An Overview of Web Surfing With Rudimentary Anonymity

Table of Contents

AWS.I **Introduction**

A fundamental part of online privacy is anonymity. Often there are times when you feel it is necessary to hide your identity online. Remember that while it is essentially impossible to ever become 100% invisible, this guide is a fairly basic overview of how to make yourself considerably anonymous. Even if you have nothing to actually hide, the pursuit of anonymity is very exciting, and is important to understand when analyzing how an attacker hid themselves while attempting to break into your computer to steal the special edition Britney Spears cover art you spent hours painstakingly pasting into iTunes. Anonymity is also a lot of fun to say. Try it three times fast.

"I disabled my cookies, so I'm safe right?"

Well, like it or not, every time you click a link, somebody somewhere can see it was you returning from *startrekporn.co.uk*. Disable your cookies, go ahead. But whenever you visit a page online, your Internet Protocol Address (IP) goes with you. When you type a Uniform Resource Locator (URL) and press Enter, you send a request to view that page, in the form of a data packet, hightailing it from your computer to the host site. Guess what is in the header of every one of those data packets. Yeah, your IP.

It gets better. Any Web site can use special software to pull your IP from a header. The software can also track what browser you are using, what pages you look at belonging to the site, and the Web site you came from.

"You mean, *christiandating.com* knows I was just at *bdsmknockers.org*??"

Well, if the God-fearing Matchmakers were curious enough about you, they could easily see that you just came from that video of Lucretia whipping the poor bald man into submission. Don't worry, the chances of them finding out you were putting clothespins on your nipples while the video was buffering are close to nil.

"So what do I do?"

Fear not, gentle reader, lest I end this pseudo-conversation with myself, thus concluding my weighty tome's introduction. Alas. Ye will soon discover the art of anonymity, as it were, my lord.

AWS.1 **Part 1: Anonymizers**

A simple, but unsafe, way to surf anonymously is through the utilization of Anonymizers. What you are basically doing is channeling your browsing through a secondary website that acts like a fat proxy. Connecting to a proxy server is called tunneling. Instead of sending those cute data packets directly to your intended domain, you take the scenic route, stopping and leaving your headers behind at the Anonymizer's server. The Anonymizer then sends data packets stripped of your IP information to the website you are going to. The Web site sends requested page to the Anonymizer and back to your computer, completing the circle of life.

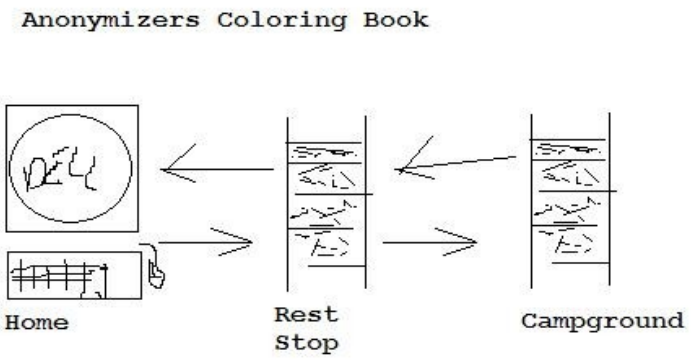
Example:

http://www.christiandating.com

becomes

http://anon.free.anonymizer.com/http://www.christiandating.com

You will notice that when using an Anonymizer, the URLs to all the Web sites you access look a little different. Copy all that stuff before the Web site you want's *http://* and you can paste it into your bookmarks and forum link posts, for a super official look. Everybody will think you are some great hacker or double agent. Impress all the ladies with your anonymous ways.



And remember that if you are a dick wiki sysop and you delete a certain user's hard work, who just spent hours Anonymizing every link on a major article, that he just spent even more hours rewriting and making into an actually useful page, so you can get more money from ad dollars, money that he will never see a cent of, your wiki may lose that user, and you need to decide if losing dedicated members is worth exercising your power control fetish about. Just a random example.

