

# The Tor Browser

## INTRODUCTION

Few Internet technologies have had more of an impact on anonymous Internet use than The Onion Router browser, commonly known as "Tor." Tor is simply an Internet browser modified from the popular Firefox Internet browser. The browser modifications hide the user's originating Internet Protocol (IP) address when surfing websites or sending e-mail. By hiding the true IP address of the user, attempts to trace or identify the user are nearly impossible without the use of extraordinary methods.

Tor combines ease of use with effective anonymity in which practically anyone can use without technical instructions. The sheer ingenuity of the Tor browser combines ease of use without any requirement of how the software operates to operate effectively. Although there are other means of browsing the Internet anonymously, the Tor browser is by far one of the simplest to use and is freely downloaded. In theory, anyone with an Internet connection and the Tor browser can anonymously surf the Internet and communicate without being identified.

## HISTORY AND INTENDED USE OF THE ONION ROUTER

Tor's intention is to allow unfettered and anonymous communication over the Internet. Tor allows anyone to connect to websites that may be blocked by oppressive governments, allows whistleblowers to communicate with officials anonymously, and gives a means for legitimate communication between businesses and persons who desire to keep their private conversations private. However, much like a car that is used to take your kids to school can also be used as a bank robbery getaway car, the Tor browser can be used to either facilitate crimes or commit crimes.

Although Tor was initially developed by the US government in 2002, it is not presently controlled by the US government. In fact, Tor is practically not controlled by any one entity but rather open for improvements

by virtually anyone with the technical ability to test and improve it. For that reason alone, Tor receives worldwide input from privacy motivated experts to ensure it remains relevant and effective. As a point of irony, the US government not only created Tor but is also researching methods to deanonymize users of it.

## Two Ways of Looking at The Onion Router

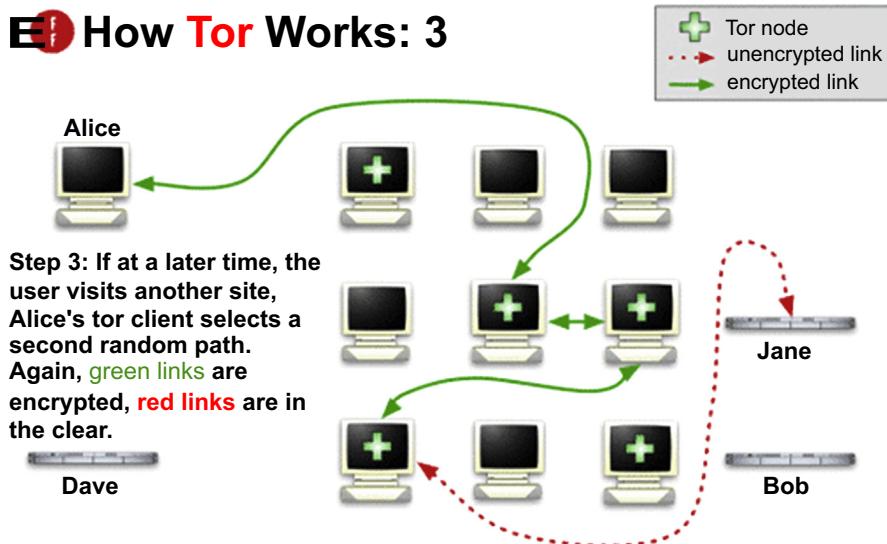
Before you finish reading this chapter, you will invariably think back to every forensic analysis you have conducted and wonder if you missed a golden nugget of evidence. The Tor browser is not typical of any other Internet browser in purpose or design. The mere existence of Tor on electronic evidence should give you concern on the evidence you can easily overlook along with the evidence you know will not be found because of Tor use.

One perspective of looking at Tor is that of forensically examining devices that may have had Tor installed. From this perspective, the examination of the device for Tor artifacts is your target and not so much an ongoing use of Tor. The forensic analysis of Tor is detailed later in this chapter, but at this point, keep in mind that a forensic analysis of Tor artifacts is one way we will be looking at Tor. Tor can run on Windows, Linux, and Mac. In the section of forensic analysis, the focus will be on the Windows operating system as it is the most commonly used operating system.

The other perspective of looking at Tor is that of it being currently used by your suspect. Without having the actual devices to examine, your investigation will have to depend solely on defeating Tor to either capture communications or identify your suspects who are using Tor. There are some aspects of Tor use that currently are unbreakable, at least to the nonintelligence agency investigator, and even then, Tor remains one of the most difficult systems to beat. Even with that, the last thing you should do is throw up your arms in defeat without trying. There are some methods that may work in your investigation now and others that may work later.

## HOW THE ONION ROUTER WORKS

In the most basic explanation, Tor directs the route of a user's Internet traffic through random relays on the Internet. The data is first layered with elliptic curve cryptography, which is currently unbreakable with brute-force. As the encrypted data enters the first relay ("entry"), one layer of encryption is stripped and sent to the next relay ("middle"). The middle relay strips another layer of encryption and sends the encrypted data to the last relay ("exit"). The exit relay now connects to the user's desired target with an unencrypted connection.

**FIGURE 2.1**

How Tor Works <https://www.torproject.org/about/overview.HTMLe.en>.

The exit relay does not know anything of the traffic route other than the single previous relay. Making Tor traffic even more difficult, if not impossible, to track is that this random route chooses a different entry, middle, and exit relay every 10 minutes or so. Fig. 2.1 shows a graphic from [Tor Project \(n.d.\)](#) visualizing this concept of Tor.

An analogy of Tor would be mailing a letter that is received and forwarded by different people. Let's say Mary wants to mail Johnny a letter, but does not want Johnny to know where the letter originated. The steps Mary needs to take to remain anonymous would be as follows:

1. Mary writes a letter and places it into an envelope addressed to Johnny in Boston.
2. Mary places that envelope into another and addresses it to Susan in Seattle.
3. Mary places that envelope into another and addresses it to Barry in Dallas.
4. Mary places that envelope into another and addresses it to Bob in Denver.
5. Mary places the letter in a mailbox from her home in San Francisco.

In this analogy, an envelope represents a layer of encryption. Using the rule that each person in this analogy can only unwrap the first envelope, the contents remain hidden (encrypted) in the most inner envelope.

Bob in Denver (“entry”) receives the letter, removes the outer envelope, and places the letter in a mailbox to Barry. Bob never saw the contents of the letter and only knows it came from San Francisco and is going to Dallas.

Barry (“middle”) receives the envelope, removes the outer envelope, and places the letter in a mailbox to Susan in Seattle. Barry never saw the contents and only knows that it originated in Denver.

Susan (“exit”) receives the envelope, removes the outer envelope, and mails the letter to Johnny in Boston. Susan only knows that the letter came to her from Dallas. At this point, the contents can be read since the envelopes are removed. Susan does not know the letter originated in San Francisco.

Johnny receives the letter and contents, but only knows it came from Seattle. If Mary wants to mail another anonymous letter to Johnny, she will send through three different people with the same process. The main difference is that where regular mail will take days to arrive, Tor is instantaneous, yet virtually and completely anonymous.

