PEARSON IT

CYBERSECURITY CURRICULUM

SECOND EDITION

A PRACTICAL GUIDE TO DIGITAL FORENSICS INVESTIGATIONS

DR. DARREN R. HAYES

A Practical Guide to Digital Forensics Investigations

Dr. Darren R. Hayes

PEARSON

221 River St. Hoboken, NJ, 07030, USA

own time. The NLRB believed that the company's Internet and social media policy violated employee rights. Ultimately, there was a settlement between the company and Souza, and the company changed its blogging and Internet use policies so as not to prohibit employees from posting their personal opinions about the company online.

In another example, at Mesa Verde High School, in California, Donny Tobolski was suspended for posting rude comments about a teacher on his Facebook account. The boy posted that his biology teacher was a "fat ass who should stop eating fast food, and is a douche bag", The American Civil Liberties Union (ACLU) argued that the school violated the student's state and federal Constitutional rights, as well as the California Education Code.

This chapter details a number of online resources, some of which are free and some of which are paid premium services, to create an online profile while investigating criminal activity. Sometimes this fake online profile is called a "sockpuppet". This chapter also describes databases that are regularly used by international, federal, state, and local agencies to gather and share intelligence on the general public.

Note

All online resources in this chapter were correct at the time of writing, but of course websites are subject to change without notice.

Working Undercover

An **undercover investigation** is the process used to acquire information without the individual or suspect knowing the true identity of the investigator. Prior to any interaction with a suspect, an investigator will perform reconnaissance on the individual. This background search involves building a profile about the suspect. The profile will include various types of personal data discussed in this chapter and will also include profiling the suspect's behavior. It is important that the investigator performs this reconnaissance incognito. As more of our personal data, attitudes, communications, and general behaviors are captured on the Web, online reconnaissance has become extremely important. Additionally, the Internet has facilitated the growth of certain types of criminal activities. It is easier for a criminal to dupe a victim into handing over credit card information online than to steal someone's wallet. Pedophiles have gravitated to the Internet as they have found it easier to find similar deviants online and even use the Internet to help plan their activities. However, the Internet also provides advantages for undercover detectives; it is relatively easy to convince a pedophile that a 40-year-old detective is a 14-year-old girl when chatting online. During the reconnaissance phase, a detective may gain access to the suspect's email account or user groups or gather information from social networking websites, if the law permits.

Following a background check of the suspect, surveillance of the suspect can begin. Detectives may begin monitoring the suspect's residence, movements, and daily routine and generally build a profile of his behavior. Similarly, online the detective will monitor the suspect's activities in chat rooms and

in user groups. During this phase of the investigation, the investigator plans how detectives will record the suspect's activities, which can include video and audio, decide whether any warrants need to be requested, and plan how the interaction between the detective and the suspect will occur.

The next phase of an investigation involves a more formal monitoring and recording of the suspect's activities. This step of the investigative process might include acting on court-approved warrants, whether search warrants or wiretaps.

Finally, there is a sting operation. This step of the investigation is designed to catch the criminal in the act of committing or planning to commit a crime. A detective might pose as an accessory to a criminal act, or in the case of a child endangerment investigation, the investigator might pose as a child and speak with the criminal suspect. The Internet makes the process easier now because an actual child does not have to be used as "bait" to capture the suspect. In many cases, the suspect believes that he has been able to lure a child to a parking lot, where, in reality, police have lured the suspect for a rendezvous.

Generating an Identity

When working undercover, an investigator often needs to create a *sockpuppet*, which is a fake online persona created to interact with a person of interest. The investigator may need to create a Gmail or Yahoo! account, and the verification process will require an established email account and telephone number. ProtonMail (protonmail.com) or Tutanota (tutanota.com) are services that will allow you to create disposable email accounts for verification. We will discuss disposable email in more detail in the next section.

Blur (abine.com) is a tool that allows you to obfuscate your email information. You can also create email accounts for use on the Dark Web, using services like Mail2Tor (mail2tor.com or mail-2tor2zyjdctd.onion) or Secmail Tor (sigaintevyh2rzvw.onion). Regarding SMS verification, for new online accounts, you can use free services, like TextNow (textnow.com) or Talkatone (talkatone.com), or you could use a burner phone.