AWS.1.X **ActiveX**

Often times you won't be able to use SSL servers, Java ,or JavaScript applications. Anonymizers do not protect from ActiveX Controls, which can still access and reveal personal information about you. ActiveX Controllers are essentially small programs, and have the ability to copy files, install programs, and much more. Microsoft developed ActiveX for web designers who wanted an easy way to make their pages interactive. This is more of a security issue than anonymity, but you need to watch out for malicious ActiveX Controls.

Cleaning Up ActiveX

If you are worried about ActiveX, the simplest method of eliminating this danger is switching to a different browser, like Firefox. But if you really want to use IE, here is how to modify ActiveX settings.

IE

1. Go to Tools>Internet Options>Security
2. Click the Internet icon and select Custom Level
3. Select “Prompt” for the following:
   - “Download Signed ActiveX Controls”
   - “Download Unsigned ActiveX Controls”
   - “Run ActiveX Controls Marked Safe For Scripting”
4. Select Disable for “Initialize and Script ActiveX Controls Not Marked As Safe”
5. Click OK>Yes>OK

Anonymizer Proxy Servers

You can use Anonymizers as permanent proxy servers, too. Make a point to connect to proxies in countries hostile to yours. That will make tracing you that much more difficult.

IE:

1. Tools>Internet Options>Connections>LAN Settings
2. Check “Use a Proxy Server for Your LAN”
3. In the Address Field, enter the Anonymizer's URL and 8080 in the Port Box.
4. Click OK

Netscape:

1. Edit>Preferences>Advanced>Proxies

2. Select “Manual Proxy Configuration”
3. In the HTTP Proxy field, enter the Anonymizer's address, and 8080 in the Port Box.
4. Click OK

Firefox:

1. Tools>Options>Advanced>Network>Settings
2. Check “Manual Proxy Configuration”
3. In the HTTP Proxy field, enter the Anonymizer's address, and 8080 in the Port Box
4. Click OK

Always be careful with Web based Anonymizers, because they often store logs of all requests and data that passes between you and the server. Using solely Web based proxies is not a safe way to be anonymous, as tracing is almost always possible.

AWS.1.V **VPNs**

VPNs are networks that are used to connect external users to a local network through the internet. This is useful for people working at home, who want to connect to their corporate intranet. So instead of visiting a web page through your network, you will be visiting through the company to which the VPN belongs. Often they are encrypted and only certain people are given access to them. As a person seeking anonymity, it is best to look at VPNs like any other proxy. As a security note, you should know that when you access a VPN, you may be granting other users on the VPN use to your printer or various other services because your firewall will see their traffic as coming through your computer.

AWS.1.R **Anonymizers Resources**

Here is a quick list of some popular Anonymizers. Not all of these are free, but they basically do the same thing. Some don't just change your headers, they give you a completely new online identity. You are given a new IP from a Virtual Private Network (VPN), and that IP identifies you, not your old one. I have not tested all of these.

@nonymouse.com (www.@nonymouse.com)
Anonymize.net (www.anonymize.net)
Anonymizer.com (www.anonymizer.com)
Circumventer Central (http://peacefire.org/circumventor/)
Anonymizers.com (www.nymproxy.com/anonymizer)
Idzap (www.idzap.com)
iPrive.com (www.iprive.com)
ProxyWay Pro (www.proxyway.com)
Rewebber (www.rewebber.de)
Secure-Tunnel (www.secure-tunnel.com)
Somebody (www.somebody.net)
Stealther (www.photono-software.de/Stealther)
Surfola.com (www.surfola.com)
Ultimate Anonymity (www.ultimate-anonymity.com)

For more information on VPNs, check out the following articles:

Wikipedia:Virtual Private Network (http://en.wikipedia.org/wiki/Virtual_private_network)
HowStuffWorks: VPN (http://www.howstuffworks.com/vpn.htm)
OpenVPN FAQ (http://openvpn.net/index.php/access-server/section-faq-openvpn-as.html)