As to the name “The Onion Router”, you can see that sending data over Tor is like an onion, where a layer of encryption is peeled off as it goes through the Tor nodes to its final destination.

---

### I'M JUST AN EXIT NODE! I'M JUST AN EXIT NODE!

**Sometimes the IP address you get is not the IP address you need.**

In 2011, Immigration and Customs Enforcement (ICE) executed a search warrant on Nolan King’s home and seized his computers because an ICE investigation found that child pornography was being distributed from his home IP address ([Hoffman, 2011](#)). No child porn was found because King was simply operating a Tor exit node

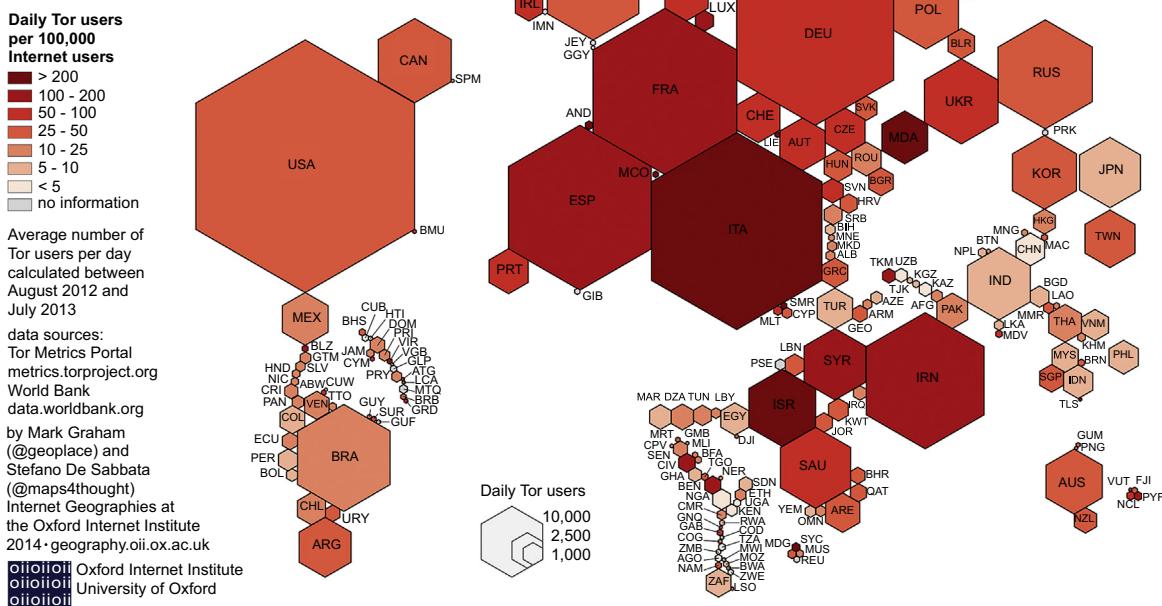
---

### A Few Important Points About Tor

Before continuing, a few more explanations are needed to describe how Tor works along with the terminology used with Tor. As we continue, you will begin to understand why breaking Tor is practically impossible without extraordinary resources, but there are some aspects of Tor that may be compromised.

The Tor network of relays is run by volunteers. Anyone, including you, can configure a server to be one of the thousands of relays used by hundreds of thousands of Tor users. Being a volunteer means your server would simply “remove the outer envelope and forward the inner envelope” to the next destination. Keep this in mind when investigating IP addresses with any investigation

## The anonymous Internet



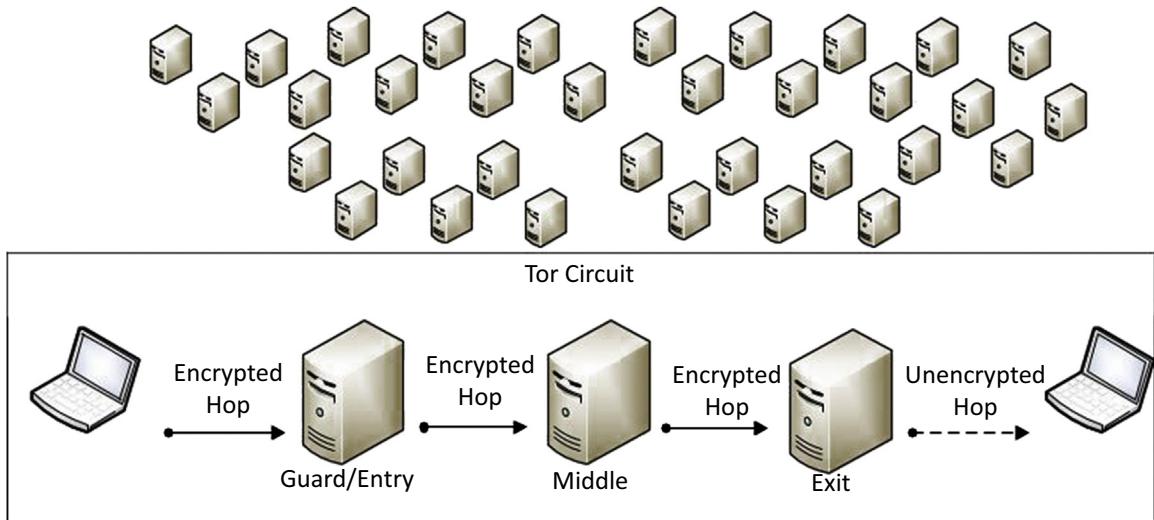
**FIGURE 2.2**

Number of daily Tor users compared to Internet users <http://geography.oi.oii.ac.uk/>.

where Tor is involved. The IP address you believe may be your target just may be an innocent volunteer running a Tor relay.

Perhaps the most enlightening aspect of Tor is the amount of users since anonymity is strengthened with more users making it difficult to find one user among many. Fig. 2.2 is a graph of the number of worldwide, daily Tor users. According to the Tor Metric Portal (Tor Metrics, n.d.), there are over 750,000 users of Tor using over 6000 relays worldwide.

From Fig. 2.2, you can see where tracing Internet traffic on a Tor network can literally take you around the world, through the relays of innocent volunteers, and still not be closer to reaching the originating target. Additionally, even if the Tor circuit could be broken, gaining cooperation in foreign countries adds another layer of legal and diplomatic issues to identify the Tor users. In short, if a victim receives a harassing e-mail that appears to have originated in Italy do not assume that the suspect was physically in Italy.



**FIGURE 2.3**

The Tor Circuit.

A simple visual of a Tor circuit can be seen in Fig. 2.3. The entry relay, or node, is also the “guard.” The Tor client chooses entry guards at random to be used only for the first encrypted hop. If an entry guard is suspected of being compromised, it is no longer used. A random middle node is chosen for the encrypted middle hop which then sends the encrypted data to the exit node. The exit node then sends unencrypted data to the target. Keep in mind that not only are there over 6000 nodes from which the Tor client will choose from but that after 10 minutes or so, the Tor circuit changes the nodes among the thousands to choose.

The middle node does not know the origin or the data nor the final destination, and by the same token, neither the origin nor destination will know the middle relay. This makes it safe as a volunteer of a middle node to avoid being wrongly suspected of criminal activity based on IP addresses.