Sometimes an investigator will need to use Bitcoin in an investigation and ensure that the Bitcoin address is untraceable or close to being untraceable. Bitcoin Laundry (bitcoin-laundry.com) may be a good solution, if approved by your department. A Bitcoin ATM is another option, and these ATMs can be located at Coin ATM Radar (coinatmradar.com). Another option is to use a prepaid debit card, which does not require that the purchaser provide a name and address. A OneVanilla prepaid Visa card may be an appropriate option (onevanilla.com). This Visa card can then be linked to a PayPal account, if needed.

When interacting online with a suspect, it is important that your identity remains a secret and that your computer is protected against malware. Therefore, you may consider using a paid VPN service. Algo VPN (github.com/trailofbits/algo) allows you to create your own VPN service. There are paid VPN services too, like NordVPN (nordvpn.com) and RSocks (rsocks.net). You might also consider using the Tor browser (www.torproject.org) with the Tails OS (tails.boum.org) to remain anonymous online.

Realistically, it is not difficult for a detective to create an undercover identity. Nevertheless, there is a service that allows the user to quickly generate a false identity. Fake Name Generator (www.fakenamegenerator.com) is a free online service that allows the user to generate an ad hoc identity (see Figure 5.1). Moreover, the service allows the user to select gender (male/female), name set (American, Chinese, Hispanic, etc.), and country (Australia, Italy, United States, etc.). Once these three criteria have been submitted, a phony name, address, email address, telephone number, credit card number, Social Security number, weight, height, and other personal data are generated. Of course, sometimes the investigator may decide to tailor an undercover identity for a specific type of investigation—perhaps posing as a young girl when chatting online with a suspected pedophile. One problem for undercover investigators is the use of photographs to create a fake persona. The website thispersondoesnotexist.com creates realistic-looking computer-generated photos of people.

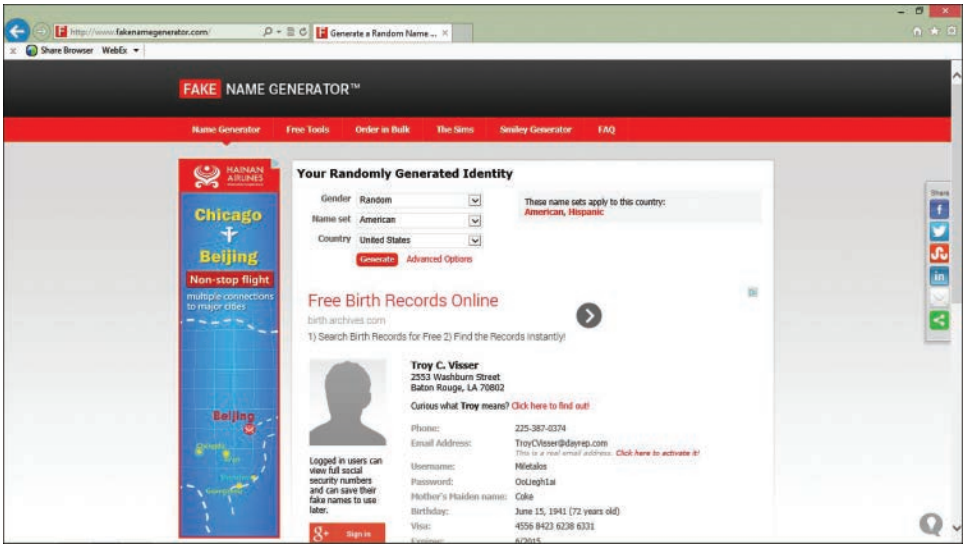

FIGURE 5.1 Fake Name Generator website results

Generating an Email Account

When working undercover, creating a temporary email account can be necessary to start a new service that will be utilized during an investigation. For example, when creating a new Gmail account, an email address is required to validate the user when setting up a new account. There are several disposable email services that allow the user to create an ad hoc email account with an inbox. Once the browser is closed, the email account is eliminated. Gmail accounts are particularly useful with undercover investigations because Google obfuscates the originating IP address from the email headers.

GuerrillaMail (www.guerrillamail.com) allows a user to create a temporary email address, which does not require any type of registration (see Figure 5.2). Your temporary email address will not have the @guerrillamail.com extension. The GuerrillaMail email address will last for 60 minutes.

FIGURE 5.2 Guerrilla Mail website

Another service, *mail expire* (www.metafilter.com), allows the user to create a disposable email account that can be set to last up to three months (see Figure 5.3). However, unlike Guerrilla Mail, mail expire does require that you register and enter an existing email address. It should be noted that some disposable email accounts are blocked by some services as a method of verification.