AWS.2 **Part 2: Remailers**

Emailing with a degree of anonymity is easier than you would think, but as the activity is inherently non-anonymous, care and precautions must be taken to ensure privacy. When you forwarded your grandma that Hallmark e-card, even she could see your email address, right there next to, "[No Subject] (Lazy... is it really that hard to type, "Happy V-Day?")." But just like Rosie O'Donnell's clothing, there is something much seedier lurking underneath. Behind every message is hidden code, called a header (Just like in Part 1. I know, one vocab word with two definitions. Could you imagine if all spelling tests were this easy?). The header contains your email, the address of your Internet Service Provider (ISP)'s outgoing mail server, IPs, and all kinds of cool stuff. Let's look at the header on that reply your grandma sent back:

Revealing Headers

Outlook Express:

1. Select a message in your inbox.
2. File>Properties>Details

Outlook:

1. Right click a message>Options
2. Look in Internet Headers under Message Options

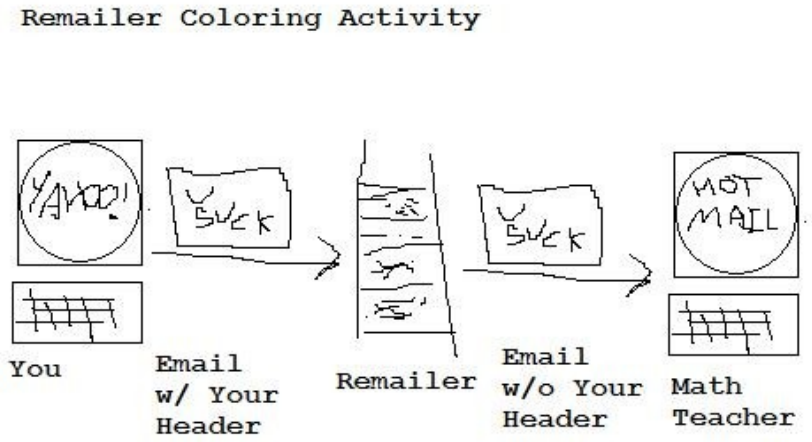
Yahoo!:

1. Open a message
2. Scroll to the bottom, click "Full Headers"

Gmail:

1. Open a message
2. Click the drop down box next to Reply
3. Click "Show Original." This will open in a new window.

To make your emails anonymous, you have to get rid of all this crazy information. The quickest way is with a Remailer. Like the Anonymizer for browsing, Remailers work in between you and who your recipient. Your header information is removed, making it difficult to trace the email back to you.



You can configure many Remailers to work with your standard Post Office Protocol (POP) email program, like Outlook, Thunderbird, or everybody's favorite, Evolution. Other Remailers are only Web-based. Some even encrypt.

Be careful, because simply making a new account on Gmail will not protect your identity, because of headers. If you want to go an extra step and make a dummy ID on one of these, go ahead, but make sure you still use a Remailer. Use multiple Remailers at once, to make it harder to trace back to you. Oh, and another thing. Remember how long it took you to open *fistedsister.ru* with forty Web

based proxies stacked up? It takes a long time for Remailed mail to reach its recipients, too. Just something to think about before you start the ten second nuclear countdown and send your warning behind a hundred Remailers.

AWS.2.R **Email Resources**
Anonymize.net (www.anonymize.net)
Anonymous.To (www.anonymous.ti)
HavenCo Anonymous Remailer (www.remailer.havenco.com)
HushMail.com (www.hushmail.com)
iPrive.com (www.iprive.com)
POP3Now (www.pop3now.com)
PrivacyX (www.privacyx.com)
SecureNym (www.securenym.net)
Send Fake Mail (www.sendfakemail.com)
Somebody (www.somebody.net)
Ultimate Anonymity (www.ultimate-anonymity.com)
W3 Anonymous Remailer (www.gilc.org/speech/anonymous/remailer.html)

AWS.3 **Part 3: Tor**

Everybody has heard of Tor. There isn't much to say that hasn't been said already. If you don't know, Tor is an Open Source project that uses onion routing, relaying traffic through Tor nodes, to provide you with a fairly strong wall of anonymity. Tor nodes are set up by volunteers through whom your internet traffic passes.