Each of these relays is publicly posted on the Internet for use by Tor clients. However, there are “bridges” which are typically not posted publicly. Since Tor relays are public, Internet Service Providers, or governments, can block them. But bridges are not normally listed publicly which makes blocking bridge relays nearly impossible. In countries where Internet blocking occurs, Tor bridges are used more commonly. Tor directory servers maintain Tor router information that is publicly listed.

---

## TOR NODES

### Fig. 2.4 Where is this list of Tor nodes?

There are several websites that provide lists of Tor nodes and allow to search for specific IP addresses to confirm if it had been, or is currently, used as a Tor node. Fig. 2.5 is one example of a website providing this information.

## ExoneraTor

---

Enter an IP address and date to find out whether that address was used by a Tor relay:

IP address	86.59.21.38	Date	mm/dd/yyyy	Search
------------	-------------	------	------------	--------

## About Tor

Tor is an international software project to anonymize Internet traffic by encrypting packets and sending them through a series of hops before they reach their destination. Therefore, if you see traffic from a Tor relay, this traffic usually originates from someone using Tor, rather than from the relay operator. The Tor Project and Tor relay operators have no records of the traffic that passes over the network and therefore cannot provide any information about its origin. Be sure to [learn more about Tor](#), and don't hesitate to contact [The Tor Project, Inc.](#) for more information.

## About ExoneraTor

The ExoneraTor service maintains a database of IP addresses that have been part of the Tor network. It answers the question whether there was a Tor relay running on a given IP address on a given date. ExoneraTor may store more than one IP address per relay if relays use a different IP address for exiting to the Internet than for registering in the Tor network, and it stores whether a relay permitted transit of Tor traffic to the open Internet at that time.

"Tor" and the "Onion Logo" are registered trademarks of The Tor Project, Inc.

### FIGURE 2.4

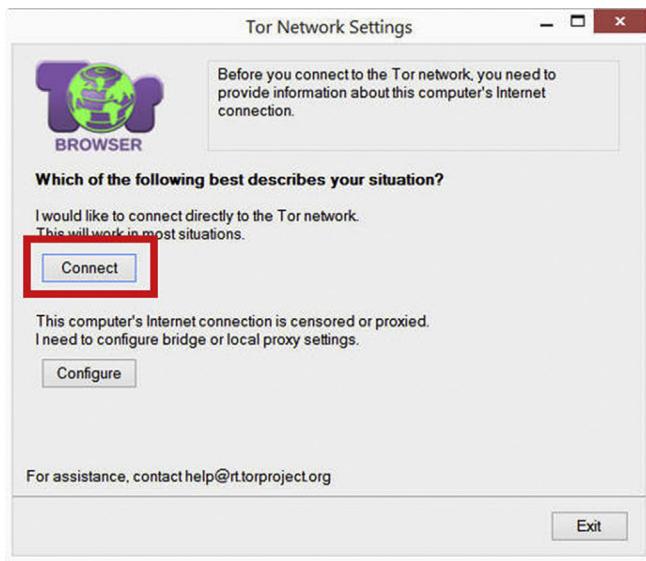
Where is this list of Tor nodes? ([ExoneraTor, n.d.](#))

---

## From a Tor User's Perspective

As mentioned, the Tor browser is simply a modified Firefox browser. Besides downloading the Tor browser, the only user technical skill required is that of entering URLs in the browser or entering terms in a search engine. Even the skill of installing a Tor is less than installing most programs. The Tor browser bundle is a portable application and only needs to be extracted, not installed, to run. The Tor browser file is self-executable to make the process even simpler for anyone to use. As the Tor browser is a portable application, it can be installed (extracted) to any location on a computer or external media device without any default paths.

From downloading to using the most anonymous browser in the world only requires about 10 mouse clicks and 10 minutes to download, extract, and configure. When accepting default settings, which fits the needs of most users, the Tor browser configuration step is completed in one click as seen in Figs. 2.5–2.7.



**FIGURE 2.5**

Step 1 of Tor setup.

Most users do not need to configure Tor to use with a bridge or local proxy settings. However, if this is necessary, it only adds a few minutes of setup time and is not terribly difficult for most computer users. Generally, Tor is just as effective with or without bridges, except in countries where Internet censoring will require bridges for Tor to work with the Tor network.



**FIGURE 2.6**

Step 2 of Tor setup, just have to wait.

**FIGURE 2.7**

Tor setup is complete.

At this point, Tor is ready to use similar to any web browser. As you can see, the simplicity of Tor coupled with the strong anonymity makes it a great choice for legitimate purposes as well as a prime choice for illicit use. It's free, fast to set up, easy to use, portable, and provides near breakable anonymity.

## So What's the Big Deal?

Using Tor as an anonymous Internet browser is more than just surfing the web anonymously. Tor allows criminals and terrorists to communicate, share files, target, and attack with near absolute anonymity. For example, information transmitted using a webmail provider without Tor for criminal activity is easily discovered by law enforcement through search warrants and subpoenas once the e-mail address is known. The user's true IP address is also captured in e-mails and web browsing. Everything the user does online is potentially able to be captured, intercepted, and recovered down to the physical address of the computer system.

However, with Tor, this is not completely possible. Using a webmail service with Tor provides that service provider with the random exit node IP addresses and not the true IP address. Even by knowing the e-mail address, obtaining the originating IP address is practically impossible. Servers logging visitors will also only be able to log the random exit node IP addresses as well. This allows criminals to communicate openly without being identified. By using encryption methods with the communications, not only are they anonymous online, but the contents may also be encrypted end-to-end. Tor works to protect innocent communications but also provides that same level of protection to criminal and terrorist communications.

### **From Your Perspective**

Generally, as an investigator, you will be looking at Tor either through the device on which it was used or the Internet traffic that is using Tor. As a forensic analyst, you may see more use of examining the Tor artifacts rather than the use of Tor, but as an investigator, you may be tasked with harassing or threatening e-mails being sent anonymously through Tor. Either way, your task to unmask Tor is more than difficult, it is overwhelming.

One thing to keep in mind is that it is the manner of use that determines whether or not Tor is a tool for legitimate use or illicit use. Businesses use Tor to browse a competitor's website to avoid the competitor logging the traffic. Whistleblowers, government agents and informants, and tourists use the Tor browser to protect their communications from being disclosed for legitimate communications. Law enforcement should encourage the use of Tor in their investigations to avoid suspects being aware of government IP addresses looking at websites being investigated.

## **FORENSIC ANALYSIS OF THE ONION ROUTER**

First things first, you have to look for the Tor browser to find it. If you have not made it a routine part of a forensic analysis to look for the Tor browser, particularly when Internet and e-mail use is part of the investigation, you may be missing a vital piece of information. Since the Tor browser is a portable application, the Tor browser folder can be anywhere on a device. Users trying to hide Tor use may even change the name of the executable while placing the folder in a path inconsistent with where you'd expect a browser to be, such as under a system folder. Obviously, the fastest and most accurate method is to search for matching hash values for Tor in addition to searching for "Tor."

