by the government for the techniques they used to ferret out an insider who was leaking sensitive information. One of the techniques used was web bugs via ReadyNotify.com. McMillian (2006) article notes: “When the question of whether web bugs are legal has been tested in the United States, courts have tended to focus on whether this type of technology violates federal wire tapping laws,” says Chris Jay Hoofnagle, senior staff attorney with the Samuelson Law, Technology and Public Policy Clinic at the University of California, Berkeley. Hoofnagle says “State courts could take up the issue of web bugs, considering the existence of anti-hacking laws in states such as California. California law prohibits certain uses of computer resources without the permission of the user, and nobody knows for sure whether HP’s actions would violate this law or similar statutes in other states.”

None of the HP investigators got into legal trouble for the use of web bugs. However, several did get into legal hot water for how they used the technique called pretexting to convince...
telephone companies to provide confidential information. In one case, the investigator used the target’s own Social Security number, thereby committing identity theft, to convince the telephone company to provide the confidential information. One result of this case was the passage of the Telephone Records and Privacy Protection Act of 2006, which prohibits pretexting to buy, sell, or obtain personal phone records, except when conducted by law enforcement or intelligence agencies.

The bottom line as always is seek legal advice for your investigative procedures before you use them (Figure 9.11).

Other methods of identifying Internet users can be through web bugs, or web beacons, designed especially for embedding in a webpage. This is already a common practice within the marketing community. Google Analytics is a commonly used web bug inserted into a webpage to track users. This same concept can be used to track and identify a target during an investigation. These can be web beacons, which are small objects embedded in the webpage, that when loaded by the user’s browser make a call back to a server controlled by the owner. Tynan (2013) notes there were more than 1,300 tracking companies following users through these techniques.

Another method that can be used to track users by their IP address is through the review of server logs from websites. The website owner with access to the server can identify users’ IP addresses when they click the website on the server. Investigators can set up a web server with an undercover website designed for the investigation and use this as a method to track users browsing to the undercover website.
PRINCIPLE 7 ONLINE UNDERCOVER FACILITIES

At the start of this chapter, we noted that Online Investigations Working Group (Working Group) had provided 11 principles concerning online investigations. Principle 7 deals with the creation of an undercover website, in part creating a consultation requirement for federal law enforcement. Principle 7 also notes several areas of concern for federal law enforcement in this area. One area is the website administrator versus law enforcement role. Principle 7 reflects: “Law enforcement agents may not circumvent the statutory restrictions on government access to information simply by covertly becoming a service provider. Thus, while law enforcement agencies may use the system provider’s authority to manage or protect the system, they may not use the system administrator’s legal powers to gather evidence normally obtainable only through procedures required by Electronic Communications Privacy Act (ECPA). To avoid legal complications, agencies should consider taking steps to separate the responsibility for administering the online facility, to which one legal framework applies, from its criminal investigative function, to which a different legal framework applies” (p. 37).

These principles were created in 1999. However, it would behoove any investigator especially, those from federal agencies, to consult with their legal authority if they are planning to create an undercover website.

CONCLUSION

In this chapter, we discussed the use of anonymization as tools for the investigator as well as for the criminal. Anonymization can be an effective method for the investigator to secure their computing systems and their actions on the Internet. Each tool discussed has its own advantages and disadvantages, and investigators need to carefully consider their tool selection and how they are implemented. The use of anonymization by criminals does not halt an investigation. There are methods by which the investigator can track users of anonymization on the Internet. It can make an investigation more complicated and requires more effort on the part of the investigator, but it does not stop the investigation itself. Clearly, understanding anonymization techniques and how they are used by criminals is become an important skill for the online investigator.

Further reading


Property of Reed Elsevier. Do not redistribute or resell.