Watch out with Tor, however. Although traffic analysis is not possible, traffic confirmation, or end to end correlation, is. In addition, data being sent from an exit node to a target server is not encrypted, so it is possible to intercept data from an exit node. Never enter personal information under any proxy, and especially not while using Tor. Be careful if you are plotting a jewel heist with your forum buddies, too, because law enforcement agencies have Tor nodes of their own, and you never know if your traffic is being directed through one of theirs.

That being said, Tor is still a highly valuable asset to your anonymity. You can have more confidence with Tor than a VPN. There is a ton of information out there about it, so I'm not going to repeat what has already been said a thousand times. If you want more information, check out the next section for Tor resources.

Tor is really easy to install, especially in Windows. It gave me a slight headache in Ubuntu, but it was essentially the first thing I had ever installed on the operating system. I had zero knowledge of Linux or UNIX and I put it on Ubuntu before Windows, so it probably isn't all that hard.

Installing and running Tor
Windows:

This whole process is a lot simpler if you just use Firefox and quit dropping Opera into ever conversation you ever have.

1. Download the Stable Vidalia Bundle and run the installer.
2. Select your language, and the Full install type.
3. Follow the rest of the prompts.
4. If it doesn't start automatically, go to Start>Vidalia Bundle>Vidalia
   You will notice a little yellow onion in your Notification Area. We want this to turn green.
5. Open Firefox. Under View, make sure Status Bar is checked.
6. In your Status Bar, tiny and red, are the words “Tor Disabled.” Click them. It will turn green and say “Tor Enabled.” Your little yellow onion should now be green, too.

If you want a cuter button, as well:

7. Right click in the general area around your Menu and Navigation Bars.
8. Select Customize, scroll through the icons until you find the one labeled TorButton. Hint: It is a picture of an onion.
9. Drag and drop it anywhere you like around the toolbars.

To verify Tor is working, go to the Tor checker. The link is in the Resources.

Ubuntu:

That could be an article in and of itself. Oh, yeah, it already is. Follow the link in Resources. It is a simple process, I just do not see the point in retyping all the information you can just click a link to see. Just remember to install Polipo, not Privoxy.

There is also the Tor Browser, which basically is portable Firefox with Tor all ready to go. You just download, extract, and run the executable (.exe). It may or may not be the computers I have used it on, but, like many portable browsers I have used, it seemed like it crashed a lot. I suggest just installing the software and calling it a day. Unless you are curious, then go ahead and try it out.

If you want to try something similar to Tor, but not Tor itself, check out the JAP Anon Proxy. It is easier to use when you just ignore the fact that its name is a racial slur. Another software you can try out is Six/Four. Resources has the links.

AWS.3.R **Tor Resources**

If you are interested in learning about how Tor works or just want general Tor information:
Tor Project (https://www.torproject.org/index.html.en)
Tor (http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29)

Downloading and Installing Tor:
Download Tor (https://www.torproject.org/download/download.html.en)
Tor-Ubuntu Community Documentation (https://help.ubuntu.com/community/Tor)

After you have installed Tor, check that it works here:
Are You Using Tor? (https://check.torproject.org/)

Alternate Programs(JAP and Six/Four):
Project: AN.ON – Anonymity.Online (http://anon.inf.tu-dresden.de/index_en.html)
The Six/Four System (http://sourceforge.net/projects/sixfour/)

AWS.4 **MAC Spoofing**

So now you have some ways to cloak your IP. But we're not out of the woods yet. Because even though your IP is changed, you still need to watch out for your Media Access Control (MAC) address. This doesn't change around like your IP. It is a 48 bit identifier, naming your computer on a local area network (LAN). Usually it is twelve characters. It will look something like this: A1:B3:C5:D7:E9:1G.

So if something identifies us, it is detrimental to our efforts for anonymity. Luckily, it is relatively simple to change a MAC address.