As the Tor browser is constantly updated, your device may have various versions of Tor in various states of active files and deleted files. Creating your

Name	Last modified
<a href="#">Parent Directory</a>	
<a href="#">3.0a1/</a>	2013-06-17 07:23
<a href="#">3.0a2/</a>	2013-07-01 19:19
<a href="#">3.0a3/</a>	2013-08-09 17:13
<a href="#">3.0a4/</a>	2013-09-26 04:03
<a href="#">3.0b1/</a>	2013-11-05 02:24
<a href="#">3.0rc1/</a>	2013-11-22 05:41
<a href="#">3.5.1/</a>	2014-01-28 04:37
<a href="#">3.5.2.1/</a>	2014-02-15 13:50
<a href="#">3.5.2/</a>	2014-02-11 08:41
<a href="#">3.5.3/</a>	2014-03-20 21:55
<a href="#">3.5.4/</a>	2014-04-08 21:44
<a href="#">3.5/</a>	2013-12-22 13:49
<a href="#">3.5rc1/</a>	2013-12-13 05:30
<a href="#">3.6-beta-1/</a>	2014-03-18 17:56
<a href="#">3.6-beta-2/</a>	2014-04-11 22:35

**FIGURE 2.8**

The Tor browser archives.

own hash set of Tor versions is as easy as downloading current and past versions to create a hash set unique to Tor browsers. The Tor Project archives all previous versions at [Index of /tor-package-archive/torbrowser \(n.d.\)](#) as can be seen in Fig. 2.8.

One of the purposes of searching for older versions of Tor that may have been used is that as an investigator, you can get a sense of how long your suspect has been using Tor as an anonymous communication and Internet surfing tool. If nothing else but to bolster your knowledge for an interview with a suspect, you may be able to determine by days, months, or years of use contrary to what a suspect may admit to using. A regular user of Tor will update their Tor browser as soon as notified that an update is available to avoid being compromised by an older browser weakness.

Internet history forensics can be one of the most enlightening aspects of a forensic analysis as it is a window to the soul of intention. Internet searches, bookmarks, visited websites give a clear description of a user's likes, intentions, wishes, and desires. Unfortunately, with the Tor browser, you most likely find no remnants of Internet use, specifically, the Internet history. The Tor browser

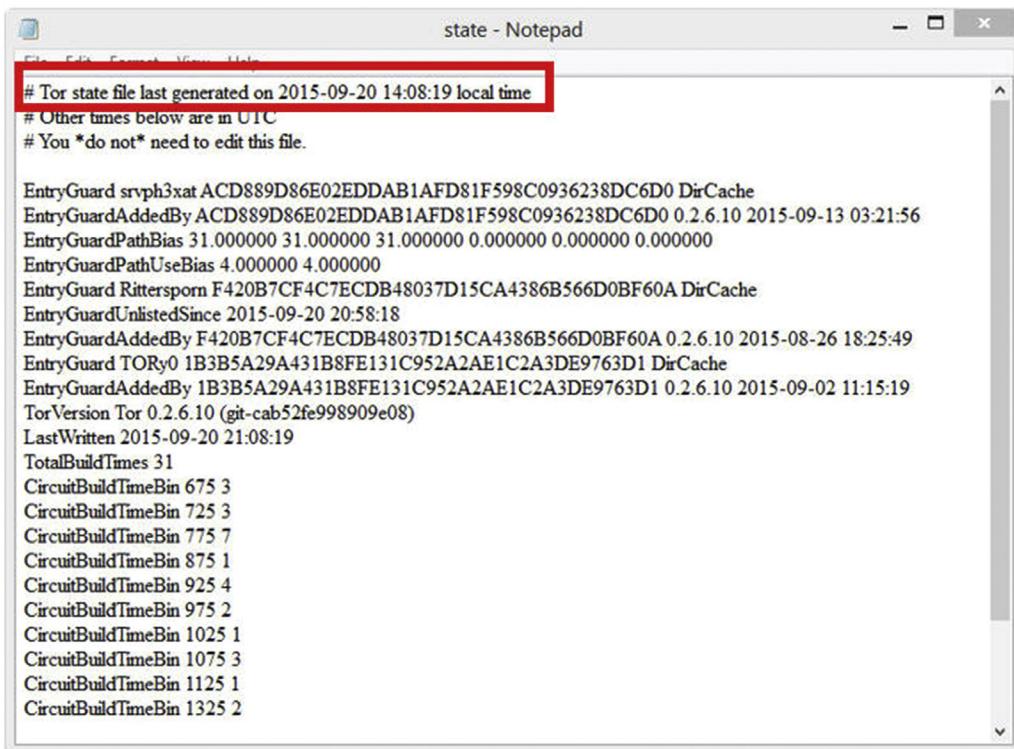
does not keep any Internet history information in the NTUSER.DAT file, nor anywhere else.

In order to recover Tor browsing history, a memory dump of the machine is needed, which of course, is another reason to capture the memory of computers before shutting down for capture. Another unfortunate investigative aspect of Tor artifacts in memory is the manner and time the data remains in memory. If the Tor browser has been run but closed, the data in memory is gone almost instantly. However, if the Tor browser is running, remnants of URLs are possible to be recovered but only for a few minutes after use. Approaching a machine that has the Tor browser running is a clear indication to capture the memory because every second counts.

Other Tor artifacts exist but are few. Mostly, the artifacts give some indication of Tor use, but not actual contents of communications or browsing history. The Windows paging file (C:\pagefile.sys) should contain the filename for the Tor browser and you may find traces of the Tor browser in cache files such as the following. The thumbcache should hold the Tor browser logo icon.

```
C:\Users\suspect\AppData\Local\Microsoft\Windows\Caches\  
cversions.1.db  
C:\Windows\AppCompat\Programs\RecentFileCache.bcf  
C:\Users\Suspect\AppData\Local\Microsoft\Windows\Explorer\  
thumbcache_32.db  
C:\Users\Suspect\AppData\Local\Microsoft\Windows\Explorer\  
thumbcache_32.db  
C:\Users\Suspect\AppData\Local\Microsoft\Windows\Explorer\  
thumbcache_96.db  
C:\Users\Suspect\AppData\Local\Microsoft\Windows\Explorer\  
thumbcache_256.db  
C:\Users\Suspect\AppData\Local\Microsoft\Windows\Explorer\  
thumbcache_ thumbcache_1024.db  
C:\Users\Suspect\AppData\Local\Microsoft\Windows\Explorer\  
thumbcache_sr.db  
C:\Users\Suspect\AppData\Local\Microsoft\Windows\Explorer\  
thumbcache_idx.db  
C:\Users\Suspect\AppData\Local\Microsoft\Windows\Explorer\  
IconCache.db
```

Conducting a keyword search for HTTP-memory-only-PB within pagefile.sys may also result in recovering websites visited with the Tor browser. Recovering Internet history in this fashion is not as satisfying as recovering history from non-Tor browsers, but if you can find the specific site that was visited that is needed for your investigation, it may be enough. Searching for any “Tor”-related keywords such as “torproject” throughout the media may also reveal information about Tor’s use in e-mails or recoverable Internet history.