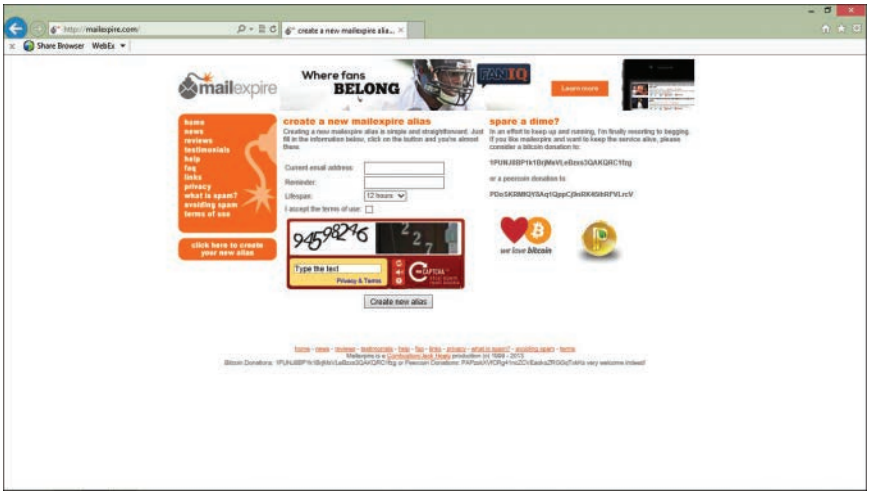

FIGURE 5.3 mail expire website

Another disposable email service that does not require any type of registration is Mailinator (mailinator.com; see Figure 5.4). Interestingly, you can select your own username with this service. For example, you could select the email address hipster@mailinator.com.

FIGURE 5.4 Mailinator website

All of these aforementioned disposable email services are advertised as beneficial to users who wish to avoid spam. Nevertheless, they provide an effective means for detectives to utilize services without providing any (genuine) personally identifiable information.

In summary, an investigator can create a phony profile for an undercover investigation. A Gmail, or other email account, can be created using the phony profile. The email required by the Gmail registration process would be a disposable email created on-the-fly by a service like mailinator. Once a confirmation email appears in the mailinator Inbox, the detective can then click the confirmation link to finalize the Gmail account setup.

Masking Your Identity

Detectives have numerous methods at their disposal to remain anonymous online. Bluffmycall.com is one service that enables the user to (1) change her caller ID to any number, (2) disguise his voice, or (3) record his calls (see Figure 5.5). SpoofCard (www.spoofcard.com) is a similar service, which is also popular.

FIGURE 5.5 Bluffmycall.com website

Spy Dialer (www.spydialer.com) is a free online service that allows a user to contact a cellphone number to hear who answers the telephone, without identifying the number of the caller (see Figure 5.6). The service can also be downloaded as an app to a smartphone.

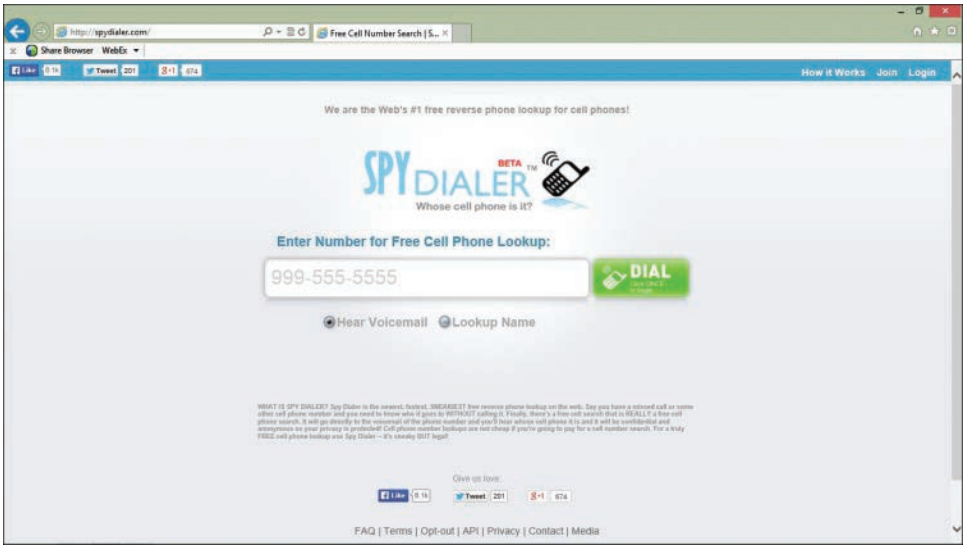

FIGURE 5.6 SpyDialer.com website