Altering a MAC Address
Windows

1. Press CTRL+R and run “regedt32.”
2. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\Class\ {4D36E972-E325-11CE-BFC1-08002BE10318}

You will find four digit numbers, representing network adapters. Example: 0010. You need to find your current adapter.

3. Double click identifier and look under “DriverDesc” for their name.
4. When you have found the right one, Add or Edit the string, “NetworkAddress”
5. Type any twelve letters or numbers (Or specific ones, if you are trying to get past MAC

filtering.).

6. Disable your network interface
7. Re-enable your network interface.
   Now you need to check if your MAC is changed.
8. Press CTRL+R and run “cmd”
9. Type “ipconfig /all” and see if your Physical Address has been altered.

Or, you can download a program that does this automatically. See Resources, below.

Linux

Linux is quicker.

1. Open Terminal (or whatever command line application you have) and type “ifconfig eth0 down”
2. Enter “ifconfig eth0 hw ether xx :xx:xx:xx:xx: xx
3. Enter “ifconfig eth0 up” and you are ready to go.

Macintosh

I do not have much experience with Macs, but look in the resources for a link that describes how to go about changing your MAC address.

AWS.4.R **MAC Spoofing Resources**

MadMACs (http://www.irongeek.com/i.php?page=security/madmacs-mac-spoofer)
mac geekery MAC Address Spoofing
(http://www.macgeekery.com/gspot/2006-04/mac_address_spoofing)
Change your Network card MAC (Media Access Control) address
(http://www.debianadmin.com/change-your-network-card-mac-media-access-control-address.html)

AWS.5 **Physical Measures**

In my initial brainstorm for this document, I didn't think about including this, but then I realized this is probably the most fun part of becoming anonymous. It may be cozy and you may get those special moments of bonding when your cat jumps in front of your monitor, but you should not be doing anything that you need to be anonymous for from home.

Are you ready for some secret agent activity? If not, rent some spy thrillers to pump you up. Not James Bond movies. Acting like 007 will get you arrested pretty quick. It's okay to tell the girl behind the counter at Starbucks that you want your coffee shaken, not stirred, but when she hands it to you, you probably should not order her to, “flame it.” You chose computers, not foreign women. I'm talking chase scene, adrenaline movies. I recommend *The Bourne Trilogy*, *Spy Game*, or *Shooter*. Now that you are motivated, its time get out of the house. Keep in mind, if somebody yells, “You with the red bag,” you are not going to escape the forty Marines about to chase you down.

Probably the best way to stay anonymous is to only surf through public Wi-Fi spots. This can be a little dangerous, because often times places that offer this have cameras everywhere. Scout out areas several weeks before hand. Only pay with cash. You cannot take chances, there is no line between paranoia and care.

There are websites that list open Wi-Fi hotspots, which can give you a general direction to head towards. If you do not want such public hotspots, you can War drive for people and businesses that unintentionally have left their wireless networks open. War Driving (or walking, boating, trampoline leaping, lacrossing, etc...) is the process of getting off the couch and using a computer or handheld device to find open networks. However, walking around with a computer may draw attention to you, and our goal is anonymity.

So what do we do? Well, there are devices that you can use to find Wi-Fi without a computer (see Intego Wi-Fi Locator, in Resources), but if you are like me, you aren't going to be buying one

anytime soon. Instead, take a look around your house. What do you see? Everybody and their mother has a smartphone, which guess what? You can use for finding networks. Don't have an iPhone, like me? Look for other things. Your sister's Nintendo DS and your Sony PSP can scan for networks. The point I am trying to make here is not utilizing the latest and greatest technology for finding networks, but something inconspicuous. If I saw a kid walking down the street holding a PSP, I'd think he's playing a majorly downgraded version of a game that was released on PC six months beforehand, not scanning for open networks to piggyback off of.

Using Handheld Devices to Detect Open Wi-Fi Networks

Sony PSP

If your PSP automatically connects to a network, we are going to have to cancel that first.