The screenshot shows a Windows Notepad window titled "state - Notepad". The content of the file is a text-based log of Tor state information. A red box highlights the first few lines:

```
# Tor state file last generated on 2015-09-20 14:08:19 local time
# Other times below are in UTC
# You *do not* need to edit this file.

EntryGuard srvph3xat ACD889D86E02EDDAB1AFD81F598C0936238DC6D0 DirCache
EntryGuardAddedBy ACD889D86E02EDDAB1AFD81F598C0936238DC6D0 0.2.6.10 2015-09-13 03:21:56
EntryGuardPathBias 31.000000 31.000000 31.000000 0.000000 0.000000 0.000000
EntryGuardPathUseBias 4.000000 4.000000
EntryGuard Rittersporn F420B7CF4C7ECDB48037D15CA4386B566D0BF60A DirCache
EntryGuardUnlistedSince 2015-09-20 20:58:18
EntryGuardAddedBy F420B7CF4C7ECDB48037D15CA4386B566D0BF60A 0.2.6.10 2015-08-26 18:25:49
EntryGuard TORy0 1B3B5A29A431B8FE131C952A2AE1C2A3DE9763D1 DirCache
EntryGuardAddedBy 1B3B5A29A431B8FE131C952A2AE1C2A3DE9763D1 0.2.6.10 2015-09-02 11:15:19
TorVersion Tor 0.2.6.10 (git-cab52fe998909e08)
LastWritten 2015-09-20 21:08:19
TotalBuildTimes 31
CircuitBuildTimeBin 675 3
CircuitBuildTimeBin 725 3
CircuitBuildTimeBin 775 7
CircuitBuildTimeBin 875 1
CircuitBuildTimeBin 925 4
CircuitBuildTimeBin 975 2
CircuitBuildTimeBin 1025 1
CircuitBuildTimeBin 1075 3
CircuitBuildTimeBin 1125 1
CircuitBuildTimeBin 1325 2
```

**FIGURE 2.9**

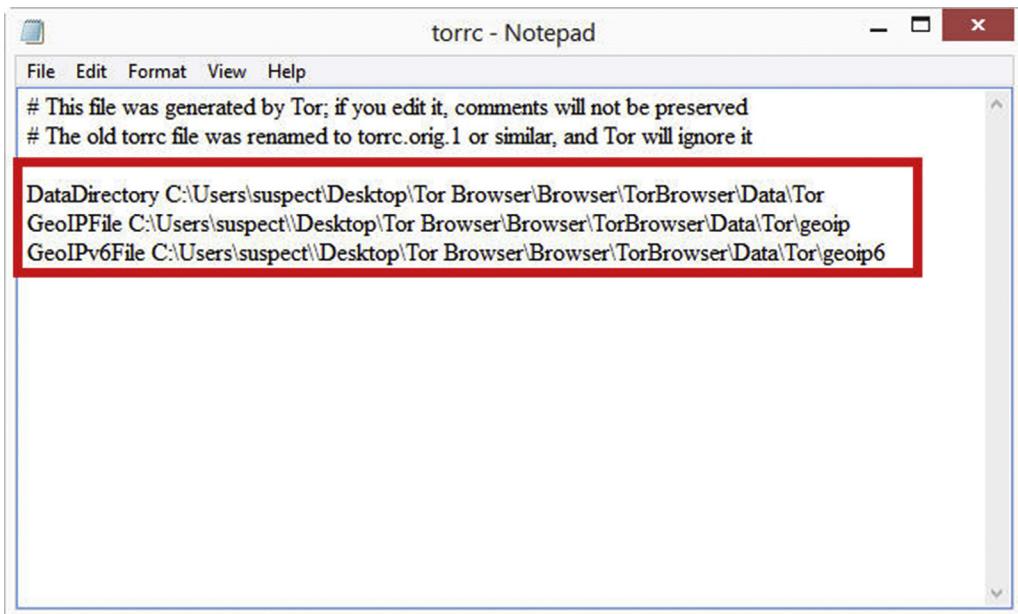
C:\Users\suspect\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor.

Within the Tor browser folder, you can find the last local execution date and time in the file named "state." If you have multiple Tor browser folders, which is likely for any Tor user, you will have multiple last execution dates and times for each browser's use. This file is viewable through Notepad or other text editors. An example is seen in Fig. 2.9.

Within the same file path as Fig. 2.9, the location of where the Tor browser was run can be found in the file torrc as seen in Fig. 2.10. Again, if the user has multiple Tor browser folders on their system, you can find multiple file paths including the drive letter from which the Tor browser was run.

Looking at the following files in the registry (HKCU) will also show the file path to the Tor Browser Bundle executable:

```
C:\Users\runa\AppData\Local\Microsoft\Windows\UsrClass.dat
C:\Users\runa\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
```

**FIGURE 2.10**

File path that the Tor browser was run.

Windows Prefetch is another source of information to recover information that may be pertinent to your investigation. One of the main purposes of a Prefetch file is to speed up the loading of applications, and the logging of Prefetch information gives a forensic analyst a wealth of application use information. For example, the following Prefetch example shows that Tor was installed on 9/20/2015 at 12:04:12PM and run about a minute later.

Filename	TORBROWSER-INSTALL-5.0.2_EN-U-51B7220A.pf
Created Time	9/20/2015 12:04:12 PM
Modified Time	9/20/2015 12:04:12 PM
File Size	33,676
Process EXE	TOR.EXE
Process Path	
Run Counter	1
Last Run Time	9/20/2015 12:05:20 PM
Missing Process	No
Filename	TOR.EXE-4FD90956.pf
Created Time	9/20/2015 12:05:30 PM
Modified Time	9/20/2015 12:05:30 PM
File Size	49,482
Process EXE	TOR.EXE
Process Path	C:\Users\suspect\Desktop\TOR BROWSER\Browser\TORBROWSER\Tor\tor.exe

```
Run Counter 1
Last Run Time 9/20/2015 12:05:20 PM
Missing Process No
```

Since Tor does not create artifacts that are helpful for analysis, other activity on the system may be related to inferring user activity. If an external drive was attached to this system in the same time period of use and files accessed from that device, it would be feasible that the files may have been e-mails or uploaded through Tor. Any files accessed during this time could be suspect as being infiltrated outside the system through Tor. A corporate network could miss data exfiltration in this manner.

Given the Prefetch sample information above and the below USB connection that occurred roughly 1 minute after starting Tor, a fair assumption that the activity may be related and would be the start of good questions of the computer user.

```
Device Name USB 2.0 FD
Description PNY USB 2.0 FD USB Device
Device Type Mass Storage
Drive Letter E:
Serial Number AAC214A100900336
Created Date 9/20/2015 12:06:30 PM
Last Plug/Unplug Date 9/20/2015 12:08:30 PM
VendorID 154b
ProductID 0059
Driver Filename USBSTOR.SYS
Device Mfg Compatible USB storage device
Driver Description USB Mass Storage Device
Driver Version 6.3.9600.17331
Instance ID USB\VID_154B&PID_0059\AAC214A980000336
```

Although a forensic analysis of Tor does not give you as much information as does that of non-Tor browsers, there is still much value in the analysis. Besides the install/first use/last use/number of uses, the possibility of recovering some URLs exists. The mere existence and use of Tor on any machine should also give immediate cause for concern for all aspects of counter/antiforensics that may have been employed on the system. With the Volume Shadow Copies, an analysis can provide an historical usage of Tor that can be compared with other activity on the system that may be related.