1. In the URL bar, enter anything you want and press X
2. When the prompt comes up to show the device connecting, press O.
3. Select [New Connection]>Scan
4. Press O>Scan again a little down the road to find more networks.

The PSP will list all networks within its wireless range, their type, and Signal Strength. Under the heading Security, look for Open. These you will be able to connect to without any passwords. Take a note of where these networks are located, and scan again as you walk. If you want to attempt to connect to them from the PSP, it will list the networks' SSIDs in the first prompt, under "Select connection."

Nintendo Products

To war drive with a DS or DSi, use the step by step guides on their website. I put links in Resources, because I'm a kind and giving individual.

iPhone

A very nice article about this is available online. Check out the link in the Resources.

Android

Like the iPhone, I do not actually own one of these, so I don't really want to write up something I cannot test myself. Check the Resources for a link to an article explaining how to use an app called Wi-Fi Scan.

Cool, so now we have a fake MAC and we're piggybacking on somebody else's network. Combine this with some of the other sections' anonymity tips and we have are pretty anonymous. And you thought we were going to have to put on camouflage pants for this...

You need to be alert when seeking anonymity in the public. We briefly talked about scouting for cameras, and you need to be mindful of them at all times. Large department stores often keep security camera footage for up to six years, as a measure of protection against false injury lawsuits. Weird thinking you walked into Target six years ago and that is still on file. Maybe now you will realize doing your hair before going grocery shopping is important.

If at all possible, try to connect to a network from outside the building it is located in. There is less of a chance of being on the store's cameras, but you still need to look out for outdoor cameras. These can be anything from mounted security cameras to news crews interviewing the pet store owner next door to automatic teller machines (ATMs) across the street. Like I said, scouting is key.

Like I said earlier, if you have to buy something, pay only in cash. If you want to go the whole nine yards, wear one outfit with with another one underneath. When you want to leave, wait for the bathroom to get crowded. Follow a group in, take off the outer clothes (hopefully in a stall), change hats, and walk out with a large crowd. Don't be fidgety or act nervous. That draws attention to you. If you are thinking you are doing something wrong in your head, it will show outside. I've never really had a reason to do this but it sounds cool.

From reading private investigator books and online resources, I discovered that following

people who change their outfits is easy, because they often do not change their shoes. So, make sure you do that. Don't throw your old outfit in the trash, especially at the establishment you were just at. Objects in the trash can be obtained without warrants, and often hair that has fallen out will be in the clothing, and DNA tests do not help anonymity. So fold your stuff up nicely and put it in a backpack, preferably a black or dark generic one, so you can easily blend in to crowds. If you want rid of something, burn in and flush the ashes.

An indispensable tool to disguises and altering appearances is the baseball cap. Put one on and look how your head changes shape. Put sunglasses on and pull the hat low. You are now Chester the Molester, but you will be impossible to identify later on. Look at pictures of wanted bank robbers in action. How many are wearing this simple cover up? There is a reason they are still wanted. Change your baseball cap like your clothing, and you will be that much harder to find. It's like proxy chains on your body.

If you are using an internet cafe or library or public computer, make sure you wipe the keyboard, mouse and table with one of those moist towelette things, to get rid of fingerprints.

Of course, this section hovers on the edges of practicality and eccentricity, but its always your call. It's all fun at the very least. That's all I'm going to get into about Physical Measures, because this is a guide to anonymity online, not hiding from the Chinese Ministry of State Security (MSS) in Nicaragua.

AWS.5.R **Physical Measures Resources**

Where is stuff on War driving:

Intego WiFi Locator (http://www.powerpc.se/files/Pdf%20Tillb/wiFiLocator.pdf)

How to connect your Nintendo DS or Nintendo DS Lite (http://www.nintendo.com/consumer/wfc/en_na/ds/connect.jsp)

How to connect your Nintendo DSi or Nintendo DSi XL to the Internet (http://www.nintendo.com/consumer/systems/dsi/en_na/usb/index.jsp)

Wardriving with the IPhone (http://synjunkie.blogspot.com/2008/09/wardriving-with-iphone.html)

War Driving with WifiScan for Android (http://blog.tangorangers.com/2009/04/war-driving-with-wifiscan-for-android/)

If you wanted some Wi-Fi maps:

Wigle (http://wigle.net/)

WeFi (http://www.wefi.com/maps/)

gWiFi (http://gwifi.net/)

Jwire (http://v4.jiwire.com/search-hotspot-locations.htm)

Reading and studying Private Investigators is pretty useful:

Guns, Gams, and Gumshoes (http://writingpis.wordpress.com/)

Surveillance Specialist Group (http://www.youtube.com/user/SSGLLCorg)

AWS.6 **Web Bugs**

Alright, alright, you still are worried about cookies. Well fine. Have you ever wondered how websites can display advertisements for things you just searched for? Do you know why you can log in to your email and still be logged in an hour after you exited the browser? This is because of cookies, which are often times placed by web bugs. Cookies are tiny files that contain information about you and your last visit to a Web site.

Cookies are only supposed to read by the Web site that created them, but thanks to marketing servers, like DoubleClick, a virtual paper trail is formed because its web bugs are on so many websites.

Web bugs work like this:

As we discussed earlier, when you visit anywhere online, that Web site's server sends your browser all the text and graphics on that page. The server needs an IP to know where to send the Web page, which is sent in the form of a HyperText Markup Language (HTML). Viewing any Web site's HTML, or source code, is easy.

View Source

IE

1.View>Source

Firefox

1.Right click>View Source

Now look at the following piece of HTML:

<img src="http://ad.doubleclick.net/img1.gif" width=1 height=1 border=0>

This is an example of a web bug. First of all, because of "<img src=" we know this is a graphic. The part that says " http://ad.doubleclick.net/img1.gif" tells us the graphic is a .gif file, and is located on DoubleClick's server. The width, height, and border show us that this picture is basically invisible, because it is only 1 pixel by 1 pixel. Even if the Web site you were on was *AmazonWomen.cu*, DoubleClick still gets your information, too. Why? Well, the server that the file is located on needs to know where to send the image to (in this case, to your browser), so it can be displayed with the rest of the HTML in the source. DoubleClick's server now has your IP, the Web page that you got the bug from, the type of browser in use, and the time and date the bug was retrieved.

If you are paranoid about the paper trail of cookies left by Web bugs, there are a couple things you can do to minimize your exposure to them. There are programs you can use to look for and warn you about bugs (Resources), and you can try to opt out of ads. Cleaning and blocking cookies can help, also. Also, Web bugs are often in spam. If somebody wants to know if your email is alive, they can see if you opened one of their messages if it contained a Web bug. So don't open spam mail.

Opt Out of DoubleClick

1. Navigate to http://www.google.com/privacy/ads/
2. Click Opt Out
3. Read the warnings and find out there really is no point in Opting out.

Honestly, I think opting out of DoubleClick for the long term isn't worth it. You won't be opted out anymore once you clear your cookies. But we are after ultimate anonymity, so for specific sessions where absolute anonymity is crucial, go ahead.

Limiting Cookies

Often times to view Web pages at all, you will need to enable some cookies at the very least. If you only surf specific sites, you can turn off all cookies except those form the sites you go on, but that makes regular browsing and searching tedious sometimes. With most browsers, it is easy to choose a level you are comfortable with.

IE

1. Select Tools>Internet Options>Privacy
2. Use the slider to choose your allowed cookie settings

Firefox

1. Select Tools>Options>Privacy
2. Set "Firefox will:" to "Use custom settings for history."
3. Check or uncheck "Accept cookies from sites" for the desired effect.

You can also choose to accept third party cookies and how long the cookies are stored by checking the desired boxes.

Chrome

1. Click the Wrench picture
2. Select Options>Under the Hood
3. Under “Privacy” select Content Settings>Cookies
4. Select “Block all cookies” or “Block all third party cookies”
5. Then to make exceptions for individual websites, click “Exceptions”

There, now will you shut up about your cookies? Oh my Gosh...