---

## IT'S PORTABLE!

### The Tor browser can run from almost anywhere

Remember, the Tor browser is portable, meaning that no installation is necessary. This also means that it can run from external devices, such as a flash drive or external hard drive, and may have never been installed (extracted) onto a system's hard drive. When Tor is run from an external device, you can expect even fewer artifacts to remain, but certainly does not make looking for Tor artifacts less important.

---

## TRACKING CRIMINALS USING TOR

By now you understand the difficulty in tracking Tor users, but do not feel alone because practically every government agency is working on deanonymizing Tor to either find criminals and terrorists or prohibit citizens from accessing the Internet. A few successes have made the national news, but for the most part, the breaks in the cases were not due to breaking Tor but rather exploiting errors made by suspects. Like the majority of investigators, having access to federal resources to investigate criminals using Tor is most likely not possible. Unless you have a terrorist connection to a case, you are on your own to investigate without the National Security Agency.

---

### IT'S POSSIBLE TO BREAK TOR!

**The FBI did it...once...at least once...**

A child pornography hosting service was identified and taken down by the FBI using an exploit of Firefox. The FBI simply infected the servers at Freedom Hosting, which in turn, infected the Tor browsers of the visitors of the criminal websites. The exploit (Firefox bug CVE-2013-1690 in version 17 ESR) captured the true IP address, MAC address, and Windows hostname from the Tor browser exploit. This information was then sent to the FBI until the exploit was discovered and patched. Linux Tor users and those who had used updated versions of Tor were apparently unaffected (The FBI TOR Exploit).

---

One of the weaknesses, if not the biggest weakness, of the Tor browser is the user. As the browser is preconfigured with security in mind, customization is not recommended. In fact, the best thing a Tor user can do is not to change any settings of the browser because anyone setting can leak information out of Tor.

A simple example is a geolocation. Some websites ask if you will allow your location to be shared. A Tor user should always choose "never" but as investigators, we rely on mistakes and hope these types of modifications are made by criminals. Other aspects of customization revolve around the entertainment factor of the Internet. Video and animation on the Internet usually require plugins to be installed and active while at the same time, these very plugins can allow the true IP address to be collected. Tor users who routinely allow scripts, java, and any other website requests to run on the browser risk having their IP address captured by those websites. But how does that help you?

The amount of research conducted on Tor to find vulnerabilities, identify users, and decrypt data has been ongoing for years. Some researchers have gone so far as to theorize deanonymizing Tor by attacking and disabling a large percentage of the Tor network to identify users ([Jansen, Tschorsh, Johnson, & Scheuermann, n.d.](#)).

Other theories include gaining control of as many entry and exit nodes as possible to correlate traffic and identify users. Even if several entry (guard) nodes are controlled, the Tor network does not automatically use new entry nodes

for weeks at a time to reduce the threat of compromised entry nodes. Entry nodes are also rotated regularly. So, to control entry nodes in hopes that your suspect's Tor circuit uses it is slim. On top of that, if the communications are encrypted end-to-end, capturing the traffic does not decrypt the contents of messages.

The man-in-the-middle attack is yet another method to bypass the security of Tor users by interjecting a capture service between the Tor user and destination. Nation-states have the resources for these types of attacks on Tor, but even then, compromising Tor is very difficult.

Each of these methods requires more resources and time than will ever be given to the common criminal unless special situations exist, such as a terror connection. Even then, the number of agencies with access to such resources is very few. Given that, the few remaining methods rely on the suspect and the suspect's errors.

The most common goal of any Internet-related investigation is obtaining the true IP address. With the true IP address, traditional investigative methods can corroborate, verify, and potentially seize physical evidence and suspects at that location. The trick is getting the IP address when Tor makes it extremely difficult.

Depending upon the investigation, you may have access to one end of the communication, such as that of a victim. When a victim receives harassing or threatening e-mails, the potential to capitalize on the suspect's mistakes increase. For example, an e-mail can be seeded with a tracking code, sent by the victim to the suspect. Once the e-mail is opened by the suspect, the tracking code can obtain the true IP address and send it to the investigator. The success depends on a couple of factors. One is that of the e-mail service being used and its configuration. If the e-mail (webmail) allows HTML, then the tracking script should work without alerting the suspect. However, if not, the suspect will be immediately notified that a script has been placed in the e-mail and not be allowed to run. This method is risky as it will tip off the suspect that e-mail may be compromised.

Another method with less risk of notifying the suspect is placing a tracking code in a document that is e-mailed to the suspect. Documents need to be downloaded and opened for viewing, usually outside the browser. When the document is opened outside the browser, the tracking code obtains the true IP address which is sent to the investigator. There are few if any, warnings, given to a computer user that opens a document with an IP address tracking code. Tor does give a warning that downloading documents can be dangerous and recommends to open the documents safely, offline or in a virtual machine to prevent the IP address from being captured.

When these methods are ineffective or may cause too much risk of compromise, identifying the Tor user outside of the Tor network may be possible. In

this manner, using all of the information you have of your suspect requires open-source and online investigative methods. Basically, finding your suspect in the open web can help identify the suspect in the Dark Web. Even if the only information you have on the suspect is a username, it may be enough to lead to more information otherwise unobtainable.

---

## ONE MISTAKE RESULTS IN A LIFETIME IN PRISON

### **One Weak Strand of the Silk Road Caused the Crash**

Silk Road found Ross Ulbricht used his personal e-mail address and real name on the open Internet to request help building a Bitcoin-venture, which led federal agents the ability to link directly to his previously unidentified Dark Web identity ([Bradbury, 2013](#)). Now he is spending the rest of his life in prison. That wasn't the only evidence in the case, but it is one example of a suspect's mistake making an investigation much easier.

---

Investigations that involve an internal corporate network are at an advantage of identifying Tor users if the network is being used with Tor. Network administrators can see Internet access using the Tor network, but cannot see the content of messages or websites accessed. However, the mere fact of being able to locate someone using Tor on the network is something impossible to do from outside a network. An example of how this can benefit an investigation is that a victim may have an idea as to who the suspect may be. If the employment can be identified, and the IT staff has the ability to find any local users accessing the Tor network, potentially e-mail traffic can be assumed based on the access date/time to the Tor network and receipt date/time of e-mails sent to the victim. Basically, if a user at the corporation accesses Tor between 3:30 pm and 3:40 pm, and the victim receives a threatening e-mail between those times, the likelihood that the suspect can be tied to a computer is high.

---

## BUT MOM, I DON'T WANT TO TAKE THE EXAM!

### **How a Harvard student was busted using Tor**

In 2013, Harvard student Eldo Kim used Tor to e-mail bomb threats to Harvard staff to avoid taking an exam. The IT staff at Harvard looked at their logs and identified Kim as accessing Tor on the school network during the time of the e-mails ([Dalton, 2013](#)). FBI agents asked Kim if he did it and Kim admitted. Tor worked. Kim broke.

---

The most common method of cases being solved is that from the "breaks" in the case. Breaks in the case are usually found by mistakes made by the suspects. In the case of Tor browser use, a suspect may be using the Tor browser properly, but might inadvertently use another browser falsely believing the non-Tor browser provides anonymity. Any e-mails or Internet connections through a non-Tor browser will show the true IP address of the suspect. In effect, a

suspect could mistakenly use a non-Tor browser and not realize it while the victim will receive the true IP address.

## USED IN COMBINATION OF OTHER TOOLS AND METHODS

Tor, when used by itself works well. When used in combination with other security methods works perfectly as an anonymous communication tool. As you have seen, the last hop of data in the Tor circuit is unencrypted. Theoretically, this data could be compromised. However, if the data was encrypted, not only is the transmission anonymous, but the information is encrypted. At that point, even if both ends of the communication are identified, the encrypted contents are secure if end-to-end encryption has been employed.

If a Tor user adds an additional layer of protection by using a nonowned computer on a nonowned network, the odds of being identified are even smaller. This would be the case of using Tor on a public computer at a library or hotel lobby as both the sender and receiver of electronic communications.

## TAILS

As Tor is a browser that can be used anonymously, Tails ([The Amnesic Incognito Live System](#)) is a complete operating system that can be used anonymously. Tails is based on Debian/Linux and runs from a DVD, USB flash drive, or SD card and does not need to be installed. In the context of the Tor browser, the Tor browser is preinstalled and preconfigured in Tails. The operation is the same as described previously with all the benefits of anonymity.

However, Tails adds even more security and anonymity to covert communications and web surfing. To run Tails, a computer must be able to boot to an external device that contains Tails. Once booted to Tails, the user needs to only connect to an active Internet connection and the Tor browser can be used immediately. The most substantial difference in using Tails compared to using the Tor browser in Windows or other installed operating system is that Tails does not leave any trace on the host computer system. A Tails user can prevent any forensic artifacts being created since Tails does not touch the host computer hard drive.

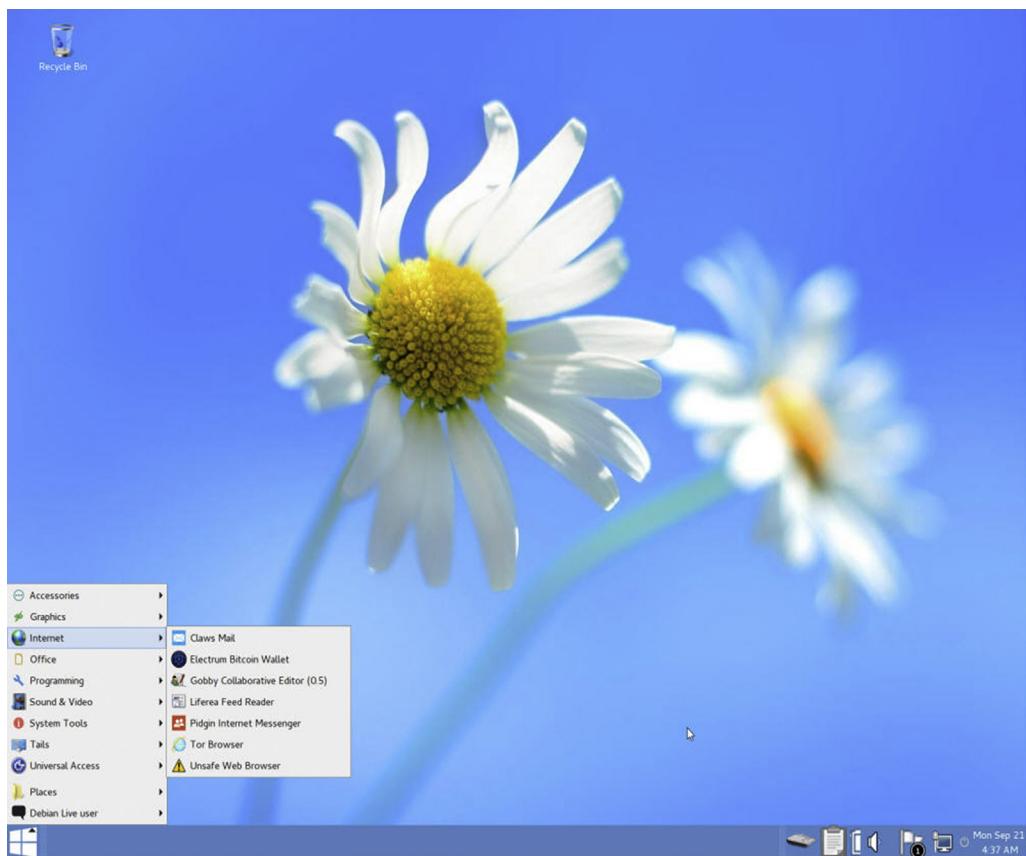
Additionally, you have seen that Tor forensic artifacts and even URLs can be found in memory and the hiberfil.sys file. Tails does not create, use, or write to a pagefile.sys or hiberfil.sys. Moreover, the live memory is wiped on shutdown. Even when run from a writable USB flash drive, data is not saved to the flash drive from the Tails use.

On Linux operating systems, the boot loader (GRUB2) can be configured to bypass the operating system and boot from an ISO that is stored on the host system hard drive. For example, a Tails ISO file can be saved on the hard drive of a Linux operating system, and through the boot loader the system will boot from the Tails ISO instead of booting from the host operating system. There is no need for external media to accomplish this, and trace evidence on the host hard drive will not be created when booting the ISO file. The host hard drive can have as many different ISO files of "live CDs" as desired, and any can be chosen to boot directly. A live CD is an operating system on an external medium that can boot a computer system and run completely from the external medium without use of the computer internal hard drive.

As an investigative point, forensic analysis of the boot loader is important to determine if the system was configured to boot from an ISO on the hard drive which could explain computer use without associated metadata and system changes to the hard drive operating system. Although the host hard drive is untouched (except for the ISO access), an analysis is not going to show user or system activity. However, the user can boot from the ISO and choose to access the hard drive to save, delete, or modify files. In this type of usage, there may be no system activity that matches user-created file creation/modification/access times, which would be indicative that the system was booted from an ISO (or even external bootable medium) and the host hard drive was accessed through the ISO operating system. A detailed instruction guide on booting Linux to a stored ISO on the hard drive can be found here: <http://www.howtogeek.com/196933/how-to-boot-linux-iso-images-directly-from-your-hard-drive/>. <http://www.howtogeek.com/196933/how-to-boot-linux-iso-images-directly-from-your-hard-drive/>

Tails provides more than just a Tor browser. It provides tools for encryption, encrypted chat, an office suite, MAC address spoofing, and a virtual keyboard that can thwart key loggers from capturing passwords. Nearly everything in Tails is designed for ease of use, portability, security, and anonymity. Upon booting Tails, the user can choose between the typical Linux configuration and a camouflage configuration that looks like the Windows operating system. [Fig. 2.11](#) is the desktop view of Tails with the Windows operating system configuration.

The same methods to defeat Tails apply to the previous discussion with Tors, but forensically, there will be no forensic artifacts to be found in a host system if Tails was the only method used to run the Tor browser. Tails is limited to the types of computers that can boot to external media. For example, many libraries are configured not to allow booting to external media which require users to run Tor on the host machine.