AWS.6.R **Web Bugs Resources**

For a general rundown on cookies:

How Internet Cookies Work (http://www.howstuffworks.com/cookie.htm)

To detect Web Bugs:

Bugnosis (http://download.cnet.com/Bugnosis/3000-2367_4-12393.html)

For information on limiting or disabling cookies:

Internet Explorer 7
(http://browserguides.com/internet-explorer/how-to-enable-or-disable-cookies)

Firefox Help
(http://support.mozilla.com/en-US/kb/enabling%20and%20disabling%20cookies)

Google Chrome Help
(http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95647)

AWS.C **Conclusion**

This concludes my document titled *An Overview of Web Surfing With Rudimentary Anonymity.* I am pretty proud of it. It takes a lot to write articles for purely intrinsic purposes.

If you have any questions, corrections, or ideas for additions, email me at Jeff_Questions@yahoo.com. Chances are I will forget the password to this account, so if I never reply do not take it personally.

If you break in, try to use some of the methods I talked about to cover your tracks. Remember my password is not “Popcorn.”

AWS.B **Bibliography**

These are sources I have drawn from while writing this document. Their opinions may not correspond with mine, nor may mine correspond with theirs. Although I am using MLA 7 to cite them, when applicable, I have included URLs, for ease of access, even if they can be found without the address.

- BinaryShinigami. "Staying Anonymous in a Heavily Monitored World - Briefings - Enigma Group." *Enigma Group's Articles*. Enigma Group, 17 Oct. 2010. Web. 01 Mar. 2011. <http://www.enigmagroup.org/articles/view/Briefings/97-Staying-Anonymous-in-a-Heavily-Monitored-World>.
- Crenshaw, Adrian. "Changing Your MAC Address In Window XP/Vista, Linux And Mac OS X (Sometimes Known as MAC Spoofing)." *Irongeek.com*. Web. 02 Mar. 2011. <http://www.irongeek.com/i.php?page=security/changemac>.
- Miller, Michael. "Chapter 26: How to Surf and Communicate Anonymously." *Absolute PC Security and Privacy*. San Francisco: Sybex, 2002. 406-417. Print.
- "Tor (anonymity Network)." *Wikipedia, the Free Encyclopedia*. Web. 01 Mar. 2011. <http://en.wikipedia.org/wiki/Tor_(anonymity_network)>.
- "Tor Project: Overview." *Tor Project: Anonymity Online*. Web. 01 Mar. 2011. <https://www.torproject.org/about/overview.html.en>.
- Wang, Wallace. *Steal This Computer Book 4.0: What They Won't Tell You about the Internet*. San Francisco: No Starch, 2006. Print.

AWS.L **Disclaimer**

Understand this is not a guide to hiding your pedophile behavior or disguising middle school bomb threats. There are countless legitimate reasons to hide who you are online, such as complaining about your employer on a forum or you are a citizen of a country where Internet is forbidden/heavily monitored. Even more importantly, understand that this is a guide to anonymity, not security. Many, if not all, of the things discussed in this document will open security threats that you must take into account while utilizing your new found camouflaging. Remember, common sense is key. Think about who else will be able to see your password when you log into Facebook through TOR nodes. Online banking is definitely not a thing to do anonymously. And finally, this document is for educational purposes only, and in no way makes guarantees to be all-inclusive, accurate, or unbiased. This document draws from various sources and experiences, all of which may or may not be legitimate or correct. The author or host website are in no way responsible for anything you do. Once again, use common sense when applying anything you read here, and watch what you do. You can blame me if you want, but I am not responsible for you or your actions. Besides, you really shouldn't be bragging about that unsolved 1987 triple-homicide you participated in, anyway.

Legal Information

Proper Citation

Schultz, Jeffrey. "An Overview of Web Surfing With Rudimentary Anonymity." Title of Website you found this document. Web. Day Month Year. <The URL is not required by MLA7, but if you were to include it it would go here>.