**FIGURE 2.11**

Tails operating system with Windows camouflage.

## RELATED TOR TOOLS AND APPLICATIONS

The Tor network works well for its intended purpose and because of its effectiveness, Third-party tools capitalize on it. One commercial example is the Anonabox (<http://www.anonabox.com>). The Anonabox is a hardware router that routes all Internet traffic through Tor, rather than only the Tor browser being routed through the Tor network. Devices such as the Anonabox should be considered when seizing computer systems for analysis.

Devices such as the Anonabox reduce security errors made by Tor browser users by eliminating the risk of using a non-Tor browser connection as the entire Internet connection runs through Tor. By running the entire Internet connection through a device such as this, suspects can use any web browser, not just Tor, without their true IP address being disclosed.

The risk of using devices like the Anonabox may not be worth the effort of just using the Tor browser. In April 2015, Anonabox recalled their devices for security flaws. The Tor network functioned, but the Anonabox was defective ([Greenberg, n.d.](#)).

Mobile applications with Tor may also become one of the most popular smartphone applications as the Tor browser can run on the Android operating system. Applications such as [Orbot \(n.d.\)](#) force Internet traffic on mobile devices to the Tor network, encrypting and sending traffic through worldwide Tor nodes. The ability to use Tor on a mobile device adds an entirely new dimension to “burner phones” in that a prepaid phone can be used to send anonymous communications via the Tor network and subsequently discarded. Virtually any and every mobile device may eventually have the option to direct Internet traffic through the Tor network, making it even more difficult to investigate crimes facilitated in this manner.

## Hidden Services

An aspect of the Tor network to consider as covert communications is that of hidden services. A hidden service is a server on the Tor network that provides a service, such as e-mail or file hosting. Hidden services are not indexed by search engines and therefore, practically invisible to the Internet. Hidden services also do not use exit nodes. If you remember, exit nodes strip off the last layer of encryption of a message. Hidden services provide end-to-end encryption since exit nodes are not needed. User connects directly to a hidden service with (currently) unbreakable encryption.

Setting up a hidden service on the Tor network is a fairly easy task that can be completed within an afternoon, which makes hidden services a prime candidate for covert communications due to being hidden and providing end-to-end encryption. Many hidden services are listed on directory websites for convenience and marketing, but can also be set up without being listed and known by certain persons for access.

Hidden service websites are most always accessed with the Tor browser with the top-level domain of the hidden services being “.onion”. A typical .onion web URL appears as <http://dppmfxaacucguzpc.onion/>. Browser plugins exist which can allow a non-Tor browser to access a hidden service website. However, there is no viable reason to use a non-Tor browser to access a hidden service, particularly since the hidden service may capture your true IP address. This would not be productive if you are investigating the hidden service and your office IP address is captured. [Fig. 2.12](#) shows one directory on the Dark Web offering drugs for sale. Note that Silk Road 3.0 is listed, which appeared right after the previous Silk Road was taken offline. There are directories of anything you can imagine, including hiring assassins and buying fake identities.

## Drugs

- [Agora](#) - Marketplace with escrow. Drugs, guns and more... Need a special link.
- [Dream Market](#) - Drugs Marketplace with Escrow. [tinyurl.com/dream-market](http://tinyurl.com/dream-market)
- [Abraxas](#) - Marketplace with escrow. Drugs, weapons and others...
- [Green Road](#) - Biggest marketplace with full working escrow (similar to the old Silkroad).
- [Silkroad 3.0](#) - The newer Silkroad.
- [ONION PHARMA](#) - Pharmacy Marketplace. PSY, Stimulants, Opioids, Ecstasy, etc.
- [Silkroad 2.0](#) - The new silkroad. Biggest marketplace for drugs on the Dark Web.
- [Hydra](#) - Marketplace with bitcoin and litecoin multi-sig escrow. Drugs and more.
- [Weed'A'Shop](#) - Weed / Cigarettes ... Prix Bas / Low Price ... weed cigarette

**FIGURE 2.12**

Directory of illegal drugs for purchase on the Dark Web.

Many, if not most, of the hidden services market illicit or restricted products or services. Drugs, firearms, credit card numbers, child pornography, and anything you can imagine are for sale on the hidden services, otherwise known as the "Dark Web." Considering the anonymity provided by the Tor browser coupled with the hidden service encryption, investigations into the Dark Web require more than IP address capturing. These investigations require a new level of traditional investigative methods to uncover and identify the networks of online criminals.

## SUMMARY

Tor is the most commonly used anonymous Internet tool in the world and is used for both legitimate and illicit communication. Although identifying the illicit users of Tor is nearly impossible, any forensics investigation should not discount the possibility of Tor use by a suspect as a means of covert communication. Identifying communications between persons requires more than just identifying the Internet traffic or identifying the persons involved. A complete picture is identifying the suspects as well as the contents of their communications.

## REFERENCES

- Bradbury, D. (October 3, 2013). *Silk road fell due to a catalogue of errors by owner Ross Ulbricht*. Retrieved September 21, 2015 from <http://www.coindesk.com/ross-ulbrichts-silk-road-head-smacking-rookie-errors/>.
- Dalton, T. (December 17, 2013). *AFFIDAVIT OF SPECIAL AGENT THOMAS M. DALTON* 835 1682. Retrieved September 21, 2015 from <https://www.washingtonpost.com/blogs/the-switch/files/2013/12/kimeldoharvard.pdf>.

- ExoneraTor. (n.d.). Retrieved September 21, 2015 from <https://exonerator.torproject.org/>.
- Greenberg, A. (n.d.). Anonabox recalls 350 'Privacy' routers for security flaws. Retrieved April 7, 2015 from <http://www.wired.com/2015/04/anonabox-recall/>.
- Hoffman, M. (August 24, 2011). *Why IP addresses alone don't identify criminals*. Retrieved September 21, 2015 from <https://www.eff.org/deeplinks/2011/08/why-ip-addresses-alone-dont-identify-criminals>.
- Index of /tor-package-archive/torbrowser. (n.d.). Retrieved September 21, 2015 from <https://archive.torproject.org/tor-package-archive/torbrowser/>.
- Jansen, R., Tschorisch, F., Johnson, A., & Scheuermann, B. (n.d.). The Sniper attack: Anonymously deanonymizing and disabling the Tor network. Retrieved September 21, 2015 from <http://www.robjanssen.com/publications/sniper-ndss2014.pdf>.
- Orbot: Mobile anonymity circumvention. (n.d.). Retrieved September 21, 2015 from <http://guardianproject.info/apps/orbot/>.
- The amnesic incognito live system. (n.d.). Retrieved September 21, 2015 from <https://tails.boum.org>.
- The FBI TOR Exploit.* (November 29, 2013). Retrieved September 21, 2015 from <http://resources.infosecinstitute.com/fbi-tor-exploit/>.
- Tor Metrics. (n.d.). Retrieved September 21, 2015 from <https://metrics.torproject.org/>.
- Tor Project. (n.d.). Retrieved September 21, 2015 from <http://www.torproject.org>.